Guide de l'administrateur Panorama

Version 10.0 (EoL)

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- To ensure you are viewing the most current version of this document, or to access related documentation, visit the Technical Documentation portal: docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page: docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2020-2020 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

December 4, 2020

Table of Contents

Présentation de Panorama 11
- À propos de Panorama 13
- Modèles Panorama 15
- Configuration centralisée de pare-feu et gestion des mises à jour 18
  - Changement de contexte : pare-feu ou Panorama 18
  - Taille de configuration totale pour Panorama 18
  - Modèles et piles de modèle 19
  - Groupes de périphériques 20
- Journalisation centralisée et génération de rapports 26
  - Collecteurs gérés et groupes de collecteurs 26
  - Collecte de journaux locale et distribuée 27
  - Mises en garde pour un groupe de collecteurs comportant plusieurs collecteurs de journaux 28
  - Options de transfert des journaux 30
  - Reporting centralisé 31
- Redistribution de données avec Panorama 33
- Contrôle d'accès basé sur les rôles 34
  - Rôles d'administrateur 34
  - Profils et séquences d'authentification 36
  - Domaines d'accès 36
  - Authentification administrateur 37
- Opérations de prévisualisation, validation ou confirmation de Panorama 39
- Planification de votre déploiement Panorama 41
- Déployer Panorama : Présentation de la tâche 43

Configurer Panorama 45
- Déterminer les besoins de stockage de journaux Panorama 47
- Configuration de l'appareil virtuel Panorama 49
  - Définir la configuration requise pour l'appareil virtuel Panorama 49
  - Installez l'appareil virtuel Panorama 52
  - Effectuer la configuration initiale de l'appareil virtuel Panorama 82
  - Configurer l'appareil virtuel Panorama en tant que collecteur de journaux local 85
  - Configurer l'appareil virtuel Panorama avec le collecteur de journaux local 91
  - Configurer un appareil virtuel Panorama en mode Panorama 95
  - Configurer un appareil virtuel Panorama en mode de Gestion seulement 96
  - Augmenter la capacité de stockage de journaux sur l'appareil virtuel Panorama 97
  - Augmenter les processeurs et la mémoire sur l'appareil virtuel Panorama 116
  - Augmentation du disque système sur l'appareil virtuel Panorama 122
  - Terminer le programme d'installation de l'appareil virtuel Panorama 127
- Configuration de l'appareil de série M 128
  - Interfaces de l'appareil de série M 128
  - Effectuer la configuration initiale de l'appareil de série M 130
  - Présentation de la configuration de la série M 134
  - Configurer l'appareil de série M en tant que collecteur de journaux 135
  - Augmenter le stockage sur l'appareil de série M 142
  - Configurer Panorama pour l'utilisation de plusieurs interfaces 149
- Enregistrer Panorama et Installer les licences 156
  - Enregistrer Panorama 156
  - Activer une licence d'assistance Panorama 157

Activer / Récupérer une licence de gestion de pare-feu lorsque l'appareil virtuel Panorama est connectée à Internet....158
Activer / Récupérer une licence de gestion de pare-feu lorsque l'appareil virtuel Panorama n'est pas connecté à Internet....159
Activer / récupérer une licence de gestion de pare-feu sur l'appareil de la série M....161
Installation du certificat du périphérique Panorama....163
Installer les mises à jour de contenu et logicielles pour Panorama....165
Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire....165
Installer les mises à jour pour Panorama dans une configuration HD....166
Installer des mises à jour pour Panorama avec une connexion Internet....167
Installer des mises à jour pour Panorama lorsqu'il n'est pas connecté à Internet....171
Installer des mises à jour de Panorama sans connexion Internet....175
Migrer les journaux de Panorama vers le nouveau format de journal....180
Transition vers un modèle Panorama différent....182
Migrer à partir d'un appareil virtuel Panorama vers un appareil de série M....182
Migrer un appareil virtuel Panorama vers un autre hyperviseur....185
Migrer d'un appareil de série M à un appareil virtuel Panorama....189
Migrer d'un appareil M-100 à un appareil M-500....194
Accéder et naviguer dans les interfaces de gestion de Panorama....198
Se connecter à l'interface Web Panorama....198
Naviguer dans l'interface Web Panorama....198
Connectez-vous à l'ILC Panorama....199
Configurer l'accès administratif à Panorama....201
Configuration d'un profil de rôle administrateur....201
Configurer un domaine d'accès....202
Configurer l'authentification et les comptes administrateurs....202
Configurer l'authentification à l'aide de certificats personnalisés....215
Comment les connexions SSL/TLS sont-elles mutuellement authentifiées ?....215
Configurer l'authentification à l'aide de certificats personnalisés sur Panorama....216
Configurer l'authentification à l'aide de certificats personnalisés sur les périphériques gérés....218
Ajouter de nouveaux périphériques clients....220
Modifier les certificats....220

Gérer les pare-feu....223
Ajouter un pare-feu en tant que périphérique géré....225
Installation du certificat de périphérique pour les pare-feux gérés....230
Installation du certificat de périphérique pour un pare-feu géré....230
Installation du certificat de périphérique pour plusieurs pare-feux gérés....232
Configurer Zero Touch Provisioning....235
Présentation de ZTP....235
Installation du plug-in ZTP....237
Configuration du compte administrateur de l'installateur ZTP....242
Importation de pare-feu ZTP sur Panorama....243
Utiliser le CLI pour les tâches ZTP....248
Désinstaller le plug-in ZTP....250
Gérer des groupes de périphériques....252
Ajouter un groupe de périphériques....252
Créer une hiérarchie de groupe de périphériques....253
Créer des objets à utiliser dans la stratégie partagée de groupe ou de périphérique....255
Revenir aux valeurs héritées de l'objet....256

Gérer les objets partagés non utilisés 257
Gérer la priorité des objets hérités 257
Déplacer ou cloner une règle de stratégie ou un objet vers un autre groupe de dispositifs 259
Sélectionner un fournisseur de filtrage des URL sur Panorama 260
Pousser une règle de stratégie à un sous-ensemble des pare-feux 264
Gérer la hiérarchie des règles 267
Gérer les modèles et les piles de modèle 269
Fonctionnalités des modèles et exceptions 269
Ajouter un modèle 269
Configuration d'une pile de modèles 271
Configurer une variable de modèle ou de pile de modèles 274
Importer et écraser les variables de la pile de modèles existante 277
Remplacer un modèle ou une valeur de pile de modèles 278
Désactiver/supprimer les paramètres de modèle 281
Gérer la clé principale de Panorama 282
Configurer Entreprise Data Loss Prevention (prévention des pertes de données - DLP) 286
Aperçu d'Entreprise Data Loss Prevention (prévention des pertes de données - DLP) 286
Avec quoi Data Loss Prevention (prévention des pertes de données - DLP) Enterprise est-il compatible ? 288
Profils prédéfinis de filtrage des données 291
Installer le plug-in Entreprise Data Loss Prevention (prévention des pertes de données - DLP) 292
Créer un modèle de données 294
Création d'un profil de filtrage des données 296
Activez Enterprise Data Loss Prevention (prévention des pertes de données - DLP) 298
Affichez les détails des journaux Enterprise Data Loss Prevention (Prévention des pertes de données - DLP) 302
Activer les Modèles de données et les Profils de filtrage existants 303
Modifier les paramètres de Enterprise Data Loss Prevention (prévention des pertes de données - DLP) 304
Désinstaller le plug-in Entreprise Data Loss Prevention (prévention des pertes de données - DLP) 308
Redistribuer les données vers les pare-feux gérés 310
Transition d'un pare-feu à une gestion Panorama 312
Planifiez la Transition vers la gestion de Panorama 312
Migrer un pare-feu vers la gestion Panorama 313
Migrer une paire HD de pare-feu vers la gestion Panorama 317
Charger une Configuration partielle de pare-feu dans Panorama 320
Surveillance de périphériques sur Panorama 323
Surveiller l'état de santé du dispositif 323
Surveiller la règle de Politique d'utilisation 325
Cas d'utilisation : Configurer des pare-feux en utilisant Panorama 330
Groupes de périphériques dans ce cas d'utilisation 330
Modèles dans ce cas d'utilisation 331
Paramétrer la configuration et les stratégies centralisées 332

Gérer les déploiements de pare-feu à grande échelle 339
Déterminer la solution optimale de déploiement à grande échelle du pare-feu 341
Capacité de gestion accrue des périphériques pour l'appareil virtuel Panorama et M-600 342
Exigences de la capacité de gestion accrue des périphériques 342

Déploiement de Panorama pour la gestion accrue des périphériques....343
Panorama Interconnect....346
Présentation de Panorama Interconnect....346
Exigences de Panorama Interconnect....347
Activer l'authentification entre le contrôleur Panorama et les nœuds....350
Configurer le plugiciel (plug-in) Panorama Interconnect....355
Synchroniser Panorama Interconnect....358
Gestion des pare-feu au moyen de Panorama Interconnect....359
Mettre à niveau le plugiciel (plug-in) Panorama Interconnect....368

Gérer la collecte des journaux....371
Configurer un collecteur géré....373
Configurer l'authentification pour un Collecteur de journaux dédié....377
Configurez un Compte administratif pour un Collecteur de journaux dédié....377
Configurer l'authentification RADIUS pour un Collecteur de journaux dédié....379
Configurer l'authentification TACACS + pour un Collecteur de journaux dédié....381
Configurer l'authentification LDAP pour un Collecteur de journaux dédié....384
Gérer les groupes de collecteurs....388
Configuration d'un groupe de collecteurs....388
Configurer l'authentification avec des certificats personnalisés entre les collecteurs de journaux....391
Déplacer un collecteur de journaux vers un autre groupe de collecteurs....393
Supprimer un pare-feu d'un groupe de collecteurs....394
Configurer le transfert des journaux vers Panorama....396
Configurez le transfert syslog vers des destinations extérieures....400
Transférer les journaux vers Cortex Data Lake....404
Vérifier le transfert des journaux vers Panorama....405
Modifier le journal de transfert et la mise en mémoire tampon par défaut....407
Configurer le transfert des journaux de Panorama vers des destinations extérieures....409
Déploiements de collecte de journaux....412
Déployer Panorama avec des collecteurs de journaux dédiés....412
Déployer les appareils de série M Panorama avec les collecteurs de journaux locaux....418
Déployer les appareils virtuels Panorama avec les collecteurs de journaux locaux....424
Déployer les appareils virtuels Panorama en mode hérité avec la collecte de journaux locale....428

Gérer les appareils WildFire....431
Ajouter des appareils WildFire autonomes à gérer avec Panorama....433
Configurer les paramètres de l'appareil WildFire de base sur Panorama....436
Configurer l'authentification pour un appareil WildFire....436
Configurer l'authentification à l'aide de certificats personnalisés sur les appareils et clusters WildFire....447
Configurer un certificat personnalisé pour un appareil WildFire géré par Panorama....447
Configurer l'authentification avec un certificat personnalisé unique pour un cluster WildFire....449
Appliquer des certificats personnalisés sur un appareil WildFire configuré via Panorama....451
Supprimer un appareil WildFire de la gestion Panorama....454
Gérer les clusters Wildfire....455
Configuration centralisée d'un cluster sur Panorama....455

Affichage de l'état du cluster d'appareils WildFire au moyen de Panorama.....477
Mise à niveau centrale d'un cluster sur Panorama à partir d'une connexion Internet.....477
Mise à niveau centrale d'un cluster sur Panorama sans connexion Internet.....480

Gestion des licences et des mises à jour.....483
Gestion des licences des pare-feux à l'aide de Panorama.....485
Déployer des mises à niveau vers des pare-feu, des collecteurs de journaux et des appareils WildFire à l'aide de Panorama.....487
Mises à jour prises en charge.....487
Planifier une mise à jour de contenu à l'aide de Panorama.....488
Mettre à niveau les collecteurs de journaux lorsque Panorama est connecté à Internet.....489
Mettre à niveau les collecteurs de journaux lorsque Panorama n'est pas connecté à Internet.....492
Mettre à niveau les pare-feu lorsque Panorama est connecté à Internet.....496
Mettre à niveau les pare-feu lorsque Panorama n'est pas connecté à Internet.....501
Mettre à niveau un pare-feu ZTP.....506
Rétablir les mises à jour du contenu depuis Panorama.....507

Surveiller l'activité réseau.....509
Utiliser Panorama pour la visibilité.....511
Surveiller le réseau avec CCA et App-Scope.....511
Analyser les Données des Journaux.....513
Générer, planifier et envoyer des rapports par courrier électronique.....514
Configurez les limites de clé pour les rapports planifiés.....517
Ingérer les journaux de l'ESM Traps sur Panorama.....519
Cas d'utilisation : Surveiller des applications en utilisant Panorama.....521
Cas d'utilisation : Répondre à un incident à l'aide de Panorama.....524
Notification d'un incident.....524
Revoir les Widgets du CCA.....524
Consultation des journaux des menaces.....525
Consultation des journaux WildFire.....526
Consultation des journaux de filtrage des données.....526
Mise à jour des règles de sécurité.....527

Panorama Haute Disponibilité.....529
Configuration requise pour Panorama HD.....531
Priorité et basculement sur Panorama en HD.....533
Déclencheurs de basculement.....534
Sondage de pulsation (heartbeat) Haute Disponibilité / HD (High Availability / HA) et messages Hello.....534
Surveillance des chemins de Haute Disponibilité / HD (High Availability / HA).....534
Remarques sur la journalisation de Panorama en HD.....536
Basculement de journalisation sur un appareil virtuel Panorama en mode hérité.....536
Basculement de journalisation sur un appareil de série M ou un appareil virtuel Panorama en mode Panorama.....537
Synchronisation entre les homologues HD Panorama.....538
Gérer une paire HD Panorama.....539
Définir la HD (haute disponibilité) sur Panorama.....539
Configurer l'authentification à l'aide de certificats personnalisés entre homologues HD.....541

Tester le basculement HD de Panorama 542
Commuter la priorité pour reprendre la journalisation NFS après un basculement sur Panorama 542
Rétablir le Panorama primaire à l'état actif 543

Gérer Panorama 545
Prévisualisation, validation ou confirmation des modifications de configuration 547
Activation de la récupération automatique de la validation 550
Gérer Panorama et les sauvegardes de configuration du pare-feu 552
Planifier l'exportation des fichiers de configuration 552
Sauvegarde et exportation de configurations de pare-feu et de Panorama 554
Annulation des modifications apportées à la configuration de Panorama 556
Configurer le nombre maximal de sauvegardes de configuration stockées sur Panorama 559
Charger une sauvegarde de configuration sur un pare-feu géré 559
Comparer les modifications dans les configurations de Panorama 560
Gérez les Verrous pour Restreindre les Modifications de Configuration 561
Ajouter des logos personnalisés à Panorama 563
Utilisez le Gestionnaire de Tâches Panorama 564
Gérer les Quotas de Stockage et les Périodes d'Expiration pour les Journaux et Rapports 565
Stockage de journaux et rapports 565
Périodes d'expiration des journaux et des rapports 566
Configurer les quotas de stockage et les périodes d'expiration pour les journaux et les rapports 566
Configurer l'heure d'exécution pour les rapports Panorama 568
Contrôler Panorama 569
Journaux système et de configuration de Panorama 569
Surveiller Panorama et les Statistiques de Collecteur de journaux en utilisant SNMP 570
Redémarrer ou arrêter Panorama 573
Configurer les profils et la complexité de mot de passe Panorama 574

Les plug-ins Panorama 575
A propos de Panorama Plugins (Plug-ins) 577
Installer les plug-ins Panorama 578
Plug-in VM-Series et plug-ins Panorama 580
Installation du plug-in VM-Series sur Panorama 580

Dépannage 583
Dépannage des problèmes système Panorama 585
Générer des fichiers de diagnostic pour Panorama 585
Diagnostic de l'état de suspension de Panorama 585
Surveiller la vérification d'intégrité des fichiers système 585
Gestion du stockage de Panorama pour les mises à jour logicielles et de contenu 586
Récupération suite à un Split Brain dans les déploiements HD de Panorama 587
Dépannage des problèmes de stockage et de connexion 588
Vérifier l'utilisation du Port de Panorama 588
Résolution du stockage zéro de journaux pour un groupe de collecteurs 591
Remplacer un disque défaillant sur un appareil de la série M 591
Remplacez le disque virtuel sur un serveur ESXi 591

Remplacez le disque virtuel sur vCloud air..... 592
Migrer les journaux vers un nouvel appareil de la série M en Mode Collecteur de Journaux..... 593
Migrer les journaux vers un nouvel appareil de la série M en Mode Panorama..... 598
Migrer les journaux vers un nouvel appareil de la série M en Mode Panorama en haute disponibilité.....605
Migrer les journaux vers le même modèle d'appareil de la série M en Mode Panorama en haute disponibilité..... 612
Migrer les collecteurs de journaux après défaillance/RMA de Panorama non-HD....618
Régénérer les métadonnées pour les appareils de la série M en paires RAID.....621
Afficher les tâches de requête de journaux..... 622
Remplacement d'un pare-feu RMA.....624
Génération d'état de périphérique partiel pour les pare-feux..... 624
Avant de commencer le remplacement d'un pare-feu RMA..... 624
Restauration de la configuration du pare-feu après un remplacement.....626
Dépanner des échecs de validation..... 629
Résoudre les problèmes d'enregistrement ou erreurs de numéro de série..... 630
Dépannage des erreurs de déclaration..... 631
Résoudre les erreurs de licence de gestion des périphériques..... 632
Dépannage des configurations de pare-feu automatiquement inversées..... 633
Effectuer la mises à jour du contenu lorsque la paire HA de Panorama est en panne.....635
Affichage de l'état de réussite ou d'échec d'une tâche..... 637
Tester la correspondance aux politiques et la connectivité des périphériques gérés..... 638
Résoudre les problèmes de correspondances du trafic à la règle de politique.....638
Résoudre les problèmes de connectivité aux ressources réseaux..... 639
Downgrader vers Panorama 10.0.....641

Présentation de Panorama

Le serveur de gestion Panorama™ assure la surveillance et la gestion centralisées de plusieurs pare-feu de nouvelle génération de Palo Alto Networks et des appareils et clusters d'appareils WildFire. Il fournit un emplacement unique à partir duquel vous pouvez superviser toutes les applications, les utilisateurs et le contenu traversant votre réseau, et ensuite utiliser ces connaissances pour créer des stratégies qui protègent et contrôlent le réseau. L'utilisation de Panorama pour la gestion centralisée des politiques et des périphériques accroît l'efficacité opérationnelle de la gestion et de l'entretien d'un réseau distribué de pare-feux. L'utilisation de Panorama pour la gestion centralisée de l'appareil WildFire et du cluster d'appareils WildFire augmente le nombre de pare-feu pris en charge par un même réseau, offre une haute disponibilité pour la tolérance aux pannes et augmente l'efficacité de la gestion.

> À propos de Panorama
> Modèles Panorama
> Configuration centralisée de pare-feu et gestion des mises à jour
> Journalisation centralisée et génération de rapports
> Redistribution de données avec Panorama
> Contrôle d'accès basé sur les rôles
> Opérations de prévisualisation, validation ou confirmation de Panorama
> Planification de votre déploiement Panorama
> Déployer Panorama : Présentation de la tâche

© 2020 Palo Alto Networks, Inc.

À propos de Panorama

Panorama vous permet de configurer, gérer et surveiller efficacement vos pare-feu Palo Alto Networks grâce à une surveillance centralisée. Les trois domaines principaux dans lesquels Panorama ajoute de la valeur sont les suivants :

- **Configuration et déploiement centralisés** : pour simplifier la gestion centralisée et le déploiement rapide des pare-feu et des appareils WildFire sur votre réseau, utilisez Panorama pour préparer les pare-feu et des appareils WildFire au déploiement. Vous pouvez ensuite assembler les pare-feu en groupes et créer des modèles pour appliquer un réseau de base et une configuration de périphérique et utiliser des groupes de périphériques pour gérer les règles de politique globalement partagées et locales. Reportez-vous à la section Configuration de pare-feu centralisée et gestion des mises à jour.
- **Journalisation agrégée avec surveillance centrale de l'analyse et des rapports** : collecte des informations sur les activités de l'ensemble des pare-feu gérés sur le réseau et analyse, enquête et rapport centralisés sur les données. Cette vue complète du trafic réseau, de l'activité utilisateur et des risques associés vous permet de répondre à des menaces potentielles grâce à un ensemble étendu de politiques permettant de mettre en œuvre en toute sécurité les applications sur votre réseau. Voir Journalisation et Création de Rapports Centralisées.
- **Administration distribuée** : vous permet de déléguer ou de restreindre l'accès aux configurations et politiques de pare-feu, globales et locales. Voir Contrôle d'Accès Basé sur les Rôles pour déléguer les niveaux d'accès appropriés dans le cadre d'une administration distribuée.

Quatre Panorama models (modèles Panorama) sont disponibles : l'appareil virtuel Panorama, l'appareil M-600, l'appareil M-500, l'appareil M-200 sont compatibles avec PAN-OS 10.0. La gestion centralisée de Panorama illustre comment vous pouvez déployer Panorama dans une configuration haute disponibilité (HA) pour gérer les pare-feu.

© 2020 Palo Alto Networks, Inc.

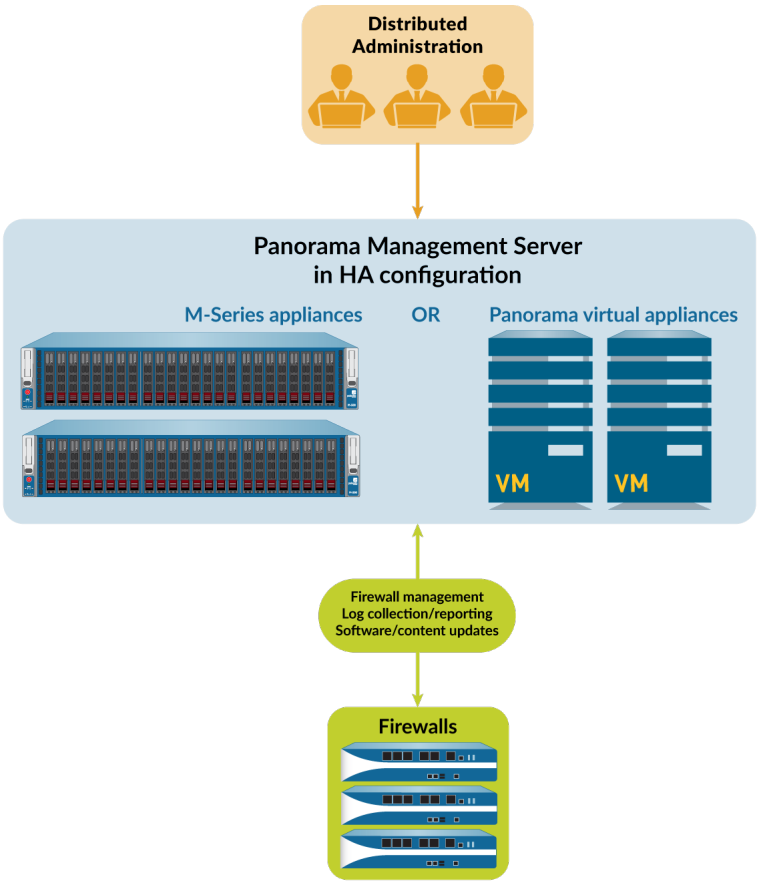


Figure 1: Gestion centralisée de Panorama

© 2020 Palo Alto Networks, Inc.

Modèles Panorama

Panorama est disponible en tant que l'un des appareils virtuels ou physiques suivants, chacun prenant en charge des licences pour gérer jusqu'à 25, 100 ou 1 000 pare-feu. De plus, les appareils M-600, et les appareils virtuels Panorama™ dotés de ressources similaires, prennent également en charge les licences pour la gestion d'un maximum de 5 000 pare-feu :

- **Appareil virtuel Panorama** : ce modèle offre une installation simple et facilite la consolidation des serveurs pour les sites qui ont besoin d'un appareil de gestion virtuel. Vous pouvez installer Panorama sur Amazon Web Services (AWS), AWS GovCloud, Microsoft Azure, Google Cloud Platform (GCP), KVM, Hyper-V, un serveur VMware ESXi ou sur VMware vCloud Air. L'appareil virtuel peut collecter des journaux de pare-feux localement à des vitesses allant jusqu'à 10 000 journaux par seconde et peut gérer des collecteurs de journaux dédiés pour des taux de journalisation plus élevés. L'appareil virtuel peut fonctionner comme un serveur de gestion dédié, un serveur de gestion Panorama avec des fonctionnalités de collecte de journaux locales ou un collecteur de journaux dédié. Pour connaître les interfaces, la capacité de stockage de journaux et les taux de collecte des journaux maximaux pris en charge, consultez la section Définir la configuration requise pour l'appareil virtuel Panorama. Vous pouvez déployer l'appareil virtuel dans les modes suivants :
  - **Mode Panorama** : dans ce mode, l'appareil virtuel Panorama prend en charge un collecteur de journaux local avec 1 à 12 disques de journalisation virtuels (voir Déployer des appareils virtuels Panorama avec des collecteurs de journaux locaux). Chaque disque de journalisation dispose de 2 To de capacité de stockage pour un total maximum de 24 To sur un appareil virtuel unique et de 48 To sur une paire haute disponibilité (HD). Seul le mode Panorama vous permet d'ajouter plusieurs disques de journalisation virtuels sans perdre les journaux sur les disques existants. Le mode Panorama offre également l'avantage d'une génération de rapport plus rapide. En mode Panorama, l'appareil virtuel ne prend pas en charge le stockage NFS.

    Il est recommandé de déployer l'appareil virtuel en mode Panorama pour optimiser le stockage des journaux et la génération de rapports.
  - **Mode hérité** : (ESXi et vCloud Air uniquement): dans ce mode, l'appareil virtuel Panorama reçoit et stocke les journaux de pare-feux sans utiliser de collecteur de journaux local (voir Déployer des appareils virtuels Panorama en mode hérité avec la collecte de journaux locale). Par défaut, l'appareil virtuel en mode hérité dispose d'une partition de disque pour toutes les données. Environ 11 Go de la partition sont alloués au stockage des journaux. Si vous avez besoin de plus de stockage de journaux local, vous pouvez ajouter un disque virtuel de 8 To maximum sur ESXi 5.5 et versions ultérieures ou sur vCloud Air. Les versions antérieures d'ESXi prennent en charge un disque virtuel d'un maximum de 2 To. Si vous avez besoin de plus de 8 To, vous pouvez monter l'appareil virtuel en mode hérité sur un magasin de données NFS, mais uniquement sur le serveur ESXi et non sur vCloud Air. Ce mode n'est disponible que si votre appareil virtuel Panorama est en mode Legacy lors de la mise à niveau vers PAN-OS 10.0. Lors de la mise à niveau vers PAN-OS 9.0 et les versions ultérieures, le mode Legacy ne sera plus disponible si vous faites passer votre appareil à un autre mode. Si vous faites passer votre appareil virtuel Panorama du mode hérité à l'un des modes disponibles, vous ne pourrez plus revenir au mode hérité.

    Bien qu'il soit toujours pris en charge, le mode Legacy n'est pas recommandé pour les environnements de production mais peut toujours être utilisé en lab ou dans des environnements de démonstration.
  - **Management Only mode (Mode de gestion uniquement)** : Dans ce mode, l'appareil virtuel Panorama est un appareil de gestion dédié pour vos périphériques gérés et vos collecteurs de journaux dédiés et, dans ce mode, un appareil virtuel Panorama doté de ressources appropriées peut gérer jusqu'à 5 000 pare-feux. L'appareil virtuel Panorama ne dispose pas de fonctionnalités de collecte de journaux, à l'exception des journaux de configuration et de configuration, et a besoin d'un collecteur de

© 2020 Palo Alto Networks, Inc.

journaux dédié pour stocker ces journaux. Par défaut, l'appareil virtuel en mode Management Only mode (Gestion uniquement) ne possède qu'une seule partition de disque pour toutes les données, de sorte que tous les journaux transmis à un appareil virtuel Panorama en mode Management Only mode (Gestion uniquement) sont supprimés. Par conséquent, afin de stocker les données de journal de vos appareils gérés, vous devez configurer le transfert de journal afin de stocker les données de journal de vos appareils gérés. Pour plus d'informations, reportez-vous à la section Exigences de la capacité de gestion accrue des périphériques.

- **Mode collecteur de journaux** : l'appareil virtuel Panorama fonctionne comme un collecteur de journaux dédié. Si plusieurs pare-feux transmettent de gros volumes de données de journal, un appareil virtuel Panorama en mode Collecteur de journaux offre une plus grande échelle et de meilleures performances. Dans ce mode, l'appareil n'a pas d'interface web pour l'accès administratif, seule une interface de ligne de commande (ILC). Toutefois, vous pouvez gérer l'appareil à l'aide de l'interface Web du serveur de gestion Panorama. L'accès CLI à un appareil virtuel Panorama en mode Collecteur de journaux n'est nécessaire que pour l'installation initiale et le débogage. Pour plus d'informations, consultez déploiement de Panorama avec les collecteurs de journaux par défaut.

- **Appareils M-Series** : Les appareils M-200, M-500 et M-600 sont des équipements matériels dédiés destinés aux déploiements à grande échelle. Dans les environnements où les taux d'exploitation élevés (plus de 10 000 journaux par seconde) avec des exigences de conservation de journaux, ces appareils permettent une mise à l'échelle de votre infrastructure de collecte des journaux. Pour connaître les interfaces, la capacité de stockage de journaux et les taux de collecte des journaux maximaux pris en charge, consultez la section Interfaces de l'appareil de série M. Tous les modèles de série M partagent les attributs suivants :

  - Disques RAID pour stocker les journaux de pare-feu et RAID 1 en miroir pour se protéger contre les pannes de disque.
  - SSD pour stocker les journaux que Panorama et les collecteurs de journaux génèrent.
  - Interfaces MGT, Eth1, Eth2 et Eth3 prenant en charge le débit 1 Gbit/s.
  - Alimentations remplaçables à chaud, redondantes
  - Flux d'air avant-arrière.

  L'appareil M-600 et l'appareil M-500 possèdent les attributs supplémentaires suivants, ce qui les rend plus adaptés aux centres de données :

  - Interfaces Eth4 et Eth5 prenant en charge un débit de 10 Gbits/s.

  De plus, l'appareil M-600 possède les attributs suivants, ce qui le rend plus adapté aux déploiements de pare-feux à grande échelle :

  - L'appareil M-600 en mode Gestion uniquement peut gérer un maximum de 5 000 pare-feu.

  Vous pouvez déployer les appareils de série M d'une des façons suivantes :

  - **Mode Panorama** : l'appareil fonctionne comme un serveur de gestion Panorama pour gérer les pare-feu et les collecteurs de journaux dédiés. L'appareil prend également en charge un collecteur de journaux local pour regrouper les journaux de pare-feu. Le mode Panorama est le mode par défaut. Pour plus d'informations sur la configuration, consultez Déployer les appareils de la série M Panorama avec les collecteurs de journaux locaux.
  - **Mode de gestion seulement** : l'appareil virtuel Panorama est un appareil de gestion dédié pour vos périphériques gérés et vos collecteurs de journaux dédiés. L'appareil Panorama ne dispose pas de fonctionnalités de collecte de journaux, à l'exception des journaux de configuration et de système, et votre déploiement a besoin d'un collecteur de journaux dédié pour stocker ces journaux. Par défaut, l'appareil Panorama en mode Management Only mode (Gestion uniquement) ne possède qu'une seule partition de disque pour toutes les données, de sorte que tous les journaux transmis à un appareil virtuel Panorama en mode Management Only mode (Gestion uniquement) sont supprimés. Par conséquent, afin de stocker les données de journal de vos appareils gérés, vous devez configurer le transfert de journal afin de stocker les données de journal de vos appareils gérés.

© 2020 Palo Alto Networks, Inc.

- **Mode collecteur de journaux** : l'appareil fonctionne comme un collecteur de journaux dédié. Si plusieurs pare-feu transmettent de grands volumes de données de journaux, un appareil de série M en mode collecteur de journaux fournit une échelle et des performances accrues. Dans ce mode, l'appareil n'a pas d'interface web pour l'accès administratif, seule une interface de ligne de commande (ILC). Toutefois, vous pouvez gérer l'appareil à l'aide de l'interface Web du serveur de gestion Panorama. L'accès CLI à un appareil de série M en mode collecteur de journaux est seulement nécessaire pour la configuration initiale et le débogage. Pour plus d'informations, consultez déploiement de Panorama avec les collecteurs de journaux par défaut.

Pour plus de détails et pour connaître les spécifications des appareils de série M, consultez les Guides de référence du matériel de l'appareil M-Series.

© 2020 Palo Alto Networks, Inc.

Configuration centralisée de pare-feu et gestion des mises à jour

Panorama utilise des *groupes de périphériques* et des *modèles* pour grouper les pare-feux en ensembles logiques nécessitant une configuration similaire. Vous utilisez les groupes de périphériques et des modèles pour gérer de manière centralisée tous les éléments de configuration, des politiques et des objets sur les pare-feu gérés. Panorama vous permet également de gérer de manière centralisée les licences, les logiciels (logiciels PAN-OS, logiciel client SSL-VPN, agents / logiciels d'applications GlobalProtect™), et mises à jour de contenu (applications, menaces, WildFire et Antivirus).

- Changement de contexte : pare-feu ou Panorama
- Taille de configuration totale pour Panorama
- Modèles et piles de modèle
- Groupes de périphériques

Changement de contexte : pare-feu ou Panorama

L'interface Web Panorama™ vous permet de basculer entre une vue centrée sur Panorama et une vue centrée sur le pare-feu en utilisant le menu déroulant **Context (Contexte)** qui figure dans le coin supérieur gauche de chaque onglet. Vous pouvez définir le **Context (Contexte)** sur **Panorama** pour gérer de manière centralisée les pare-feu, ou changer le contexte à l'interface Web d'un pare-feu spécifique pour le configurer localement. La similarité des interfaces Web de Panorama et du pare-feu vous permet de les déplacer de manière transparente pour surveiller et gérer les pare-feu.

Le menu déroulant **Context (Contexte)** répertorie uniquement les pare-feu qui sont connectés à Panorama. Pour un administrateur de groupe de périphériques et de modèle, la liste déroulante ne répertorie que les pare-feu connectés qui se trouvent dans les domaines d'accès affectés à cet administrateur. Pour rechercher une longue liste, utilisez les filtres dans le menu déroulant.

Pour les pare-feu dans une configuration haute disponibilité (HA), les icônes ont des arrière-plans colorés pour indiquer l'état HA (comme suit). Connaître l'état HD est utile lors de la sélection d'un contexte de pare-feu. Par exemple, vous faites généralement des modifications de configuration spécifiques de pare-feu sur un pare-feu actif.

- **Vert** : Actif.
- **Jaune** : passif ou le pare-feu se lance (l'état d'initiation dure jusqu'à 60 secondes après le démarrage).
- **Rouge** : le pare-feu n'est pas fonctionnel (état d'erreur), est suspendu (un administrateur l'a désactivé), ou à l'état provisoire (pour un événement de surveillance des liaisons ou des chemins dans une configuration HD active/active).

Taille de configuration totale pour Panorama

La taille du fichier de configuration totale des appareils virtuels de M-Series et Panorama™ est un élément important de la mesure de performance lorsqu'il s'agit de déterminer quel appareil M-Series oula quantité minimale de ressources virtuelles que vous devez allouer à votre appareil virtuel Panorama afin de vous assurer que vous remplissez les obligations de sécurité. Le dépassement de la taille du fichier de configuration totale possible du serveur de gestion Panorama a pour conséquence une plus faible performance lorsque l'on effectue les modifications de configuration, valide et applique aux pare-feux gérés.

Le serveur de gestion Panorama en mode Panorama est compatible avec une taille de fichier de configuration totale de 80 MB pour toutes les configurations de template (modèle), device group (groupe d'appareils), et spécifiques à Panorama. Panorama en mode Gestion uniquement est compatible avec une taille de fichier de configuration totale allant de 120 MB à 150 MB en fonction du modèle Panorama ou des

© 2020 Palo Alto Networks, Inc.

ressources que vous allouez à l'appareil virtuel Panorama. Reportez-vous au tableau ci-dessous pour la taille de fichier de configuration maximale sur la base du modèle d'appareil M-Series Panorama ou des ressources que vous allouez à l'appareil virtuel Panorama.

Modèle Panorama	Ressources virtuelles nécessaires	Taille de fichier de configuration Panorama maximale recommandée
M-200	S. O.	120 MB
M-500		120 MB
M-600		150 MB
Appareil virtuel Panorama Reportez-vous àDéfinir la configuration requise pour l'appareil virtuel Panorama pour des informations supplémentaires sur la configuration.	• 16 vCPU • 128 Go de mémoire	120 MB
	• 56 vCPU • 16 Go de mémoire.	150 MB

Modèles et piles de modèle

Vous utilisez des modèles et des piles de modèles pour configurer les paramètres qui permettent aux pare-feu de fonctionner sur le réseau. Les modèles sont les blocs de construction de base que vous utilisez pour configurer les onglets **Network (Réseau)** et **Device (Périphérique)** sur Panorama™. Vous pouvez utiliser des modèles pour définir des configurations d'interface et de zone, pour gérer les profils de serveur pour la consignation et l'accès à Syslog ou pour définir des configurations VPN. Les piles de modèles vous permettent de superposer plusieurs modèles et de créer une configuration combinée. Les piles de modèles simplifient la gestion, car elles vous permettent de définir une configuration de base commune pour tous les périphériques connectés à la pile de modèles et vous permettent de créer des couches pour créer une configuration combinée. Cela vous permet de définir des modèles avec des paramètres spécifiques à l'emplacement ou à la fonction, puis de superposer les modèles par ordre décroissant de priorité afin que les pare-feu héritent des paramètres en fonction de l'ordre des modèles dans la pile.

Les modèles et les piles de modèles prennent en charge les variables. Les variables vous permettent de créer des objets d'espace réservé avec leur valeur spécifiée dans le modèle ou la pile de modèles en fonction de vos besoins de configuration. Créez un modèle ou une variable de pile de modèles pour remplacer les adresses IP, les ID de groupe et les interfaces dans vos configurations. Les variables de modèle sont héritées par la pile de modèles et vous pouvez les remplacer pour créer une variable de pile de modèles. Cependant, les modèles n'héritent pas des variables définies dans la pile de modèles. Lorsqu'une variable est définie dans la pile de modèles ou de modèles et qu'elle est transmise au pare-feu, la valeur définie pour la variable est affichée sur le pare-feu.

Pour prendre en charge les pare-feu dotés de paramètres uniques, vous pouvez utiliser des modèles pour remplacer la configuration de la pile de modèles. Vous pouvez également utiliser une configuration de base commune plus étendue, puis remplacer certains paramètres poussés par des valeurs spécifiques au pare-feu sur les pare-feu individuels. Lorsque vous remplacez un paramètre sur le pare-feu, le pare-feu enregistre ce paramètre dans sa configuration locale et Panorama ne gère plus le paramètre. Pour restaurer les valeurs de modèle après les avoir écrasées, utilisez Panorama pour forcer la configuration du modèle ou de la pile de modèles sur le pare-feu. Par exemple, après avoir défini un serveur NTP commun dans un modèle et remplacé la configuration du serveur NTP sur un pare-feu pour prendre en compte un fuseau horaire local, vous pouvez ultérieurement revenir au serveur NTP défini dans le modèle.

© 2020 Palo Alto Networks, Inc.

Lors de la définition d'une pile de modèles, envisagez d'affecter des pare-feu qui sont le même modèle matériel et requièrent un accès à des ressources réseau similaires, telles que des passerelles et des serveurs syslog. Cela vous permet d'éviter la redondance de l'ajout de chaque paramètre à chaque pile de modèles. La figure suivante illustre un exemple de configuration dans laquelle vous affectez des pare-feu de centre de données dans la région Asie-Pacifique (APAC) à une pile avec des paramètres globaux, un modèle avec des paramètres spécifiques APAC et un modèle avec des paramètres spécifiques au centre de données. Pour gérer les pare-feux dans un bureau de la branche APAC, vous pouvez ensuite réutiliser les modèles globaux et spécifiques APAC en les ajoutant à une autre pile qui comprend un modèle avec des paramètres spécifiques à la branche. Les modèles dans une pile ont un ordre de priorité configurable qui assure que Panorama insère une seule valeur pour tout réglage en double. Panorama évalue les modèles répertoriés dans une configuration de pile de haut en bas, les modèles supérieurs ayant la priorité. La figure suivante illustre une pile de centre de données dans lequel le modèle de centre de données a une priorité plus élevée que le modèle global : Panorama insère la valeur du délai d'inactivité à partir du modèle du centre de données et ignore la valeur du modèle global.

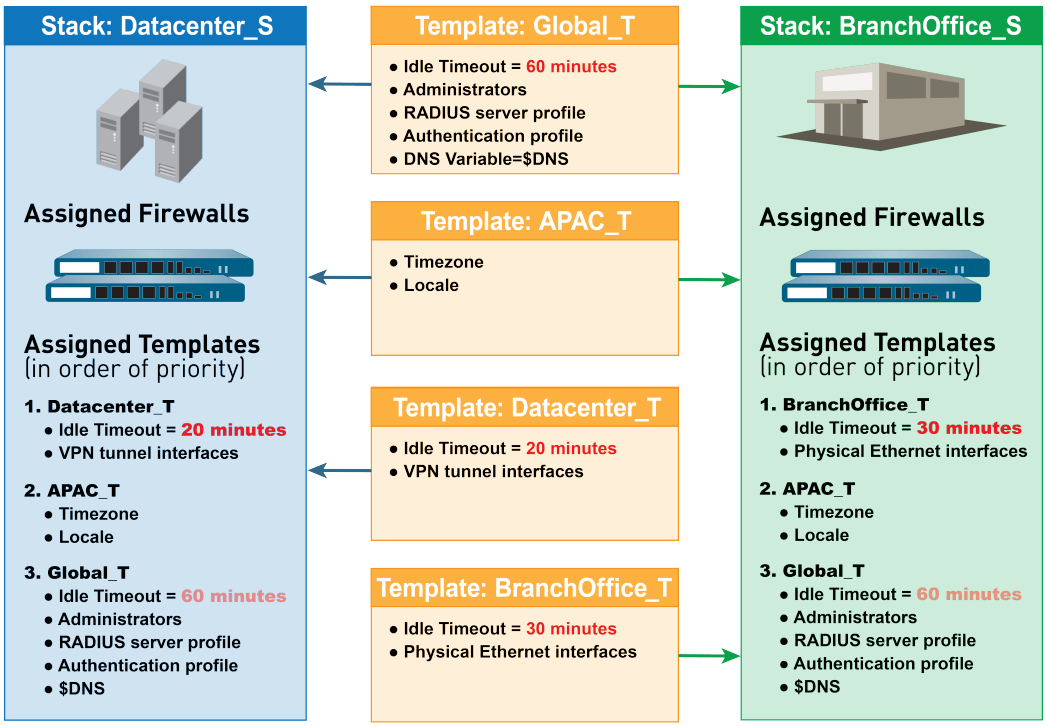


Figure 2: Piles de Modèles

Vous ne pouvez pas utiliser de modèles ou de piles de modèles pour définir les modes de pare-feu: mode réseau privé virtuel (VPN), plusieurs systèmes virtuels (multi-vsys) ou modes opérationnels (mode normal ou FIPS-CC). Pour plus d'informations, consultez fonctionnalités de modèle et exceptions. Cependant, vous pouvez attribuer des pare-feux qui ont des modes non-correspondants sur le même modèle ou pile. Dans de tels cas, Panorama insère les paramètres spécifiques au mode que pour les pare-feu qui prennent en charge ces modes. À titre d'exception, vous pouvez configurer Panorama pour qu'il transfère les paramètres de la version par défaut de vsys dans un modèle vers des pare-feu qui ne prennent pas en charge les systèmes virtuels ou qui n'ont aucun système virtuel configuré.

Pour les procédures appropriées, consultez gérer les modèles et les piles de modèle.

Groupes de périphériques

Pour utiliser Panorama efficacement, vous devez regrouper les pare-feu de votre réseau en unités logiques appelées *groupes de périphériques.* Un groupe de périphériques permet un regroupement basé sur la

© 2020 Palo Alto Networks, Inc.

segmentation du réseau, la localisation géographique, la fonction d'organisation, ou tout autre aspect commun des pare-feux qui requièrent des politiques de configurations similaires. En utilisant des groupes de périphériques, vous pouvez configurer les règles de stratégie et les objets auxquels ils font référence. Vous pouvez organiser un groupe de périphériques hiérarchisé, avec des règles communes et des objets en haut, et les règles spécifiques aux groupes périphériques et des objets à des niveaux ultérieurs. Cela vous permet de créer une hiérarchie de règles qui imposent la façon dont les pare-feux gèrent le trafic. Par exemple, vous pouvez définir un ensemble de règles communes en tant que politique d'utilisation acceptable de l'entreprise. Puis, pour autoriser uniquement aux bureaux régionaux d'accéder au trafic peer-to-peer tels que BitTorrent, vous pouvez définir une règle de groupe de périphériques qui fait que Panorama la force uniquement aux bureaux régionaux (ou définir une règle de sécurité partagée et cibler les bureaux régionaux). Pour les procédures pertinentes, voir Gérer des groupes de périphériques. Les rubriques suivantes décrivent les concepts et les composants du groupe de périphériques plus en détail :

- Hiérarchie de groupe de périphériques
- Politique de groupe de périphériques
- Objets de groupe de périphériques

Hiérarchie de groupe de périphériques

Vous pouvez Créer une hiérarchie de groupe de périphériques imbriquer des groupes de périphériques dans une hiérarchie d'arborescence jusqu'à quatre niveaux, avec des groupes de niveau inférieur héritant des paramètres (règles de la politique et objets) des groupes de niveau supérieur. Au niveau inférieur, un groupe de périphériques peut avoir des parents, des grands - parents, et des groupes de périphériques grand-grands-parents (*ancêtres*). Au niveau supérieur, un groupe de périphériques peut avoir un enfant, un petit-enfant, et des groupes de périphériques des arrière-petits-enfants (*descendants*). Tous les groupes de périphériques héritent des paramètres de la localisation *partagée* d' un conteneur au sommet de la hiérarchie pour les configurations qui sont communes à tous les groupes de périphériques.

La création d'une hiérarchie de groupe de périphériques vous permet d'organiser des dispositifs basés sur les exigences des politiques communes sans configuration redondante. Par exemple, vous pouvez configurer les paramètres partagés qui sont globaux à tous les pare-feux, configurer des groupes de périphériques avec des paramètres spécifiques à une fonction de premier niveau, et configurer des groupes de périphériques avec des paramètres spécifiques à l'emplacement à des niveaux inférieurs. Sans une hiérarchie, vous devez configurer les deux paramètres, fonction et localisation, spécifiques à l'emplacement pour chaque groupe de périphériques dans un seul niveau sous partage.

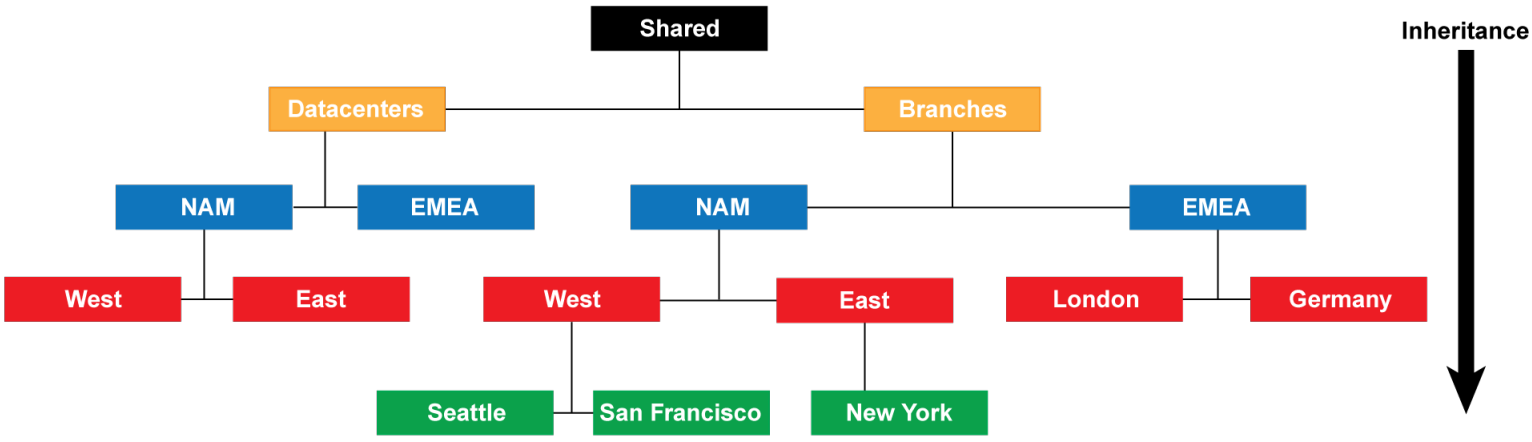
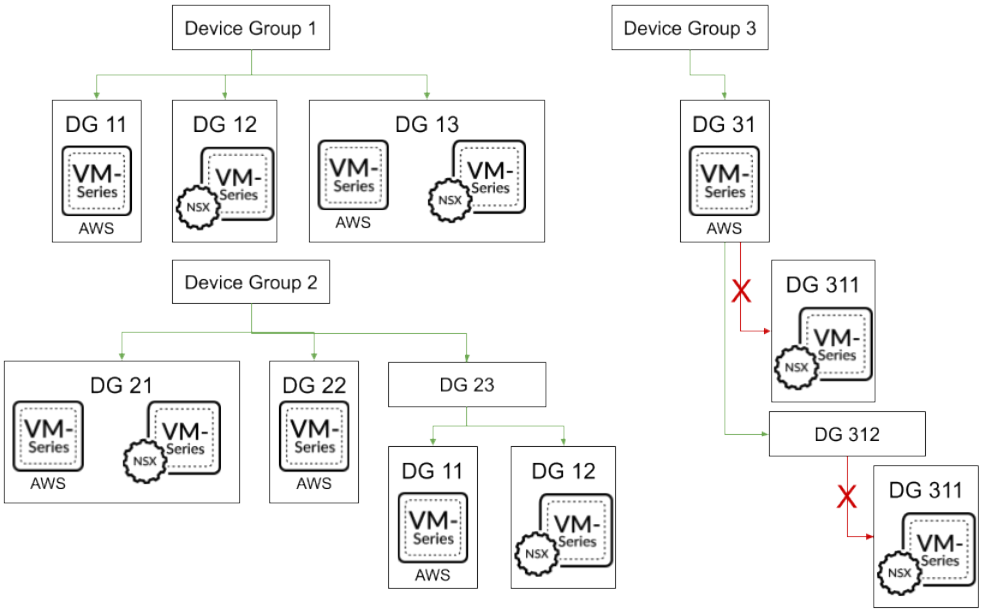


Figure 3: Hiérarchie de groupe de périphériques

Pour plus de détails sur l'ordre dans lequel les pare - feu évaluent les règles de politique dans une hiérarchie de groupe de périphériques, voir Politique de groupe de périphériques. Pour plus de détails sur le remplacement des valeurs des objets dont les groupes de périphériques héritent de groupes de périphériques ancêtres, voir Objets de groupe de périphériques.

© 2020 Palo Alto Networks, Inc.

Lorsque l'on veut faire un déploiement de multiples plug-ins sur Panorama, un groupe de périphériques contenant les pare-feux déployés sur un hyperviseur donné ne peut être dépendant ou parent d'un groupe de périphériques contenant des pare-feux déployés sur un hyperviseur différent. Par exemple, si Panorama reçoit des mises à jour d'adresses IP de VMware NSX-V et AWS, vous ne pouvez pas créer un groupe de périphériques de pare-feux VM-Series NSX-V qui est dépendant d'un groupe de périphériques de pare-feux VM-Series AWS.

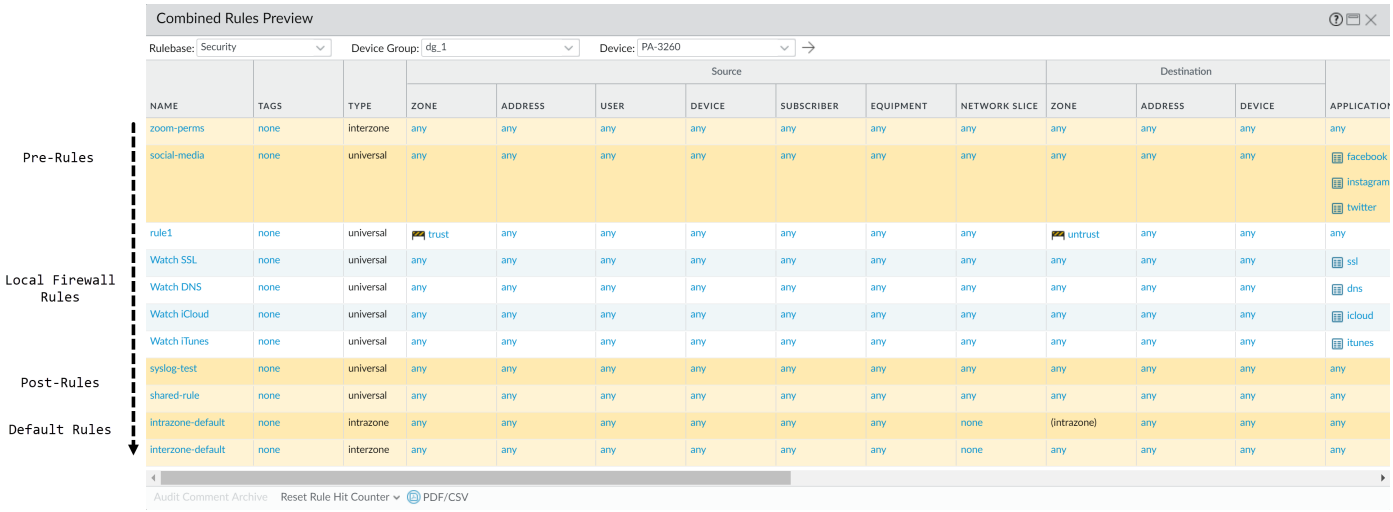


Politique de groupe de périphériques

Les groupes de périphériques fournissent un moyen de mettre en œuvre une approche multidimensionnelle de la gestion des politiques à travers un réseau de pare-feu gérés. Un pare-feu évalue les règles de la politique par couche (commune, groupe de périphériques, et local) et par type (pré-règles, post-règles, et des règles par défaut) dans l'ordre suivant, de haut en bas. Lorsque le pare-feu reçoit le trafic, il exécute l'action définie dans la première règle qui correspond à une évaluation du trafic et ne tient pas compte de toutes les règles suivantes. Pour modifier l'ordre d'évaluation des règles au sein d' une couche particulière, le type et la règle de base (par exemple, la sécurité partagée- pré-règles), voir Gérer la hiérarchie des règles.

Que vous affichiez les règles sur un pare - feu ou sur Panorama, l'interface web les affiche dans l' ordre d'évaluation. Tous les paramètres partagés, groupe de périphériques et les règles par défaut que le pare-feu hérite de panorama sont en orange ombragé. Les règles locales de pare-feu affichent entre les pré-règles et les post-règles.

© 2020 Palo Alto Networks, Inc.



Ordre d'évaluation	Portée de règle et description	Périphérique d’administration
Pré-règles partagées	Panorama insère les pré-règles partagées dans tous les pare-feux dans tous les groupes de périphériques. Panorama pousse les pré-règles d'un groupe de périphériques spécifiques à tous les pare-feux dans un groupe de dispositif particulier et à ses groupes de périphériques descendant. Si un pare-feu hérite des règles de groupes de périphériques à plusieurs niveaux dans la hiérarchie du groupe de périphériques, il évalue les pré-règles dans l'ordre du plus haut au plus bas niveau. Cela signifie que les pare-feux évaluent d'abord les règles partagées et, en dernier, évaluent les règles de groupes de périphériques sans descendants. Vous pouvez utiliser les pré-règles pour faire respecter la politique d'utilisation acceptable d'une organisation. Par exemple, une pré-règle peut bloquer l'accès à des catégories d'URL spécifiques ou permettre du trafic de Domain Name System (DNS) pour tous les utilisateurs.	Ces règles sont visibles sur les pare-feux, mais vous ne pouvez les gérer que dans Panorama.
Pré-règles de groupes de périphériques		
Règles de pare-feux locaux	Les règles locales sont spécifiques à un seul pare-feu ou système virtuel (VSYS).	Un administrateur local de pare-feu ou un administrateur Panorama qui passe à un contexte de pare-feu local, peut modifier les règles de pare-feux locaux.

© 2020 Palo Alto Networks, Inc.

Ordre d'évaluation	Portée de règle et description	Périphérique d'administration
Post-règles de groupes de périphériques Post-règles communes	Panorama insère les pré-règles partagées à tous les pare-feux dans tous les groupes de périphériques. Panorama insère les pré-règles d'un groupe de périphériques spécifiques à tous les pare-feux dans un groupe de dispositif particulier et à ses groupes de périphériques descendants. Si un pare-feu hérite des règles de groupes de périphériques à plusieurs niveaux dans la hiérarchie du groupe de périphériques, il évalue les pré-règles dans l'ordre du plus haut au plus bas niveau. Cela signifie que le pare-feu évalue d'abord les règles de groupes de périphériques sans descendants et, en dernier, évalue des règles communes. Les post-règles comprennent généralement des règles pour refuser l'accès au trafic sur la base des signatures App-ID™, des informations User-ID™ (utilisateurs ou des groupes d'utilisateurs), ou d'un service.	Ces règles sont visibles sur les pare-feux, mais vous ne pouvez les gérer que dans Panorama.
Intrazone par défaut Interzone par défaut	Les règles par défaut s'appliquent uniquement à la base de règles de sécurité, et sont prédéfinies sur Panorama (au niveau partagé) et le pare-feu (dans chaque VSYS). Ces règles précisent comment PAN-OS gère le trafic qui ne correspond pas à toute autre règle. La règle intrazone par défaut autorise tout le trafic dans une zone. La règle interzone par défaut refuse tout le trafic entre les zones. Si vous remplacez des règles par défaut, leur ordre de priorité court à partir du contexte le plus bas au plus haut : les paramètres redéfinis au niveau du pare-feu ont préséance sur les paramètres au niveau du groupe de périphériques, qui ont priorité sur les paramètres au niveau partagé.	Les règles par défaut sont d'abord en lecture seule, soit parce qu'elles font partie de la configuration prédéfinie ou parce que Panorama les a insérés dans les pare-feux. Cependant, vous pouvez remplacer les paramètres de la règle pour les étiquettes, l'action, la journalisation et les profils de sécurité. Le contexte de l'appareil détermine le niveau auquel vous pouvez remplacer les règles : • Panorama - Au niveau partagé ou au niveau du groupe de périphériques, vous pouvez remplacer les règles par défaut qui font partie de la configuration prédéfinie. • Pare-feu - Vous pouvez remplacer les règles par défaut qui font partie de la configuration prédéfinie sur le pare-feu ou VSYS, ou que Panorama a forcé depuis l'emplacement partagé ou un groupe de périphériques.

© 2020 Palo Alto Networks, Inc.

Objets de groupe de périphériques

Les objets sont des éléments de configuration des règles de politique de référence, par exemple : Les adresses IP, les catégories URL, les profils de sécurité, les utilisateurs, les services et les applications. Les règles de tout type (pré-règles, post-règles, règles par défaut et des règles définies localement sur un pare-feu) et tout règle de base (sécurité, NAT, QoS, Transfert basé sur une politique, décryptage, outrepasser une application, portail captif, et la protection DoS) peuvent faire référence à des objets. Vous pouvez réutiliser un objet dans n'importe quel nombre de règles qui ont la même portée que cet objet dans la hiérarchie des groupes de périphériques. Par exemple, si vous ajoutez un objet à l'emplacement partagé, toutes les règles de la hiérarchie peuvent faire référence à l' *objet partagé* parce que tous les groupes de périphériques héritent des objets partagés. Si vous ajoutez un objet à un groupe de périphériques particulier, seules les règles de ce groupe de périphériques et de ses groupes de périphériques descendants peuvent référencer l'*objet du groupe de périphériques*. Si les valeurs d'objet dans un groupe de périphériques doivent différer de celles héritées d'un groupe de périphériques ancêtres, vous pouvez remplacer les valeurs d'objet héritées (voir l'étape Remplacez les valeurs d'objet héritées). Vous pouvez également revenir à des valeurs d'objet héritées à tout moment. Lorsque vous créez des objets à utiliser en partage ou une stratégie de groupe de périphériques une fois et les utilisez plusieurs fois, vous réduisez les frais administratifs et assurez la cohérence entre les stratégies de pare-feu.

Vous pouvez configurer la façon dont Panorama traite les objets l'échelle du système :

- **Forcer les objets inutilisés** — Par défaut, Panorama force tous les objets vers les pare-feux, indépendamment du fait que toutes les règles partagées ou politique de groupe d'appareils se réfèrent aux objets. En option, vous pouvez configurer Panorama pour forcer uniquement des objets référencés. Pour plus d'informations, reportez-vous à gestion des objets partagés inutilisés.
- **Priorité des objets ancêtres et descendants**— Par défaut, lorsque le dispositif de groupes à niveaux multiples dans la hiérarchie comporte un objet portant le même nom mais a des valeurs différentes (pour cause de remplacement, par exemple), les règles de stratégie dans un groupe de périphériques descendants utilisent les valeurs de l'objet en que descendant au lieu d'utiliser les valeurs de l'objet hérité de groupes de périphériques ancêtres ou partagés. En option, vous pouvez inverser l'ordre de priorité pour forcer les valeurs du plus haut ancêtre contenant l'objet à tous les groupes de périphériques descendants. Pour plus d'informations, consultez gérer la priorité des objets hérités.

© 2020 Palo Alto Networks, Inc.

Journalisation centralisée et génération de rapports

Panorama rassemble les journaux de tous les pare-feu gérés et offre une visibilité sur tout le trafic sur le réseau. Il fournit également une piste d'audit pour toutes les modifications de politique et de configuration apportées aux pare-feux gérés. Outre l'agrégation des journaux, Panorama peut les transférer en tant qu'interruptions SNMP, notifications par e-mail, messages Syslog et charges utiles HTTP vers un serveur externe.

Pour la journalisation et la génération de rapports centralisées, vous avez également la possibilité d'utiliser le Cortex Data Lake basé sur le cloud, dont l'architecture est conçue pour fonctionner de manière transparente avec Panorama. Cortex Data Lake permet à vos pare-feux gérés de transférer les journaux vers l'infrastructure Cortex Data Lake plutôt que vers Panorama ou vers les collecteurs de journaux gérés. Vous pouvez ainsi accroître votre configuration de collecte de journaux distribués existante ou modifier votre infrastructure de journalisation actuelle sans avoir à investir du temps et des efforts vous-même.

Le Centre de commande d'application (CCA) de Panorama offre un volet unique de reporting unifié dans tous les pare-feux. Il vous permet de manière centralisées de Surveiller l'Activité Réseau, d'analyser, enquêter et faire rapport sur les incidents de circulation et de sécurité. Sur Panorama, vous pouvez afficher des journaux et générer des rapports à partir de journaux transmis à Cortex Data Lake, à Panorama ou à des collecteurs de journaux gérés (si configurés) ou interroger directement les pare-feux gérés. Par exemple, vous pouvez générer des rapports sur le trafic, la menace, et/ou l'activité de l'utilisateur dans le réseau géré sur la base des informations enregistrées sur Panorama (et les collecteurs gérés) ou en accédant aux journaux stockés localement sur les pare-feux gérés ou à Cortex Data Lake.

Si vous choisissez de ne pas configurer le transfert de journaux à Panorama ou Cortex Data Lake, vous pouvez planifier des rapports à exécuter sur chaque pare-feu géré et transmettre les résultats à Panorama pour une vue combinée de l'activité des utilisateurs et du trafic réseau. Bien que les rapports ne fournissent pas un examen approfondi granulaire des informations et des activités spécifiques, ils fournissent toujours une approche de surveillance unifiée.

- Collecteurs gérés et groupes de collecteurs
- Collecte de journaux locale et distribuée
- Mises en garde pour un groupe de collecteurs comportant plusieurs collecteurs de journaux
- Options de transfert des journaux
- Reporting centralisé

Collecteurs gérés et groupes de collecteurs

Panorama utilise les collecteurs de journaux pour agréger les journaux des pare-feu gérés. Lors de la génération de rapports, Panorama interroge les collecteurs de journaux à la recherche d'informations sur le journal, vous offrant ainsi une visibilité sur toute l'activité réseau surveillée par vos pare-feu. Parce que vous utilisez Panorama pour configurer et gérer les Collecteurs de Journaux, ils sont également connus comme *collecteurs gérés*. Panorama peut gérer deux types de collecteurs de journaux :

- **Collecteur de journal local** : ce type de collecteur de journaux s'exécute localement sur le serveur de gestion Panorama. Seuls les appareils M-600, M-500, M-200, M-100 ou Panorama en mode Panorama prennent en charge un collecteur de journaux local.

  Si vous transférez des journaux vers un appareil virtuel Panorama en mode hérité, les journaux sont stockés localement sans collecteur de journaux.
- **Collecteur de journaux dédié** : Il s'agit d'une appareil M-600, M-500, M-200, M-100 ou d'un appareil virtuelle Panorama en mode Log Collector. Vous pouvez utiliser un appareil M-Series en mode Panorama

© 2020 Palo Alto Networks, Inc.

ou un appareil virtuel Panorama en mode Panorama ou hérité (ESXi et vCloud Air) pour gérer les collecteurs de journaux dédiés. Pour utiliser l'interface Web de Panorama pour la gestion des collecteurs de journaux dédiés, vous devez les ajouter en tant que collecteurs gérés. Sinon, l'accès administratif à un collecteur de journaux dédié est disponible uniquement par le biais de sa CLI en utilisant le compte utilisateur administratif prédéfini (*admin*). Les collecteurs de journaux dédiés ne prennent pas en charge des comptes d'utilisateurs administratifs supplémentaires.

Vous pouvez utiliser l'un des deux types de collecteurs de journaux ou les deux pour obtenir la meilleure solution de consignation pour votre environnement (voir Collecte de journaux locale et distribuée).

Un groupe de collecteurs contient entre 1 et 16 collecteurs gérés qui fonctionnent comme une seule unité logique de collecte de journaux. Si le groupe de collecteurs contient des collecteurs de journaux dédiés, Panorama répartit uniformément les journaux sur tous les disques de chaque collecteur de journaux et sur tous les collecteurs de journaux du groupe. Cette distribution optimise l'espace de stockage disponible. Pour permettre à un collecteur de journaux de recevoir des journaux, vous devez l'ajouter à un groupe de collecteurs. Vous pouvez activer la redondance des journaux en affectant plusieurs collecteurs de journaux à un groupe de collecteurs (consultez Mise en garde pour un Groupe Collecteur avec Plusieurs Collecteurs de Journaux. La configuration de Groupe de Collecteurs indique quels pare-feux gérés peuvent envoyer des journaux aux Collecteurs de Journaux du groupe.

Pour configurer les Collecteurs de Journaux et les Groupes Collecteurs, consultez Gérer la Collecte de Journaux

Collecte de journaux locale et distribuée

Avant de configurer le transfert de journaux vers Panorama, vous devez décider d'utiliser des collecteurs de journaux locaux, des collecteurs de journaux dédiés ou les deux.

Un collecteur de journaux local est facile à déployer car il ne nécessite aucune instance de matériel ou d'ordinateur virtuel supplémentaire. Dans une configuration à haute disponibilité (HD), vous pouvez envoyer des journaux au collecteur de journaux local sur les deux homologues Panorama ; le Panorama passif n'attend pas le basculement pour commencer à collecter les journaux.

Pour la collecte de journaux locale, vous pouvez également transférer des journaux vers un appareil virtuel Panorama en mode hérité, qui stocke les journaux sans utiliser de collecteur de journaux en tant que conteneur logique.

Les collecteurs de journaux dédiés sont des appareils M-600, M-500, M-200 ou virtuel Panorama en mode Log Collector. Étant donné qu'ils n'effectuent que la collecte de journaux et non la gestion de pare-feu, les collecteurs de journaux dédiés permettent un environnement plus robuste que les collecteurs de journaux locaux. Les collecteurs de journaux dédiés offrent les avantages suivants :

- Ils permettent au serveur de gestion de Panorama d'utiliser plus de ressources pour les fonctions de gestion au lieu de la journalisation.
- Ils fournissent un volume de stockage de journaux très élevé sur un appareil matériel dédié.
- Ils permettent un taux d'enregistrement plus élevé.
- Ils offrent une visibilité horizontale et la redondance avec un stockage RAID 1.
- Ils optimisent les ressources de bande passante dans des réseaux où plus de bande passante est disponible pour que les pare-feu envoient des journaux aux collecteurs de journaux proches plutôt qu'à un serveur de gestion Panorama distant.
- Ils vous permettent de répondre aux exigences réglementaires régionales (par exemple, des réglementations peuvent ne pas permettre aux journaux de quitter une région donnée).

La collecte de journaux distribuée illustre une topologie dans laquelle les homologues Panorama dans une configuration HD gèrent le déploiement et la configuration des pare-feu et des collecteurs de journaux dédiés.

© 2020 Palo Alto Networks, Inc.

Vous pouvez déployer le serveur de gestion Panorama dans une configuration HD, mais pas les collecteurs de journaux dédiés.

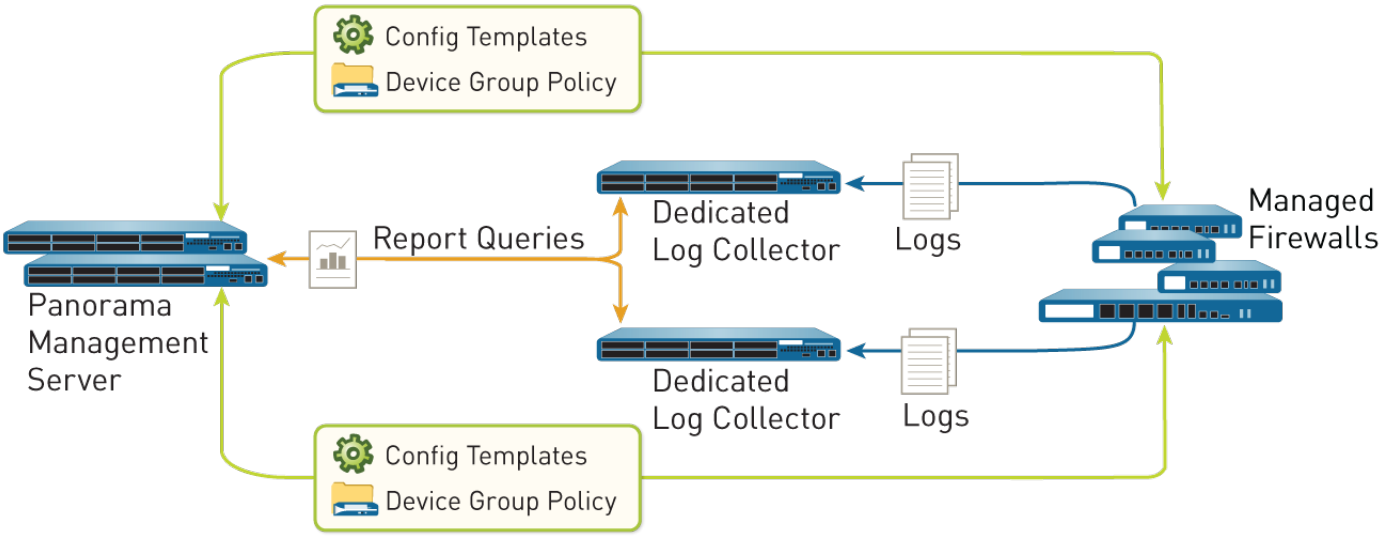


Figure 4: Collecte de journaux distribuée

Mises en garde pour un groupe de collecteurs comportant plusieurs collecteurs de journaux

Vous pouvez configurer un groupe de collecteurs avec plusieurs collecteurs de journaux (jusqu'à 16) pour assurer la redondance des journaux, augmenter la période de conservation des journaux et tenir compte des taux de journalisation qui dépassent la capacité d'un seul collecteur géré (voir Modèles Panorama pour des informations sur la capacité). Dans un même groupe de collecteurs, tous les collecteurs de journaux doivent être exécutés sur le même modèle Panorama : uniquement des appareils M-600, uniquement des appareils M-500, uniquement des appareils M-200 ou uniquement des appareils M-100, ou uniquement des appareils virtuels Panorama. Par exemple, si un seul pare-feu géré génère 48 To de journaux, le groupe de collecteurs qui reçoit ces journaux demandera au moins six collecteurs de journaux qui sont des appareils M-200 ou deux collecteurs de journaux qui sont des appareils M-500 ou des appareils virtuels Panorama.

Un groupe de collecteurs avec plusieurs collecteurs de journaux utilise l'espace de stockage disponible comme une unité logique et distribue uniformément les journaux à travers ses collecteurs de journaux. La distribution de journaux est basée sur la capacité des collecteurs de journaux (voir Modèles Panorama) et un algorithme de hachage qui détermine de façon dynamique le collecteur de journaux propriétaire des journaux et écrit sur le disque. Bien que Panorama utilise une liste de préférences pour établir les priorités de la liste des collecteurs de journaux auxquels un pare-feu géré peut transférer ses journaux, Panorama ne va pas nécessairement écrire les journaux sur le premier collecteur de journaux de la liste de préférences. Par exemple, considérez la liste de préférence suivante :

Pare-feu géré	Journal de transmission de la liste de préférence définie dans un groupe de collecteurs
FW1	L1,L2,L3
FW2	L4,L5,L6

© 2020 Palo Alto Networks, Inc.

À l'aide de cette liste, FW1 transmet les journaux à L1 tant que ce collecteur de journaux principal est disponible. Toutefois, en fonction de l'algorithme de hachage, Panorama peut choisir L2 comme propriétaire qui écrit les journaux sur ses disques. Si L2 devient inaccessible, ou en cas de panne de châssis, FW1 ne le saura pas car il peut toujours se connecter à L1.

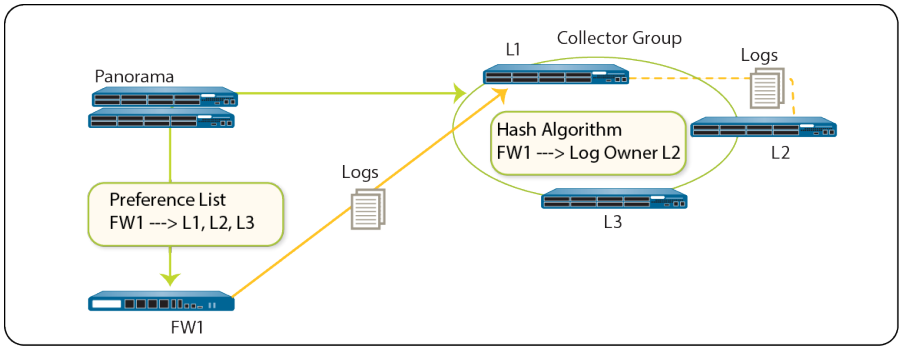


Figure 5: Exemple - Configuration d'un groupe de collecteurs de journaux type

Dans le cas où un groupe de collecteurs dispose d'un seul collecteur de journaux et que le collecteur de journaux présente une panne, le pare-feu stocke les journaux sur son disque dur / SSD (l'espace de stockage disponible varie en fonction du modèle de pare-feu). Dès que la connectivité est restaurée au collecteur de journaux, le pare-feu reprend le transfert des journaux là où il s'était arrêté avant que la panne ne se produise.

Dans le cas d'un groupe de collecteurs avec plusieurs collecteurs de journaux, le pare-feu ne met pas les journaux en mémoire tampon sur son stockage local si un seul collecteur de journaux est hors service. Dans l'exemple de scénario où L2 est en panne, FW1 continue d'envoyer des journaux à L1 et L1 stocke les données des journaux qui sont envoyées à L2. Une fois que L2 est de nouveau actif, L1 ne stocke plus les données des journaux qui sont destinés à L2, et la distribution reprend, comme prévu. En cas de défaillance de l'un des collecteur de journaux du groupe de collecteurs de journaux, les journaux qui seraient rédigés pour le collecteur de journaux indisponible sont redistribués au prochain collecteur de journaux dans la liste de préférence.

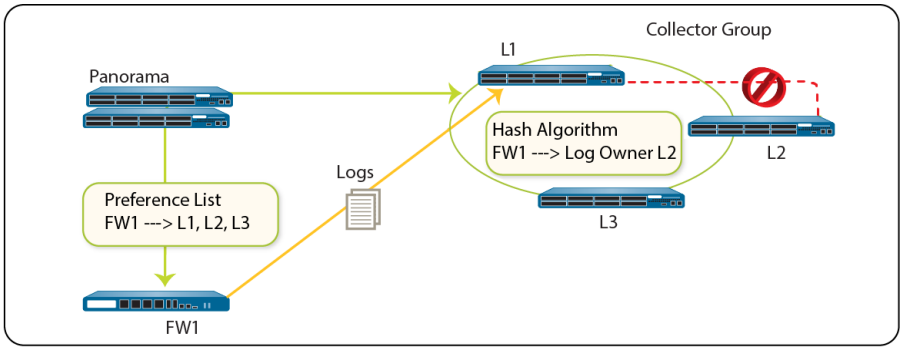


Figure 6: Exemple - Échec d'un collecteur de journaux

Palo Alto Networks recommande les mesures d'atténuation suivantes si vous utilisez plusieurs collecteurs de journaux dans un groupe de collecteurs :

- Activez la redondance de journaux lorsque vous configurez un groupe de collecteurs. Cela garantit que les journaux ne soient pas perdus si un collecteur de journaux du groupe de collecteurs devient indisponible. Chaque journal aura deux copies et chaque copie va résider sur un collecteur de journaux différent. La redondance du journal n'est disponible que si chaque collecteur de journaux du groupe de collecteurs a le même nombre de disques de journalisation.

© 2020 Palo Alto Networks, Inc.

L'activation de la redondance générant un plus grand nombre de journaux, cette configuration nécessite une capacité de stockage supérieure. Lorsque l'espace vient à manquer sur un groupe de collecteurs, il supprime les journaux les plus antérieurs.

L'activation de la redondance multiplie par deux le trafic de traitement des journaux dans un groupe de collecteurs, réduisant ainsi de moitié son débit de journalisation maximum car chaque collecteur de journaux doit distribuer une copie de chaque journal qu'il reçoit.

- Ayez à disposition un OSS (On-Site-Spare, pièce de rechange sur site) pour pouvoir remplacer rapidement en cas de panne d'un collecteur de journaux.
- En plus de transférer des journaux à Panorama, configurez le transfert à un service externe comme stockage de sauvegarde. Le service externe peut être un serveur Syslog, un serveur de messagerie, un serveur d'interruption SNMP ou un serveur HTTP.

Options de transfert des journaux

Par défaut, chaque pare-feu stocke tous les fichiers journaux localement. Pour utiliser Panorama pour la surveillance des journaux et la génération centralisée de rapports, vous devez Configurer le transfert des journaux vers Panorama. Panorama prend en charge les journaux de transfert vers un collecteur de journaux, le Cortex Data Lake ou les deux en parallèle. Vous pouvez également utiliser des services externes pour l'archivage, la notification ou l'analyse en transférant les journaux aux services directement depuis les pare-feu ou depuis Panorama. Les services externes incluent les serveurs syslog, les serveurs de messagerie, les serveurs de déroutement SNMP ou les services HTTP. En plus de transférer les journaux des pare-feu, vous pouvez transférer les journaux générés par le serveur de gestion Panorama et les collecteurs de journaux. Le serveur de gestion Panorama, le collecteur de journaux ou le pare-feu qui transfère les journaux les convertit au format approprié pour la destination (message Syslog, notification par e-mail, interruption SNMP ou charge utile HTTP).

Les pare-feu de Palo Alto Networks et Panorama prennent en charge les options de transfert de journaux suivantes. Avant de choisir une option, prenez en compte les capacités de journalisation de vos modèles Panorama et déterminez les besoins de stockage des journaux panoramiques.

- Transmettre les journaux des pare-feu à Panorama et de Panorama aux services externes — cette configuration est préférable pour les déploiements dans lesquels les connexions entre les pare-feu et les services externes ont une bande passante insuffisante pour maintenir la fréquence d'enregistrement, ce qui est souvent le cas lorsque les connexions sont éloignées. Cette configuration améliore les performances du pare-feu en déchargeant Panorama de certains traitements.

Vous pouvez configurer chaque groupe de collecteur pour transférer les journaux vers différentes destinations.

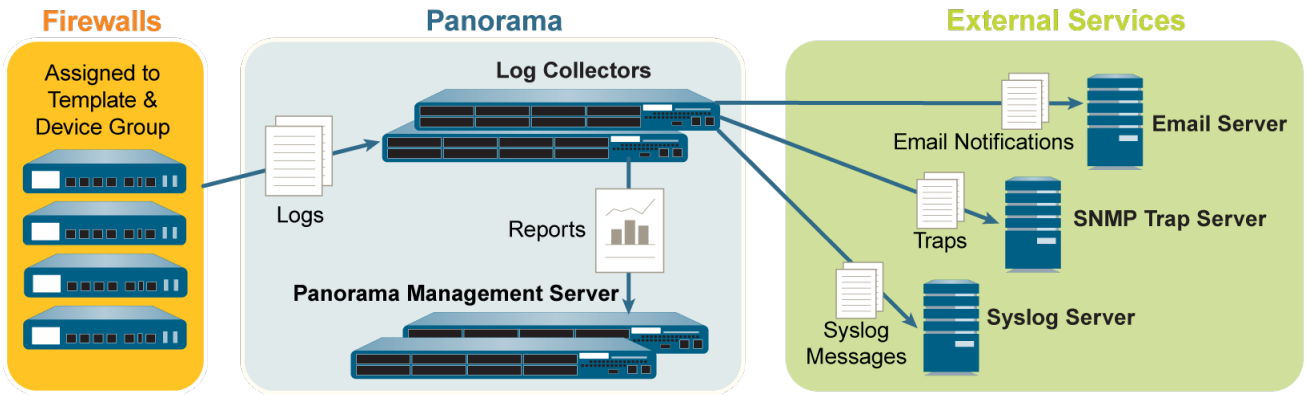


Figure 7: Transfert des journaux vers Panorama, puis vers des services externes

© 2020 Palo Alto Networks, Inc.

- Transférer les journaux des pare-feu vers Panorama et les services externes en parallèle. Dans cette configuration, Panorama et les services externes sont des points d'extrémité de flux de transfert de journal distincts; Les pare-feu ne dépendent pas de Panorama pour transmettre des journaux à des services externes. Cette configuration est la meilleure pour les déploiements dans lesquels les connexions entre les pare-feu et les services extérieurs ont une bande passante suffisante pour maintenir le taux de journalisation, ce qui est souvent le cas lorsque les connexions sont locales.

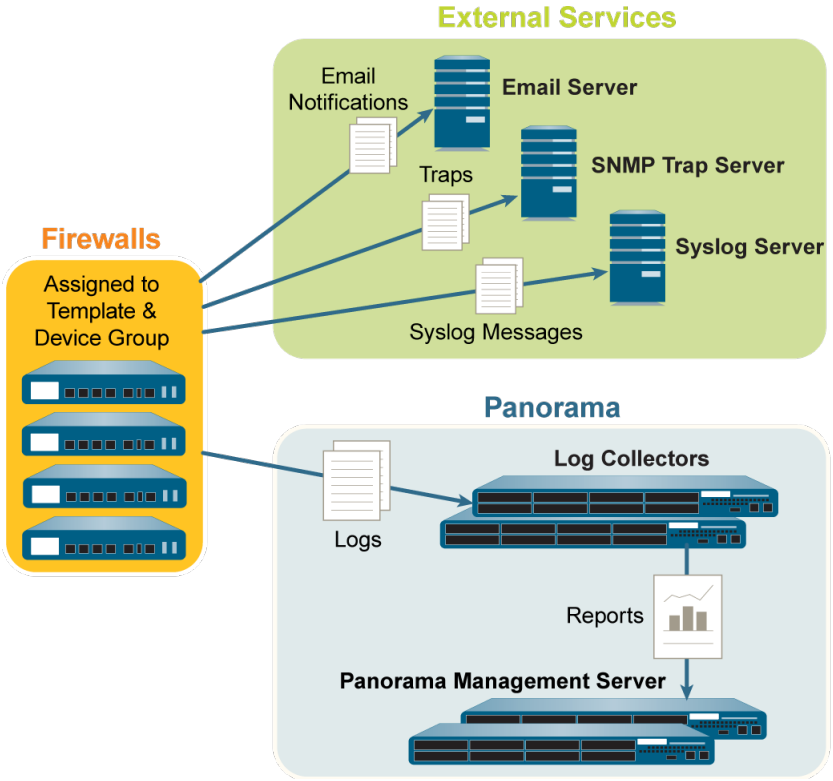


Figure 8: Transfert des journaux vers les services externes et vers Panorama en parallèle

Reporting centralisé

Panorama agrège les journaux de tous les pare-feu gérés et permet de générer des rapports sur les données obtenues afin d'obtenir une vue d'ensemble de l'utilisation de l'application, de l'activité de l'utilisateur et des schémas de trafic sur l'ensemble du réseau. Dès que les pare-feux sont ajoutés à Panorama, le CCA peut afficher tout le trafic traversant votre réseau. Lorsque la journalisation est activée, un clic sur une entrée de journal dans lc CCA offre un accès direct à des détails granulaires sur l'application.

Pour générer des rapports, Panorama utilise deux sources : la base de données locale Panorama et les pare-feux distants qu'il gère. La base de données Panorama fait référence au stockage local sur Panorama affecté au stockage des journaux récapitulatifs et certains journaux détaillés. Si vous disposez d'un déploiement de collecteur de journaux distribué, la base de données Panorama comprend le stockage local sur Panorama et tous les collecteurs de journaux gérés. Panorama récapitule les informations (trafic, application, menaces) collectées auprès de tous les pare-feu gérés, toutes les 15 minutes. L'utilisation de la base de données Panorama locale permet des temps de réponse plus courts. Cependant, si vous préférez ne pas transmettre les journaux à Panorama, ce dernier peut accéder directement au pare-feu distant et générer des rapports sur les données stockées localement sur les pare-feux gérés.

Panorama offre plus de 40 rapports prédéfinis qui peuvent être utilisés tels quels, ou peuvent être personnalisés en combinant des éléments d'autres rapports pour générer des rapports personnalisés et des groupes de rapports qui peuvent être sauvegardés. Les rapports peuvent être générés sur demande, selon un schéma récurrent, et peuvent être planifiés pour être distribués par e-mail. Ces rapports fournissent

© 2020 Palo Alto Networks, Inc.

des informations sur l'utilisateur et le contexte afin que vous mettiez en relation les événements et les modèles d'identification, les tendances et les domaines d'intérêt éventuels. Avec l'approche intégrée de la journalisation et de la création de rapports, le CCA permet d'établir une corrélation des entrées issues de plusieurs journaux relatives au même événement.

Pour plus d’informations, reportez-vous à la section Surveiller l'activité réseau.

© 2020 Palo Alto Networks, Inc.

Redistribution de données avec Panorama

Grâce à la redistribution des données, vous n'avez qu'à configurer chaque source une fois, puis vous pouvez redistribuer plusieurs types de données à autant de clients que nécessaire. Cela vous aide à échelonner votre réseau afin de facilement ajouter ou supprimer des sources et des clients lorsque votre réseau a besoin d'être modifié.

La redistribution des données offre aussi de la granularité en redistribuant uniquement les types d'informations aux seuls pare-feux et systèmes de gestion Panorama que vous indiquez. Vous pouvez utiliser des sous-réseaux, des catégories et des régions afin de réduire encore le trafic du réseau et de maximiser la capacité du périphérique.

L'un des principaux avantages du pare-feu de Palo Alto Networks est qu'il peut appliquer des politiques et générer des rapports en fonction des noms et des étiquettes (tags) d'utilisateur au lieu des adresses IP. Le défi pour les réseaux à grande échelle est de s'assurer que chaque pare-feu qui applique les politiques et génère des rapports dispose des mappages et des étiquettes qui s'appliquent à toutes vos règles de politique. De plus, tous les pare-feu qui appliquent une politique d'authentification nécessitent un ensemble complet et identique d'horodatages d'authentification pour votre base d'utilisateurs. Chaque fois que les utilisateurs s'authentifient pour accéder aux services et aux applications, les pare-feu individuels enregistrent les horodatages associés, mais ne les partagent pas automatiquement avec d'autres pare-feu pour assurer la cohérence. La redistribution des données résout ces problèmes pour les réseaux à grande échelle en vous permettant de redistribuer les données nécessaires. Cependant, au lieu de configurer des connexions supplémentaires pour redistribuer les données entre les pare-feux, vous pouvez vous appuyer sur votre infrastructure Panorama pour Redistribuer les données vers les pare-feux gérés.. L'infrastructure possède des connexions existantes qui vous permettent de redistribuer les données selon des couches, depuis les pare-feux vers Panorama. Panorama peut ensuite redistribuer les informations aux pare-feux qui appliquent les politiques et génèrent des rapports.

Chaque pare-feu ou serveur de gestion Panorama peut recevoir des données depuis 100 points de redistribution maximum. Les points de redistribution peuvent être d'autres pare-feux ou serveurs de gestion Panorama. Toutefois, vous pouvez également utiliser des agents User-ID basés sur Windows pour effectuer le mappage et redistribuer les informations aux pare-feu. Seuls les pare-feu enregistrent les horodatages d'authentification lorsque le trafic de l'utilisateur correspond aux règles de politiques d'authentification.

© 2020 Palo Alto Networks, Inc.

Contrôle d'accès basé sur les rôles

Le contrôle d'accès basé sur les rôles (CABR) vous permet de définir les privilèges et les responsabilités des utilisateurs administratifs (administrateurs). Chaque administrateur doit disposer d'un compte d'utilisateur qui spécifie une méthode de rôle et d'authentification. Rôles d’administrateur définissent l’accès aux paramètres de configuration, journaux et rapports spécifiques au sein des contextes de pare-feu et de Panorama. PourDomaines d'accès les administrateurs du groupe de périphériques et de modèles, vous pouvez mapper des rôles qui définissent l' accès à des groupes de périphériques, de modèles et de pare-feu spécifiques (par le changement de contexte). En combinant chaque domaine d'accès avec un rôle, vous pouvez appliquer la séparation de l'information entre les domaines fonctionnels ou régionaux de votre organisation. Par exemple, vous pouvez limiter un administrateur aux activités de surveillance des pare-feux du centre de données, mais permettre que l'administrateur définisse des politiques de pare-feux de test de laboratoire. Par défaut, chaque appareil Panorama (appareil virtuel ou appareil de série M) a un compte administratif prédéfini (admin) qui fournit un accès en lecture-écriture complète (accès super-utilisateur) à tous les domaines fonctionnels et à tous les groupes de périphériques, modèles et pare-feu. Pour chaque administrateur, vous pouvez définir un profil d’authentification qui détermine comment Panorama vérifie les informations d’identification d’accès des utilisateurs.

Au lieu d'utiliser le compte par défaut pour tous les administrateurs, il est recommandé de créer un compte administratif distinct pour chaque personne qui a besoin d'accéder aux fonctions administratives ou aux rapports sur Panorama. Ceci permet d'obtenir une meilleure protection contre les modifications de configuration non autorisées et permet à Panorama de se connecter et d'identifier les actions de chaque administrateur.

- Rôles d’administrateur
- Profils et séquences d'authentification
- Domaines d'accès
- Authentification administrateur

Rôles d’administrateur

Vous configurez des comptes d'administrateur sur la base des exigences de sécurité de votre organisation, les services d'authentification que votre réseau utilise, ainsi que les rôles administratifs nécessaires. Un *rôle* définit le type d'accès au système qui est disponible pour un administrateur. Vous pouvez définir et restreindre l'accès ou large ou granulaire au besoin, en fonction des exigences de sécurité de votre organisation. Par exemple, vous pouvez décider que l'administrateur du centre de données peut avoir accès à toutes les configurations de périphériques et de réseautage, mais un administrateur de sécurité peut contrôler uniquement les définitions de la politique de sécurité, tandis que d'autres personnes clés peuvent avoir une ILC limitée ou l'accès aux API XML. Les types de rôles sont les suivants :

- **Rôles dynamiques** : rôles intégrés qui permettent d'accéder à Panorama et aux périphériques gérés. Lors de l'ajout de nouvelles fonctionnalités, Panorama met automatiquement à jour les définitions des rôles dynamiques. Vous ne devez les jamais les mettre à jour manuellement. Le tableau suivant répertorie les privilèges d'accès associés aux rôles dynamiques.

Rôle dynamique	Privilèges
Super utilisateur	Accès complet en lecture/écriture à Panorama
Super utilisateur (lecture seule)	Accès en lecture seule à Panorama

© 2020 Palo Alto Networks, Inc.

Rôle dynamique	Privilèges
Administrateur de Panorama	Accès complet à Panorama, à l'exception des actions suivantes : • Créer, modifier ou supprimer des administrateurs de Panorama ou de pare-feu et des rôles. • Exporter, valider, rétablir, enregistrer, charger ou importer une configuration dans la page **Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opérations)**. • Configurer la fonctionnalité **Scheduled Config Export (Exportation programmée des configurations)** dans l'onglet **Panorama**.

- **Profils de Rôle Administrateur** : pour définir un contrôle d'accès plus granulaire aux zones fonctionnelles de l'interface Web, de la CLI et de l'API XML, vous pouvez créer des rôles personnalisés. Lors de l'ajout de nouvelles fonctionnalités au produit, vous devez mettre à jour les rôles avec les privilèges d'accès correspondants : Panorama n'ajoute pas automatiquement les nouvelles fonctions aux définitions de rôles personnalisés. Vous sélectionnez l' un des types de profils suivants lorsque vous Configuration d'un profil de rôle administrateur.

Profil du rôle admin	Description
Panorama	Pour ces rôles, vous pouvez accorder un accès en lecture/écriture, un accès en lecture seule ou aucun accès à l'ensemble des fonctionnalités Panorama accessibles au rôle dynamique de super utilisateur, à l'exception de la gestion des administrateurs Panorama et des rôles Panorama. Pour ces deux dernières fonctionnalités, vous pouvez accorder un accès en lecture seule ou aucun accès, mais vous ne pouvez pas accorder un accès en lecture/écriture. Un exemple d'utilisation d'un rôle Panorama est celui des administrateurs de sécurité qui doivent accéder aux définitions de politiques de sécurité, aux journaux et aux rapports sur Panorama.

Groupe de périphériques et modèle de périphérique	Pour ces rôles, vous pouvez attribuer un accès en lecture-écriture, lecture seule, ou pas d'accès à des zones fonctionnelles spécifiques au sein des groupes de périphériques, des modèles et des contextes de pare-feu. En combinant ces rôles avec Domaines d'accès, vous pouvez appliquer la séparation de l'information entre les domaines fonctionnels ou régionaux de votre organisation. Les Groupes de périphériques et les rôles modèles ont les limitations suivantes :
	• Aucun accès à la CLI ou à l'API XML
	• Aucun accès à la configuration ou aux journaux système
	• Aucun accès aux sources d'informations de l'appareil virtuel
	• Dans l'onglet **Panorama**, l' accès est limité à :
	  • Fonctionnalités de déploiement de l'appareil (lecture-écriture, lecture seule, ou pas d'accès)
	  • Les groupes de périphériques spécifiés dans le compte administrateur (lecture-écriture, lecture seule, ou pas d'accès)
	  • Les modèles et les périphériques gérés spécifiés dans le compte de l'administrateur (en lecture seule ou pas d'accès)
	Un exemple d'utilisation de ce rôle concerne les administrateurs de votre personnel d'exploitation qui doivent accéder aux zones de configuration

© 2020 Palo Alto Networks, Inc.

Profil du rôle admin	Description
	de périphériques et de réseau de l'interface Web pour des groupes de périphériques et/ou modèles spécifiques.

Profils et séquences d'authentification

Un profil d'authentification définit le service d'authentification qui valide les informations de connexion des administrateurs lorsqu'ils accèdent à Panorama. Il peut s'agir d'un service d'authentification locale ou un service d'authentification externe. Certains services (SAML, TACACS, et RAYON) offrent la possibilité de gérer à la fois l'authentification et l'autorisation des comptes administrateur sur le serveur externe plutôt que sur Panorama. En plus du service d'authentification, le profil d'authentification définit des options telles que l'authentification unique Kerberos (SSO) et la déconnexion unique SAML (SSO).

Certains réseaux disposent de plusieurs bases de données (par exemple, TACACS+ et LDAP) pour différents utilisateurs et groupes d'utilisateurs. Dans de telles situations, pour authentifier les administrateurs, configurez une séquence d'authentification : une liste classée de profils d'authentification à laquelle Panorama compare un administrateur lors de la connexion. Panorama vérifie chaque profil en suivant la séquence établie jusqu'à ce qu'il en atteigne un qui permet d'authentifier l'administrateur. Un administrateur se voit refuser l'accès si l'authentification de tous les profils qui figurent dans la séquence d'authentification a échoué.

Domaines d'accès

Les domaines d'accès contrôlent l'accès administratif à des groupes de périphériques et modèles spécifiques, et contrôlent également la capacité dechanger de contexte vers l'interface web des pare-feu gérés. Les domaines d'accès s'appliquent uniquement aux administrateurs avec un Groupe de Périphériques et des Rôles Modèles. Le mappage des rôles d'administrateur pour accéder aux domaines vous permet d'obtenir un contrôle très granulaire sur les informations auxquelles les administrateurs accèdent sur Panorama. Par exemple, imaginez un scénario où vous configurez un domaine d'accès qui inclut tous les groupes de périphériques pour les pare-feu dans vos centres de données et où vous attribuez ce domaine d'accès à un administrateur qui est autorisé à surveiller le trafic du centre de données, mais qui n'est pas autorisé à configurer les pare-feu. Dans ce cas, vous pouvez schématiser le domaine d'accès à un rôle qui active tous les privilèges de surveillance, mais qui désactive l'accès aux paramètres du groupe de périphériques. De plus, les admins du Groupe de périphériques et des modèles peuvent effectuer des tâches administratives pour les pare-feux gérés de leur domaine d'accès comme l'affichage de la configuration et les journaux système, effectuer des audits de configuration, examiner les tâches en attente et accéder directement aux opérations du pare-feu comme le redémarrage, générer un fichier d'assistance technique, exécuter une suppression des stats et exporter un fichier noyau.

Vous configurez les domaines d'accès dans la configuration Panorama locale, puis vous les affectez aux comptes administrateur et aux rôles. Vous pouvez effectuer l'affectation localement ou utiliser un serveur SAML, TACACS+ ou RADIUS externe. L'utilisation d'un serveur externe vous permet de réaffecter rapidement les domaines d'accès via votre service d'annuaire au lieu de reconfigurer les paramètres sur Panorama. Pour utiliser un serveur externe, vous devez définir un profil de serveur permettant à Panorama d'accéder au serveur. Vous devez également définir les Vendor-Specific Attributes (Attributs spécifiques au fournisseur ; VSA) sur le serveur RADIUS ou TACACS, ou les attributs SAML sur le serveur IdP SAML.

Par exemple, si vous utilisez un serveur RADIUS, vous devez définir un nombre et une valeur VSA pour chaque administrateur. La valeur définie doit correspondre au domaine d'accès configuré sur Panorama. Lorsqu'un administrateur tente de se connecter à Panorama, Panorama interroge le serveur RADIUS pour le domaine d'accès administrateur et numéro d'attribut. Sur la base de la réponse du serveur RADIUS, l'administrateur est autorisé pour l'accès et est limité aux pare-feux, systèmes virtuels, groupes de périphériques, et les modèles qui sont affectés au domaine d'accès.

Pour les procédures pertinentes, voir :

© 2020 Palo Alto Networks, Inc.

- Configurer un domaine d'accès.
- Configurer l'authentification RADIUS pour les administrateurs de Panorama.
- Configurer l'authentification TACACS pour les administrateurs de Panorama.
- Configurer l'authentification SAML pour les administrateurs de Panorama.

Authentification administrateur

Vous pouvez configurer les types d'authentification et d'autorisation suivants (rôles d'administrateur et domaines d'accès) pour les administrateurs Panorama :

Méthode d'authentificati	Méthode d'autorisation	Description
Local	Local	Les informations d'identification du compte administrateur et les méthodes d'authentification sont locales à Panorama. Vous utilisez Panorama pour attribuer des rôles administrateurs et des domaines d'accès aux comptes. Pour sécuriser davantage les comptes, vous pouvez créer un profil de mot de passe qui définit une période de validité pour les mots de passe et définir les paramètres de complexité du mot de passe à l'échelle de Panorama. Pour plus de détails, reportez-vous à la section Configuration de l'authentification locale ou externe des administrateurs Panorama.
Clé SSH	Local	Les comptes administrateur se trouvent localement sur Panorama, mais l'authentification à la CLI est basée sur des certificats SSH. Vous utilisez Panorama pour attribuer des rôles administrateurs et des domaines d'accès aux comptes. Pour plus de détails, reportez-vous à la section Configurer un administrateur avec une clé d'authentification SSH basée sur l'ILC.
Certificats	Local	Les comptes administrateur se trouvent localement sur Panorama, mais l'authentification à l'interface Web est basée sur des certificats clients. Vous utilisez Panorama pour attribuer des rôles administrateurs et des domaines d'accès aux comptes. Pour plus de détails, reportez-vous à la section Configurer un administrateur Panorama avec authentification basée sur les certificats pour l'interface Web.
Service externe	Local	Les comptes administrateur que vous définissez localement sur Panorama servent de références aux comptes définis sur un serveur d'authentification à plusieurs facteurs, SAML, Kerberos, TACACS+, RADIUS ou LDAP externe. Le serveur externe effectue l'authentification. Vous utilisez Panorama pour attribuer des rôles administrateurs et des domaines d'accès aux comptes. Pour plus de détails, reportez-vous à la section Configuration de l'authentification locale ou externe des administrateurs Panorama.
Plate-forme	Service externe	Les comptes administrateur définis uniquement sur un serveur SAML, TACACS+ ou RADIUS externe. Le serveur effectue l'authentification et l'autorisation. Pour l'autorisation, vous définissez les Vendor-Specific Attributes (Attributs spécifiques au fournisseur ; VSA) sur le serveur TACACS+ ou RADIUS, ou les attributs SAML sur le serveur SAML. Panorama mappe les attributs aux rôles d'administrateur et

© 2020 Palo Alto Networks, Inc.

Méthode d'authentificati	Méthode d'autorisation	Description
		aux domaines d'accès que vous définissez sur Panorama. Pour plus de détails, reportez-vous aux sections : • Configurer l'authentification SAML pour les administrateurs de Panorama • Configurer l'authentification TACACS pour les administrateurs de Panorama • Configurer l'authentification RADIUS pour les administrateurs de Panorama

© 2020 Palo Alto Networks, Inc.

Opérations de prévisualisation, validation ou confirmation de Panorama

Lorsque vous êtes prêt à activer les modifications que vous avez apportées à la configuration candidate sur Panorama ou à apporter des modifications aux périphériques gérés par Panorama (pare-feu, collecteurs de journaux et appareils WildFire et clusters d'appareils), vous pouvez Prévisualisation, validation ou confirmation des modifications de configuration. Par exemple, si vous ajoutez un collecteur de journaux à la configuration Panorama, les pare-feu ne peuvent pas envoyer de journaux à ce collecteur de journaux tant que vous n'avez pas validé la modification dans Panorama et appliqué cette dernière au groupe de collecteurs contenant le collecteur de journaux.

Vous pouvez filtrer les modifications par administrateur ou *emplacement*, puis vous pouvez confirmer, appliquer, valider ou prévisualiser uniquement ces modifications. L'emplacement peut être des groupes de périphériques spécifiques, des modèles, des groupes de collecteurs, des collecteurs de journaux, des paramètres partagés ou le serveur de gestion Panorama.

Lorsque vous validez des modifications, elles deviennent partie intégrante de la configuration actuelle. Les modifications que vous n'avez pas validées font partie de la configuration candidate. Panorama met les demandes de validation en file d'attente pour que vous puissiez initier de nouvelles validations alors qu'une validation antérieure est en cours d'exécution. Panorama exécute les validations dans l'ordre dans lequel elles sont initiées, mais donne la priorité aux validations que Panorama initie automatiquement, comme les actualisations du nom de domaine complet. Cependant, si la file d'attente possède déjà le nombre maximum de validations lancées par l'administrateur (10), vous devez attendre que Panorama termine le traitement d'une validation en attente avant d'en lancer une nouvelle. Vous pouvez Utilisez le Gestionnaire de Tâches Panorama (Tasks) pour annuler des validations ou pour voir des détails au sujet des validations dont l'état est en attente, en cours, terminée ou échouée. Pour vérifier les modifications qu'une validation activera, vous pouvez exécuter un aperçu de validation.

Lorsque vous lancez une validation, panorama vérifie la validité des modifications avant de les activer. La sortie de validation affiche les conditions qui bloquent la validation (erreurs) ou qui sont importantes à savoir (avertissements). Par exemple, la validation peut indiquer une destination d'itinéraire non valide que vous devez corriger pour que la validation réussisse. Le processus de validation vous permet de trouver et de corriger les erreurs avant la validation (il ne modifie pas la configuration en cours d'exécution). Cette option est utile si vous avez une fenêtre de validation fixe et que vous souhaitez vous assurer que la validation sera une réussite exempte d'erreur.

La récupération automatique de la validation est activée par défaut, permettant aux pare-feux gérés de tester localement la configuration transmise depuis Panorama pour vérifier que les nouvelles modifications ne rompent pas la connexion entre Panorama et le pare-feu géré. Si la configuration validée rompt la connexion entre Panorama et un pare-feu géré, le pare-feu échoue automatiquement la validation et la configuration revient à la configuration précédente et le statut de la politique partagée ou du modèle (**Panorama** > **Managed Devices (Appareils gérés)** > **Summary (Résumé)**) est désynchronisé en fonction des objets de configuration qui ont été transmis. De plus, les pare-feux gérés testent leur connexion à Panorama toutes les 60 minutes et si un pare-feu géré détecte qu'il ne peut plus se connecter avec succès à Panorama, il revient à la configuration précédente.

Pour plus de détails sur les configurations candidates et actuelles, reportez-vous à la section Gérer Panorama et les sauvegardes de configuration du pare-feu.

Pour empêcher plusieurs administrateurs d'effectuer des modifications de configuration lors des sessions simultanées, reportez-vous à la section Gérez les Verrous pour Restreindre les Modifications de Configuration.

© 2020 Palo Alto Networks, Inc.

Lorsque vous déplacez des configurations vers des pare-feux gérés, Panorama applique la configuration en cours. Par conséquent, Panorama ne vous permet pas d'appliquer des modifications aux pare-feux gérés tant que vous ne validez pas d'abord les modifications à Panorama.

© 2020 Palo Alto Networks, Inc.

Planification de votre déploiement Panorama

- Déterminez l'approche de gestion. Prévoyez-vous d'utiliser Panorama pour configurer et gérer les stratégies de manière centralisée, pour administrer de manière centralisée les mises à jour logicielles, des contenus et de licence, et/ou pour centraliser la journalisation et la génération de rapports sur les périphériques gérés sur le réseau ?

  Si vous avez déjà déployé et configuré les pare-feu Palo Alto Networks sur votre réseau, déterminez si vous devez passer à une gestion centralisée des périphériques. Ce processus requiert une migration de toutes les configurations et stratégies depuis vos pare-feu sur Panorama. Pour plus de détails, voir Transition d'un pare-feu à la gestion Panorama.
- Vérifiez les versions logicielles de Panorama et du pare-feu. Panorama peut gérer les pare-feux exécutant des versions logicielles Pan-OS qui correspondent à la version panorama ou sont antérieures à la version de panorama. Par exemple, Panorama version 8.0 ne peut pas gérer des pare-feux exécutant PAN-OS 8.1. De plus, Panorama 8.1 ne peut pas gérer les pare-feu exécutant PAN-OS 6.0.0 à 6.0.3 et ne peut pas gérer les pare-feu qui exécutent une version plus récente de PAN-OS que la version Panorama.
- Prévoyez d'utiliser la même base de données de filtrage d'URL (BrightCloud ou PAN-DB) dans tous les pare-feux gérés. Si certains pare-feux utilisent la base de données BrightCloud et d'autres utilisent PAN-DB, Panorama ne peut gérer les règles de sécurité pour l'une ou l'autre base de données de filtrage d'URL. Les règles de filtrage d'URL pour l'autre base de données doivent être gérées localement sur les pare-feux qui utilisent cette base de données.
- Déterminez votre méthode d'authentification entre Panorama et ses périphériques gérés et l'homologue haute disponibilité. Par défaut, Panorama utilise des certificats prédéfinis pour authentifier les connexions SSL utilisées pour la gestion et la communication entre appareils. Toutefois, vous pouvez configurer une authentification basée sur un certificat personnalisé pour améliorer la sécurité des connexions SSL entre Panorama, les pare-feu et les collecteurs de journaux. En utilisant des certificats personnalisés, vous pouvez établir une chaîne de confiance unique pour garantir une authentification mutuelle entre Panorama et les périphériques qu'il gère. Vous pouvez importer les certificats à partir de votre infrastructure à clé publique d'entreprise (PKI) ou les générer sur Panorama.
- Prévoyez d'utiliser Panorama dans une configuration Haute Disponibilité. Configurez-le en tant que paire Haute Disponibilité active/passive. Voir Panorama Haute disponibilité.
- Planifiez la prise en compte des exigences de segmentation et de sécurité réseau dans un déploiement à grande échelle. Par défaut, Panorama exécuté sur un appareil de la série M utilise l'interface de gestion (MGT) pour l'accès administratif à Panorama et la gestion des périphériques (pare-feu, collecteurs de journaux et appareils et clusters d'appareils WildFire), la collecte des journaux, la communication avec les groupes de collecteurs et le déploiement de mises à jour logicielles et de contenu sur les périphériques. Cependant, pour améliorer la sécurité et permettre la segmentation du réseau, vous pouvez réserver l'interface MGT à un accès administratif et utiliser les interfaces dédiés de la série M (Eth1, Eth2, Eth3, Eth4 et Eth5) pour les autres services.
- Pour obtenir des rapports significatifs sur l'activité du réseau, planifiez une solution de journalisation :
  - Vérifiez l'allocation des ressources pour votre dispositif virtuel Panorama déployé en mode Log Collector sur AWS ou Azure. Le dispositif virtuel Panorama ne conserve pas le mode Log Collector s'il est redimensionné. Cela entraîne une perte de données de journal.
  - Estimez la capacité de stockage de journaux dont votre réseau a besoin pour satisfaire aux exigences de sécurité et de conformité. Prenez en compte des facteurs tels que les capacités de journalisation de vos modèles Panorama, la topologie du réseau, le nombre de pare-feu envoyant des journaux, le type de trafic de journaux (par exemple, le filtrage d'URL et les journaux de menaces par rapport aux journaux de trafic), le taux auquel les pare-feu génèrent des journaux et le nombre de jours pendant lesquels vous souhaitez enregistrer les journaux sur Panorama. Pour plus de détails, voir Déterminer les exigences de stockage de journaux Panorama.
  - Avez-vous besoin de transmettre les journaux à des services externes (comme un serveur Syslog), en plus de Panorama ? Consultez Options de transfert de journal.

© 2020 Palo Alto Networks, Inc.

- Voulez-vous posséder ou gérer votre propre stockage de journaux sur site, ou souhaitez-vous tirer parti de Cortex Data Lake fourni par Palo Alto Networks?
- Si vous avez besoin d'une solution de stockage à long terme, disposez-vous d'une solution SIEM (Gestion des informations et des événements de sécurité), comme Splunk ou ArcSight, à laquelle transmettre les journaux ?
- Avez-vous besoin de redondance dans la journalisation ?

  Si vous configurez un groupe de collecteurs avec plusieurs collecteurs de journaux, vous pouvez activer la redondance pour garantir qu'aucun journal n'est perdu si un collecteur de journal devient indisponible (voirMises en garde pour un groupe de collecteurs avec plusieurs collecteurs de journaux).

  Si vous déployez des appareils virtuels Panorama en mode hérité dans une configuration HD, les pare-feu gérés peuvent envoyer des journaux aux deux homologues HD afin qu'une copie de chaque journal réside sur chaque homologue. Cette option de redondance est activée par défaut (voir Modifier les paramètres de journalisation et de mise en mémoire tampon des journaux).
- Vous connecterez-vous à un NFS (Network File System) ? Si l'appareil virtuel Panorama est en mode hérité et ne gère pas les collecteurs de journaux dédiés, le stockage NFS est la seule option permettant d'augmenter la capacité de stockage des journaux au-delà de 8 To. Le stockage NFS est disponible uniquement si Panorama fonctionne sur un serveur ESXi. Si vous utilisez le stockage NFS, notez que les pare-feu peuvent envoyer des journaux uniquement à l'homologue principal de la paire HD, et que seul l'homologue principal est monté sur le NFS et peut y écrire.

- ❑ Déterminez les privilèges d'accès en fonction des rôles requis par les administrateurs pour accéder aux pare-feu gérés et à Panorama. Voir Configurer l'accès administratif à Panorama.
- ❑ Planifiez les groupes de périphériques requis. Examiner si les pare-feux de groupe sont basés sur la fonction, la politique de sécurité, la situation géographique ou la segmentation du réseau. Un exemple de groupe de périphériques basé sur une fonction est un groupe contenant tous les pare-feux utilisés par l'équipe de Recherche & Développement. Considérez s'il faut créer des groupes de périphériques plus petits basés sur des points communs, des groupes de périphériques plus importantsà mettre à l'échelle plus facilement ou une hiérarchie de groupe de périphériques pour simplifier des couches complexes d'administration.
- ❑ Planifiez une stratégie en couches pour administrer les stratégies. Voyez comment les pare-feux héritent et évaluent les règles de politique au sein de la hiérarchie de groupe de périphériques et comment mettre en œuvre des meilleures règles communes, les règles du groupe de périphériques, et les règles spécifiques du pare-feu pour répondre à vos besoins en matière de réseau. Pour la visibilité et la gestion centralisée des stratégies, envisagez d'utiliser Panorama pour administrer les règles, même si vous avez besoin d'exceptions spécifiques de pare-feu pour des règles communes ou groupes de périphériques. Si nécessaire, vous pouvez insérer une règle de stratégie dans un sous-ensemble de pare-feux dans un groupe de périphériques.
- ❑ Planifiez l'organisation de vos pare-feux en fonction de la façon dont ils héritent des paramètres de configuration réseau des modèles et des piles de modèles. Par exemple, envisagez d'affecter les pare-feu à des modèles en fonction des modèles matériels, de leur proximité géographique et des besoins de réseau similaires pour les fuseaux horaires, le serveur DNS, et les paramètres d'interface.

© 2020 Palo Alto Networks, Inc.

Déployer Panorama : Présentation de la tâche

La liste de tâches suivante récapitule les étapes à exécuter pour démarrer avec Panorama. Pour un exemple d'utilisation de Panorama pour la gestion centralisée, reportez-vous à la section Cas d'utilisation : Configurer des pare-feux en utilisant Panorama.

STEP 1 | (Appareil de série M uniquement) Montez l'appareil dans une baie.

STEP 2 | Effectuez la configuration initiale pour permettre l'accès au réseau à Panorama. Reportez-vous à la section Configuration de l'appareil virtuel Panorama ou Configuration de l'appareil de série M.

STEP 3 | Enregistrer Panorama et Installer les licences.

STEP 4 | Installer les mises à jour de contenu et logicielles pour Panorama.

STEP 5 | (Recommandé) Installez Panorama avec une configuration haute disponibilité. Reportez-vous à la section Panorama Haute Disponibilité.

STEP 6 | Ajouter un pare-feu en tant que périphérique géré.

STEP 7 | Ajouter un groupe de périphériques ou Créer une hiérarchie de groupe de périphériques, Ajouter un modèle, et (si applicable) Configuration d'une pile de modèles.

STEP 8 | (Facultatif) Configurez le transfert des journaux vers Panorama et/ou des services externes. Reportez-vous à la section Gérer la collecte des journaux.

STEP 9 | Surveiller l'activité réseau en utilisant les outils d'affichage et de création de rapports de Panorama.

© 2020 Palo Alto Networks, Inc.

Configurer Panorama

Pour la création centralisée de rapports et la gestion de politiques homogènes sur tous les pare-feux de votre réseau, vous pouvez déployer le serveur de gestion Panorama™ en tant qu'appareil virtuel ou qu'appareil matériel (appareil M-200, M-500, M-600 ou M-600).

Les rubriques suivantes décrivent comment configurer Panorama sur votre réseau :

- Déterminer les besoins de stockage de journaux Panorama
- Configuration de l'appareil virtuel Panorama
- Configuration de l'appareil de série M
- Enregistrer Panorama et Installer les licences
- Installation du certificat du périphérique Panorama
- Installer les mises à jour de contenu et logicielles pour Panorama
- Transition vers un modèle Panorama différent
- Accéder et naviguer dans les interfaces de gestion de Panorama
- Configurer l'accès administratif à Panorama
- Configurer l'authentification à l'aide de certificats personnalisés

© 2020 Palo Alto Networks, Inc.

Déterminer les besoins de stockage de journaux Panorama

Lorsque vous planifiez votre déploiement Panorama, estimez la capacité de stockage de journaux dont Panorama a besoin pour déterminer les modèles Panorama à déployer, que ce soit pour étendre le stockage sur ces appareils au-delà de leurs capacités par défaut, que ce soit pour déployer des collecteurs de journaux dédiés et pour configurer le transfert de journaux depuis Panorama depuis des destinations extérieures. Lorsque le stockage de journaux atteint la capacité maximale, Panorama supprime automatiquement les journaux plus anciens pour créer un espace pour les nouveaux.

Effectuez les étapes suivantes pour déterminer le stockage de journaux approximatif que Panorama requiert. Pour plus de détails et cas d'utilisation, reportez-vous au Guide de dimensionnement et de conception de Panorama.

STEP 1 | Déterminez les exigences de conservation des journaux de votre organisation.

Les facteurs qui affectent les exigences de rétention du journal incluent :

- Politique informatique de votre organisation
- Redondance des journaux — si vous activez la redondance de journaux lorsque vous configurez un groupe de collecteurs, chaque journal aura deux copies, ce qui double votre besoin requis de stockage de journaux.
- Les exigences réglementaires, telles que celles spécifiées par la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS), la loi Sarbanes-Oxley et la loi américaine sur la transférabilité et la responsabilité des assurances de santé (HIPAA).



Si votre organisation exige le retrait des journaux après une certaine période, vous pouvez définir la période d'expiration pour chaque type de journal. Vous pouvez également définir un quota de stockage pour chaque type de journal en tant que pourcentage de l'espace total si vous avez besoin de prioriser la rétention du journal par type. Consultez également Gérer les quotas de stockage et de délais d'expiration pour les journaux et rapports.

STEP 2 | Déterminez les taux de journalisation quotidiens moyens.

Faites cela plusieurs fois par jour, à la pointe et hors pointe, pour estimer la moyenne. Plus souvent vous échantillonnez les taux, plus votre estimation est précise.

1. Affichez le taux de génération de journal en cours dans les journaux par seconde :
   - Si Panorama ne collecte pas encore les journaux, accédez à l'ILC de chaque pare-feu, exécutez la commande suivante et calculez les taux totaux pour tous les pare-feu. Cette commande affiche le nombre de journaux reçus dans la dernière seconde.

```
> debug log-receiver statistics
```

   - Si Panorama recueille déjà les journaux, exécutez la commande suivante à l'ICL de chaque appareil qui reçoit les journaux (serveur de gestion Panorama ou collecteur de journaux dédié) et calculez les taux totaux. Cette commande donne le taux de journalisation moyen pour les cinq dernières minutes.

```
> debug log-collector log-collection-stats show incoming-logs
```


© 2020 Palo Alto Networks, Inc.



Vous pouvez également utiliser un gestionnaire SNMP pour déterminer les taux de journalisation des collecteurs de journaux (voir la MIB panLogCollector, OID 1.3.6.1.4.1.25461.1.1.6) et les pare-feu (voir le panDeviceLogging, OID 1.3.6.1.4.1.25461.2.1.2. 7).

2. Calculez la moyenne des taux d'échantillon.
3. Calculez le taux d'enregistrement quotidien en multipliant les journaux par seconde par 86.400.

STEP 3 | Estimez la capacité de stockage nécessaire.



Cette formule ne fournit qu'une estimation ; la quantité exacte de stockage requis diffère du résultat de la formule.

Utilisez la formule :

<required_storage_duration> x <average_log_size> x <average_logging_rate>

La taille moyenne du journal varie considérablement selon le type de journal. Toutefois, vous pouvez utiliser 500 octets comme taille moyenne approximative de journal.

Par exemple, si Panorama doit stocker les journaux pendant 30 jours et le taux de journalisation moyen pour tous les pare-feu est 21.254.400 journaux par jour, la capacité de stockage de journal requise est : 30 x 500 x 21 254 400 = 318 816 000 000 octets (environ 230 Go).

STEP 4 | Étapes suivantes...

Si vous déterminez que Panorama nécessite plus de capacité de stockage de journaux :

- Augmentez la capacité de stockage de journaux sur l'appareil virtuel Panorama.
- Augmentez le stockage sur l'appareil de série M.

© 2020 Palo Alto Networks, Inc.

Configuration de l'appareil virtuel Panorama

L'appareil virtuel Panorama vous permet d'utiliser votre infrastructure virtuelle VMware existante pour gérer et surveiller de manière centralisée les pare-feu Palo Alto Networks et les collecteurs de journaux dédiés. Vous pouvez installer l'appareil virtuel sur un serveur ESXi, Amazon Web Services (AWS), AWS GovCloud, Microsoft Azure, Google Cloud Platform (GCP), KVM, Hyper-V ou vCloud Air. En plus ou à la place du déploiement de collecteurs de journaux dédiés, vous pouvez transférer les journaux du pare-feu directement vers l'appareil virtuel Panorama. Pour une plus grande capacité de stockage des journaux et une génération de rapports plus rapide, vous avez la possibilité de basculer l'appareil virtuel du mode hérité au mode Panorama, et de configurer un collecteur de journaux local. Pour plus de détails sur l'appareil virtuel Panorama et ses modes, consultez Modèles Panorama.

Ces rubriques supposent que vous êtes familiarisé avec les produits de l'hyperviseur public et privé nécessaires à la création de l'appareil virtuel et ne couvrent pas les concepts ou la terminologie connexes.

- Définir la configuration requise pour l'appareil virtuel Panorama
- Installez l'appareil virtuel Panorama
- Effectuer la configuration initiale de l'appareil virtuel Panorama
- Configurer l'appareil virtuel Panorama en tant que collecteur de journaux local
- Configurer l'appareil virtuel Panorama avec le collecteur de journaux local
- Configurer un appareil virtuel Panorama en mode Panorama
- Configurer un appareil virtuel Panorama en mode de Gestion seulement
- Augmenter la capacité de stockage de journaux sur l'appareil virtuel Panorama
- Augmenter les processeurs et la mémoire sur l'appareil virtuel Panorama
- Augmentation du disque système sur l'appareil virtuel Panorama
- Terminer le programme d'installation de l'appareil virtuel Panorama

Définir la configuration requise pour l'appareil virtuel Panorama

Complétez les tâches suivantes avant d'installer l'appareil virtuel Panorama :

- Utilisez votre navigateur pour accéder au site web de support Palo Alto Networks et enregistrer Panorama. Vous aurez besoin du numéro de série Panorama que vous avez reçu dans l'email d'exécution des commandes. Après avoir enregistré Panorama, vous pouvez accéder à la page Panorama de téléchargement de logiciels.
- Passez en revue les hyperviseurs Panorama pris en charge pour vérifier que l'hyperviseur respecte le exigences de version minimales pour déployer Panorama.
- Si vous installez Panorama sur un serveur VMware ESXi, vérifiez que le serveur répond aux exigences minimales répertoriées dans System Requirements for the Panorama Virtual Appliance (Configuration système requise pour l'appareil virtuel Panorama).. Ces exigences s'appliquent à Panorama 5.1 et aux versions ultérieures. Les exigences varient selon que vous exécuterez l'appareil virtuel en mode Panorama ou en mode Gestion uniquement. Pour plus de détails sur les modes, voir Modèles de Panorama .

  Si vous installez Panorama sur VMware vCloud Air, vous définissez les paramètres système lors de l'installation.

Passez en revue les exigences minimales en matière de ressources pour le déploiement de l'appareil virtuel Panorama sur Amazon Web Services (AWS), AWS GovCloud, Microsoft Azure, Google Cloud Platform (GCP), Hyper-V, KVM et VMware ESXi pour vous assurer que la machine virtuelle respecte les ressources minimales requises pour le mode souhaité (Panorama, Gestion uniquement ou Collecteur de journaux). Les

© 2020 Palo Alto Networks, Inc.

ressources minimales requises pour l'appareil virtuel Panorama sont conçues pour vous aider à atteindre le nombre maximum de journaux par seconde (LPS) pour la collecte de journaux en mode Panorama et en mode Collecteur de journaux. Si vous ajoutez ou supprimez des disques de journalisation virtuels, ce qui entraîne une configuration qui n'atteint pas ou dépasse le nombre de disques de journalisation virtuels recommandé (ci-dessous), votre LPS sera réduit.

Si ces exigences de ressources minimales ne sont pas satisfaites pour le mode Panorama lorsque vous Installez l'appareil virtuel Panorama, Panorama revient par défaut au mode Gestion uniquement pour tous les hyperviseurs publics (AWS, AWS GovCloud, Azure et GCP) et privés (Hyper-V, KVM et VMware ESXi) pris en charge. Si les exigences de ressources minimales ne sont pas satisfaites pour le mode Gestion uniquement, Panorama revient par défaut au mode Maintenant pour tous les hyperviseurs publics, Hyper-V et KVM pris en charge. Si les exigences de ressources minimales ne sont pas satisfaites pour le mode Gestion uniquement lorsque vous Installez Panorama sur VMware, Panorama revient par défaut au mode Hérité.

Il est recommandé de déployer le serveur de gestion Panorama en mode Panorama pour les capacités de gestion des périphériques et de collecte de journaux. Bien qu'il soit toujours pris en charge, le mode Legacy n'est pas recommandé pour les environnements de production. Par ailleurs, vous ne pouvez plus faire passer Panorama à ce mode. Pour plus de détails sur les modes pris en charge, voir la section Modèles Panorama.

Table 1: Exigences système de l'appareil virtuel Panorama

Exigences	Appareil virtuel Panorama en mode Gestion uniquement.	Appareil virtuel Panorama en mode Panorama	Appareil virtuel Panorama en mode Collecteur de journaux.
Version du matériel virtuel	• **VMware ESXi et vCloud Air**—VMware ESXi 5.5, 6.0, 6.5, ou 6.7 basée sur noyau 64 bits. La version prise en charge du type de famille de matériel virtuel (aussi connu comme la version du matériel virtuel VMware) sur le serveur ESXi est vmx-10. • **Hyper-V** : Windows Server 2016 avec rôle Hyper-V ou Hyper-V 2016 • **KVM** : Ubuntu version 16.04 ou CentOS7 En mode Panorama, l'appareil virtuel exécuté sur une version ESXi prend en charge jusqu'à 12 disques de journalisation virtuels avec 2 To de stockage de journaux chacun, pour une capacité maximale totale de 24 To. (VMware ESXi et vCloud Air uniquement) En mode Legacy, l'appareil virtuel prend en charge un disque de journalisation virtuel. ESXi 5.5 et ultérieur prend en charge un disque pouvant aller jusqu'à 8 To. Les versions antérieures d'ESXi prennent en charge un disque de 2 To maximum.		
(ESXi et vCloud Air uniquement) Ordinateur client	Pour installer l'appareil virtuel Panorama et gérer ses ressources, vous devez installer Client VMware vSphere ou Infrastructure Client VMware compatible avec votre serveur ESXi.		
Disque système	• **Par défaut** : 81 Go • **Mis à jour** : 224Go	• **Par défaut** : 81 Go • **Mis à jour** : 224 Go (Requis pour SD-WAN) Pour le stockage de journaux, Panorama utilise des disques de journalisation virtuels à	81 Go Pour le stockage de journaux, Panorama utilise des disques de journalisation virtuels à la place du disque

© 2020 Palo Alto Networks, Inc.

Exigences	Appareil virtuel Panorama en mode Gestion uniquement.	Appareil virtuel Panorama en mode Panorama	Appareil virtuel Panorama en mode Collecteur de journaux.
		la place du disque système ou d'un magasin de données NFS.	système ou d'un magasin de données NFS.

Processeurs, mémoire et disques de journalisation	• Exploiter jusqu'à 500 appareils gérés
	  • 16 processeurs
	  • 32 Go de mémoire.
	  • Le stockage des journaux locaux n'est pas pris en charge
	• Exploiter jusqu'à 1 000 appareils gérés
	  • 32 processeurs
	  • 128 Go de mémoire
	  • Le stockage des journaux locaux n'est pas pris en charge
	• Pour gérer plus de 1 000 pare-feux, consultez la page Exigences de la capacité de gestion accrue des périphériques.
		• Jusqu'à 10 000 journaux/sec :
		  • 16 processeurs
		  • 32 Go de mémoire.
		  • 4 disques de journalisation de 2 To
		  • Exploiter jusqu'à 500 appareils gérés
		• Jusqu'à 20 000 journaux/sec
		  • 32 processeurs
		  • 128 Go de mémoire
		  • 8 disques de journalisation de 2 To
		  • Exploiter jusqu'à 1 000 appareils gérés
			• Jusqu'à 15 000 journaux/sec
			  • 16 processeurs
			  • 32 Go de mémoire.
			  • 4 disques de journalisation de 2 To
			• Jusqu'à 25 000 journaux/sec
			  • 32 processeurs
			  • 128 Go de mémoire
			  • 8 disques de journalisation de 2 To

Capacité de stockage de journaux	Le mode Panorama en mode Gestion uniquement requiert le transfert de journal vers un collecteur de journaux dédié.	2 To à 24 To	2 To à 24 To

Interfaces prises en charge

Les interfaces peuvent être utilisées pour la gestion des périphériques, la collecte des journaux, la communication avec les groupes de collecteurs, les licences et les mises à jour logicielles.

*** Untranslated ***	Amazon Web Services (AWS) et AWS GovCloud	Microsoft A	Google Cloud Platform (GCP)	KVM	Hyper-V	VMware (ESXi, vCloud Air)
Gestion des périphériques	Toute interface prise en charge					

© 2020 Palo Alto Networks, Inc.

*** Untranslated ***	Amazon Web Services (AWS) et AWS GovCloud		Microsoft A	Google Cloud Platform (GCP)	KVM	Hyper-V	VMware (ESXi, vCloud Air)
Collecte des journaux de périphérique	Toute interface prise en charge						
Communication avec les groupes de collecteurs	Toute interface prise en charge						
Licences et mises à jour logicielles	Interface MGT uniquement	Interface MGT uniquement	Interface MGT uniquement	Interface MGT uniquement	Toute interface prise en charge	Toute interface prise en charge	Toute interface prise en charge

Installez l'appareil virtuel Panorama

Avant l'installation, décidez si vous souhaitez exécuter l'appareil virtuel en mode Panorama, en mode Gestion uniquement, en mode Collecteur de journaux ou en mode hérité (VMware uniquement). Chaque mode a des besoins en ressources différents, comme décrit dans Configuration requise pour l'appareil virtuel Panorama. Vous devez disposer de la configuration requise avant de commencer l'installation.

Il est recommandé d'installer l'appareil virtuel en mode Panorama pour optimiser le stockage des journaux et la génération de rapports. Pour plus d'informations sur Panorama et le mode hérité, reportez-vous à la section les modèles Panorama.

- Installez Panorama sur VMware
- Installer Panorama sur AWS
- Installer Panorama sur AWS GovCloud
- Installer Panorama sur Azure
- Installer Panorama sur la plateforme Google Cloud
- Installer Panorama sur KVM
- Installer Panorama sur Hyper-V

Installez Panorama sur VMware

Vous pouvez installer l'appareil virtuel Panorama sur les plates-formes ESXi et vCloud Air VMware.

- Installer Panorama sur un serveur ESXi
- Installer Panorama sur vCloud Air
- Prise en charge des outils VMware sur l'appareil virtuel Panorama

Installer Panorama sur un serveur ESXi

Utilisez ces instructions pour installer un nouvel appareil virtuel Panorama sur un serveur VMware ESXi. Si vous mettez à niveau un appareil virtuel Panorama existant, passez à l'étape installer les mises à jour de contenu et logicielles pour Panorama.

STEP 1 | Téléchargez le fichier Open Virtual Appliance (OVA) de l'image de base Panorama 10.0.

© 2020 Palo Alto Networks, Inc.

1. Allez au Site de téléchargements de logiciels Palo Alto Networks. (si vous ne pouvez pas vous connecter, accédez au site Web de l'assistance à la clientèle de Palo Alto Networks pour obtenir de l'aide.)
2. Dans la colonne des téléchargements de la section des images de la base de Panorama, téléchargez la dernière version du fichier OVA de Panorama (`Panorama-ESX-10.0.0.ova`).

STEP 2 | Installez Panorama.

1. Lancez le client VMware vSphere et connectez-le au serveur VMware.
2. Sélectionnez le **File (fichier)** > **Deploy OVF Template (modèle de déploiement OVF)**.
3. **Browse (Rechercher)** pour sélectionner le fichier Panorama OVA et cliquez sur **Next (Prochain)**.
4. Vérifiez que le nom et la description du produit correspondent bien à la version téléchargée, puis cliquez sur **Next (Suivant)**.
5. Saisissez un nom descriptif pour l'appareil virtuel Panorama, puis cliquez sur **Next (Suivant)**.
6. Sélectionnez un emplacement de magasin de données (disque système) sur lequel installer l'image Panorama. Consultez le Définir la configuration requise pour l'appareil virtuel Panorama pour connaître les tailles de disque système compatibles. Après avoir sélectionné le magasin de données, cliquez sur **Next (Suivant)**.
7. Sélectionnez **Thick Provision Lazy Zeroed** comme format de disque, puis cliquez sur **Next (Suivant)**.
8. Spécifiez quels réseaux dans l'inventaire sont à utiliser pour l'appareil virtuel Panorama, puis cliquez sur Next (Suivant).
9. Confirmez les options sélectionnées, cliquez sur **Finish (Terminer)** pour démarrer le processus d'installation, et cliquez sur **Close (Fermer)** lorsqu'il est terminé. Ne mettez pas encore l'appareil virtuel Panorama sous tension.

STEP 3 | Configurez les ressources sur l'appareil virtuel Panorama.

1. Cliquez droit sur l'appareil virtuel Panorama et sélectionnez **Edit Settings (Modifier les paramètres)**.
2. Dans les paramètres **Hardware (Matériel)**, attribuez les processeurs et la mémoire en fonction des besoins.

   L'appareil virtuel démarre en mode Panorama si vous allouez suffisamment de CPUs (Processeurs) et de Memory (Mémoire) et ajoutez un disque de journalisation virtuel (plus tard dans cette procédure). Sinon, l'appareil démarre en mode Gestion uniquement. Pour plus de détails sur les modes, voir Modèles de Panorama .
3. Mettez le **SCSI Controller (Contrôleur SCSI)** sur **LSI Logic Parallel (LSI Logic Parallel)**.
4. Ajoutez un disque de journalisation virtuel.

   Cette étape est nécessaire dans les scénarios suivants :

   - *En mode Panorama pour stocker les journaux sur un disque de journalisation dédié.*
   - *Gérez votre déploiement SD-WAN en mode Gestion uniquement.*

   1. **Add (Ajoutez)** un disque, sélectionnez **Hard Disk (Disque dur)** pour le type de matériel et cliquez sur **Next (Suivant)**.
   2. **Create a new virtual disk (Créer un nouveau disque virtuel)** et cliquez sur **Next (Suivant)** .
   3. Configurez la **taille du disque** à exactement 2 To.

      En mode Panorama, vous pouvez ajouter d'autres disques de journalisation *(pour un total de 12) avec 2 To de stockage chacun. L'extension de la taille d'un disque de journalisation déjà ajouté à Panorama n'est pas prise en charge.*
   4. Sélectionnez le format de disque que vous préférez pour l'**Approvisionnement du disque**.

© 2020 Palo Alto Networks, Inc.

Tenez compte des besoins de votre entreprise lorsque vous choisissez le format d'approvisionnement du disque. Pour obtenir plus d'informations sur les considérations relatives aux performances d'approvisionnement du disque, consultez le document VMware Thick vs Thin Disks and All Flash Arrays, ou la documentation additionnelle de VMware.

Lors de l'ajout de plusieurs disques de journalisation, il est préférable de sélectionner le même format d'approvisionnement de disque pour tous les disques afin d'éviter tout problème de performance inattendu qui pourrait survenir.

5. Sélectionnez **Specify a datastore or datastore structure (Spécifier un magasin de données ou une structure de magasin de données)** comme emplacement, **Browse (Recherchez)** un magasin de donnée disposant d'un espace de stockage suffisant, cliquez sur **OK** et cliquez sur **Next (Suivant)**.
6. Sélectionnez un **Virtual Device Node (nœud de périphérique virtuel)** SCSI (vous pouvez utiliser la sélection par défaut) et cliquez sur **Next (Suivant)**.

   Panorama ne parviendra pas à démarrer si vous sélectionnez un format autre que SCSI.
7. Vérifiez que les paramètres sont corrects, puis cliquez sur **Finish (Terminer)**.

5. Cliquez sur **OK** pour enregistrer vos modifications.

STEP 4 | Mettez l'appareil virtuel Panorama sous tension.

1. Dans le vSphere Client, cliquez droit sur l'appareil virtuel Panorama et sélectionnez **Power (Alimentation)** > **Power On (Allumer)**. Attendez que Panorama redémarre avant de continuer.
2. Vérifiez que l'appareil virtuel fonctionne dans le mode correct :
   1. Cliquez droit sur l'appareil virtuel Panorama et sélectionnez **Open Console (Ouvrir la console)**.
   2. Entrez votre nom d'utilisateur et mot de passe pour ouvrir une session (par défaut, **admin** pour les deux).
   3. Affichez le mode en exécutant la commande suivante :

      ```
      > show system info
      ```

      Dans la sortie, `system-mode` indique soit le mode `Panorama`, soit le mode `management-only` (gestion uniquement).

STEP 5 | Augmentation du disque système pour Panorama sur un serveur ESXi si vous avez l'intention d'utiliser l'appareil virtuel Panorama pour :

- Gérer votre déploiement SD-WAN en mode Panorama.
- Nécessite un espace de stockage supplémentaire pour les mises à jour dynamiques lors de la gestion de déploiements de pare-feu à grande échelle.

Vous êtes maintenant prêt à effectuer la configuration initiale de l'appareil virtuel Panorama.

Installer Panorama sur vCloud Air

Utilisez ces instructions pour installer une nouvelle application virtuelle Panorama dans VMware vCloud Air. Si vous mettez à niveau un appareil virtuel panorama déployé dans vCloud air, sautez à installer le contenu et les mises à jour logicielles pour Panorama.

STEP 1 | Téléchargez le fichier Open Virtual Appliance (OVA) de l'image de base Panorama 10.0.

1. Allez au Site de téléchargements de logiciels Palo Alto Networks. (si vous ne pouvez pas vous connecter, accédez au site Web de l'assistance à la clientèle de Palo Alto Networks pour obtenir de l'aide.)

© 2020 Palo Alto Networks, Inc.

2. Dans la colonne des téléchargements de la section des images de la base de Panorama, téléchargez le fichier OVA de la version 10.0 de Panorama (`Panorama-ESX-10.0.0.ova`).

STEP 2 | Importez l'image Panorama au catalogue vCloud Air.

Pour plus de détails sur ces étapes, reportez-vous au Guide de l'utilisateur Outil OVF.

1. Installez l'outil OVF sur votre système client.
2. Accédez à l'ILC du système client.
3. Accédez au répertoire d'outils de l'outil de recherche (par exemple, c:\Program VMware: Tool).
4. Convertir le fichier OVA en package de la version :

```
ovftool.exe <OVA#file#pathname> <OVF#file#pathname>
```

5. Utilisez un navigateur pour accéder à la console Web vCloud air, sélectionnez votre **Virtual Private Cloud OnDemand (emplacement virtuel Private Cloud OnDemand)**, et enregistrez l'URL du navigateur. Vous utiliserez les informations d'URL pour compléter la prochaine étape. Le format d'URL est : **https://*<emplacement du cloud virtuel>*.vchs.vmware.com/compute/cloud/org/*<numéro de compte du cloud virtuel>*/#/catalogVAppTemplateList?catalog=*<ID du catalogue>***.
6. Importez le paquet OVF, en utilisant les informations de l'URL vCloud Air pour compléter les variables <virtual-cloud-location>, <vCloud-account-number>, and <catalog-ID>. Les autres variables sont votre nom d'utilisateur vCloud Air et le domaine à <user>@<domain>, un centre virtuel de données <datacenter> et un modèle vCloud Air template.

```
ovftool.exe -st="OVF" "<OVF#file#pathname>"
 "vcloud://<user>@<domain>:password@<virtual-cloud-
location>.vchs.vmware.com?vdc=<datacenter>&org=<vCloud-account-
number>&vappTemplate=<template>.ovf&catalog=default-catalog"
```

STEP 3 | Installez Panorama.

1. Accéder à la console Web vCloud Air et sélectionner votre **Virtual Private Cloud OnDemand (Cloud Virtuel Privé sur Demande)** région.
2. Créer une machine virtuelle Panorama. Pour les étapes, reportez-vous à Ajouter une machine virtuelle à partir d'un modèle dans le Centre de documentation vCloud Air. Configurez le **CPU (Processeur)**, **Memory (Mémoire)** et **Storage (Stockage)** comme suit :
   - Configurez le **CPU** et la **Memory (Mémoire)** en fonction du mode de l'appareil virtuel : voir Définir la configuration requise pour l'appareil virtuel Panorama.
   - Configurez le **Storage (Stockage)** pour configurer le disque système de l'appareil virtuel Panorama. Consultez Définir la configuration requise pour l'appareil virtuel Panoramapour connaitre les tailles de disque compatibles sur la base du mode de l'appareil virtuel Panorama. Pour une meilleure journalisation et performance de rapports, sélectionnez l'option **SSD-Accelerated (Accéléré par SSD)**.

     Pour augmenter la capacité de stockage du journal, vous devez ajouter un disque virtuel à Panorama sur vCloud air. En mode Panorama, l'appareil virtuel n'utilise pas le disque système pour le stockage des journaux ; vous devez ajouter un disque de journalisation virtuel.

STEP 4 | Créer des règles vCloud Air NAT sur la passerelle pour autoriser le trafic entrant et sortant pour l'application virtuelle Panorama.

Faire référence à Ajouter une règle NAT dans le Centre de documentation vCloud Air pour les instructions détaillées :

© 2020 Palo Alto Networks, Inc.

1. Ajouter une règle NAT qui permet à Panorama de recevoir le trafic provenant des pare-feux et permet aux administrateurs d'accéder Panorama.
2. Ajouter une règle NAT qui permet Panorama de récupérer les mises à jour à partir du serveur de mise à jour de Palo Alto Networks et d'accéder aux pare-feux.

STEP 5 | Créer une règle de pare-feu vCloud Air pour autoriser le trafic entrant sur l'appareil virtuel Panorama.

Le trafic sortant est autorisé par défaut.

Faire référence à Ajouter une règle NAT dans le Centre de documentation vCloud Air pour les instructions détaillées.

STEP 6 | Ouvrir l'appareil virtuel Panorama si ce n'est déjà fait.

Dans la console Web vCloud Air, sélectionnez le **Virtual Machines (Machines virtuelles)** onglet, sélectionnez la machine virtuelle Panorama, puis cliquez sur **Power On (Allumer)**.

Vous êtes maintenant prêt à effectuer la configuration initiale de l'appareil virtuel Panorama.

Prise en charge des outils VMware sur l'appareil virtuel Panorama

VMware Tools est livré avec l'image logicielle pour l'appareil virtuel Panorama. Le support pour VMware Tools vous permet d'utiliser l'environnement vSphere (vCloud Director et vCenter Server) pour ce qui suit :

- Affichez l'adresse IP attribuée à l'interface de gestion de Panorama.
- Affichez les mesures d'utilisation des ressources sur le disque dur, la mémoire et le processeur. Vous pouvez utiliser ces métriques pour activer des alarmes ou des actions sur le serveur vCenter ou le directeur vCloud.
- Arrêt gracieux et redémarrage de Panorama à l'aide de la fonction de mise hors tension sur le serveur vCenter ou Directeur vCloud.
- Active un mécanisme de pulsation entre le serveur vCenter et Panorama pour vérifier que le panorama fonctionne, ou si le pare-feu/Panorama est redémarré. Si le pare-feu passe en mode maintenance, les pulsations sont désactivées de sorte que le serveur vCenter ne ferme pas le pare-feu. Désactiver les pulsations permet au pare-feu de rester opérationnel en mode maintenance lorsqu'il ne peut pas envoyer de pulsations au serveur vCenter.

Installer Panorama sur AWS

Vous pouvez maintenant déployer Panorama ™ et un collecteur de journaux dédié sur Amazon Web Services (AWS). Vous devez apporter votre propre licence (BYOL) pour déployer Panorama sur AWS, celui-ci prend en charge tous les modes de déploiement (Panorama, Collecteur de journaux et Gestion uniquement) et partage les mêmes processus et fonctionnalités que les appareils matériels de la série M. Pour plus de détails sur les modes Panorama, voir Modèles de Panorama .

STEP 1 | Connectez-vous à AWS Web Service Console et sélectionnez le tableau de bord EC2.

- Amazon Web Service Console
- AWS GovCloud Web Service Console

STEP 2 | Configurez le VPC en fonction de vos besoins réseau.

Que vous lanciez l'appareil virtuel Panorama dans un VPC existant ou que vous créiez un nouveau VPC, l'appareil virtuel Panorama doit pouvoir recevoir le trafic des instances EC2 et effectuer des communications entrantes et sortantes entre le VPC et Internet.

Reportez-vous à la documentation d'AWS VPC pour obtenir des instructions sur la création d'un VPC et sur sa configuration pour l'accès.

© 2020 Palo Alto Networks, Inc.

1. Créez un nouveau VPC ou utilisez un VPC existant. Reportez-vous à la documentation d'AWS sur le Démarrage.
2. Vérifiez que les composants réseau et de sécurité sont définis de manière appropriée.
   - Activez la communication avec Internet. Le VPC par défaut inclut une passerelle Internet et, si vous installez le dispositif virtuel Panorama dans le sous-réseau par défaut, le VPC peut accéder à Internet.
   - Créez des sous-réseaux. Les sous-réseaux sont des segments de la plage d'adresses IP affectée au VPC dans lequel vous lancez les instances EC2. L'appareil virtuel Panorama doit appartenir au sous-réseau public afin que vous puissiez le configurer pour accéder à Internet.
   - Si nécessaire, créez des groupes de sécurité pour gérer le trafic entrant et sortant des instances EC2/sous-réseaux.
   - Ajoutez des itinéraires à la table de routage pour un sous-réseau privé pour vous assurer que vous pouvez acheminer le trafic peut être routé entre des sous-réseaux et des groupes de sécurité dans le VPC, le cas échéant.

STEP 3 | Déployez Panorama sur Amazon Web Services.

1. Sur le tableau de bord EC2, cliquez sur **Instances (Instances)** > **Launch Instance (Lancer l'instance)**.
2. Sélectionnez **AWS Marketplace**, recherchez **`Palo Alto Networks Panorama`**, puis **Select (Sélectionnez)** l'AMI Panorama et **Continue (Continuez)**.
3. Choisissez le **EC2 instance type (Type d'instance EC2)** pour allouer les ressources nécessaires à l'appareil virtuel Panorama, puis cliquez sur **Next: Configure Instance Details (Suivant : Configurez les détails de l'instance)**. Passez en revue la section Définir la configuration requise pour l'appareil virtuel Panorama pour connaître les exigences en matière de ressources.

   Si vous prévoyez d'utiliser l'appareil virtuel Panorama en tant que collecteur de journaux dédié, assurez-vous de configurer l'appareil de sorte qu'il dispose des ressources requises lors du déploiement initial. Un appareil virtuel Panorama en mode Collecteur de journaux ne reste pas en mode Collecteur de journaux si vous dimensionnez à nouveau la machine virtuelle après son déploiement, et que cela peut entraîner une perte de données de journal.
4. Configurez les détails de l'instance.
   1. Sélectionnez **Next: Configure Instance Details (Suivant : Configurez les détails de l'instance)**.
   2. Sélectionnez le **Network (réseau)** que vous avez créé à l'étape précédente ou utilisez le VPC par défaut fourni par AWS. Si
   3. Sélectionnez le **Subnet (sous-réseau)** que vous avez créé à l'étape précédente ou utilisez les sous-réseaux par défaut fournis par AWS.
   4. Pour **Auto-assign Public IP (attribuer automatiquement l'adresse IP publique)**, sélectionnez **Enable (Activer).**

      Cette adresse IP doit être accessible aux pare-feux que vous envisagez de gérer à l'aide de Panorama. Cela vous permet d'obtenir une adresse IP accessible au public pour l'interface de gestion de l'appareil virtuel Panorama. Vous pouvez lier une adresse IP élastique à l'interface de gestion ultérieurement. Contrairement à l'adresse IP publique qui est dissociée du pare-feu lorsque l'instance est fermée, l'adresse IP élastique est persistante et peut être reliée à une nouvelle instance (ou de remplacement) de l'appareil Panorama virtuel sans devoir reconfigurer l'adresse IP si vous devez y faire référence, chaque fois que l'instance de l'appareil virtuel Panorama est éteinte.
   5. Configurez les détails supplémentaires de l'instance, le cas échéant.
5. Configurez la taille de stockage de l'appareil virtuel Panorama.
   1. Sélectionnez **Next: Add Storage (Suivant : Ajouter du stockage)**.

© 2020 Palo Alto Networks, Inc.

2. Vérifiez la taille du disque racine du système et déterminez si vous devez passer à un disque système de 224 Go. Augmentez la **taille** du disque système à 224 Go, le cas échéant.

   Pour prendre en charge de grands ensembles de données, un disque système de 224 Go est nécessaireGérer les déploiements de pare-feu à grande échelle afin de disposer d'un espace disque suffisant pour des éléments tels que les mises à jour dynamiques.

   (SD-WAN uniquement) Un disque système de 224 Go permet d'augmenter le stockage des données de surveillance et de rapport sur l'état du pare-feu géré si vous avez l'intention d'utiliser l'appareil virtuel Panorama en mode Panorama pour gérer votre déploiement SD-WAN.

   Si vous déployez une instance d'appareil virtuel Panorama avec un disque système de 224 Go, vous ne pourrez pas migrer vers un disque système plus petit à l'avenir.
3. **Add New Volume (Ajoutez un nouveau volume)** pour ajouter un stockage supplémentaire de journaux.

   (SD-WAN uniquement) Si vous prévoyez de gérer votre déploiement SD-WAN en mode Gestion uniquement, vous devez ajouter un disque de journalisation de 2 To.

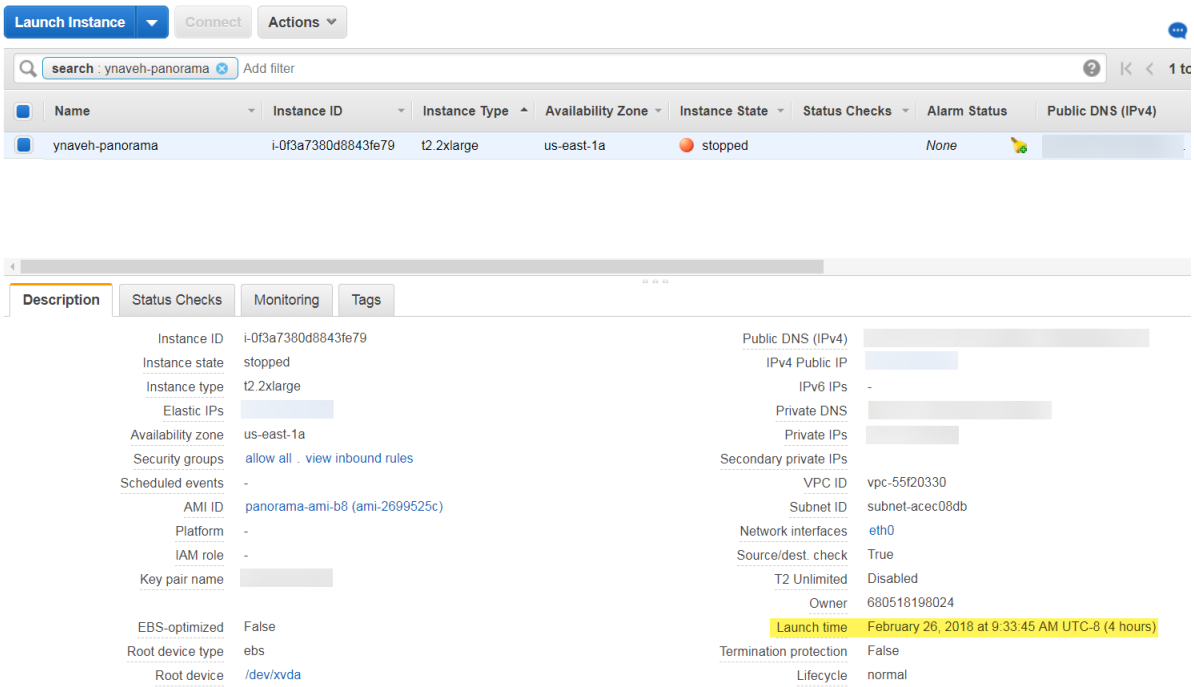
   Si vous envisagez d'utiliser l'appareil Panorama virtuel en mode Panorama ou en tant que collecteur de journaux dédié, ajoutez les disques d'enregistrement virtuels lors du déploiement initial. Par défaut, l'appareil Panorama virtuel est en mode Panorama pour le déploiement initial lorsque vous répondez aux besoins en ressources du mode Panorama et que vous avez ajouté au moins un disque de journalisation virtuel. Sinon, l'appareil virtuel Panorama utilise par défaut le mode gestion uniquement. Modifiez l'appareil virtuel Panorama en mode gestion uniquement si vous souhaitez uniquement gérer les périphériques et les collecteurs de journaux dédiés et ne pas collecter les journaux localement.

   L'appareil virtuel Panorama sur AWS prend uniquement en charge les disques de journalisation 2 To et prend en charge jusqu'à 24 To de stockage de journaux. Vous ne pouvez pas ajouter un disque de journalisation inférieur à 2 To ou un disque de journalisation dont la taille ne peut être divisée par 2 To (exigence applicable au disque de journalisation). L'appareil virtuel Panorama partitionne les disques de plus de 2 To dans des partitions de 2 To.
6. (Facultatif) Sélectionnez **Next: Add Tags (Suivant : ajouter des étiquettes)** et ajoutez une ou plusieurs étiquettes en tant que métadonnées pour vous aider à identifier et à regrouper l'appareil virtuel Panorama. Par exemple, ajouter une balise **Name (nom)** avec une **Value (valeur)** qui vous aide à identifier les pare-feu gérés par l'appareil virtuel Panorama.
7. Configurez le groupe de sécurité de l'instance.
   1. Sélectionnez **Next: Configure Security Group (Suivant: configurer le groupe de sécurité)**.
   2. Créez un nouveau **Security Group (Groupe de sécurité)** ou sélectionnez-en un existant dont HTTPS et SSH est activé au minimum. Ce groupe de sécurité vise à limiter l'accès à l'interface de gestion.
8. **Review and Launch (Vérifiez et lancez)** l'instance de l'appareil virtuel Panorama et assurez-vous que vos sélections sont correctes avant le **Launch (Lancement)**.
9. Sélectionnez une paire de clés existante ou créez-en une, et acceptez l'avis de non-responsabilité.

   Si vous créez une nouvelle clé depuis AWS, téléchargez et sauvegardez la clé dans un endroit sécurisé. L'extension du fichier est `.pem`. Vous devez charger la clé publique dans PuTTYgen et l'enregistrer au format `.ppk`. Vous ne pouvez pas régénérer cette clé en cas de perte.

   Le déploiement de l'appareil virtuel Panorama prend environ 30 minutes après son lancement sur AWS. Le déploiement de l'appareil virtuel Panorama peut prendre plus de temps en fonction du nombre et de la taille des disques attachés à l'instance. Affichez l'heure de lancement en sélectionnant l'instance de l'appareil virtuel Panorama (**Instances**).

© 2020 Palo Alto Networks, Inc.



Si vous prévoyez d'utiliser l'appareil virtuel Panorama en tant que collecteur de journaux dédié, assurez-vous qu'il dispose des ressources requises. Un appareil virtuel Panorama en mode Collecteur de journaux ne reste pas en mode Collecteur de journaux si vous dimensionnez à nouveau la machine virtuelle après son déploiement, et que cela peut entraîner une perte de données de journal.

STEP 4 | Éteignez l'appareil virtuel Panorama.

1. Sur le tableau de bord EC2, sélectionnez **Instances**.
2. Sélectionnez l'appareil virtuel Panorama et cliquez sur **Actions** > **Instance State (État de l'instance)** > **Stop (Arrêter)**.

STEP 5 | Créez une adresse IP élastique (EIP) ou attribuez-en une à l'interface de gestion.

1. Dans la console AWS, sélectionnez **Elastic IPs (IP élastiques)** et **Allocate New Address (Allouer une nouvelle adresse)**.
2. Cliquez sur **Allocate (Allouer)** pour générer une nouvelle adresse EIP, cliquez sur **Actions** et **Associate address (Associez une adresse)**.
3. Sélectionnez **Instance**, sélectionnez l'instance de l'appareil virtuel Panorama à laquelle attribuer l'adresse EIP et entrez la **Private IP address (Adresse IP privée)** associée à l'interface de gestion, puis cliquez sur **Associate (Associer)**.

STEP 6 | Mettez l'appareil virtuel Panorama sous tension.

1. Sur le tableau de bord EC2, sélectionnez **Instance**.
2. À partir de la liste, sélectionnez l'appareil virtuel Panorama et cliquez sur **Actions** > **Instance State (État de l'instance)** > **Start (Démarrer)**.

STEP 7 | Configurez un nouveau mot de passe administratif pour l'appareil virtuel Panorama.

Vous devez configurer un mot de passe d'administration unique avant de pouvoir accéder à l'interface Web de l'appareil virtuel Panorama. Pour accéder à l'interface de ligne de commande, la clé privée utilisée pour lancer l'appareil virtuel Panorama est requise.

© 2020 Palo Alto Networks, Inc.

- Si vous avez un service SSH installé sur votre ordinateur :

1. Entrez la commande suivante pour vous connecter à l'appareil virtuel Panorama :

```
ssh -i <private_key.ppk> admin@<adresse-ip-publique>
```

2. Configurez un nouveau mot de passe en utilisant les commandes suivantes et suivez les instructions à l'écran :

```
admin> configure
admin# set mgt-config users admin password
```

3. Si vous devez activer un BYOL, définissez l'adresse IP du serveur DNS afin que l'appareil virtuel Panorama puisse accéder au serveur de licences Palo Alto Networks. Saisissez la commande suivante pour établir l'adresse IP du serveur DNS :

```
admin# set deviceconfig system dns-setting servers primary <ip_address>
```

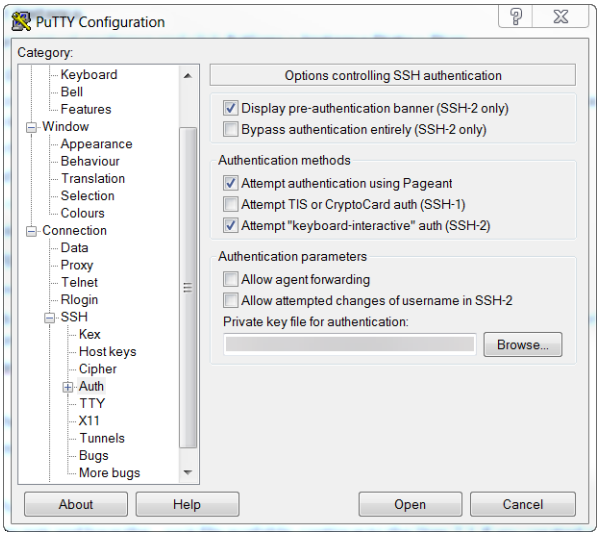
4. Validez vos modifications à l'aide de la commande suivante :

```
admin# commit
```

5. Fermez la session SSH.

- Si vous utilisez PuTTY vers SSH dans le dispositif virtuel Panorama :

1. Si vous utilisez une paire de clés existante et que le fichier `.ppk` est disponible, passez à l'étape 7.3. Si vous avez créé une nouvelle paire de clés ou avez uniquement le fichier `.pem`de la paire de clés existante, ouvrez PuTTYgen et **chargez** le fichier `.pem`.
2. **Save the private key (Enregistrez la clé privée)** dans une destination accessible localement.
3. Ouvrez PuTTY et sélectionnez **SSH** > **Auth** et **Browse (Naviguez)** pour aller chercher le fichier `.ppk` de l'étape suivante.



4. Sélectionnez **Sessions** et entrez l'adresse IP publique de l'appareil virtuel Panorama. Cliquez sur **Open (Ouvrez)** et cliquez sur **Yes (Oui)** quand le certificat de sécurité apparaitra.
5. Connectez-vous en tant qu'administrateur.
6. Configurez un nouveau mot de passe à l'aide de la commande suivante, et suivez les invites affichées à l'écran :

© 2020 Palo Alto Networks, Inc.

```
admin> configure
admin# set mgt-config users admin password
```

7. Définissez l'adresse IP du serveur DNS afin que l'appareil virtuel Panorama puisse accéder au serveur de licences Palo Alto Networks. Saisissez la commande suivante pour établir l'adresse IP du serveur DNS :

```
admin# set deviceconfig system dns-setting servers primary <ip_address>
```

8. Validez vos modifications à l'aide de la commande suivante :

```
admin# commit
```

9. Fermez la session SSH.

STEP 8 | Activez la licence de gestion de périphérique et la licence de support sur l'appareil virtuel Panorama.

- Activer / Récupérer une licence de gestion de pare-feu lorsque l'appareil virtuel Panorama est connectée à Internet.
- Activer / Récupérer une licence de gestion de pare-feu lorsque l'appareil virtuel Panorama n'est pas connecté à Internet
- Activer une licence d'assistance Panorama

STEP 9 | Terminez la configuration de l'appareil virtuel Panorama pour vos besoins de déploiement.

- (Mode gestion uniquement) Configurez un appareil virtuel Panorama en mode Gestion uniquement.
- (Mode Collecteur de journaux) Commencez à l'étape 6 pour passer du mode Panorama au mode collecteur de journaux.

  Entrez l'adresse IP publique du collecteur de journaux dédié lorsque vous ajoutez le collecteur de journaux en tant que collecteur géré au serveur de gestion Panorama. Vous ne pouvez spécifier la IP Address (address (Adresse IP), le Netmask (masque de réseau) ou la Gateway (passerelle).

- (Mode Panorama et gestion uniquement) Configurer un collecteur géré pour ajouter un collecteur de journaux dédié à l'appareil virtuel Panorama. Le mode Gestion uniquement ne prend pas en charge la collecte de journaux locaux et nécessite un collecteur de journaux dédié pour stocker les journaux de périphériques gérés.

Installer Panorama sur AWS GovCloud

Vous pouvez maintenant déployer Panorama ™ et un collecteur de journaux dédié sur Amazon Web Services (AWS) GovCloud. AWS GovCloud est une région AWS isolée qui satisfait aux exigences réglementaires et de conformité des agences gouvernementales et des clients des États-Unis. Vous devez apporter votre propre licence (BYOL) pour déployer Panorama sur AWS GovCloud, celui-ci prend en charge tous les modes de déploiement (Panorama, Collecteur de journaux et Gestion uniquement). Pour plus de détails sur les modes Panorama, voir la section Modèles Panorama.

Pour sécuriser vos charges de travail qui contiennent toutes les catégories de données d'informations contrôlées non classées (Controlled Unclassified Information ; CUI) et de données orientées gouvernement disponibles au public dans la région AWS GovCloud (US), l'appareil virtuel Panorama offre les mêmes fonctionnalités de sécurité robustes dans le cloud public AWS standard et sur AWS GovCloud. L'appareil virtuel Panorama sur AWS GovCloud et sur le cloud public AWS standard prend en charge les mêmes fonctions et fonctionnalités.

© 2020 Palo Alto Networks, Inc.

Passez en revue la section Définir la configuration requise pour l'appareil virtuel Panorama pour voir les types d'instance EC2 qui sont pris en charge. Lorsque vous êtes prêt, consultez la section Installer Panorama sur AWS pour installer l'appareil virtuel Panorama sur AWS GovCloud.

Consultez les procédures suivantes pour ajouter du stockage de journalisation supplémentaire à votre appareil virtuel Panorama ou pour accroître la mémoire et les cœurs alloués :

- Ajoutez un disque virtuel à Panorama sur AWS
- Augmenter les processeurs et la mémoire pour Panorama sur AWS

Installer Panorama sur Azure

Vous pouvez maintenant déployer Panorama ™ et un collecteur de journaux dédié sur Microsoft Azure. Vous devez apporter votre propre licence (BYOL) pour déployer Panorama sur Azure, celui-ci prend en charge tous les modes de déploiement (Panorama, Collecteur de journaux et Gestion uniquement) et partage les mêmes processus et fonctionnalités que les appareils matériels de la série M. Pour plus de détails sur les modes Panorama, voir Modèles de Panorama .

STEP 1 | Connectez-vous au Portail de Microsoft Azure.

STEP 2 | Redémarrez l'appareil virtuel Panorama.

1. Dans le tableau de bord de Azure, sélectionnez **Virtual machines (Machine virtuelles)** et **Add (Ajouter)** une nouvelle machine virtuelle.
2. Recherchez Palo Alto Networks et sélectionnez la dernière image de l'appareil virtuel Panorama.
3. **Create (Créez)** l'appareil virtuel Panorama.

STEP 3 | Configurez l'appareil virtuel Panorama.

1. Sélectionnez votre **Subscription (Abonnement)** Azure.
2. Sélectionnez le **Resource Group (Groupe de ressources)** Azure pour contenir toutes les ressources de votre instance Azure.
3. Donnez un **Virtual machine name (Nom à l'appareil virtuel)** à l'appareil virtuel Panorama.
4. Sélectionnez la **Region (Région)** dans laquelle l'appareil virtuel Panorama doit être déployé.
5. (Facultatif) Sélectionnez les **Availability options (Options de disponibilité)**. Pour plus de renseignements, reportez-vous à la section Comment utiliser un groupe à haute disponibilité.
6. Sélectionnez l'**Image** utilisée pour déployer le serveur de gestion Panorama. **Parcourez toutes les images publiques et privées** pour déployer le serveur de gestion Panorama à partir de l'image Panorama sur Azure marketplace.
7. Configurez la taille de l'appareil virtuel Panorama. Passez en revue la section Définir la configuration requise pour l'appareil virtuel Panorama pour connaître les exigences en matière de taille.

   Si vous prévoyez d'utiliser l'appareil virtuel Panorama en tant que collecteur de journaux dédié, assurez-vous de configurer l'appareil de sorte qu'il dispose des ressources requises lors du déploiement initial. Un appareil virtuel Panorama en mode Collecteur de journaux ne reste pas en mode Collecteur de journaux si vous dimensionnez à nouveau la machine virtuelle après son déploiement, et que cela peut entraîner une perte de données de journal.
8. Saisissez un **Username (Nom d'utilisateur)** pour l'administrateur de l'appareil virtuel Panorama. Dans le but d'assurer la sécurité du système, le nom d'utilisateur admin n'est pas valide.
9. Saisissez un **Password (Mot de passe)** ou effectuez un copier-coller d'une **SSH public key (clé publique SSH)** pour la sécurisation de l'accès admin à l'appareil virtuel Panorama

   Vous devez activer l'authentification par clé SSH si vous prévoyez d'utiliser cette installation de l'appareil virtuel Panorama en mode opérationnel FIPS-CC. Bien que vous puissiez déployer l'appareil virtuel Panorama en utilisant un nom d'utilisateur et

© 2020 Palo Alto Networks, Inc.

un mot de passe, vous ne pourrez pas vous authentifier en utilisant le nom d'utilisateur et le mot de passe après avoir modifié le mode opérationnel en FIPS-CC. Après être passé en mode FIPS-CC, vous devez utiliser la clé SSH pour vous connecter et pouvoir ensuite configurer un nom d'utilisateur et un mot de passe que vous pourrez utiliser pour une connexion ultérieure à l'interface web de Panorama. Pour plus de détails sur la création de la clé SSH, reportez-vous à la Azure documentation (documentation d'Azure).

10. Configurez l'instance de l'appareil virtuel Panorama **Networking (Mise en réseau)**.
    1. Sélectionnez un **Virtual network (réseau virtuel)** existant ou créez un nouveau réseau virtuel.
    2. Configurez un **Subnet (Sous-réseau)**. Le sous-réseau dépend du réseau virtuel que vous avez sélectionné ou créé à l'étape précédente. Si vous avez sélectionné un réseau virtuel existant, vous pouvez choisir l'un des sous-réseaux pour le réseau virtuel sélectionné.
    3. Sélectionnez un **Security Group (Groupe de sécurité)** existant ou créez-en un nouveau. Vous créez ainsi l'interface de gestion utilisée pour accéder à votre appareil virtuel Panorama.
    4. Sélectionnez un **NIC Network Security Group (Groupe de sécurité réseau NIC)** existant ou créez-en un nouveau. Les groupes de sécurité réseau contrôlent le trafic vers la machine virtuelle. Assurez-vous que HTTPS et SSH sont autorisés pour les règles entrantes.
11. Configurez les paramètres **Management (Gestion)** de l'instance.
    1. Indiquez si vous souhaitez activer le **Auto-shutdown (Arrêt automatique)**. L'arrêt automatique vous permet de configurer une heure d'arrêt automatique de la machine virtuelle dont vous désactivez l'arrêt automatique pour éviter qu'une nouvelle adresse IP publique soit affectée à la machine virtuelle, que les journaux soient supprimés, que les journaux disparaissent ou que vous ne parveniez pas à gérer vos pare-feux lors de l'arrêt de l'appareil virtuel Panorama.
    2. Indiquez si vous souhaitez activer la **Monitoring (Surveillance)** au démarrage. Sélectionnez le compte de stockage diagnostic s'il est activé. Le système de surveillance envoie automatiquement les journaux de diagnostic de démarrage à votre Compte de stockage diagnostics. Pour plus d'informations, voir Vue d'ensemble de la surveillance dans Microsoft Azure.
    3. Si nécessaire, configurez d'autres paramètres.
12. Vérifiez le résumé, acceptez les termes et conditions d'utilisation et la politique de confidentialité, puis cliquez sur **Create (Créer)** pour l'appareil virtuel Panorama.

STEP 4 | Vérifiez que l'appareil virtuel Panorama a été déployé avec succès.

1. Sélectionnez **Dashboard (Tableau de bord)** > **Resource Groups (Groupes de ressources)** et sélectionnez le groupe de ressources auquel appartient l'appareil Panorama virtuel.
2. Dans paramètres, sélectionnez **Deployments (Déploiements)** pour l'état de déploiement de la machine virtuelle.

Le déploiement de l'appareil virtuel Panorama prend environ 30 minutes. Le lancement de l'appareil virtuel Panorama peut prendre plus de temps en fonction des ressources configurées pour la machine virtuelle. Microsoft Azure n'autorise pas le protocole ICMP à tester s'il a été déployé avec succès.

Si vous envisagez d'utiliser l'appareil virtuel Panorama en tant que collecteur de journaux dédié, vérifiez que vous avez correctement configuré l'appareil avec les ressources requises. Un appareil virtuel Panorama en mode Collecteur de journaux ne reste pas en mode Collecteur de journaux si vous dimensionnez à nouveau la machine virtuelle après son déploiement, et que cela peut entraîner une perte de données de journal.

STEP 5 | Configurez une adresse IP publique statique.

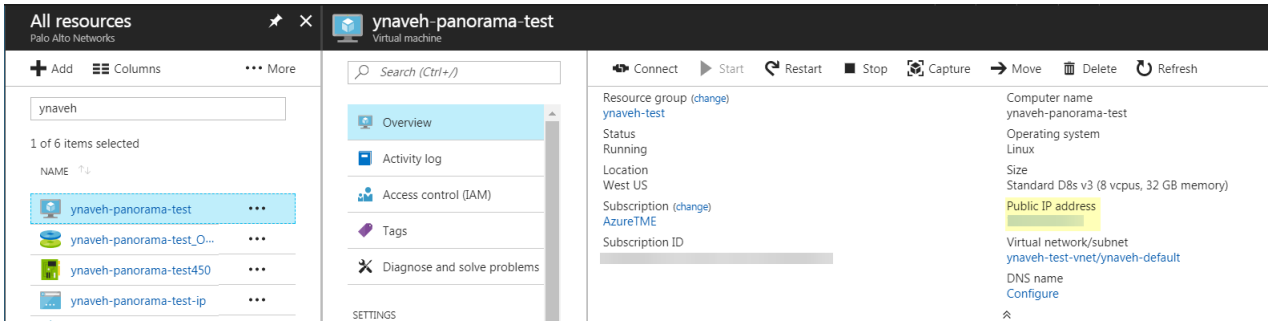
1. Dans le portail Azure, sélectionnez **Virtual Machines (Machines virtuelles)** et sélectionnez la machine virtuelle Panorama.

© 2020 Palo Alto Networks, Inc.

2. Selectionnez **Overview (Vue d'ensemble)** et cliquez sur **Public IP address (Adresse IP publique**.
3. Sous Affectation, sélectionnez **Static (Statique)** et **Save (Sauvegardez)** la nouvelle adresse IP configurée.

STEP 6 | Connectez-vous à l'interface Web du de l'appareil virtuel Panorama.

1. Sur le portail Azure, dans **All Resources (Toutes les ressources)**, sélectionnez l'appareil virtuel Panorama et affichez l'adresse IP publique située dans la section Présentation.



2. Utilisez une connexion sécurisée (https) depuis votre navigateur Web pour vous connecter à l'appareil virtuel Panorama à l'aide de l'adresse IP publique.
3. Entrez le nom d'utilisateur et le mot de passe de l'appareil virtuel Panorama Vous serez invité à accepter un certificat d'avertissement. Acceptez le certificat et continuez vers la page Web.

STEP 7 | Activez la licence de gestion de périphérique et la licence de support sur l'appareil virtuel Panorama.

- Activer / Récupérer une licence de gestion de pare-feu lorsque l'appareil virtuel Panorama est connectée à Internet.
- Activer / Récupérer une licence de gestion de pare-feu lorsque l'appareil virtuel Panorama n'est pas connecté à Internet
- Activer une licence d'assistance Panorama

STEP 8 | Terminez la configuration de l'appareil virtuel Panorama pour vos besoins de déploiement.

(SD-WAN uniquement) Si vous prévoyez de gérer votre déploiement SD-WAN en mode Gestion uniquement, vous devez ajouter un disque de journalisation de 2 To.

1. Ajoutez un disque virtuel à Panorama sur vCloud Air. Par défaut, le disque système 81 Go est créé automatiquement lors du déploiement initial.

   L'ajout d'un disque de journalisation virtuel est requis avant de pouvoir basculer l'appareil virtuel Panorama en mode Panorama ou en mode collecteur de journaux

   Par défaut, l'appareil virtuel Panorama sur Azure est en mode Gestion uniquement lors du déploiement initial. Si vous envisagez d'utiliser l'appareil Panorama virtuel en mode Panorama ou en tant que collecteur de journaux dédié, ajoutez les disques d'enregistrement virtuels après avoir déployé Panorama sur Azure.

   L'appareil virtuel Panorama sur Azure prend uniquement en charge les disques de journalisation 2 To et prend en charge jusqu'à 24 To de stockage de journaux. Vous ne pouvez pas ajouter un disque de journalisation inférieur à 2 To ou un disque de journalisation dont la taille ne peut être divisée par 2 To (exigence applicable au disque de journalisation). L'appareil virtuel Panorama partitionne les disques de plus de 2 To dans des partitions de 2 To.
2. Configurez le mode de l'appareil virtuel Panorama.

   Par défaut, l'appareil virtuel Panorama sur Azure est déployé en mode Gestion uniquement. Pour passer en mode Panorama ou en mode Collecteur de journaux, vous devez ajouter au moins un disque de journalisation après le déploiement initial. Modifiez l'appareil virtuel Panorama en mode

© 2020 Palo Alto Networks, Inc.

gestion uniquement si vous souhaitez uniquement gérer les périphériques et les collecteurs de journaux dédiés et ne pas collecter les journaux localement.

- Configurez un appareil virtuel Panorama en mode Panorama.
- (Mode Collecteur de journaux) Commencez à l'étape 6 pour passer du mode Panorama au mode collecteur de journaux.



Entrez l'adresse IP publique du collecteur de journaux dédié lorsque vous ajoutez le collecteur de journaux en tant que collecteur géré au serveur de gestion Panorama. Vous ne pouvez spécifier la IP Address (address (Adresse IP), le Netmask (masque de réseau) ou la Gateway (passerelle).

3. (Mode Panorama et gestion uniquement) Configurez un collecteur géré pour ajouter un collecteur de journaux dédié à l'appareil virtuel Panorama. Le mode Gestion uniquement ne prend pas en charge la collecte de journaux locaux et nécessite un collecteur de journaux dédié pour stocker les journaux de périphériques gérés.

Installer Panorama sur la plateforme Google Cloud

Vous pouvez maintenant déployer Panorama ™ et un collecteur de journaux dédié sur Google Cloud Platform (GCP). Vous devez apporter votre propre licence (BYOL) pour déployer Panorama sur GCP, celui-ci prend en charge tous les modes de déploiement (Panorama, Collecteur de journaux et Gestion uniquement) et partage les mêmes processus et fonctionnalités que les appareils matériels de la série M. Pour plus de détails sur les modes Panorama, voir Modèles de Panorama .

Pour déployer l'appareil virtuel Panorama sur GCP, vous devez créer une image personnalisée. Pour lancer ce processus, vous devez télécharger le fichier `tar.gz` de Panorama depuis le portail de support client Palo Alto Networks et le charger sur le compartiment de stockage de GCP. Vous pouvez ensuite créer l'image personnalisée et utiliser cette dernière pour déployer l'appareil virtuel Panorama sur GCP.

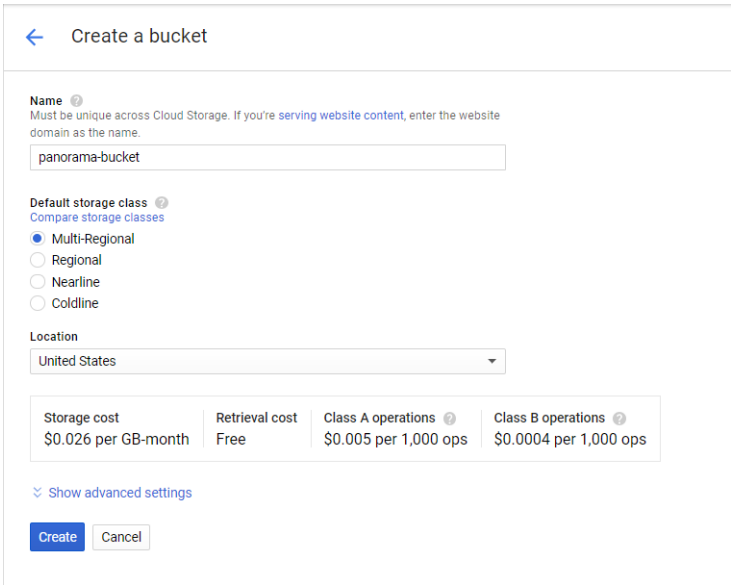
STEP 1 | Téléchargez l'image de l'appareil virtuel Panorama.

1. Connectez-vous au portail de support de Palo Alto Networks.
2. Sélectionnez **Updates (Mises à jour)** > **Software Updates (Mises à jour logicielles)**, puis filtrez selon les **Panorama Base Images (Images de la base de Panorama)**.
3. Téléchargez la dernière version de l'image `tar.gz` de Panorama sur GCP.

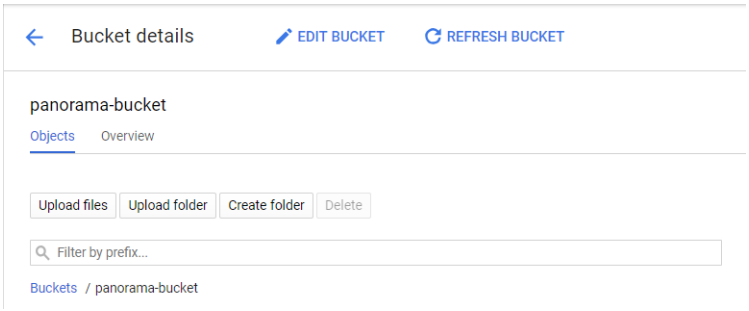
STEP 2 | Chargez l'image de l'appareil virtuel Panorama sur la plateforme Google Cloud.

1. Connectez-vous à Google Cloud Console.
2. Dans le menu **Products and Services (Produits et services)**, choisissez **Storage (Stockage)**.
3. Cliquez sur **Create Bucket (Créer un compartiment)**, configurez le nouveau compartiment de stockage, puis cliquez sur **Create (Créer)**.

© 2020 Palo Alto Networks, Inc.

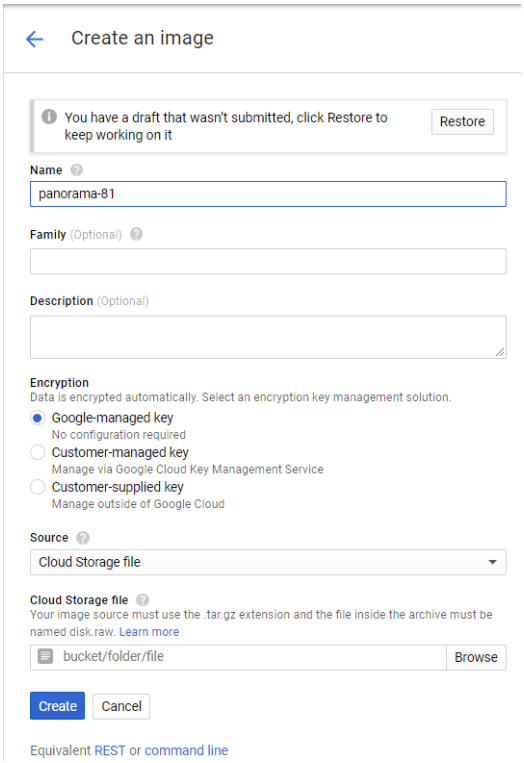


4. Sélectionnez le compartiment de stockage que vous avez créé à l'étape précédente, cliquez sur **Upload files (Charger les fichiers)**, puis sélectionnez l'image de l'appareil virtuel Panorama que vous avez téléchargée.



5. Dans le menu **Products and Services (Produits et services)**, sélectionnez **Compute Engine (Moteur de calcul)** > **Images**.
6. Cliquez sur **Create Image (Créer une image)**, et créez l'image de l'appareil virtuel Panorama :
    1. **Name (Nommez)** l'image de l'appareil virtuel Panorama.
    2. Dans le champ **Source**, sélectionnez le **Cloud Storage file (Fichier de stockage sur le nuage)** dans le menu déroulant.
    3. Cliquez sur **Browse (Parcourir)** et accédez au compartiment de stockage où vous avez chargé l'image de l'appareil virtuel Panorama, puis **Select (Sélectionnez)** l'image chargée.
    4. **Create (Créez)** l'image de l'appareil virtuel Panorama.

© 2020 Palo Alto Networks, Inc.



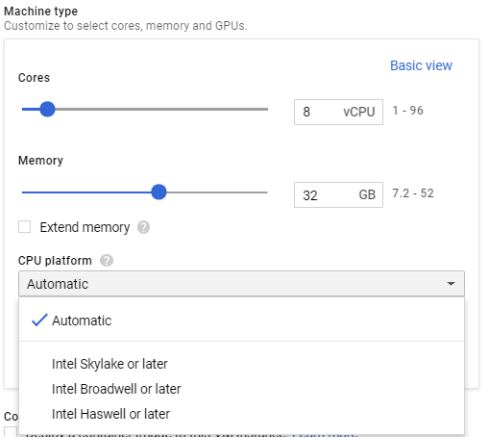
STEP 3 | Configurez l'appareil virtuel Panorama.

1. Dans le menu **Products and Services (Produits et services)**, sélectionnez le **Compute Engine (Moteur de calcul)**.
2. Cliquez sur **Create Instance (Créer une instance)** pour commencer le déploiement d'un appareil virtuel Panorama.
3. Ajoutez un **Name (Nom)** descriptif pour identifier facilement l'appareil virtuel Panorama.
4. Sélectionnez la **Region (Région)** et la **Zone** où vous voulez déployer l'appareil virtuel Panorama.
5. Allouer le **Machine Type (Type de machine)** et **Customize (Personnalisez)** les cœurs, la mémoire et la plateforme du processeur. Passez en revue la section Définir la configuration requise pour l'appareil virtuel Panorama pour connaître les exigences minimales en matière de ressources.

Si vous prévoyez d'utiliser l'appareil virtuel Panorama en tant que collecteur de journaux dédié, assurez-vous de configurer l'appareil de sorte qu'il dispose des ressources requises lors du déploiement initial. Un appareil virtuel Panorama en mode Collecteur de journaux ne reste pas en mode Collecteur de journaux si vous dimensionnez à nouveau la machine virtuelle après son déploiement, et que cela peut entraîner une perte de données de journal.

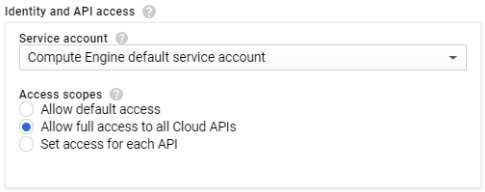
La sélection de la zone de GCP détermine les plateformes du processeur qui sont mises à votre disposition. Pour de plus amples renseignements, veuillez vous reporter à la section Régions et zones.

© 2020 Palo Alto Networks, Inc.

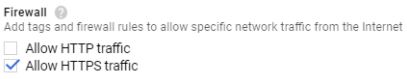


6. Configurer le disque de démarrage de Panorama.
   1. Sous **Boot Disk (Disque de démarrage)**, cliquez sur **Change (Modifier)** > **Custom image (Image personnalisée)**, et sélectionnez l'image de Panorama que vous avez chargée à l'étape 2.
   2. Configurez la taille du disque de démarrage. Par défaut, le disque système est de 81 Go, mais vous pouvez augmenter la taille du disque système à 224 Go.

      (SD-WAN uniquement) Si vous prévoyez de gérer votre déploiement SD-WAN en utilisant cet appareil virtuel Panorama en mode Panorama, vous devez augmenter la taille du disque système à 224 Go. Si vous prévoyez de gérer votre déploiement SD-WAN en mode Gestion uniquement, vous devez ajouter un disque de journalisation de 2 To.
   3. Cliquez sur **Select (Sélectionner)** pour enregistrer votre configuration.
7. Sous **Identity and API access (Identité et accès API)**, sélectionnez **Allow full access to all Cloud APIs (Autoriser un accès complet à toutes les API Cloud)**.



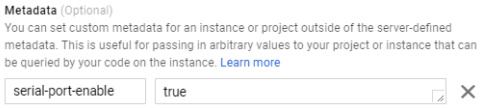
8. Sous **Firewall (pare-feu)**, sélectionnez **Allow HTTPS traffic (Autoriser le trafic HTTPS)**.



STEP 4 | Développez **Management, security, disks, networking, sole tenancy (Gestion, sécurité, disques, réseautage, location unique)** Management, security, disks, networking, sole tenancy .

STEP 5 | Activez l'accès au port série pour pouvoir gérer l'appareil virtuel Panorama.
1. Sélectionnez **Management (Gestion)**.
2. Entrez la paire nom-valeur suivante en tant que métadonnées :

   `serial-port-enable true`



STEP 6 | Réservez une adresse IP à affecter à l'interface de gestion.

© 2020 Palo Alto Networks, Inc.

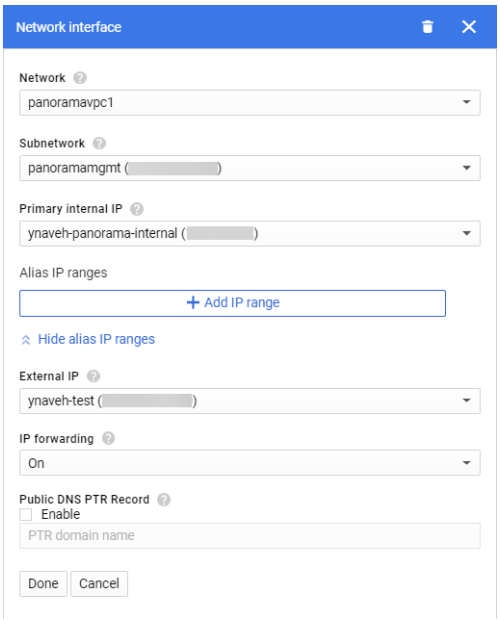
Réservez des adresses IP internes et externes statiques à affecter à l'interface de gestion pour que si l'appareil virtuel Panorama est redémarré, vos périphériques gérés ne perdent pas leur connexion à l'appareil virtuel Panorama lors de la réaffectation des adresses IP.

Pour plus de renseignements sur la manière de réserver des adresses IP, reportez-vous aux sections Réservation d'une adresse IP interne statique et Réservation d'une adresse UP externe statique.

1. Sélectionnez **Networking (Mise en réseau)**.
2. **Edit (Modifiez)** l'interface réseau.



3. Sélectionnez le **Network (réseau)** de l'appareil virtuel Panorama.
4. Sélectionnez le **Subnetwork (sous-rréseau)** de l'appareil virtuel Panorama. Les instances du même sous-réseau communiquent entre elles en utilisant leurs adresses IP internes.
5. Définissez l'adresse **Primary internal IP (IP interne principale)**.
   - **Ephemeral (Automatic) (Ephémère (Automatique))** : Affecte automatiquement une adresse IP interne principale.
   - **Ephemeral (Custom) (Ephémère (Personnalisé))** : Configure une plage IP personnalisée utilisée par GCP pour attribuer une adresse IP interne principale.
   - **Reserve a static internal IP address (Réserver une adresse IP interne statique)** : configurez manuellement une adresse IP interne principale statique.
6. Définissez l'adresse **External IP (IP externe)**.
   - **Ephemeral (Éphémère)** : attribue automatiquement une adresse IP externe à partir d'un pool IP partagé.
   - Sélectionnez une adresse IP externe existante.
   - **Create IP address (Créer une adresse IP)** : réservez une adresse IP externe.
7. Définissez l'adresse **IP forwarding (IP de redirection IP)** sur **On (Activer)** pour permettre à l'appareil virtuel Panorama de recevoir des paquets provenant ou d'adresses IP source ou de destination non correspondantes.

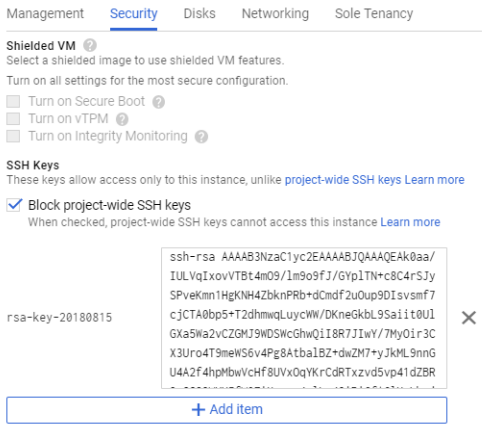


© 2020 Palo Alto Networks, Inc.

STEP 7 | Configurez la clé SSH. Vous devez disposer d'une clé SSH pour accéder à la CLI de l'appareil virtuel Panorama afin de configurer le mot de passe de l'administrateur après le déploiement initial.

1. Sélectionnez **Security (Sécurité)**.
2. Cochez la case **Block project-wide SSH keys (Bloquer les clés SSH à l'échelle du projet)**. Seules les clés de l'instance sont actuellement prises en charge pour la connexion à l'appareil virtuel Panorama après le déploiement initial.
3. Collez la clé SSH dans la boîte de commentaire. Pour plus d'informations sur le format de clé SSH correct et comment générer des clés SSH pour GCP, reportez-vous à la section Gestion des clés SSH dans les métadonnées.

Lors de la génération de la clé SSH, enregistrez la clé privée au format .ppk. La clé privée est requise pour se connecter à l'appareil virtuel Panorama après le déploiement initial avant de pouvoir configurer le mot de passe d'administration.



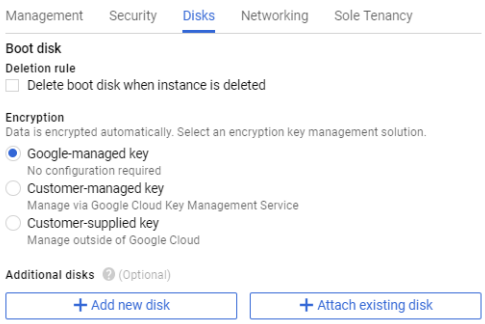
STEP 8 | (Mode Panorama et collecteur de journaux) Ajoutez du stockage supplémentaire pour la collecte de journaux. Répétez cette étape si nécessaire pour ajouter des disques de journalisation virtuels supplémentaires.

Si vous envisagez d'utiliser l'appareil Panorama virtuel en mode Panorama ou en tant que collecteur de journaux dédié, ajoutez les disques d'enregistrement virtuels lors du déploiement initial. Par défaut, l'appareil Panorama virtuel est en mode Panorama pour le déploiement initial lorsque vous répondez aux besoins en ressources du mode Panorama et que vous avez ajouté au moins un disque de journalisation virtuel. Autrement, l'appareil virtuel Panorama revient par défaut au mode Gestion uniquement, à partir duquel vous pouvez gérer les périphériques et les collecteurs de journaux dédiés et ne pouvez pas collecter les journaux localement.

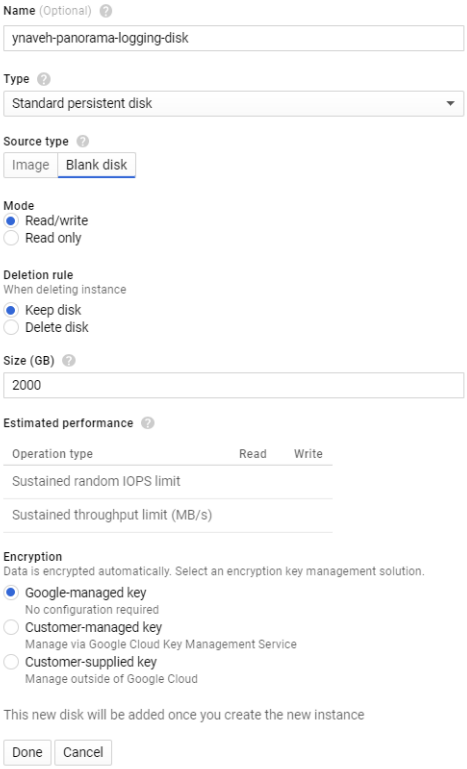
L'appareil virtuel Panorama sur GCP prend uniquement en charge les disques de journalisation 2 To et prend en charge jusqu'à 24 To de stockage de journaux. Vous ne pouvez pas ajouter un disque de journalisation inférieur à 2 To ou un disque de journalisation dont la taille ne peut être divisée par 2 To (exigence applicable au disque de journalisation). L'appareil virtuel Panorama partitionne les disques de plus de 2 To dans des partitions de 2 To.

1. Sélectionnez **Disks (Disques)** > **Add new disk (Ajouter le nouveau disque)**.

© 2020 Palo Alto Networks, Inc.



2. Saisissez un **Name (Nom)**.
3. Développez le menu déroulant **Type** et sélectionnez le type souhaité.
4. Sous **Source type (Type de source)**, sélectionnez **Blank disk Disque vide)**.
5. Sous **Mode**, sélectionnez **Read/write (Lecture/écriture)**.
6. Sélectionnez la **Deletion rule (Règle de suppression)** afin de préciser si le disque de journalisation virtuel doit être supprimé lors de la suppression de l'instance de l'appareil virtuel Panorama. A
7. Définissez la **Size (GB) (Taille (Go))** du disque de journalisation virtuel.
8. Définissez votre solution de **Encryption (Déchiffrement)** privilégiée des données contenues sur le disque de journalisation virtuel.
9. Cliquez sur **Terminé**.



STEP 9 | **Create (Créez)** l'appareil virtuel Panorama. L'amorçage des appareils virtuels Panorama prend environ 10 minutes après leur déploiement initial.

STEP 10 | Configurez un nouveau mot de passe administratif pour l'appareil virtuel Panorama.

© 2020 Palo Alto Networks, Inc.

Vous devez configurer un mot de passe d'administration unique avant de pouvoir accéder à l'interface Web de l'appareil virtuel Panorama. Pour accéder à l'interface CLI, utilisez la clé privée pour lancer l'appareil virtuel Panorama.

- Si vous avez un service SSH installé sur votre ordinateur :

1. Entrez la commande suivante pour vous connecter à l'appareil virtuel Panorama :

```
ssh -i <private_key.ppk> admin@<adresse-ip-publique>
```

2. Configurez un nouveau mot de passe à l'aide de la commande suivante, et suivez les invites affichées à l'écran :

```
admin> configure
admin# set mgt-config users admin password
```

3. Si vous avez besoin d'un BYOL, définissez l'adresse IP du serveur DNS afin que l'appareil Panorama puisse accéder au serveur de licences Palo Alto Networks. Saisissez la commande suivante pour établir l'adresse IP du serveur DNS :

```
admin# set deviceconfig system dns-setting servers primary <ip_address>
```

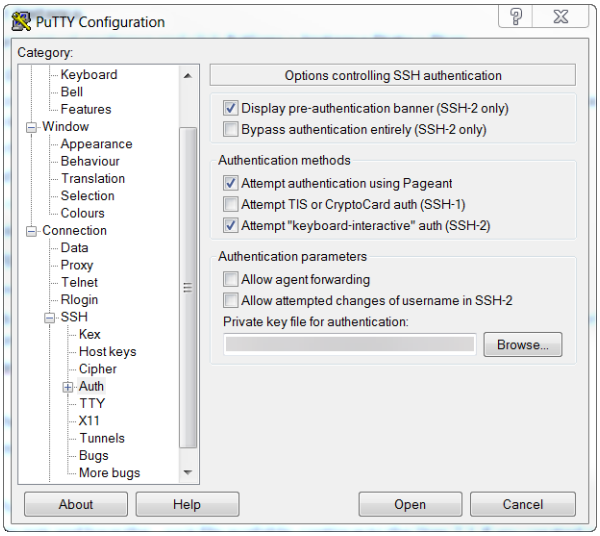
4. Validez vos modifications :

```
admin# commit
```

5. Fermez la session SSH.

- Si vous utilisez PuTTY vers SSH dans le dispositif virtuel Panorama :

1. Si vous utilisez une paire de clés existante et que le fichier `.ppk` est disponible, passez à l'étape 11.3. Si vous avez créé une nouvelle paire de clés ou avez uniquement le fichier `.pem`de la paire de clés existante, ouvrez PuTTYgen et **Load (Chargez)** le fichier `.pem`.
2. **Save the private key (Enregistrez la clé privée)** dans une destination accessible localement.
3. Ouvrez PuTTY et sélectionnez **SSH** > **Auth** et **Browse (Naviguez)** pour aller chercher le fichier `.ppk` de l'étape suivante.



4. Sélectionnez **Sessions** et entrez l'adresse IP publique de l'appareil virtuel Panorama. Cliquez ensuite sur **Open (Ouvrez)** et cliquez sur **Yes (Oui)** quand le certificat de sécurité apparaîtra.
5. Accédez en tant qu'administrateur.

© 2020 Palo Alto Networks, Inc.

6. Configurez un nouveau mot de passe en utilisant les commandes suivantes et suivez les instructions à l'écran :

```
admin> configure
admin# set mgt-config users admin password
```

7. Définissez l'adresse IP du serveur DNS afin que l'appareil virtuel Panorama puisse accéder au serveur de licences Palo Alto Networks. Saisissez la commande suivante pour établir l'adresse IP du serveur DNS :

```
admin# set deviceconfig system dns-setting servers primary <ip_address>
```

8. Validez vos modifications à l'aide de la commande suivante :

```
admin# commit
```

9. Fermez la session SSH.

STEP 11 | Activez la licence de gestion de périphérique et la licence de support sur l'appareil virtuel Panorama.

- Activer / Récupérer une licence de gestion de pare-feu lorsque l'appareil virtuel Panorama est connectée à Internet.
- Activer / Récupérer une licence de gestion de pare-feu lorsque l'appareil virtuel Panorama n'est pas connecté à Internet
- Activer une licence d'assistance Panorama

STEP 12 | Terminez la configuration de l'appareil virtuel Panorama pour vos besoins de déploiement.

- (Mode gestion uniquement) Configurez un appareil virtuel Panorama en mode Gestion uniquement.
- (Mode Collecteur de journaux) Commencez à l'étape 6 pour passer du mode Panorama au mode collecteur de journaux.

  Entrez l'adresse IP publique du collecteur de journaux dédié lorsque vous ajoutez le collecteur de journaux en tant que collecteur géré au serveur de gestion Panorama. Vous ne pouvez spécifier la IP Address (address (Adresse IP), le Netmask (masque de réseau) ou la Gateway (passerelle).

- (Mode Panorama et gestion uniquement) Configurer un collecteur géré pour ajouter un collecteur de journaux dédié à l'appareil virtuel Panorama. Le mode Gestion uniquement ne prend pas en charge la collecte de journaux locaux et nécessite un collecteur de journaux dédié pour stocker les journaux de périphériques gérés.

Installer Panorama sur KVM

Vous pouvez maintenant déployer Panorama ™ et un collecteur de journaux dédié sur Microsoft Azure. Vous devez apporter votre propre licence (BYOL) pour déployer Panorama sur KVM, celui-ci prend en charge tous les modes de déploiement (Panorama, Collecteur de journaux et Gestion uniquement) et partage les mêmes processus et fonctionnalités que les appareils matériels de la série M. Pour plus de détails sur les modes Panorama, voir Modèles de Panorama .

STEP 1 | Téléchargez l'image de l'appareil virtuel Panorama pour KVM.

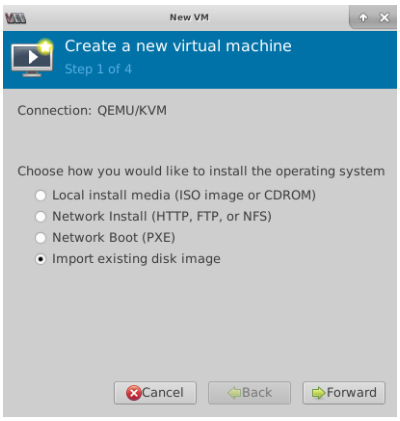
1. Connectez-vous au portail de support de Palo Alto Networks.
2. Sélectionnez **Software Updates (mises à jour logicielles)** et trouvez l'image de base de Panorama pour KVM.

© 2020 Palo Alto Networks, Inc.

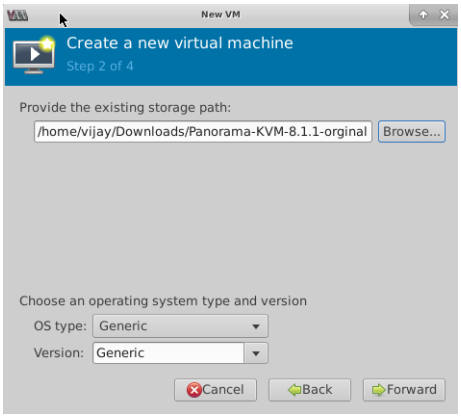
3. Téléchargez le dernier fichier .qcow2 disponible de Panorama.

STEP 2 | Créez une nouvelle image de machine virtuelle et ajoutez l'image de l'appareil virtuel Panorama pour KVM au gestionnaire de machine virtuelle.

1. Sur le gestionnaire de machine virtuelle, sélectionnez **Create a new virtual machine (Créer une nouvelle machine virtuelle)**.
2. Sélectionnez **Import Existing disk image (importation d'une image disque)** et cliquez sur **Forward (suivant)**.



3. **Browse (naviguez)** et sélectionnez le volume image de l'appareil virtuel Panorama et **Choose volume (choisissez le volume)**.
4. Cliquez sur **Forward (suivant)**.



STEP 3 | Configurez les paramètres de la mémoire et du processeur.

Passez en revue la section Définir la configuration requise pour l'appareil virtuel Panorama pour connaître les exigences minimales en matière de ressources.

Si vous prévoyez d'utiliser l'appareil virtuel Panorama en tant que collecteur de journaux dédié, assurez-vous de configurer l'appareil de sorte qu'il dispose des ressources requises lors du déploiement initial. Un appareil virtuel Panorama en mode Collecteur de journaux ne reste pas en mode Collecteur de journaux si vous dimensionnez à nouveau la machine virtuelle après son déploiement, et que cela peut entraîner une perte de données de journal.

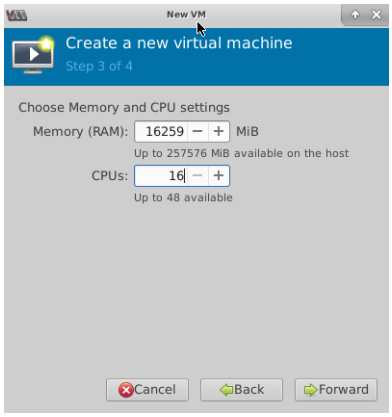
1. Configurez la **Memory (Mémoire)** selon les exigences du mode opérationnel désiré.

Le gestionnaire de machine virtuelle peut utiliser MiB (mebibyte) pour allouer de la mémoire en fonction de la version que vous utilisez. Si MiB est utilisé, assurez-

© 2020 Palo Alto Networks, Inc.

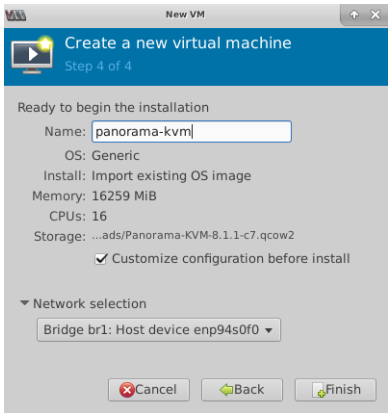
vous de convertir correctement l'allocation de mémoire requise pour éviter un sous approvisionnement de l'appareil virtuel Panorama.

2. Configurez le **CPU (Processeur)** selon les exigences du mode opérationnel désiré.
3. Cliquez sur **Forward (suivant)**.



STEP 4 | Nommez l'appareil virtuel Panorama, activez la personnalisation de la configuration et sélectionnez le pont de l'interface de gestion.

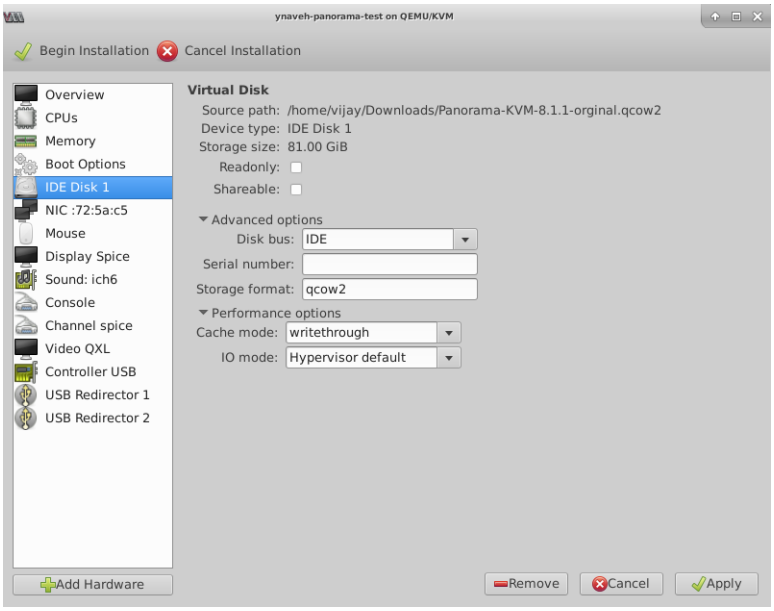
1. Donnez un **Name (Nom)** descriptif à l'appareil virtuel Panorama.
2. **Customize configuration before install (Personnalisez la configuration avant l'installation)**.
3. Faites une **Network Selection (Sélection réseau)** : sélectionnez le pont pour l'interface de gestion et acceptez les valeurs par défaut.
4. Cliquez sur **Finish (Terminer)**.



STEP 5 | Configurez les paramètres du disque virtuel.

1. Sélectionnez **IDE Disk 1**, cliquez sur **Advanced options (Options avancées)**, et sélectionnez l'option suivante :
   - **Disk Bus (Bus de disque)**—**VirtIO** ou **IDE**, selon votre configuration.
   - **Storage format (Format de stockage)**—**qcow2**
2. Cliquez sur **Performance options (Option de performance)** et définissez le **Cache mode (Mode cache)** sur **writethrough (double écriture)**. Ce paramètre réduit la durée d'installation et optimise la vitesse d'exécution sur l'appareil virtuel Panorama.
3. Cliquez sur **Apply (Appliquer)**.

© 2020 Palo Alto Networks, Inc.

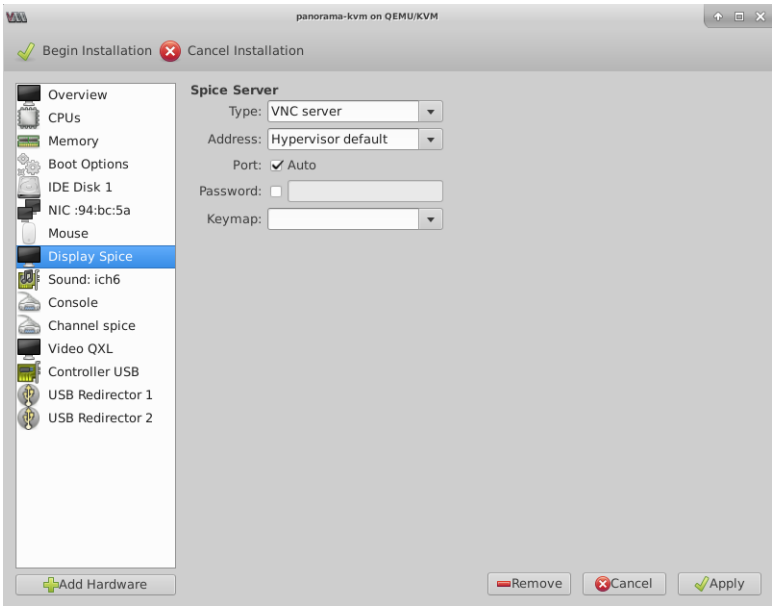


STEP 6 | Configurez la console de machine virtuelle , pour que le serveur VNC pour interagisse avec la machine virtuelle.

1. Sélectionnez **Display Spice (Afficher Spice)**.

   Continuez à la prochaine étape si Display VNC (Afficher VNC) apparaît dans la liste matériel, car la machine virtuelle est déjà configurée pour utiliser le serveur VNC pour l'affichage.

2. Dans la liste déroulante **Type (Type)**, sélectionnez **VNC Server (Serveur VNC)**.
3. Cliquez sur **Apply (Appliquer)**.



STEP 7 | (Mode Panorama et collecteur de journaux) Ajoutez du stockage supplémentaire pour la collecte de journaux. Répétez cette étape si nécessaire pour ajouter des disques de journalisation virtuels supplémentaires.

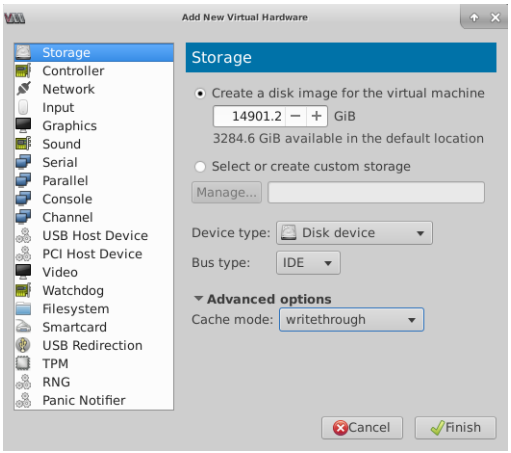
© 2020 Palo Alto Networks, Inc.

Si vous envisagez d'utiliser l'appareil Panorama virtuel en mode Panorama ou en tant que collecteur de journaux dédié, ajoutez les disques d'enregistrement virtuels lors du déploiement initial. Par défaut, l'appareil Panorama virtuel est en mode Panorama pour le déploiement initial lorsque vous répondez aux besoins en ressources du mode Panorama et que vous avez ajouté au moins un disque de journalisation virtuel. Sinon, l'appareil virtuel Panorama utilise par défaut le mode gestion uniquement. Modifiez l'appareil virtuel Panorama en mode gestion uniquement si vous souhaitez uniquement gérer les périphériques et les collecteurs de journaux dédiés et ne pas collecter les journaux localement.

L'appareil virtuel Panorama sur KVM prend uniquement en charge les disques de journalisation 2 To et prend en charge jusqu'à 24 To de stockage de journaux. Vous ne pouvez pas ajouter un disque de journalisation inférieur à 2 To ou un disque de journalisation dont la taille ne peut être divisée par 2 To (exigence applicable au disque de journalisation). L'appareil virtuel Panorama partitionne les disques de plus de 2 To dans des partitions de 2 To.

1. **Add Hardware (Ajoutez le matériel)**.
2. Configurez le nouveau disque de **Storage (stockage)** :
    1. **Create a disk image for a virtual machine (Créez une image disque pour une machine virtuelle)** et configurez la capacité de stockage de disque virtuel sur 14901.2 GiB (équivalent à 2 To).

        Le gestionnaire de machine virtuelle peut utiliser GiB (Gibibyte) pour allouer de la mémoire en fonction de la version que vous utilisez. Si GiB est utilisé, assurez-vous de bien convertir la capacité de stockage requise pour éviter de sous-approvisionner le disque de journalisation virtuel et d'envoyer l'appareil virtuel Panorama en mode maintenance.
    2. Définissez le **Device type (type de périphérique)** sur périphérique **Disk (disque)**.
    3. **Disk Bus (disque bus)** : **VirtIO** ou **IDE**, selon votre configuration.
    4. Cliquez sur **Advanced options (Option avancées)** et définissez le **Cache mode (Mode Cache)** sur **writethrough (double écriture)**.
3. Cliquez sur **Finish (Terminer)**.



STEP 8 | **Begin Installation (Commencez l'installation)** (Begin Installation). L'amorçage des appareils virtuels Panorama prend environ 10 minutes.

STEP 9 | Configurez les paramètres d'accès réseau pour l'interface de gestion.

1. Ouvrez une connexion à la console.
2. Connectez-vous au pare-feu en utilisant le nom d'utilisateur par défaut et le mot de passe (admin / admin).
3. Passez en mode Configuration en utilisant la commande suivante :

© 2020 Palo Alto Networks, Inc.

```
admin> configure
```

4. Utilisez les commandes suivantes pour configurer l'interface de gestion :

```
admin# set deviceconfig system type static
admin# set deviceconfig system ip-address <Panorama-IP> netmask <masque
 réseau> default-gateway <IP de la passerelle> dns-setting servers primary
 <IP DNS>
```

où *<Adresse IP de Panorama>* est l'adresse IP que vous voulez affecter à l'interface de gestion, *<masque réseau>* est le masque de sous-réseau, *<Adresse IP de passerelle>* est l'adresse IP de la passerelle réseau et *<Adresse IP de DNS>* est l'adresse IP du serveur DNS.

```
admin# commit
```

STEP 10 | Activez la licence de gestion de périphérique et la licence de support sur l'appareil virtuel Panorama.

- Activer / Récupérer une licence de gestion de pare-feu lorsque l'appareil virtuel Panorama est connectée à Internet.
- Activer / Récupérer une licence de gestion de pare-feu lorsque l'appareil virtuel Panorama n'est pas connecté à Internet
- Activer une licence d'assistance Panorama

STEP 11 | Terminez la configuration de l'appareil virtuel Panorama pour vos besoins de déploiement.

- (Mode gestion uniquement) Configurez un appareil virtuel Panorama en mode Gestion uniquement.
- (Mode Collecteur de journaux) Commencez à l'étape 6 pour passer du mode Panorama au mode collecteur de journaux.

  Entrez l'adresse IP publique du collecteur de journaux dédié lorsque vous ajoutez le collecteur de journaux en tant que collecteur géré au serveur de gestion Panorama. Vous ne pouvez spécifier la IP Address (address (Adresse IP), le Netmask (masque de réseau) ou la Gateway (passerelle).
- (Mode Panorama et gestion uniquement) Configurer un collecteur géré pour ajouter un collecteur de journaux dédié à l'appareil virtuel Panorama. Le mode Gestion uniquement ne prend pas en charge la collecte de journaux locaux et nécessite un collecteur de journaux dédié pour stocker les journaux de périphériques gérés.

Installer Panorama sur Hyper-V

Vous pouvez maintenant déployer Panorama ™ et un collecteur de journaux dédié sur Hyper-V. Vous devez apporter votre propre licence (BYOL) pour déployer Panorama sur Hyper-V, celui-ci prend en charge tous les modes de déploiement (Panorama, Collecteur de journaux et Gestion uniquement) et partage les mêmes processus et fonctionnalités que les appareils matériels de la série M. Pour plus de détails sur les modes Panorama, voir Modèles de Panorama . L'appareil virtuel Panorama et le collecteur de journaux dédié virtuel sur Hyper-V est disponible uniquement sur PAN-OS 8.1.3 et les versions ultérieures.

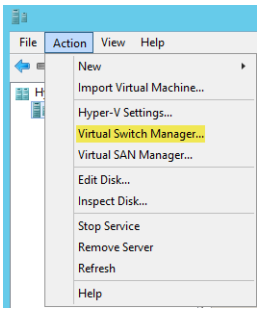
STEP 1 | Téléchargez le fichier VHAX.

1. Connectez-vous au portail de support de Palo Alto Networks.
2. Sélectionnez **Updates (Mises à jour)** > **Software Updates (Mises à jour logicielles)**, filtrez selon les **Panorama Base Images (Images de la base Panorama)**, puis téléchargez le fichier VHDX.

© 2020 Palo Alto Networks, Inc.

STEP 2 | Configurez tous les vSwitch nécessaires. Pour obtenir de plus amples renseignements, passez en revue les types de commutateurs virtuels.

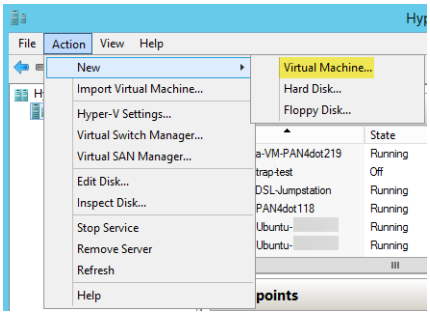
1. Dans Hyper-V Manager, sélectionnez l'hôte et sélectionnez **Action** > **Virtual Switch Manager (Gestionnaire de commutateur virtuel)** pour ouvrir la fenêtre Gestionnaire de commutateur virtuel.



2. Dans **Create virtual switch (Créer un commutateur virtuel)**, sélectionnez le type de vSwitch à créer et cliquez sur **Create Virtual Switch (Créer un commutateur virtuel)**.

STEP 3 | Installez l'appareil virtuel Panorama

1. Sur Hyper-V Manager, sélectionnez l'hôte et sélectionnez **Action** > **New (Nouveau)** > **Virtual Machine (Machine virtuelle).** Configurez les paramètres suivants dans l'assistant de nouvelle machine virtuelle :



1. Choisissez un **Name (Nom)** et un **Location (Emplacement)** pour l'appareil virtuel Panorama. L'appareil virtuel Panorama stocke le fichier VHDX à l'emplacement spécifié.
2. Choisissez **Generation 1 (Génération 1)**. Il s'agit de l'option par défaut et de la seule version prise en charge.
3. Sous **Startup Memory (Mémoire au démarrage)**, allouez la mémoire selon le mode système visé. Consultez la rubrique Définir la configuration requise pour l'appareil virtuel Panorama pour connaître les exigences en matière de mémoire pour chaque mode.

   N'activez pas la mémoire dynamique ; l'appareil virtuel Panorama exige une allocation de mémoire statique.
4. Configurez le **Networking (Réseau)**. Sélectionnez un vSwitch externe pour connecter l'interface de gestion sur le pare-feu.
5. Pour connecter le **Virtual Hard Disk (Disque dur virtuel)**, sélectionnez **Use an existing virtual hard disk (Utiliser un disque dur virtuel existant)** et recherchez le fichier VHAX que vous avez téléchargé au préalable.
6. Examinez le récapitulatif et cliquez sur **Finish (Terminer)**.

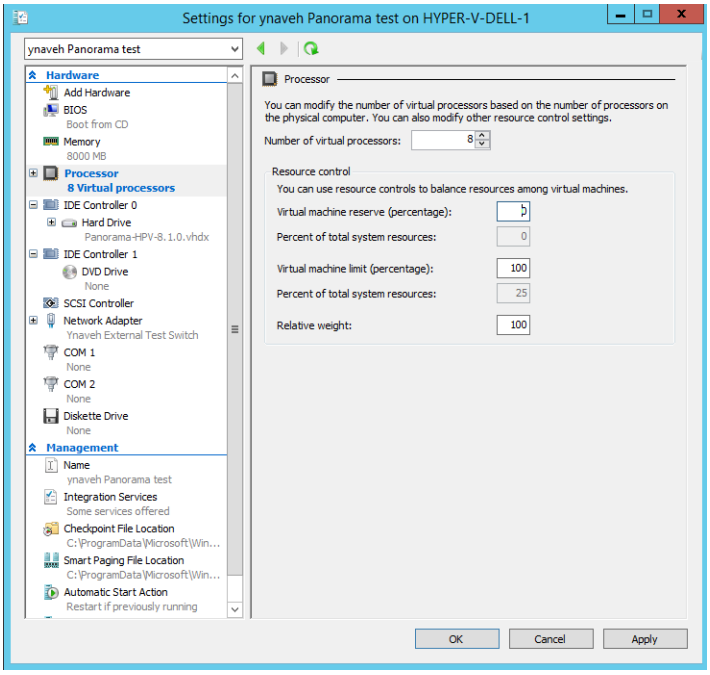
STEP 4 | Allouez les cœurs du processeur à l'appareil virtuel Panorama.

Passez en revue la section Définir la configuration requise pour l'appareil virtuel Panorama pour connaître les exigences minimales en matière de ressources.

© 2020 Palo Alto Networks, Inc.

Si vous prévoyez d'utiliser l'appareil virtuel Panorama en tant que collecteur de journaux dédié, assurez-vous de configurer l'appareil de sorte qu'il dispose des ressources requises lors du déploiement initial. Un appareil virtuel Panorama en mode Collecteur de journaux ne reste pas en mode Collecteur de journaux si vous dimensionnez à nouveau la machine virtuelle après son déploiement, et que cela peut entraîner une perte de données de journal.

1. Dans la liste **Hardware (Matériel)**, sélectionnez **Processor (Processus)**.
2. Modifiez le **Number of virtual processors (Nombre de processus virtuels)** actuellement alloués.



STEP 5 | Connectez au moins une carte réseau pour l'interface du plan de données sur le pare-feu. Répétez cette étape pour créer les interfaces réseau supplémentaires sur l'appareil virtuel Panorama.

1. Sélectionnez **Settings (Paramètres)** > **Hardware (Matériel)** > **Add Hardware (Ajouter du matériel)** et sélectionnez le **Hardware type (Type de matériel)** pour votre carte réseau.

   Carte réseau héritée et SR-IOV ne sont pas pris en charge. Si ces options sont sélectionnées, le pare-feu redémarrera en mode maintenance.

2. Cliquez sur **OK**.

STEP 6 | (Mode Panorama et collecteur de journaux) Ajoutez du stockage supplémentaire pour la collecte de journaux. Répétez cette étape si nécessaire pour ajouter des disques de journalisation virtuels supplémentaires. Si vous voulez déployer l'appareil virtuel Panorama en mode Gestion uniquement, passez à l'étape 6.

Si vous envisagez d'utiliser l'appareil Panorama virtuel en mode Panorama ou en tant que collecteur de journaux dédié, ajoutez les disques d'enregistrement virtuels lors du déploiement initial. Par défaut, l'appareil Panorama virtuel est en mode Panorama pour le déploiement initial lorsque vous répondez aux besoins en ressources du mode Panorama et que vous avez ajouté au moins un disque de journalisation virtuel. Sinon, l'appareil virtuel Panorama utilise par défaut le mode gestion uniquement. Modifiez l'appareil virtuel Panorama en mode gestion uniquement si vous souhaitez uniquement gérer les périphériques et les collecteurs de journaux dédiés et ne pas collecter les journaux localement.

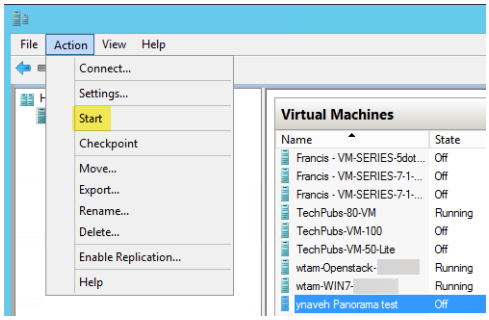
© 2020 Palo Alto Networks, Inc.

L'appareil virtuel Panorama sur Hyper-V prend uniquement en charge les disques de journalisation 2 To et prend en charge jusqu'à 24 To de stockage de journaux. Vous ne pouvez pas ajouter un disque de journalisation inférieur à 2 To ou un disque de journalisation dont la taille ne peut être divisée par 2 To (exigence applicable au disque de journalisation). L'appareil virtuel Panorama partitionne les disques de plus de 2 To dans des partitions de 2 To.

1. Sur Hyper-V Manager, sélectionnez l'hôte et sélectionnez **Action** > **New (Nouveau)** > **Hard Disk (Disque dur).**
2. Si l'invite Before You Begin (Avant de commencer) s'affiche, cliquez sur **Next (Suivant)** pour commencer l'ajout du disque de journalisation virtuel.
3. Comme format de disque, sélectionnez **VHDX**. Cliquez sur **Next (Suivant)** pour continuer.
4. Comme type de disque, sélectionnez **Fixed Size (Taille fixe)** ou **Dynamically Expanding (Augmentant de manière dynamique)**, selon vos besoins. Cliquez sur **Next (Suivant)** pour continuer.
5. Précisez le **Name (Nom)** et le **Location (Emplacement)** du fichier du disque de journalisation virtuel. Cliquez sur **Next (Suivant)** pour continuer.
6. Pour configurer le disque, sélectionnez **Create a new virtual hard disk (Créer un nouveau disque dur virtuel)**, puis saisissez la taille du disque. Cliquez sur **Next (Suivant)** pour continuer.
7. Passez en revue le résumé et **Finish (Terminez)** l'ajout du disque dur de journalisation virtuel.

STEP 7 | Mettez l'appareil virtuel Panorama sous tension.

1. Sélectionnez l'appareil virtuel Panorama dans la liste des **Virtual Machines (Machines virtuelles)**.
2. Sélectionnez **Action** > **Start (Démarrer)** pour allumer l'instance de l'appareil virtuel Panorama.



STEP 8 | Configurez l'adresse IP de l'interface de gestion.

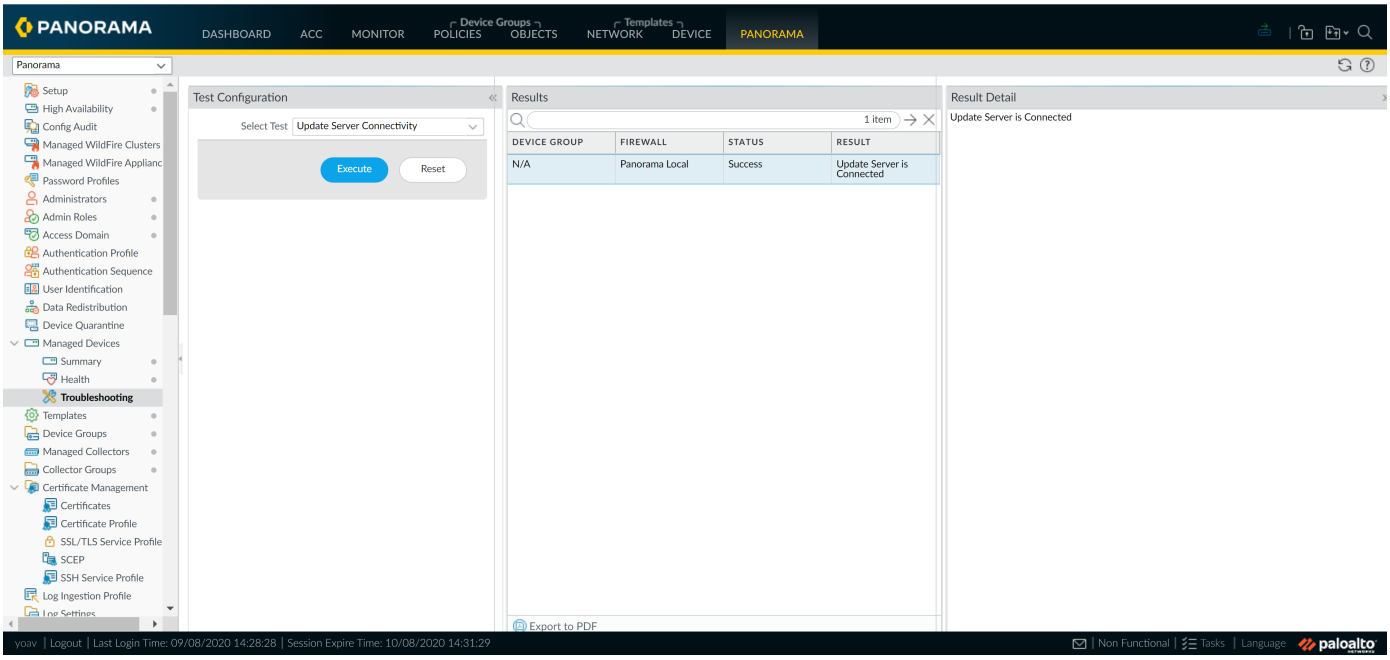
Si vous avez un service DHCP activé sur le réseau de commutateur virtuel, vous pouvez sauter cette étape.

1. Dans la liste de **Virtual Machines (Machines virtuelles)**, sélectionnez l'appareil virtuel Panorama.
2. Sélectionnez **Actions** > **Connect (Se connecter)**, puis entrez le nom d'utilisateur et le mot de passe pour ouvrir une session (par défaut, admin pour les deux).
3. Entrez les commandes suivantes, où *<Panorama IP>* est l'adresse IP que vous souhaitez attribuer à l'interface de gestion Panorama, *<masque réseau>* est le masque de sous-réseau, *<adresse IP de la passerelle>* est l'adresse IP de la passerelle réseau, et *<IP DNS>* est l'adresse IP du serveur DNS :

```
admin> configure
admin# set deviceconfig system ip-address <Panorama-IP> netmask <masque
 réseau> default-gateway <IP de la passerelle> dns-setting servers primary
 <IP DNS>
admin# commit
admin# exit
```

4. Résoudre les problèmes de connectivité aux ressources réseaux pour vérifier l'accès au réseau à des services externes nécessaires à la gestion de pare-feu, comme la passerelle par défaut, serveur DNS et le Serveur de mise à jour Palo Alto Networks, comme le montre l'exemple suivant :

© 2020 Palo Alto Networks, Inc.



STEP 9 | Activez la licence de gestion de périphérique et la licence de support sur l'appareil virtuel Panorama.

- Activer / Récupérer une licence de gestion de pare-feu lorsque l'appareil virtuel Panorama est connectée à Internet.
- Activer / Récupérer une licence de gestion de pare-feu lorsque l'appareil virtuel Panorama n'est pas connecté à Internet
- Activer une licence d'assistance Panorama

STEP 10 | Terminez la configuration de l'appareil virtuel Panorama pour vos besoins de déploiement.

- (Mode gestion uniquement) Configurez un appareil virtuel Panorama en mode Gestion uniquement.
- (Mode Collecteur de journaux) Commencez à l'étape 6 pour passer du mode Panorama au mode collecteur de journaux.

  Entrez l'adresse IP publique du collecteur de journaux dédié lorsque vous ajoutez le collecteur de journaux en tant que collecteur géré au serveur de gestion Panorama. Vous ne pouvez spécifier la IP Address (address (Adresse IP), le Netmask (masque de réseau) ou la Gateway (passerelle).

- (Mode Panorama et gestion uniquement) Configurer un collecteur géré pour ajouter un collecteur de journaux dédié à l'appareil virtuel Panorama. Le mode Gestion uniquement ne prend pas en charge la collecte de journaux locaux et nécessite un collecteur de journaux dédié pour stocker les journaux de périphériques gérés.

Effectuer la configuration initiale de l'appareil virtuel Panorama

Selon votre modèle de Panorama, utilisez l'interface web de AWS, Azure, ou GCP, le gestionnaire de machine virtuelle KVM, le gestionnaire Hyper-V, le client VMware vSphere ou la console Web vCloud Air pour configurer l'accès réseau à l'appareil virtuel Panorama. Par défaut, l'appareil virtuel Panorama sur Azure est déployé en mode Panorama. Pour un reporting unifié, pensez à utiliser Greenwich Mean Time (GMT) ou au temps universel coordonné (TUC) comme fuseau horaire uniforme à travers Panorama et tous les périphériques gérés.

© 2020 Palo Alto Networks, Inc.

STEP 1 | Contactez votre administrateur réseau pour obtenir les informations requises.

Recueillez les informations suivantes pour l'interface de gestion (MGT) :

- ❑ Adresse IP pour l'Interface de gestion (MGT)
- ❑ netmask
- ❑ Passerelle par défaut
- ❑ Adresse IP du serveur DNS



Pour procéder à la configuration de l'interface de gestion, vous devez indiquer l'adresse IP, le masque réseau (pour IPv4) ou la longueur de préfixe (pour IPv6) et la passerelle par défaut. Si vous omettez des paramètres (comme la passerelle par défaut), vous pouvez uniquement accéder à Panorama via le port de la console pour des modifications ultérieures de la configuration. Il est recommandé de toujours valider toujours une configuration complète de l'interface MGT.

STEP 2 | Accédez à la console de l'appareil virtuel Panorama.

1. Accédez à la console.

   Sur un serveur ESXi :

   1. Lancez le client VMware vSphere.
   2. Sélectionnez le **Console** onglet pour l'application virtuelle Panorama et appuyez sur Entrée pour accéder à l'écran de connexion.

   Sur vCloud Air :

   1. Accéder à la console Web vCloud Air et sélectionner votre **Virtual Private Cloud OnDemand (Cloud Virtuel Privé sur Demande)** région.
   2. Sélectionnez l' **Virtual Machines (Machines virtuelles)** onglet, clic-droit sur la machine virtuelle Panorama, et sélectionnez **Open In Console (Ouvrir dans la Console)**.
2. Entrez votre nom d'utilisateur et mot de passe pour ouvrir une session (par défaut, admin pour les deux).

   Sur AWS, Azure, GCP, KVM et Hyper-V :

   - Connectez-vous à l'ILC de Panorama.

STEP 3 | Changer le mot de passe administrateur par défaut.



À partir de PAN-OS 9.0.4, le mot de passe de l'administrateur prédéfini par défaut (admin/admin) doit être modifié lors de la première connexion à l'appareil. Le nouveau mot de passe doit comporter au moins huit caractères et comprendre au moins une lettre minuscule et une lettre majuscule ainsi qu'un chiffre ou un caractère spécial.

Veillez à respecter les bonnes pratiques en matière de robustesse des mots de passe *pour vous assurer de créer un mot de passe fort et de revoir les* paramètres de complexité des mots de passe*.*



Pour garantir que l'interface de gestion reste sécurisée, configurez la complexité minimale de mot de passe (Panorama > Setup (Paramétrage) > Management (Gestion)).

1. Cliquez sur le lien **admin** sur le côté gauche du pied de page de l'interface Web.
2. Entrer l'**Old Password (ancien mot de passe)** et le **New Password (nouveau mot de passe)** et enregistrer le nouveau mot de passe dans un endroit sûr.
3. Cliquez sur **OK**.

© 2020 Palo Alto Networks, Inc.

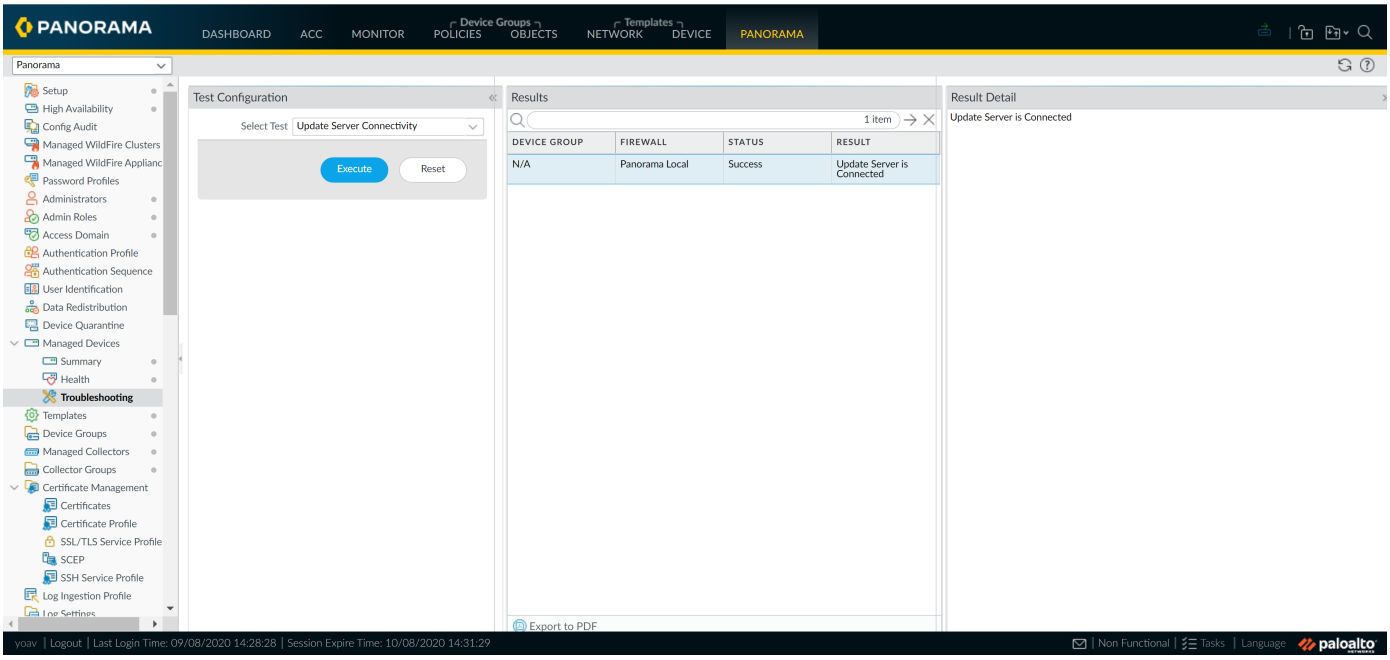
STEP 4 | Configurez les paramètres d'accès réseau pour l'interface MGT.

Panorama utilise l'interface MGT pour le trafic de gestion, la synchronisation de haute disponibilité, la collecte des journaux, et la communication au sein des groupes Collectors.

1. Entrez les commandes suivantes, où *<Panorama IP>* est l'adresse IP que vous souhaitez attribuer à l'interface de gestion Panorama, *<masque réseau>* est le masque de sous-réseau, *<adresse IP de la passerelle>* est l'adresse IP de la passerelle réseau, et *<IP DNS>* est l'adresse IP du serveur DNS :

```
> configure
# set deviceconfig system ip-address <Panorama-IP> netmask <masque réseau>
 default-gateway <IP de la passerelle> dns-setting servers primary <IP
 DNS>
# commit
# exit
```

2. Résoudre les problèmes de connectivité aux ressources réseaux pour vérifier l'accès au réseau à des services externes nécessaires à la gestion de pare-feu, comme la passerelle par défaut, serveur DNS et le Serveur de mise à jour Palo Alto Networks, comme le montre l'exemple suivant :



STEP 5 | Configurez les paramètres généraux.

1. Utiliser une connexion sécurisée (HTTPS) à partir d'un navigateur Web, connectez-vous à l'interface Web Panorama en utilisant l'adresse IP et le mot de passe que vous avez attribué à l'interface de gestion (https : // <adresse IP>).
2. Sélectionnez **Panorama (Panorama)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les Paramètres Généraux.
3. Saisissez un **Hostname (Nom d'hôte)** pour le serveur et entrez le nom de **Domain (Domaine)** du réseau. Le nom de domaine est un simple intitulé ; Panorama ne l'utilise pas pour y accéder.
4. Aligner l'horloge sur Panorama et les pare-feu gérés d'utiliser le même **Time Zone (Fuseau horaire)**, Par exemple GMT ou UTC. Si vous prévoyez d'utiliser Cortex Data Lake, vous devez configurer NTP pour que Panorama puisse rester synchronisé avec Cortex Data Lake.

   Les Timestamps sont enregistrés au moment où Panorama reçoit les journaux et les pare-feu gérés génèrent les journaux. L'alignement des fuseaux horaires sur Panorama et les pare-feu assure que

© 2020 Palo Alto Networks, Inc.

les horodateurs sont synchronisés et le processus d'interrogation des journaux et la génération de rapports sur Panorama est harmonieux.

5. Entrez la **Latitude** et la **Longitude** afin de permettre un positionnement précis du serveur de gestion de Panorama sur la carte du monde.
6. Entrer le **Serial Number (Numéro de série)** vous avez reçu dans l'email de l'exécution des commandes.
7. Cliquez sur **OK** pour enregistrer vos modifications.

STEP 6 | (Facultatif) Modifiez les paramètres de l'interface de gestion.

1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Interfaces** et cliquez sur **Management (Gestion)**.
2. Si votre pare-feu se connecte au serveur de gestion Panorama au moyen d'une adresse IP publique qui est traduite en une adresse IP privée (NAT), saisissez l'adresse IP publique dans le champ **Public IP Address (Adresse IP publique)** et l'adresse IP privée dans le champ **IP Address (Adresse IP)** pour transmettre les deux adresses à vos pare-feu.
3. Sélectionnez les services de connectivité réseau à autoriser sur l'interface (tels que l'accès **SSH**).

   Ne sélectionnez pas Telnet ou HTTP. Ces services utilisent des messages en clair et sont moins sûrs que les autres services.
4. Cliquez sur **OK** pour enregistrer vos modifications d'interface.

STEP 7 | Validez vos modifications de configuration.

Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

STEP 8 | Étapes suivantes...

1. Si nécessaire, augmentez la capacité de stockage de journaux sur l'appareil virtuel Panorama.
2. (Recommandée) Remplacez le certificat par défaut que Panorama utilise pour sécuriser le trafic HTTPS sur l'interface gestion (MGT).
3. Activer une licence d'assistance Panorama.
4. Activer / Récupérer une licence de gestion de pare-feu lorsque l'appareil virtuel Panorama est connectée à Internet.
5. Installer les mises à jour de contenu et logicielles pour Panorama.
6. Configurer l'accès administratif à Panorama

Configurer l'appareil virtuel Panorama en tant que collecteur de journaux local

Si vous souhaitez disposer d'un appareil virtuel dédié pour la collecte de journaux, configurez un appareil virtuel Panorama sur ESXi, AWS, AWS GovCloud, Azure, Google Cloud Platform, KVM ou Hyper-V en mode Collecteur de journaux. Pour ce faire, vous effectuez d'abord la configuration initiale de l'appareil virtuel en mode Panorama, qui comprend les licences, l'installation de logiciels et les mises à jour de contenu, et la configuration de l'interface de gestion (MGT). Vous faites ensuite passer l'appareil virtuel Panorama au mode Collecteurs de journaux et terminez la configuration des Collecteurs de journaux. En outre, si vous souhaitez utiliser des interfaces d'appareils de série M dédiées (recommandé) au lieu de l'interface de gestion pour la collecte de journaux et le groupe de collecteurs, vous devez d'abord configurer les interfaces pour le serveur de gestion Panorama, puis les configurer pour le collecteur de journaux, et effectuer une validation de Panorama suivie d'une validation du groupe de collecteurs.

Effectuez les étapes suivantes pour configurer un nouvel appareil en tant que collecteur de journaux ou pour convertir un appareil existant précédemment déployé en tant que serveur de gestion de Panorama.

© 2020 Palo Alto Networks, Inc.

Le passage de l'appareil virtuel du mode Panorama au mode collecteur de journaux redémarre l'appareil, supprime le collecteur de journaux local, supprime toutes les données existantes du journal et supprime toutes les configurations à l'exception des paramètres d'accès de gestion. La désactivation du mode ne supprime pas les licences, les mises à jour logicielles ou les mises à jour de contenu.

STEP 1 | Configurez le serveur de gestion de l'appareil virtuel Panorama qui gérera le collecteur de journaux si vous ne l'avez déjà fait.

Effectuez l'une des tâches suivantes :

- Configuration de l'appareil virtuel Panorama
- Configuration de l'appareil de série M

STEP 2 | Enregistrez les adresses IP de gestion du serveur de gestion Panorama.

Si vous avez déployé panorama dans une configuration haute disponibilité (HD), vous avez besoin de l'adresse IP de chaque homologue HD.

1. Connectez-vous à l'interface Web du serveur de gestion de Panorama.
2. Enregistrez l'**IP Address (Adresse IP)** du Panorama solitaire (non HD) ou actif (HD) en sélectionnant **Panorama** > **Setup (Configuration)** > **Management (Gestion)** et en vérifiant les paramètres de l'interface de gestion.
3. Pour un déploiement HD, enregistrez la **Peer HD IP Address (Adresse IP de l'homologue HD)** du Panorama passif en sélectionnant **Panorama** > **High Availability (Haute disponibilité)** et en vérifiant la section Setup (Configuration).

STEP 3 | Configurez l'appareil virtuel Panorama qui servira de collecteur de journaux dédié.

Si vous avez précédemment déployé cet appareil en tant que serveur d'administration Panorama, vous pouvez ignorer cette étape car l'interface de gestion est déjà configurée et les licences et mises à jour sont déjà installées.

L'appareil virtuel Panorama en mode Collecteur de journaux ne dispose pas d'une interface Web pour les tâches de configuration, mais uniquement d'une interface de ligne de commande. Par conséquent, avant de modifier le mode sur l'appareil virtuel Panorama, utilisez l'interface Web en mode Panorama pour :

1. Configurer l'appareil virtuel Panorama dans l'un des hyperviseurs pris en charge suivants :
   - Installer Panorama sur un serveur ESXi
   - Installer Panorama sur AWS.
   - Installer Panorama sur AWS GovCloud
   - Installer Panorama sur Azure.
   - Installer Panorama sur Google Cloud Platform.
   - Installer Panorama sur Hyper-V
2. Effectuez la configuration initiale de l'application virtuelle Panorama.
3. Enregistrer Panorama et installer les licences.
4. Installer les mises à jour de contenu et logicielles pour Panorama.

STEP 4 | (Panorama sur Azure seulement) Modifiez le mot de passe administrateur.

Le collecteur de journaux dédié ne prend en charge que l'administrateur utilisateur administrateur pour passer en mode collecteur de journal. Modifiez le mot de passe administrateur pour vous permettre de vous connecter à l'aide de l'administrateur utilisateur administrateur.

1. Connectez-vous à l'interface Web Panorama.
2. Sélectionnez **Panorama** > **Administrators (Administrateurs)** et sélectionnez **admin**.
3. Entrez le **Password (Mot de passe)**, **Confirm Password (Confirmez le mot de passe)** et cliquez sur **OK**.

© 2020 Palo Alto Networks, Inc.

4. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

STEP 5 | (Seulement pour Panorama sur AWS et Azure) Effacez tous les utilisateurs, sauf l'utilisateur administrateur.

1. Connectez-vous à l'interface Web Panorama en tant qu'administrateur.
2. Sélectionnez **Panorama** > **(Administrateurs)**.
3. Sélectionnez les administrateurs existants, sauf admin, et **Delete (Supprimez)**.
4. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

STEP 6 | Connectez-vous à l'ILC de Panorama.

STEP 7 | Passez du mode Panorama au mode collecteur de journaux.

1. Pour passer à une session en mode collecteur de journaux, entrez la commande suivante :

```
> request system system-mode logger
```

2. Entrez **Y** pour confirmer le changement de mode. L'appareil virtuel redémarre. Si le processus de redémarrage met fin à votre session du logiciel d'émulation de terminal, reconnectez-vous à l'appareil virtuel pour afficher l'invite de connexion Panorama.

   *Si vous voyez une invite de **connexion CMS**, cela signifie que le collecteur de journaux n'a pas terminé le redémarrage. Appuyez sur ENTER à l'invite sans taper un nom d'utilisateur ou un mot de passe.*

3. Connectez-vous à l'ILC.
4. Vérifiez que la bascule en mode collecteur de journaux a réussi :

```
> show system info | match system-mode
```

   Si le changement de mode a réussi, la sortie affiche :

```
system-mode: logger
```

STEP 8 | Activer la connectivité entre chaque collecteur de journaux et le serveur de gestion de Panorama.

Saisissez les commandes suivantes dans l'ILC du collecteur de journaux, où *<IPaddress1>* est pour l'interface de gestion du panorama solitaire (non HD) ou actif (HD) et *<IPaddress2>* est pour l'interface de gestion du panorama passif (HD), le cas échéant.

```
> configure
# set deviceconfig system panorama-server <IPaddress1> panorama-server-2
 <IPaddress2>
# commit
# exit
```

STEP 9 | Enregistrez le numéro de série du collecteur de journaux.

Vous avez besoin des numéros de série pour ajouter les collecteurs de journaux en tant que collecteurs gérés sur le serveur de gestion de Panorama.

© 2020 Palo Alto Networks, Inc.

1. Dans l'ILC du collecteur de journaux dédié, saisissez les commandes suivantes pour afficher le numéro de série :

```
> show system info | match serial
```

2. Enregistrez le numéro de série.

STEP 10 | Ajoutez le collecteur de journaux en tant que collecteur géré au serveur de gestion de Panorama.

1. Sélectionnez **Panorama (Panorama)** > **Managed Collectors (Collecteurs gérés)** et **Add (ajoutez)** le collecteur géré.
2. Dans les paramètres **General (Général)**, saisissez le numéro de série (**Collector S/N (N° de série du collecteur)**) que vous avez enregistré pour le collecteur de journaux.
3. Dans le champ **Panorama Server IP (IP du serveur Panorama)** entrez l'adresse IP ou le nom de domaine complet du Panorama solitaire (non-HD) ou primaire (HD). Pour un déploiement HD, entrez l'adresse IP ou le nom de domaine complet de l'homologue secondaire de Panorama dans le champ **Panorama Server IP 2 (Serveur Panorama IP 2)**.

   Ces adresses IP doivent spécifier une interface Panorama sont les services **Device Management and Device Log Collection (Gestion des périphériques et collecte des journaux de périphériques)** sont activés. Par défaut, ces services sont activés uniquement sur l'interface MGT. Toutefois, vous avez peut-être activé les services sur d'autres interfaces lors de l'étape Configurer l'appareil de série M qui est un serveur de gestion Panorama.
4. Sélectionnez **Interfaces**, cliquez sur **Management (Gestion)**, et entrez la **Public IP Address (Adresse publique IP)** du collecteur de journaux dédié.
5. Cliquez deux fois sur **OK** pour enregistrer les modifications au groupe de collecteurs.
6. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos modifications à la configuration Panorama.
7. Vérifiez que la page **Panorama** > **Managed Collectors (Collecteurs gérés)** répertorie le collecteur de journaux que vous avez ajouté. La colonne Connecté affiche une icône de coche pour indiquer que le collecteur de journaux est connecté à Panorama. Vous devrez peut-être attendre quelques minutes avant que la page affiche le statut de connexion actualisée.

   À ce stade, la colonne État de configuration affiche Désynchronisé et la colonne État d'exécution affiche Déconnecté. L'état passera à Synchronisé et Connecté une fois que vous aurez configuré un groupe de collecteurs.

STEP 11 | Activer les disques de journalisation.

1. Sélectionnez **Panorama (Panorama)** > **Managed Collectors (Collecteurs gérés)** et modifiez le collecteur de journaux.
2. Sélectionnez **Disks (Disques)** et **Add (Ajoutez)** chaque disque.
3. Cliquez sur **OK** pour enregistrer vos modifications.
4. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos modifications à la configuration Panorama.

STEP 12 | (Recommandé) Configurez les interfaces **Ethernet1**, **Ethernet2**, **Ethernet3**, **Ethernet4**, et **Ethernet5** si le collecteur de journaux et le serveur de gestion Panorama les utiliseront pour la **Device Log Collection (Collecte de journaux de périphériques)** (réception des journaux des pare-feu) et la **Collector Group Communication (Communication du groupe de collecteurs)**.

Si vous avez précédemment déployé le collecteur de journaux en tant que serveur de gestion Panorama et configuré ces interfaces, vous devez les reconfigurer car le passage en mode collecteur de journaux aurait supprimé toutes les configurations, sauf les paramètres d'accès de gestion.

© 2020 Palo Alto Networks, Inc.

1. Configurez chaque interface sur le serveur de gestion Panorama (autre que l'interface MGT) si vous n'avez pas déjà réalisé les étapes suivantes :
    1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Interfaces** et cliquez sur le nom de l'interface.
    2. Sélectionnez *<interface-name> (nom de l'interface)* pour activer l'interface.
    3. Remplissez un ou les deux des ensembles de champs suivants, selon les protocoles IP de votre réseau :
        - Pour ESXi
            - IPv4 : **Adresse publique IP**, **Adresse IP**, **Masque de réseau**, et **passerelle par défaut**

              IPv6 : **IPv6 Address/Prefix Length (Longueur du préfixe / de l'adresse IPv6)** et **Default IPv6 Gateway (Passerelle IPv6 par défaut)**
        - Pour AWS, Azure, et Google™ Cloud Platform
            - **Adresse IP publique :**
    4. Sélectionnez les services de gestion de périphériques pris en charge par l'interface :

       Device Management and Device Log Collection (Gestion des périphériques et collecte des journaux de périphériques) : vous pouvez assigner une ou plusieurs interfaces.

       Collector Group Communication (Communication du groupe de collecteurs) : vous ne pouvez attribuer qu'une seule interface.

       Device Deployment (Déploiement de périphériques) (mises à jour de logiciels et de contenu) : vous ne pouvez attribuer qu'une seule interface.
    5. Cliquez sur **OK** pour enregistrer vos modifications.
2. Configurez chaque interface sur le collecteur de journaux (autre que l'interface MGT) :
    1. Sélectionnez **Panorama (Panorama)** > **Managed Collectors (Collecteurs gérés)** et modifiez le collecteur de journaux.
    2. Sélectionnez **Interfaces** et cliquez sur le nom de l'interface.
    3. Sélectionnez *<interface-name> (nom de l'interface)* pour activer l'interface.
    4. Remplissez un ou les deux des ensembles de champs suivants, selon les protocoles IP de votre réseau :
        - Pour ESXi
            - IPv4 : **Adresse publique IP**, **Adresse IP**, **Masque de réseau**, et **passerelle par défaut**

              IPv6 : **IPv6 Address/Prefix Length (Longueur du préfixe / de l'adresse IPv6)** et **Default IPv6 Gateway (Passerelle IPv6 par défaut)**
        - Pour AWS et Azure
            - **Adresse IP publique :**
    5. Sélectionnez les services de gestion de périphériques pris en charge par l'interface :

       Device Log Collection (Collecte de journaux de périphériques) : vous pouvez assigner une ou plusieurs interfaces.

       Collector Group Communication (Communication du groupe de collecteurs) : vous ne pouvez attribuer qu'une seule interface.
    6. Cliquez sur **OK** pour enregistrer vos modifications d'interface.
3. Cliquez sur **OK** pour enregistrer les modifications au collecteur de journaux.
4. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos modifications à la configuration Panorama.

STEP 13 | (Facultatif) Si votre déploiement utilise des certificats personnalisés pour l'authentification entre Panorama et les périphériques gérés, déployez le certificat de périphérique client

© 2020 Palo Alto Networks, Inc.

personnalisé. Pour plus d'informations, consultez Configurer l'authentification à l'aide de certificats personnalisés.

1. Sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificat)** et choisissez le profil de certificat dans la liste déroulante ou cliquez sur **New Certificate Profile (Nouveau profil de certificat)** pour en créer un.
2. Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** > **Add (Ajouter)** > **Communication** pour un collecteur de journaux.
3. Cochez la case **Secure Client Communication (Sécurisation des communications avec le client)**.
4. Sélectionnez le type de certificat de périphérique dans la liste déroulante Type.
   - Si vous utilisez un certificat de périphérique local, sélectionnez **Certificate (Certificat)** et **Certificate Profile (Profil de certificat)** à partir des listes déroulantes respectives.
   - Si vous utilisez SCEP comme certificat de périphérique, sélectionnez **SCEP Profile (Profil SCEP)** et **Certificate Profile (Profil de certificat)** à partir des listes déroulantes respectives.
5. Cliquez sur **OK**.

STEP 14 | (Facultatif) Configurez Secure Server Communication (Communication sécurisée avec le serveur) sur un collecteur de journaux. Pour plus d'informations, consultez Configurer l'authentification à l'aide de certificats personnalisés.

1. Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** > **Add (Ajouter)** > **Communication**
2. Vérifiez que la case **Custom Certificate Only (Certificat personnalisé uniquement)** n'est pas cochée. Cela vous permet de continuer à gérer tous les périphériques lors de la migration vers des certificats personnalisés.

   Lorsque la case Custom Certificate Only (Certificat personnalisé uniquement) est cochée, le collecteur de journaux ne s'authentifie pas et ne peut pas recevoir les journaux des périphériques à l'aide de certificats prédéfinis.
3. Sélectionnez le profil de service SSL/TLS depuis le menu déroulant **SSL/TLS Service Profile (Profil de service SSL/TLS)**. Ce profil de service SSL/TLS s'applique à toutes les connexions SSL entre le collecteur de journaux et les périphériques qu'il enregistre.
4. Sélectionnez le profil du certificat depuis la liste déroulante **Certificate Profile (Profil du certificat)**.
5. Sélectionnez **Authorize Client Based on Serial Number (Autoriser le client en fonction du numéro de série)** pour que le serveur vérifie les clients par rapport aux numéros de série des périphériques gérés. Le certificat client doit avoir le mot clé spécial $UDID défini en tant que CN à autoriser en fonction des numéros de série.
6. Dans **Disconnect Wait Time (min) (Délai d'attente de déconnexion (min))**, saisissez le nombre de minutes que Panorama doit attendre avant de mettre fin et de rétablir la connexion avec ses périphériques gérés. Ce champ est vide par défaut et la plage est comprise entre 0 et 44 640 minutes.

   Le délai d'attente de déconnexion de déconnexion ne commence pas à décompter tant que vous n'avez pas validé la nouvelle configuration.
7. (Facultatif) Configurez une liste d'autorisation.
   1. Cliquez sur **Add (Ajouter)** sous Authorization List (Liste d'autorisation).
   2. Sélectionnez **Subject (Objet)** ou **Subject Alt Name (Autre nom de l'objet)** comme type d'identifiant.
   3. Entrez un identifiant du type sélectionné.
   4. Cliquez sur **OK**.
   5. Sélectionnez **Check Authorization List (Vérifier la liste d'autorisation)** pour appliquer la liste d'autorisation.
8. Cliquez sur **OK**.
9. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)**.

© 2020 Palo Alto Networks, Inc.

STEP 15 | Affectez le Collecteur de journaux à un groupe collecteur.

1. Configurer un groupe de collecteurs. Vous devez effectuer une validation de Panorama et ensuite créer un groupe de collecteurs pour synchroniser la configuration du collecteur de journaux avec Panorama et mettre les interfaces Eth1, Eth2, Eth3, Eth4 et Eth5 (si vous les avez configurées) dans un état opérationnel sur le collecteur de journaux.

   Dans un même groupe de collecteurs, tous les collecteurs de journaux doivent être exécutés sur le même modèle Panorama : uniquement des appareils M-600, uniquement des appareils M-500, uniquement des appareils M-200 ou uniquement des appareils virtuels Panorama.

   Il est recommander d'activer l'option Enable log redundancy across collectors (Activer la redondance des journaux entre les collecteurs) si vous ajoutez plusieurs collecteurs de journaux à un seul groupe de collecteurs. Cette option nécessite que chaque collecteur de journaux ait le même nombre de disques de journalisation.
2. Sélectionnez **Panorama (Panorama)** > **Managed Collectors (Collecteurs gérés)** pour vérifier que la configuration de Collecteur de journaux est synchronisée avec Panorama.

   La colonne Configuration Status (État de configuration) doit afficher In Sync (synchronisation) et la colonne Run Time Status (État d'exécution) doit afficher Connected (Connecté).
3. Accédez à l'interface ILC du collecteur de journaux et saisissez la commande suivante pour vérifier que ses interfaces sont opérationnelles :

   ```
   > show interface all
   ```

   La sortie affiche l'`État` comme `haut` pour chaque interface qui est opérationnelle.
4. Si le groupe de collecteurs possède plusieurs collecteurs de journaux, Résoudre les problèmes de connectivité aux ressources réseaux pour vérifier qu'ils peuvent communiquer entre eux en exécutant un test de connectivité Ping pour chaque interface que les collecteurs de journaux utilisent. Pour l'adresse IP `source`, précisez l'interface de l'un des collecteurs de journaux. Pour l'adresse IP de l'`hôte`, spécifiez l'interface correspondante d'un autre collecteur de journaux dans le même groupe de collecteurs.

STEP 16 | Étapes suivantes...

Pour activer le collecteur de journaux afin de recevoir les journaux du pare-feu :

1. Configurer le transfert des journaux vers Panorama.
2. Vérifier le transfert des journaux vers Panorama.

Configurer l'appareil virtuel Panorama avec le collecteur de journaux local

Si l'appareil virtuel Panorama est en mode hérité après la mise à niveau de Panorama 8.0 ou d'une version antérieure vers Panorama 8.1 (ou toute version ultérieure), basculez en mode Panorama pour créer un collecteur de journaux local, ajouter plusieurs disques de journalisation sans perdre les journaux existants, augmenter le stockage de journaux jusqu'à 24 To et accroître la rapidité de la génération des rapports.

Une fois que vous passez du mode Hérité au mode Panorama, le mode Hérité n'est plus disponible.

Après la mise à niveau vers Panorama 8.1, la première étape consiste à augmenter les ressources système de l'appareil virtuel au minimum requis pour le mode Panorama. Panorama redémarre lorsque vous

© 2020 Palo Alto Networks, Inc.

augmentez les ressources. Effectuez cette procédure lors d'une fenêtre de maintenance. Vous devez installer un disque système plus volumineux (81 Go), augmenter les processeurs et la mémoire en fonction de la capacité de stockage de journaux et ajouter un disque de journalisation virtuel. Le nouveau disque de journalisation doit avoir une capacité au moins égale à celle que l'appareil utilise actuellement en mode hérité et ne peut pas être inférieur à 2 To. L'ajout d'un disque virtuel vous permet de migrer les journaux existants vers le collecteur de journaux et permet au collecteur de journaux de stocker de nouveaux journaux.

Si Panorama est déployé dans une configuration HD, effectuez les étapes suivantes sur l'homologue secondaire en premier, puis sur l'homologue principal.

STEP 1 | Déterminez les ressources système dont vous avez besoin pour l'augmentation avant que l'appareil virtuel puisse fonctionner en mode Panorama.

Vous devez exécuter la commande spécifiée dans cette étape, même si vous avez déterminé que Panorama dispose déjà des ressources adéquates.

1. Accédez à la CLI de Panorama :
   1. Utilisez un logiciel d'émulation de terminal tel que PuTTY pour ouvrir une session SSH à l'adresse IP que vous avez spécifiée pour l'interface MGT de Panorama.
   2. Connectez-vous à l'ILC lorsque vous y êtes invité.
2. Vérifiez les ressources que vous devez augmenter en exécutant la commande suivante :

```
> request system system-mode panorama
```

Saisissez **y** lorsque vous êtes invité à continuer. La sortie spécifie les ressources que vous devez augmenter. Par exemple :

```
Panorama mode not supported on current system disk of size 52.0 GB.
Please attach a disk of size 81.0 GB, then use 'request system clone-
system-disk' to migrate the current system disk
Please add a new virtual logging disk with more than 50.00 GB of storage
 capacity.
Not enough CPU cores: Found 4 cores, need 8 cores
```

STEP 2 | Augmentez les processeurs et la mémoire, et remplacez le disque système par un disque plus volumineux.

1. Dans le VMware ESXi vSphere Client, sélectionnez **Virtual Machines**, cliquez droit sur l'appareil virtuel Panorama et sélectionnez **Power (Alimentation)** > **Power Off (Mettre hors tension)**.
2. Cliquez droit sur l'appareil virtuel Panorama et sélectionnez **Edit Settings (Modifier les paramètres)**.
3. Sélectionnez **Memory (Mémoire)** et entrez la nouvelle **Memory Size (Taille mémoire)**.
4. Sélectionnez **CPUs (Processeurs)** et spécifiez le nombre de processeurs (le **Number of virtual sockets (Nombre de sockets virtuels)** multiplié par le **Number of cores per socket (Nombre de cœurs par socket)**).
5. Ajouter un disque virtuel

   Vous utiliserez ce disque pour remplacer le disque système existant.

   1. Sans les paramètres **Hardware (Matériel)**, **Add (Ajoutez)** un disque, sélectionnez **Hard Disk (Disque dur)** comme type de matériel, et cliquez sur **Next (Suivant)**.
   2. **Create a new virtual disk (Créer un nouveau disque virtuel)** et cliquez sur **Next (Suivant)** .
   3. Définissez la **Disk Size (Taille du disque)** à exactement 81 Go et sélectionnez le format de disque **Thick Provision Lazy Zeroed**.

© 2020 Palo Alto Networks, Inc.

4. Sélectionnez **Specify a datastore or datastore structure (Spécifier un magasin de données ou une structure de magasin de données)** comme emplacement, **Browse (Recherchez)** un magasin de donnée d'au moins 81 Go, cliquez sur **OK** et cliquez **Next (Suivant)**.
5. Sélectionnez un **Virtual Device Node (nœud de périphérique virtuel)** SCSI (vous pouvez utiliser la sélection par défaut) et cliquez sur **Next (Suivant)**.

   Panorama ne parviendra pas à démarrer si vous sélectionnez un format autre que SCSI.
6. Vérifiez que les paramètres sont corrects, puis cliquez sur **Finish (Terminer)** et **OK**.

6. Cliquez droit sur l'appareil virtuel Panorama et sélectionnez **Power (Alimentation)** > **Power On (Mettre sous tension)**. Attendez que Panorama redémarre avant de continuer.
7. Revenez à la CLI de Panorama et copiez les données du disque système d'origine sur le nouveau disque système :

   ```
   > request system clone-system-disk target sdb
   ```

   Saisissez **y** lorsque vous êtes invité à continuer.

   Le processus de copie prend environ 20 à 25 minutes, pendant lesquelles Panorama redémarre. Lorsque le processus se termine, la sortie vous indique d'arrêter Panorama.
8. Retournez à la console de vSphere Client, cliquez droit sur l'appareil virtuel Panorama et sélectionnez **Power (Alimentation)** > **Power Off (Mettre hors tension)**.
9. Cliquez droit sur l'appareil virtuel Panorama et sélectionnez **Edit Settings (Modifier les paramètres)**.
10. Sélectionnez le disque système d'origine, cliquez sur **Remove (Retirer)**, sélectionnez **Remove from virtual machine (Supprimer de la machine virtuelle)** et cliquez sur **OK**.
11. Cliquez droit sur l'appareil virtuel Panorama et sélectionnez **Edit Settings (Modifier les paramètres)**.
12. Sélectionnez le nouveau disque système, définissez le **Virtual Device Node (Nœud de périphérique virtuel)** sur **SCSI (0:0)** et cliquez sur **OK**.
13. Cliquez droit sur l'appareil virtuel Panorama et sélectionnez **Power (Alimentation)** > **Power On (Mettre sous tension)**. Avant de continuer, attendez que Panorama redémarre sur le nouveau disque système (environ 15 minutes).

STEP 3 | Ajoutez un disque de journalisation virtuel.

Il s'agit du disque sur lequel vous allez migrer les journaux existants.

1. Dans VMware ESXi vSphere Client, faites un clic droit sur l'appareil virtuel Panorama et sélectionnez **Power (Alimentation)** > **Power Off (Mettre sous tension)**.
2. Cliquez droit sur l'appareil virtuel Panorama et sélectionnez **Edit Settings (Modifier les paramètres)**.
3. Répétez les étapes pour ajouter un disque virtuel. Définissez la **Disk Size (Taille du disque)** à un multiple de 2 To en fonction de la quantité de stockage de journaux dont vous avez besoin. La capacité doit être au moins aussi grande que le disque virtuel ou le stockage NFS existant que Panorama utilise actuellement pour les journaux. La capacité du disque doit être un multiple de 2 To et peut aller jusqu'à 24 To. Par exemple, si le disque existant dispose de 5 To de stockage de journaux, vous devez ajouter un nouveau disque d'au moins 6 To.

   Après avoir basculé en mode Panorama, Panorama divisera automatiquement le nouveau disque en partitions de 2 To, chacune fonctionnant comme un disque virtuel distinct.
4. Cliquez droit sur l'appareil virtuel Panorama et sélectionnez **Power (Alimentation)** > **Power On (Mettre sous tension)**. Attendez que Panorama redémarre avant de continuer.

STEP 4 | Passez du mode hérité au mode Panorama.

Après avoir basculé le mode, l'appareil redémarre à nouveau, puis crée automatiquement un collecteur de journaux local et un groupe de collecteurs. Les journaux existants ne seront pas disponibles pour

© 2020 Palo Alto Networks, Inc.

l'interrogation ou la génération de rapports tant que vous ne les aurez pas migrés ultérieurement dans cette procédure.

1. Revenez à la CLI de Panorama et exécutez la commande suivante.

   ```
   > request system system-mode panorama
   ```

   Saisissez **y** lorsque vous êtes invité à continuer. Après le redémarrage, Panorama crée automatiquement un collecteur de journaux local (nommé Panorama) et crée un groupe de collecteurs (nommé par défaut) pour le contenir. Panorama configure également le disque de journalisation virtuel que vous avez ajouté et le divise en disques distincts de 2 To. Attendez que le processus se termine et que Panorama redémarre (environ cinq minutes) avant de continuer.
2. Connectez-vous à l'interface Web Panorama.
3. Dans les paramètres **Dashboard (Tableau de bord)**, **General Information (Informations générales)**, vérifiez que le **Mode** est maintenant **panorama**.

   Dans un déploiement HD, l'homologue secondaire est, à ce stade, dans un état suspendu, car son mode (Panorama) ne correspond pas au mode sur l'homologue principal (hérité). Vous devrez annuler la suspension de l'homologue secondaire après avoir basculé l'homologue principal en mode Panorama ultérieurement dans cette procédure.
4. Sélectionnez **Panorama** > **Collector Groups (Groupes de collecteurs)**pour vérifier que le groupe de collecteurs **default (par défaut)** a été créé et que le collecteur de journaux local fait partie du groupe de collecteurs par défaut.
5. Appliquez la configuration aux périphériques gérés.
   - S'il n'y a aucun changement en attente :
     1. Sélectionnez **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)** et **Edit Selections (Modifier les sélections)**.
     2. Sélectionnez **Collector Group (Groupe de collecteurs)** et assurez-vous que le groupe de collecteurs **default (par défaut)** est sélectionné.
     3. Cliquez sur **OK** et **Push (Appliquer)**.
   - Si des changements sont en attente :
     1. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** et **Edit Selections (Modifier les sélections)**.
     2. Vérifiez que votre **Device Group (groupe de périphériques)** et vos **Templates (modèles)** sont inclus.
     3. Sélectionnez **Collector Group (Groupe de collecteurs)** et assurez-vous que le groupe de collecteurs **default (par défaut)** est sélectionné.
     4. Cliquez sur **OK** et sur **Commit and Push (Valider et appliquer)**.
6. Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** et vérifiez que les colonnes affichent les informations suivantes pour le collecteur de journaux local :
   - Collector Name (Nom du collecteur) : par défaut, le nom d'hôte Panorama. Il doit être répertorié sous le groupe de collectes **default (par défaut)**.
   - Connected (connecté) : crochet.
   - Configuration Status (État de configuration) : In sync (En synchronisation).
   - Run Time Status (État d'exécution) : connected (connecté).

STEP 5 | (HD uniquement) Basculez le Panorama principal depuis le mode hérité vers le mode Panorama.

Cette étape déclenche le basculement.

© 2020 Palo Alto Networks, Inc.

1. Répétez les étapes 1 à 4 sur le Panorama principal.

   Attendez que le Panorama principal redémarre et retourne à un état HD actif. Si la préemption n'est pas activée, vous devez réaliser manuellement la restauration : sélectionnez **Panorama** > **High Availability (Haute disponibilité)** et, dans la section Operational Commands (Commandes opérationnelles), **Make local Panorama functional (Rendre le Panorama local fonctionnel)**.
2. Sur le Panorama principal, sélectionnez **Dashboard (Tableau de bord)** et, dans la section High Availability (Haute disponibilité), **Sync to peer (Synchroniser avec l'homologue)**, cliquez sur **Yes (Oui)** et attendez que **Running config (Configuration actuelle)** affiche le statut **Synchronized (Synchronisé)** .
3. Sur le Panorama secondaire, sélectionnez **Panorama** > **High Availability (Haute Disponibilité)** et, dans la section Operational Commands (Commandes opérationnelles), cliquez sur **Make local Panorama functional (Rendre le Panorama local fonctionnel)**.

   Cette étape est nécessaire pour sortir le Panorama secondaire de son état HD suspendu.

STEP 6 | Migrez les journaux existants vers les nouveaux disques de journalisation virtuels.

Si vous avez déployé Panorama dans une configuration HD, effectuez cette opération uniquement sur l'homologue principal.

1. Retournez à la CLI de Panorama.
2. Démarrez la migration des journaux :

```
> request logdb migrate vm start
```

   La durée du processus varie en fonction du volume de données de journal que vous migrez. Pour vérifier l'état de la migration, exécutez la commande suivante :

```
> request logdb migrate vm status
```

   Lorsque la migration se termine, la sortie affiche : `migration has been done` (la migration est terminée).
3. Vérifiez que les journaux existants sont disponibles.
   1. Connectez-vous à l'interface Web Panorama.
   2. Sélectionnez **Panorama** > **Monitor (Surveillance)**, sélectionnez un type de journal dont vous savez qu'il correspond à certains journaux existants (par exemple, **Panorama** > **Monitor (Surveillance)** > **System (Système)**), et vérifiez que les journaux s'affichent.

STEP 7 | Étapes suivantes...

Configurez le transfert des journaux vers Panorama afin que le collecteur de journaux reçoive les nouveaux journaux des pare-feu.

Configurer un appareil virtuel Panorama en mode Panorama

Le mode Panorama permet à l'appareil virtuel Panorama™ de fonctionner en tant que serveur de gestion Panorama avec des capacités de collecte de journaux locales. Par défaut, l'appareil virtuel Panorama est déployé en mode Panorama lorsqu'au moins un disque de journalisation virtuel est connecté à un appareil virtuel Panorama sur Amazon Web Services (AWS), AWS GovCloud, Google Cloud Platform (GCP), KVM, Hyper-V, ESXi ou vCloud Air lors du déploiement initial.

© 2020 Palo Alto Networks, Inc.

Bien que cela soit toujours possible, le basculement du mode hérité avec un disque d'enregistrement de 50 Go vers le mode Panorama n'est pas conseillé pour des environnements de production. Si vous basculez en mode Panorama avec un disque d'enregistrement de 50 Go, vous ne pouvez pas ajouter d'autres disques d'enregistrement.

STEP 1 | Connectez-vous à l'ILC de Panorama.

STEP 2 | Passez en mode Panorama.

1. Changez en mode Panorama :

```
> request system system-mode panorama
```

2. Entrez **Y** pour confirmer le changement de mode. Redémarrez l'appareil virtuel Panorama. Si le processus de redémarrage met fin à la session de votre logiciel d'émulation de terminal, reconnectez-vous à l'appareil virtuel Panorama pour voir l'invite de connexion Panorama.

   Si vous voyez une invite de `connexion CMS`, cela signifie que le collecteur de journaux n'a pas terminé le redémarrage. Appuyez sur ENTER à l'invite sans taper un nom d'utilisateur ou un mot de passe.

STEP 3 | Vérifiez que le passage au mode Panorama a réussi :

1. Connectez-vous à l'ILC.
2. Vérifiez que le passage au mode Panorama a réussi :

```
> show system info | match system-mode
```

   Si le changement de mode a réussi, la sortie affiche :

```
> system mode:panorama
```

Configurer un appareil virtuel Panorama en mode de Gestion seulement

Le mode Gestion uniquement permet au dispositif virtuel Panorama de fonctionner strictement comme un serveur de gestion Panorama sans capacités de collecte de journaux locaux. Par défaut, l'appareil virtuel Panorama est en mode Panorama pour le déploiement initial. Il est recommandé de faire passer l'appareil virtuel Panorama au mode Gestion uniquement immédiatement après le déploiement initial, car ce passage au mode Gestion uniquement nécessite qu'aucun fichier journal ne soit transféré vers le serveur de gestion Panorama car l'appareil virtuel Panorama en mode Gestiond uniquement ne prend pas en charge la collecte de journaux. Lorsque vous passez en mode Gestion uniquement, toutes les données de journal existantes stockées sur le dispositif virtuel Panorama deviennent inaccessibles et les fonctions ACC et de génération de rapports ne peuvent pas interroger les journaux stockés sur le dispositif virtuel Panorama.

STEP 1 | Connectez-vous à l'ILC de Panorama.

STEP 2 | Passez au mode de Gestion uniquement.

1. Changez au mode de Gestion uniquement :

```
> request system system-mode management-only
```


© 2020 Palo Alto Networks, Inc.

2. Entrez **`Y`** pour confirmer le changement de mode. Redémarrez l'appareil virtuel Panorama. Si le processus de redémarrage met fin à la session de votre logiciel d'émulation de terminal, reconnectez-vous à l'appareil virtuel Panorama pour voir l'invite de connexion Panorama.

   Si vous voyez une invite de `connexion CMS`, cela signifie que le collecteur de journaux n'a pas terminé le redémarrage. Appuyez sur ENTER à l'invite sans taper un nom d'utilisateur ou un mot de passe.

STEP 3 | Vérifiez que le passage en mode Management Only a réussi :

1. Connectez-vous à l'ILC.
2. Vérifiez que le passage en mode Gestion uniquement a réussi :

```
> show system info | match system-mode
```

Si le changement de mode a réussi, la sortie affiche :

```
> system mode:management-only
```

Augmenter la capacité de stockage de journaux sur l'appareil virtuel Panorama

Après avoir effectué la configuration initiale de l'appareil virtuel Panorama, la capacité de stockage des journaux disponible et les options d'extension dépendent de la plateforme virtuelle (VMware ESXi, vCloud Air, AWS, AWS GovCloud, Azure, Google Cloud Platform, KVM ou Hyper-V) et du mode (Hérité, Panorama ou collecteur de journaux) : voir Modèles panoramiques pour obtenir plus de détails.

Pour augmenter la capacité de stockage des journaux sur l'appareil virtuel Panorama, vous devez ajouter des disques de journalisation supplémentaires. L'augmentation de la capacité de stockage des journaux d'un disque de journalisation existant n'est pas prise en charge, et Panorama ne reconnaît pas la capacité de stockage supplémentaire. Par exemple, si vous avez ajouté un disque de journalisation de 2 To, puis augmenté ce disque de journalisation existant à 4 To, Panorama continue à reconnaître le disque de journalisation comme ayant une capacité de stockage de 2 To et ignore les 2 To supplémentaires de capacité de stockage.



Pour le stockage de journaux supplémentaire, vous pouvez également transférer les journaux des pare-feu vers des collecteurs de journaux dédiés (voir Configurer un collecteur géré*) ou* Configurez le transfert des journaux de Panorama vers des destinations extérieures*.*

Avant d'étendre la capacité de stockage du journal, déterminez les exigences de stockage de journaux de Panorama.

- Conserver les journaux existants lors de l'ajout de stockage sur l'appareil virtuel Panorama en mode hérité
- Ajouter un disque virtuel à Panorama sur un serveur ESXi
- Ajouter un disque virtuel à Panorama sur vCloud Air
- Ajoutez un disque virtuel à Panorama sur AWS
- Ajoutez un disque virtuel à Panorama sur Azure
- Ajouter un disque virtuel à Panorama sur Google Cloud Platform
- Ajouter un disque virtuel à Panorama sur KVM
- Ajouter un disque virtuel à Panorama sur Hyper-V
- Monter le serveur Panorama ESXi dans un serveur de données NFS

© 2020 Palo Alto Networks, Inc.

Conserver les journaux existants lors de l'ajout de stockage sur l'appareil virtuel Panorama en mode hérité

L'appareil virtuel Panorama en mode hérité peut utiliser un seul disque virtuel pour la journalisation. Par conséquent, si vous ajoutez un disque virtuel dédié à la journalisation, Panorama cesse d'utiliser le stockage de journaux de 11 Go par défaut sur le disque système et copie automatiquement tous les journaux existants sur le nouveau disque. (Panorama continue à utiliser le disque système pour les données autres que les journaux.)

Si vous remplacez un disque d'enregistrement dédié existant jusqu'à la capacité de stockage jusqu'à 2 To avec un disque de jusqu'à 8 To, vous perdrez les journaux sur le disque existant. Pour préserver les journaux, vos choix sont :

- Configurez le transfert de journaux vers des destinations externes avant de remplacer le disque virtuel.
- Configurez un nouvel appareil virtuel Panorama pour le nouveau disque de 8 To et maintenez l'accès à Panorama contenant l'ancien disque aussi longtemps que vous avez besoin des journaux. Pour transférer des journaux de pare-feu sur le nouvel appareil virtuel Panorama, une option consiste à reconfigurer les pare-feu pour se connecter à la nouvelle adresse IP de Panorama (sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les paramètres de Panorama), ajoutez les pare-feu en tant que périphériques gérés au nouveau Panorama et Configurer le transfert des journaux vers Panorama. Pour réutiliser l'ancienne adresse IP panorama sur le nouveau panorama, une autre option est d'exporter la configuration de l'ancien Panorama, puis d'importer et de charger la configuration sur le nouveau panorama.
- Copiez les journaux de l'ancien disque vers le nouveau disque. La copie peut prendre plusieurs heures, selon le nombre de journaux que le disque stocke actuellement, et Panorama ne peut pas recueillir de journaux pendant le processus. Contactez Palo Alto Networks support à la clientèle pour les instructions.

Ajouter un disque virtuel à Panorama sur un serveur ESXi

Pour étendre la capacité de stockage des journaux sur l'appareil virtuel Panorama, vous pouvez ajouter des disques de journalisation virtuels. Si l'appareil est en mode Panorama, vous pouvez ajouter 1 à 12 disques de journalisation virtuels de 2 To chacun ou 1 disque de journalisation de 24 To, pour un total de 24 To maximum. Si l'appareil est en mode hérité, vous pouvez ajouter un disque de journalisation virtuel d'un maximum de 8 To sur ESXi 5.5 et versions ultérieures, ou un disque de 2 To maximum sur les versions antérieures d'ESXi. Par ailleurs, il est recommandé d'ajouter des disques de journalisation ayant le même format d'approvisionnement afin d'éviter toute performance inattendue pouvant résulter du fait d'avoir plusieurs disques ayant des formats d'approvisionnement différents.



Si Panorama perd la connectivité avec le nouveau disque virtuel, Panorama peut perdre des journaux pendant l'intervalle d'échec.

Pour permettre la redondance, utilisez le disque virtuel dans une configuration RAID. RAID 10 offre les meilleures performances d'écriture pour des applications avec des besoins de journalisation importants.

Si nécessaire, vous pouvez remplacer le disque virtuel sur un serveur ESX*.*

© 2020 Palo Alto Networks, Inc.

STEP 1 | Ajoutez des disques supplémentaires à Panorama.

Dans tous les modes, le premier disque de journalisation de la machine virtuelle Panorama doit avoir une taille minimale de 2 To afin d'ajouter des disques supplémentaires. Si le premier disque de journalisation est inférieur à 2 To, vous ne pourrez pas ajouter d'espace disque supplémentaire.

1. Accédez au client VMware vSphere et sélectionnez l'onglet **Virtual Machines (Machines virtuelles)**.
2. Cliquez droit sur l'appareil virtuel Panorama et sélectionnez **Power (Alimentation)** > **Power Off (Mettre hors tension)**.
3. Cliquez droit sur l'application virtuelle Panorama et sélectionnez **Edit Settings (Modifier les paramètres)**.
4. Cliquez sur **Add (Ajouter)** dans l'onglet **Hardware (Matériel)** pour lancer l'assistant d'ajout de matériel.
5. Sélectionnez **Hard Disk (Disque dur)** pour le type de matériel et cliquez sur **Next (Suivant)**.
6. **Create a new virtual disk (Créer un nouveau disque virtuel)** et cliquez sur **Next (Suivant)** .
7. Définissez la **Disk Size (Taille du disque)**. Si l'appareil virtuel Panorama est en mode Panorama, définissez la taille sur au moins 2 To. Si l'appareil est en mode hérité, vous pouvez définir une taille pouvant atteindre 8 To.

   En mode Panorama, vous pouvez ajouter des tailles de disque supérieures à 2 To et Panorama créera automatiquement autant de partitions de 2 To que possible. Par exemple, si le disque sdc était de 24 To, il créerait 12 partitions de 2 To. Ces disques seront nommés sdc1-12.
8. Sélectionnez le format **Disk Provisioning (Approvisionnement du disque)** et cliquez sur **Next (Suivant)**.
9. **Specify a datastore or datastore structure (Spécifier un magasin de données ou une structure de magasin de données)**, **Browse (Parcourir)** à un magasin de données avec suffisamment d'espace pour la **Disk Size (Taille du disque)** spécifiée, cliquez sur **OK** puis sur **Next (Suivant)**.
10. Sélectionnez un **Virtual Device Node (nœud de périphérique virtuel)** SCSI (vous pouvez utiliser la sélection par défaut) et cliquez sur **Next (Suivant)**.

    Le nœud sélectionné doit être au format SCSI ; Panorama ne démarre pas si vous sélectionnez un autre format.
11. Vérifiez que les paramètres sont corrects, puis cliquez sur **Finish (Terminer)** et **OK**.

    Le nouveau disque apparaît dans la liste des périphériques pour l'application virtuelle.
12. Répétez l'étape 4 à l'étape 11 pour ajouter des disques supplémentaires à l'appareil virtuel Panorama si nécessaire.
13. Cliquez droit sur l'appareil virtuel Panorama et sélectionnez **Power (Alimentation)** > **Power On (Mettre sous tension)**. Le disque virtuel s'initialise pour la première utilisation. La taille du nouveau disque détermine la durée de l'initialisation.

STEP 2 | Configurez chaque disque.

L'exemple suivant utilise le disque virtuel sdc.

1. Connectez-vous à l'ILC de Panorama.
2. Entrez la commande suivante pour afficher les disques sur l'appareil virtuel Panorama :

   `show system disk details`

   L'utilisateur verra la réponse suivante :

```
 Name
: sdb
 State : Present
```


© 2020 Palo Alto Networks, Inc.

```
Size : 2048 MB
Status : Available
Reason : Admin enabled
Name : sdc
State : Present
Size : 2048 MB
Status : Available
Reason : Admin disabled
```

3. Entrez la commande suivante et confirmez la requête lorsque vous y êtes invité pour tous les disques avec la réponse `Reason : Admin disabled (Raison : Admin désactivé)` :

   `request system disk add sdc`

   *La commande **`request system disk add`** n'est pas disponible sur un serveur de gestion Panorama en mode Gestion uniquement car la journalisation n'est pas prise en charge par ce mode. Si vous ne voyez pas la commande, il suffit de Configurer un appareil virtuel Panorama en mode Panorama pour activer les disques de journalisation. Une fois que vous passez en mode Panorama, connecter à l'interface de ligne de commande Panorama et passez à l'étape 4 pour vérifier l'ajout des disques.*

4. Saisissez la commande **`show system disk details`** pour vérifier l'état de l'ajout des disques. Passez à l'étape 3 lorsque toutes les réponses de disque nouvellement ajoutés affichent la réponse `Reason : Admin disabled (Raison : Admin désactivé)`.

STEP 3 | Rendez les disques disponibles pour la journalisation.

1. Connectez-vous à l'interface Web Panorama.
2. Sélectionnez **Panorama (Panorama)** > **Managed Collectors (Collecteurs gérés)** et modifiez le collecteur de journaux.
3. Sélectionnez **Disks (Disques)** et ajoutez chaque disque nouvellement ajouté.
4. Cliquez sur **OK**.
5. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** et **Commit and Push (Validez et appliquez)** vos changements.

STEP 4 | Configurez Panorama pour recevoir les journaux.

Cette étape est destinée aux nouveaux déploiements de Panorama en mode Panorama. Si vous ajoutez des disques de journalisation à un appareil virtuel Panorama existant, passez à l'étape 5.

1. Configurer un collecteur géré.
2. Configurer un groupe de collecteurs.
3. Configurer le transfert des journaux vers Panorama.

STEP 5 | Vérifiez que la capacité de stockage du journal de Panorama a été augmentée.

1. Connectez-vous à l'interface Web Panorama.
2. Sélectionnez **Panorama** > **Collector Groups (Groupes de collecteurs)** et sélectionnez le groupe de collecteurs auquel appartient l'appareil Panorama virtuel.
3. Vérifiez que la capacité de **Log Storage (Stockage des journaux)** affiche avec précision la capacité du disque.

Ajouter un disque virtuel à Panorama sur vCloud Air

Vous pouvez ajouter des disques de journalisation virtuels pour accroître la capacité de stockage des journaux sur le dispositif virtuel Panorama ™. Si l'appareil est en mode Panorama, vous pouvez ajouter 1 à 12 disques de journalisation virtuels de 2 To chacun ou 1 disque de journalisation de 24 To, pour un total

© 2020 Palo Alto Networks, Inc.

de 24 To maximum. Si l'appareil est en mode hérité, vous pouvez ajouter un disque de journalisation virtuel d'un maximum de 8 To.

Si Panorama perd la connectivité au nouveau disque virtuel, Panorama risque de perdre des journaux pendant la durée de l'incident.

Si nécessaire, vous pouvez remplacer le disque virtuel sur vCloud Air*.*

STEP 1 | Ajoutez des disques supplémentaires à Panorama.

Dans tous les modes, le premier disque de journalisation sur la machine virtuelle Panorama doit avoir au moins 2 To pour ajouter des disques supplémentaires. Si le premier disque de journalisation est inférieur à 2 To, vous ne pourrez pas ajouter d'espace disque supplémentaire.

1. Accédez à la console Web vCloud Air et sélectionnez votre région de **Virtual Private Cloud OnDemand (Cloud virtuel privé sur demande)**.
2. Sélectionnez l'application virtuelle Panorama dans la **Virtual Machines (Machines virtuelles)** onglet.
3. **Add another disk (Ajoutez un autre disque)** (**Actions** > **Edit Resources (Modifier les ressources)**).
4. Définissez la taille du **Storage (Stockage)**. Si l'appareil virtuel Panorama est en mode Panorama, définissez la taille sur au moins 2 To. Si l'appareil est en mode hérité, vous pouvez définir une taille pouvant atteindre 8 To.

   En mode Panorama, vous pouvez ajouter des tailles de disque supérieures à 2 To et Panorama créera automatiquement autant de partitions de 2 To que possible. Par exemple, si le disque sdc était de 24 To, il créerait 12 partitions de 2 To. Ces disques seront nommés sdc1 à sdc12.
5. Définissez le niveau de stockage sur **Standard** ou **SSD-Accelerated (Accéléré par SSD)**.
6. Répétez les étapes précédentes pour ajouter des disques supplémentaires au dispositif virtuel Panorama si nécessaire..
7. Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.

STEP 2 | Configurez chaque disque.

L'exemple suivant utilise le disque virtuel sdc.

1. Connectez-vous à l'ILC de Panorama.
2. Entrez la commande suivante pour afficher les disques sur l'appareil virtuel Panorama :

   `show system disk details`

   L'utilisateur verra la réponse suivante :

```
 Name
: sdb
 State : Present
 Size : 2048 MB
 Status : Available
 Reason : Admin enabled
 Name : sdc
 State : Present
 Size : 2048 MB
 Status : Available
 Reason : Admin disabled
```

3. Entrez la commande suivante et confirmez la requête lorsque vous y êtes invité pour tous les disques avec la réponse `Reason : Admin disabled` (Raison : Admin désactivé) :

© 2020 Palo Alto Networks, Inc.

```
request system disk add sdc
```

*La **`commande request system disk add`** n'est pas disponible sur un serveur de gestion Panorama en mode Gestion uniquement car la journalisation n'est pas prise en charge par ce mode. Si vous ne voyez pas la commande, il suffit de* Configurer un appareil virtuel Panorama en mode Panorama *pour activer les disques de journalisation. Une fois que vous passez en mode Panorama,* connecter à l'interface de ligne de commande Panorama *et passez à l'*étape 4 *pour vérifier l'ajout des disques.*

4. Saisissez la commande **`show system disk details`** pour vérifier l'état de l'ajout des disques. Passez à l'étape suivante lorsque toutes les réponses de disque nouvellement ajoutés affichent la réponse `Reason : Admin disabled (Raison : Admin désactivé).`

STEP 3 | Rendez les disques disponibles pour la journalisation.

1. Connectez-vous à l'interface Web Panorama.
2. Sélectionnez **Panorama (Panorama)** > **Managed Collectors (Collecteurs gérés)** et modifiez le collecteur de journaux.
3. Sélectionnez **Disks (Disques)** et **Add (Ajoutez)** chaque nouveau disque.
4. Cliquez sur **OK**.
5. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** et **Commit and Push (Validez et appliquez)** vos changements.

STEP 4 | Configurez Panorama pour recevoir les journaux.

Cette étape est destinée aux nouveaux déploiements de Panorama en mode Panorama. Si vous ajoutez des disques de journalisation à un appareil Panorama virtuel existant, passez à l'étape suivante.

1. Configurer un collecteur géré.
2. Configurer un groupe de collecteurs.
3. Configurer le transfert des journaux vers Panorama.

STEP 5 | Vérifiez que la capacité de stockage du journal de Panorama a été augmentée.

1. Connectez-vous à l'interface Web Panorama.
2. Sélectionnez **Panorama** > **Collector Groups (Groupes de collecteurs)** et sélectionnez le groupe de collecteurs auquel appartient l'appareil Panorama virtuel.
3. Vérifiez que la capacité de **Log Storage (Stockage des journaux)** affiche avec précision la capacité du disque.

Ajoutez un disque virtuel à Panorama sur AWS

Après avoir Installé Panorama sur KVM ou Installer Panorama sur AWS GovCloud, ajoutez des disques de journalisation virtuels à l'instance d'appareil virtuel Panorama™ pour fournir du stockage aux journaux générés par les pare-feu gérés. Vous pouvez ajouter des disques virtuels à un collecteur de journaux local pour un appareil virtuel Panorama en mode Panorama ou pour un collecteur de journaux dédié. Pour ajouter des disques virtuels, vous devez avoir accès au portail Amazon Web Services, à l'interface de ligne de commande Panorama (CLI) et à l'interface Web Panorama.

L'appareil virtuel Panorama sur KVM ne prend en charge que les disques de journalisation 2 To et prend en charge jusqu'à 24 To de stockage de journaux. Vous ne pouvez pas ajouter un disque de journalisation inférieur à 2 To ou un disque de journalisation dont la taille ne peut être divisée par 2 To, car l'appareil virtuel Panorama partitionne les disques de journalisation en partitions de 2 To. Par exemple, si vous joignez un disque de journalisation de 4 To, Panorama créera deux partitions de 2 To. Toutefois, vous ne pouvez

© 2020 Palo Alto Networks, Inc.

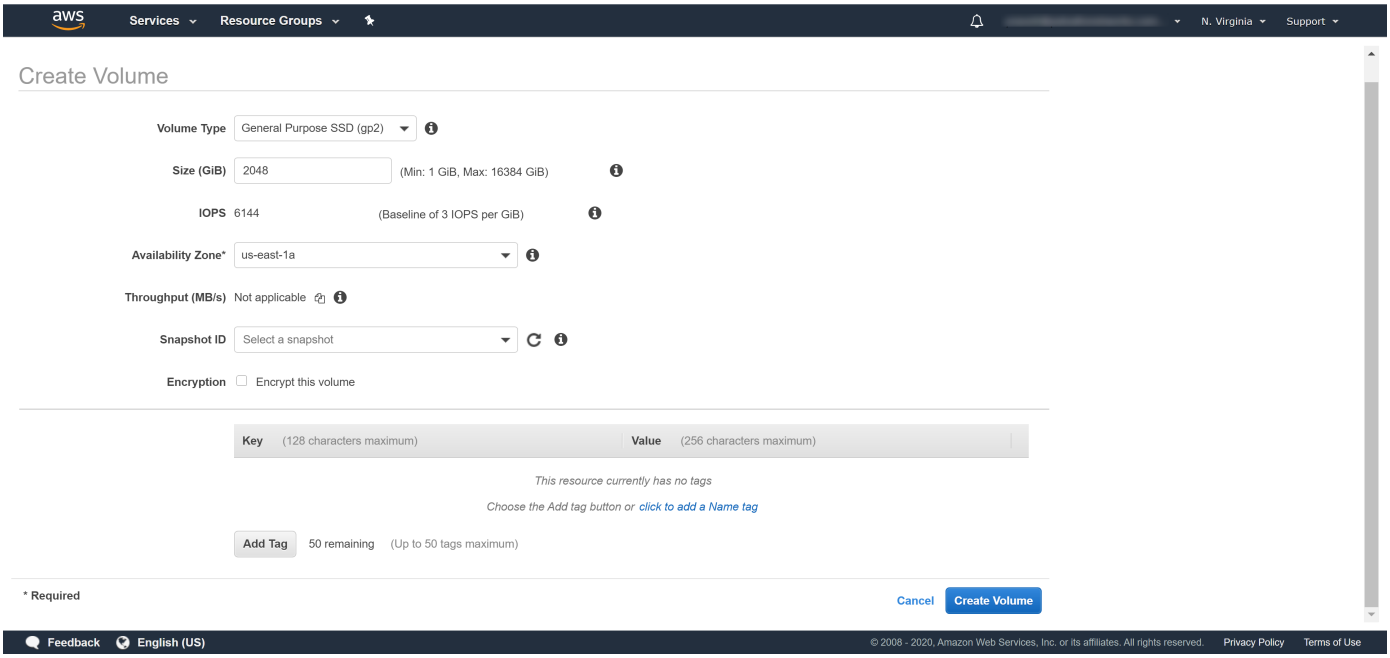
pas ajouter un disque de journalisation de 5 To car les 1 To restants ne sont pas pris en charge en tant que partition.

STEP 1 | Connectez-vous à AWS Web Service Console et sélectionnez le tableau de bord EC2.

- Amazon Web Service Console
- AWS GovCloud Web Service Console

STEP 2 | Ajoutez un disque de journalisation virtuel sur Panorama.

1. Sur le panneau de bord de EC2, sélectionnez **Volumes** et **Créez volume**:
   - Sélectionnez votre volume préféré. Pour utilisation générale, sélectionnez **General Purpose SSD (GP2) (Utilisation générale SSD (GP2))**.
   - Configurez la **Size (taille)** du volume sur 2048 GiB.
   - Sélectionnez la même zone de disponibilité que l'instance de votre appareil virtuel Panorama.
   - (Facultatif) Chiffrez le volume.
   - (Facultatif) Ajoutez des balises au volume.
2. Cliquez sur **Create Volume (Créer un volume)**.



3. Sur la page Volumes, sélectionnez un volume, sélectionnez **Actions** > **Attach Volume (Joindre le volume)**.
4. Joignez l'instance de l'appareil virtuel Panorama.

STEP 3 | Configurez chaque disque.

L'exemple suivant utilise le disque virtuel sdc.

1. Connectez-vous à l'ILC de Panorama.
2. Entrez la commande suivante pour afficher les disques sur l'appareil virtuel Panorama :

   `show system disk details`

   L'utilisateur verra la réponse suivante :

```
 Name
: sdb
 State : Present
```


© 2020 Palo Alto Networks, Inc.

```
Size : 2048 MB
Status : Available
Reason : Admin enabled
Name : sdc
State : Present
Size : 2048 MB
Status : Available
Reason : Admin disabled
```

3. Entrez la commande suivante et confirmez la requête lorsque vous y êtes invité pour tous les disques avec la réponse `Reason : Admin disabled (Raison : Admin désactivé)` :

   `request system disk add sdc`

   *La commande **`request system disk add`** n'est pas disponible sur un serveur de gestion Panorama en mode Gestion uniquement car la journalisation n'est pas prise en charge par ce mode. Si vous ne voyez pas la commande, il suffit de Configurer un appareil virtuel Panorama en mode Panorama pour activer les disques de journalisation. Une fois que vous passez en mode Panorama, connecter à l'interface de ligne de commande Panorama et passez à l'étape 4 pour vérifier l'ajout des disques.*

4. Saisissez la commande **`show system disk details`** pour vérifier l'état de l'ajout des disques. Passez à l'étape suivante lorsque toutes les réponses de disque nouvellement ajoutés affichent la réponse `Reason : Admin disabled (Raison : Admin désactivé)`.

STEP 4 | Rendez les disques disponibles pour la journalisation.

1. Connectez-vous à l'interface Web Panorama.
2. Modifiez un Collecteur de journaux (**Panorama** > **Managed Collectors (Collecteurs gérés)**).
3. Sélectionnez **Disques** et **Add (Ajoutez)** chaque nouveau disque.
4. Cliquez sur **OK**.
5. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** et **Commit and Push (Validez et appliquez)** vos changements.

STEP 5 | (Nouveaux déploiements Panorama en mode Panorama uniquement) Configurez Panorama pour recevoir les journaux.

Si vous ajoutez des disques de journalisation à un appareil virtuel Panorama existant, passez à l'étape 6.

1. Configurer un groupe de collecteurs.
2. Configurer le transfert des journaux vers Panorama.

STEP 6 | Vérifiez que la capacité de stockage du journal de Panorama a été augmentée.

1. Connectez-vous à l'interface Web Panorama.
2. Sélectionnez le groupe de collecteurs auquel appartient l'appareil virtuel Panorama (**Panorama** > **Collector Groups (Groupe de collecteurs)**).
3. Vérifiez que la capacité de **Log Storage (Stockage des journaux)** affiche avec précision la capacité du disque.

Ajoutez un disque virtuel à Panorama sur Azure

Après avoir Installé Panorama sur Azure, ajoutez des disques de journalisation virtuels à l'instance de dispositif virtuel Panorama ™ pour fournir le stockage des journaux générés par les pare-feu gérés. Vous pouvez ajouter des disques virtuels à un collecteur de journaux local pour un appareil virtuel Panorama en mode Panorama ou pour un collecteur de journaux dédié. Pour ajouter des disques virtuels, vous devez avoir accès au portail Microsoft Azure, à l'interface de ligne de commande Panorama (CLI) et à l'interface Web Panorama.

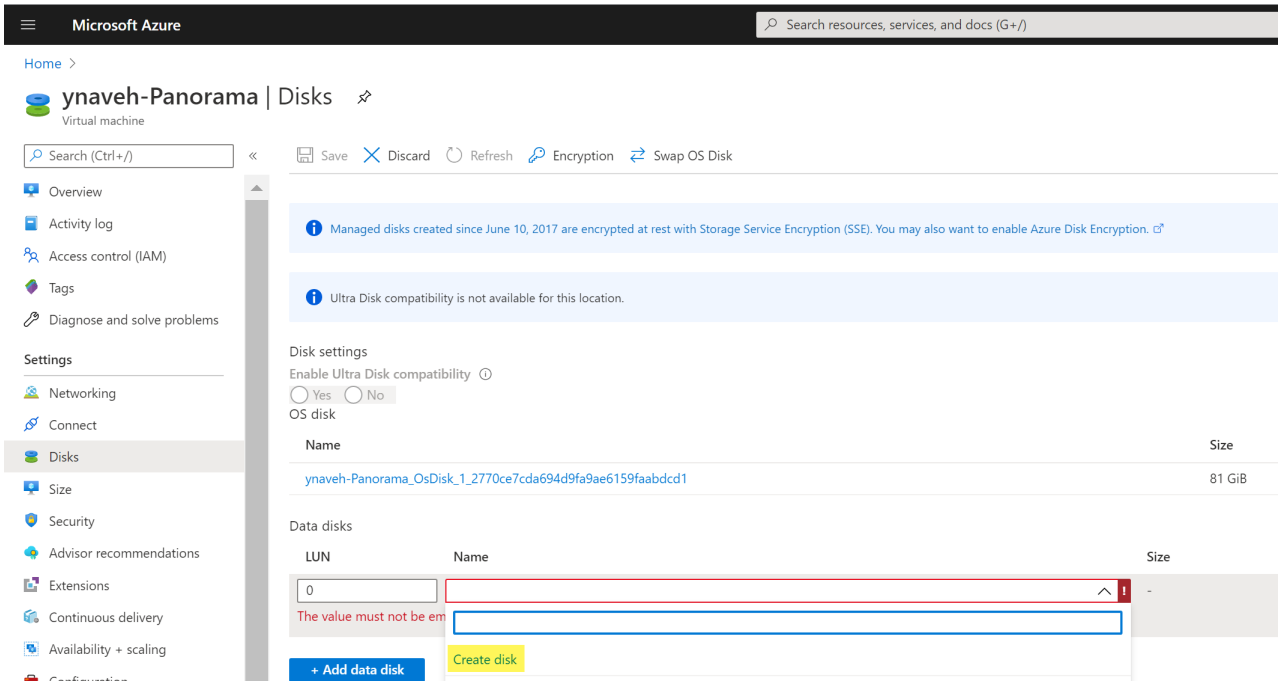
© 2020 Palo Alto Networks, Inc.

L'appareil virtuel Panorama sur KVM ne prend en charge que les disques de journalisation 2 To et prend en charge jusqu'à 24 To de stockage de journaux. Vous ne pouvez pas ajouter un disque de journalisation inférieur à 2 To ou un disque de journalisation dont la taille n'est pas divisible de 2 To, car le dispositif virtuel Panorama partitionne les disques de journalisation en partitions de 2 To. Par exemple, si vous joignez un disque de journalisation de 4 To, Panorama créera deux partitions de 2 To. Toutefois, vous ne pouvez pas ajouter un disque de journalisation de 5 To car les 1 To restants ne sont pas pris en charge en tant que partition.

STEP 1 | Connectez-vous au Portail Microsoft Azure.

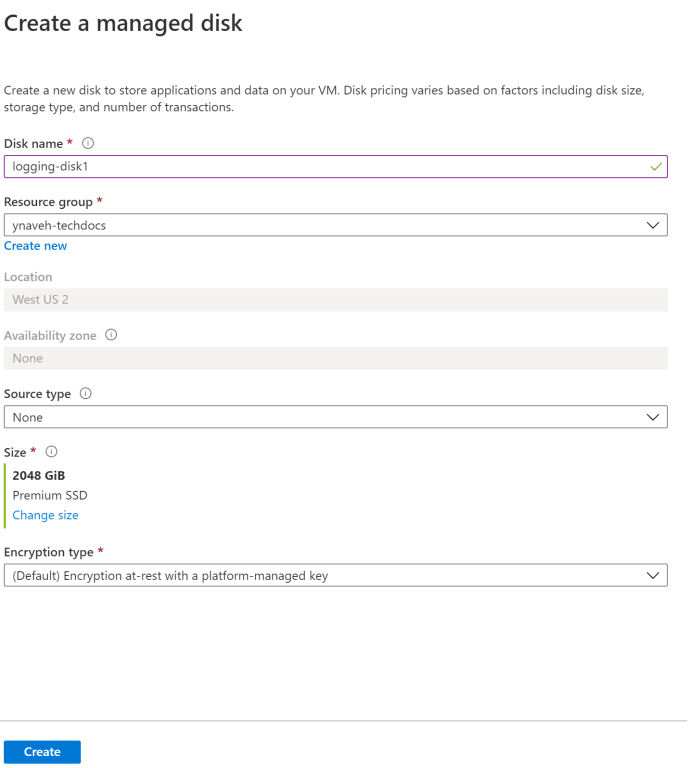
STEP 2 | Ajoutez un disque de journalisation virtuel sur Panorama.

1. Dans le tableau de bord de Azure, sélectionnez les **Virtual Machines (Machines virtuelles)** Panorama sur lesquelles vous voulez ajouter un disque de journalisation.
2. Sélectionnez **Disks (Disques)**.
3. **+Add another disk (+Ajouter un autre disque)**.
4. Dans le menu déroulant du nouveau disque, **Create disk (Créer un disque)**.

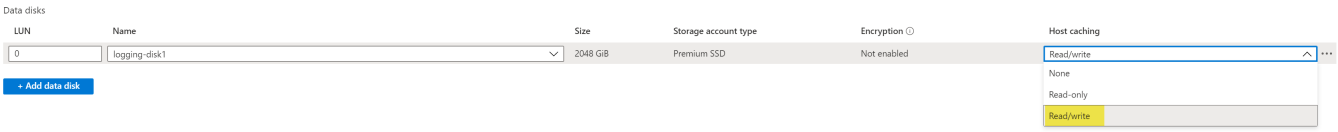


5. Configurez le disque de journalisation.
    1. Entrez le **Name (Nom)** du disque.
    2. Sélectionnez le groupe de ressources. Si vous **Create new (Créez de nouveaux)** groupes de ressources, entrez le nom des groupes.
    3. Vérifiez le **Account Type (Type de compte)** (ce champ est rempli automatiquement).
    4. Dans la liste déroulante du **Source type (type de source**, sélectionnez **None (aucun)**.
    5. Sélectionnez **Change Size (Modifier la taille)** et sélectionnez un disque de journalisation de 2048 GiB.
    6. **Create (Créer)** le nouveau disque de journalisation.

© 2020 Palo Alto Networks, Inc.



7. Pour la **Host caching (mise en cache de l'hôte)**, sélectionnez **Read/write (Lire/écrire)**.



STEP 3 | Activez chaque disque.

L'exemple suivant utilise le disque virtuel sdc.

1. Connectez-vous à l'ILC de Panorama.
2. Entrez la commande suivante pour afficher les disques sur l'appareil virtuel Panorama :

   `show system disk details`

   L'utilisateur verra la réponse suivante :

```
 Name
: sdb
 State : Present
 Size : 2048 MB
 Status : Available
 Reason : Admin enabled
 Name : sdc
 State : Present
 Size : 2048 MB
 Status : Available
 Reason : Admin disabled
```

3. Entrez la commande suivante et confirmez la requête lorsque vous y êtes invité pour tous les disques avec la réponse `Reason : Admin disabled (Raison : Admin désactivé)` :

   `request system disk add sdc`

© 2020 Palo Alto Networks, Inc.

La commande ***request system disk add*** *n'est pas disponible sur un serveur de gestion Panorama en mode Gestion uniquement car la journalisation n'est pas prise en charge par ce mode. Si vous ne voyez pas la commande, il suffit de* Configurer un appareil virtuel Panorama en mode Panorama *pour activer les disques de journalisation. Une fois que vous passez en mode Panorama,* connecter à l'interface de ligne de commande Panorama *et passez à l'*étape 4 *pour vérifier l'ajout des disques.*

4. Saisissez la commande **`show system disk details`** pour vérifier l'état de l'ajout des disques. Passez à l'étape suivante lorsque toutes les réponses de disque nouvellement ajoutés affichent la réponse `Reason : Admin disabled (Raison : Admin désactivé).`

STEP 4 | Rendez les disques disponibles pour la journalisation.

1. Connectez-vous à l'interface Web Panorama.
2. Modifiez un Collecteur de journaux (**Panorama** > **Managed Collectors (Collecteurs gérés)**).
3. Sélectionnez **Disques** et **Add (Ajoutez)** chaque nouveau disque.
4. Cliquez sur **OK**.
5. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** et **Commit and Push (Validez et appliquez)** vos changements.

STEP 5 | (Nouveaux déploiements Panorama en mode Panorama uniquement) Configurez Panorama pour recevoir les journaux.

Si vous ajoutez des disques de journalisation à un appareil virtuel Panorama existant, passez à l'étape 6.

1. Configurer un groupe de collecteurs.
2. Configurer le transfert des journaux vers Panorama.

STEP 6 | Vérifiez que la capacité de stockage du journal de Panorama a été augmentée.

1. Connectez-vous à l'interface Web Panorama.
2. Sélectionnez le groupe de collecteurs auquel appartient l'appareil virtuel Panorama (**Panorama** > **Collector Groups (Groupe de collecteurs)**).
3. Vérifiez que la capacité de **Log Storage (Stockage des journaux)** affiche avec précision la capacité du disque.

Ajouter un disque virtuel à Panorama sur Google Cloud Platform

Après avoir Installé Panorama sur Google Cloud Platform, ajoutez des disques de journalisation virtuels à l'instance de l'appareil virtuel Panorama ™ pour fournir le stockage des journaux générés par les pare-feu gérés. Vous pouvez ajouter des disques virtuels à un collecteur de journaux local pour un appareil virtuel Panorama en mode Panorama ou pour un collecteur de journaux dédié. L'appareil virtuel Panorama sur Google Cloud Platform ne prend en charge que les disques de journalisation 2 To et prend en charge jusqu'à 24 To de stockage de journaux. Vous ne pouvez pas ajouter un disque de journalisation inférieur à 2 To ou un disque de journalisation dont la taille ne peut être divisée par 2 To, car l'appareil virtuel Panorama partitionne les disques de journalisation en partitions de 2 To. Par exemple, si vous joignez un disque de journalisation de 4 To, Panorama créera deux partitions de 2 To. Toutefois, vous ne pouvez pas ajouter un disque de journalisation de 5 To car les 1 To restants ne sont pas pris en charge en tant que partition.

STEP 1 | Connectez-vous à Google Cloud Console.

STEP 2 | Ajoutez les disques de journalisation virtuels.

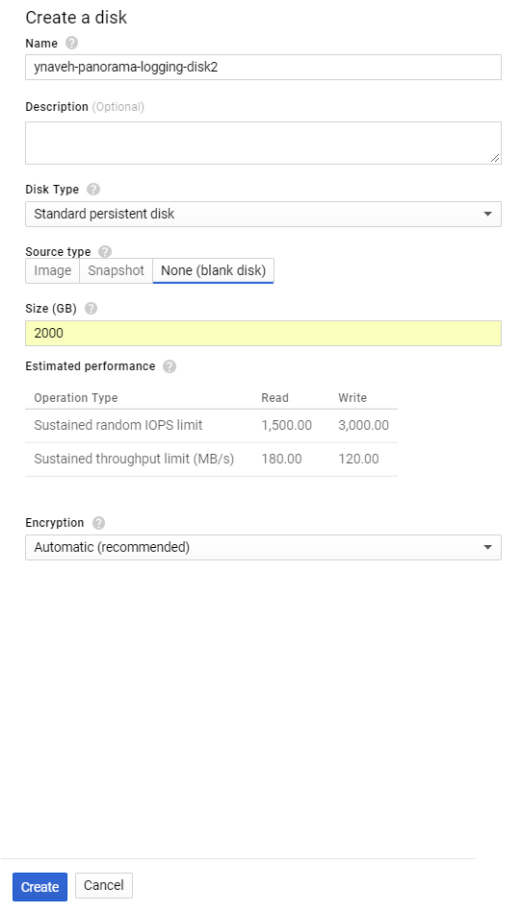
1. Dans le menu des produits et services, sélectionnez et ensuite **Edit (Modifiez)** l'instance de l'appareil virtuel Panorama (**Compute Engine** > **Instances VM**).

© 2020 Palo Alto Networks, Inc.

2. À la section Disques additionnels, **Add Item (ajoutez un item)**.
3. **Create disk (Créez un disque)** (liste déroulante **Name (Nom)**).

STEP 3 | Configurez les disques de journalisation virtuels.

1. Saisissez un **Name (Nom)**.
2. Développez le menu déroulant **Disk Type (Type de disque)** et sélectionnez le type souhaité.
3. Sous **Source type (Type de source)**, sélectionnez **None (blank disk) (Aucun (disque vide))**.
4. Définissez la **Size (GB) (Taille (Go))** du disque de journalisation virtuel.
5. Cliquez sur **Create (Créer)**.



6. **Save (Enregistrez)** les modifications pour mettre à jour l'instance de l'appareil virtuel Panorama.

STEP 4 | Configurez chaque disque.

L'exemple suivant utilise le disque virtuel sdc.

1. Connectez-vous à l'ILC de Panorama.
2. Entrez la commande suivante pour afficher les disques sur l'appareil virtuel Panorama :

   `show system disk details`

   L'utilisateur verra la réponse suivante :

```
 Name
: sdb
 State : Present
 Size : 2048 MB
```


© 2020 Palo Alto Networks, Inc.

```
Status : Available
Reason : Admin enabled
Name : sdc
State : Present
Size : 2048 MB
Status : Available
Reason : Admin disabled
```

3. Entrez la commande suivante et confirmez la requête lorsque vous y êtes invité pour tous les disques avec la réponse `Reason : Admin disabled` (Raison : Admin désactivé) :

   `request system disk add sdc`

   *La commande **`request system disk add`** n'est pas offert sur un serveur de gestion Panorama en mode Gestion uniquementm car la journalisation n'est pas prise en charge par ce mode. Si vous ne voyez pas la commande, il suffit de Configurer un appareil virtuel Panorama en mode Panorama pour activer les disques de journalisation. Une fois que vous passez en mode Panorama, connecter à l'interface de ligne de commande Panorama et passez à l'étape 4 pour vérifier l'ajout des disques.*

4. Saisissez la commande **`show system disk details`** pour vérifier l'état de l'ajout des disques. Passez à l'étape suivante lorsque toutes les réponses de disque nouvellement ajoutés affichent la réponse `Reason : Admin enabled`. (Raison : admin activé)

STEP 5 | Rendez les disques disponibles pour la journalisation.

1. Connectez-vous à l'interface Web Panorama.
2. Modifiez un Collecteur de journaux (**Panorama** > **Managed Collectors (Collecteurs gérés)**).
3. Sélectionnez **Disques** et **Add (Ajoutez)** chaque nouveau disque.
4. Cliquez sur **OK**.
5. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** et **Commit and Push (Validez et appliquez)** vos changements.

STEP 6 | (Nouveaux déploiements Panorama en mode Panorama uniquement) Configurez Panorama pour recevoir les journaux.

Si vous ajoutez des disques de journalisation à un appareil virtuel Panorama existant, passez à l'étape 7.

1. Configurer un groupe de collecteurs.
2. Configurer le transfert des journaux vers Panorama.

STEP 7 | Vérifiez que la capacité de stockage du journal de Panorama a été augmentée.

1. Connectez-vous à l'interface Web Panorama.
2. Sélectionnez le groupe de collecteurs auquel appartient l'appareil virtuel Panorama (**Panorama** > **Collector Groups (Groupe de collecteurs)**).
3. Vérifiez que la capacité de **Log Storage (Stockage des journaux)** affiche avec précision la capacité du disque.

Ajouter un disque virtuel à Panorama sur KVM

Après avoir Installé Panorama sur KVM, ajoutez des disques de journalisation virtuels à l'instance de l'appareil virtuel Panorama ™ pour fournir le stockage des journaux générés par les pare-feu gérés. Vous pouvez ajouter des disques virtuels à un collecteur de journaux local pour un appareil virtuel Panorama en mode Panorama ou pour un collecteur de journaux dédié. L'appareil virtuel Panorama sur KVM ne prend en charge que les disques de journalisation 2 To et prend en charge jusqu'à 24 To de stockage de journaux. Vous ne pouvez pas ajouter un disque de journalisation inférieur à 2 To ou un disque de journalisation dont la taille ne peut être divisée par 2 To, car l'appareil virtuel Panorama partitionne les disques de journalisation

© 2020 Palo Alto Networks, Inc.

en partitions de 2 To. Par exemple, si vous joignez un disque de journalisation de 4 To, Panorama créera deux partitions de 2 To. Toutefois, vous ne pouvez pas ajouter un disque de journalisation de 5 To car les 1 To restants ne sont pas pris en charge en tant que partition.

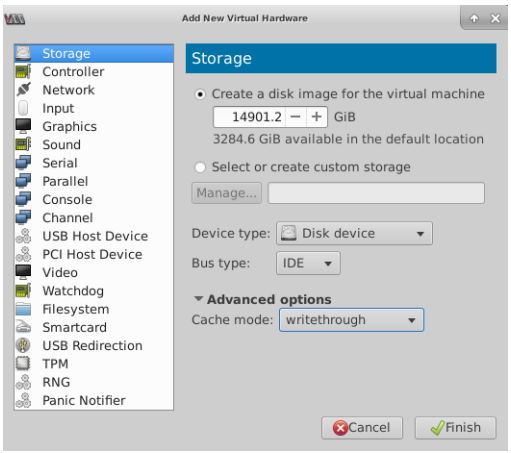
STEP 1 | **Shutdown (Arrêtez)** l'instance de l'appareil virtuel Panorama sur le Virtual Machine Manager (Gestionnaire de machine virtuelle).

STEP 2 | Double-cliquez sur l'instance de l'appareil virtuel Panorama dans le Virtual Machine Manager (Gestionnaire de machine virtuelle) et **Show virtual hardware details (Affichez les détails de la machine virtuelle)** .

STEP 3 | Ajoutez les disques de journalisation virtuels. Répétez cette étape autant de fois que vous en avez besoin.

1. **Create a disk image for a virtual image (Créez une image disque pour une image virtuelle)** (**Add Hardware (Ajoutez le matériel)** > **Storage (Stockage)**) et configurez la capacité de stockage de disque virtuel sur la valeur 2 To appropriée : 2000 Go ou 14901.2 Gbit selon votre Virtual Machine Manager (gestionnaire de machine virtuelle).

   Selon la version, certains Virtual Machine Managers (gestionnaires de machine virtuelle) utilisent les GiB (gibibytes) pour allouer de la mémoire. Assurez-vous de bien convertir la capacité de stockage requise pour éviter de sous-approvisionner le disque de journalisation virtuel et d'envoyer l'appareil virtuel Panorama en mode maintenance.
2. Dans la liste déroulante **Device type (Type d'appareil)**, sélectionnez **Disk device (Périphérique de disque)**.
3. Dans le **Disk Bus (disque bus)** sélectionnez **VirtIO** ou **IDE**, selon votre configuration.
4. Ouvrez **Advanced options (Option avancées)** et, dans le **Cache mode (Mode cache)** descendez et sélectionnez **writethrough (double écriture)**.
5. Cliquez sur **Finish (Terminer)**.



STEP 4 | Mettez l'appareil virtuel Panorama **Power on (sous tension)**

STEP 5 | Configurez chaque disque.

L'exemple suivant utilise le disque virtuel sdc.

1. Connectez-vous à l'ILC de Panorama.
2. Entrez la commande suivante pour afficher les disques sur l'appareil virtuel Panorama :

   `show system disk details`

© 2020 Palo Alto Networks, Inc.

L'utilisateur verra la réponse suivante :

```
 Name
: sdb
 State : Present
 Size : 2048 MB
 Status : Available
 Reason : Admin enabled
 Name : sdc
 State : Present
 Size : 2048 MB
 Status : Available
 Reason : Admin disabled
```

3. Entrez la commande suivante et confirmez la requête lorsque vous y êtes invité pour tous les disques avec la réponse `Reason : Admin disabled` (Raison : Admin désactivé) :

   `request system disk add sdc`

   *La commande **`request system disk add`** n'est pas offert sur un serveur de gestion Panorama en mode Gestion uniquementm car la journalisation n'est pas prise en charge par ce mode. Si vous ne voyez pas la commande, il suffit de* Configurer un appareil virtuel Panorama en mode Panorama *pour activer les disques de journalisation. Une fois que vous passez en mode Panorama,* connecter à l'interface de ligne de commande Panorama *et passez à l'*étape 4 *pour vérifier l'ajout des disques.*
4. Saisissez la commande **`show system disk details`** pour vérifier l'état de l'ajout des disques. Passez à l'étape suivante lorsque toutes les réponses de disque nouvellement ajoutés affichent la réponse `Reason : Admin enabled`. (Raison : admin activé)

STEP 6 | Rendez les disques disponibles pour la journalisation.

1. Connectez-vous à l'interface Web Panorama.
2. Modifiez un Collecteur de journaux (**Panorama** > **Managed Collectors (Collecteurs gérés)**).
3. Sélectionnez **Disques** et **Add (Ajoutez)** chaque nouveau disque.
4. Cliquez sur **OK**.
5. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** et **Commit and Push (Validez et appliquez)** vos changements.

STEP 7 | (Nouveaux déploiements Panorama en mode Panorama uniquement) Configurez Panorama pour recevoir les journaux.

Si vous ajoutez des disques de journalisation à un appareil virtuel Panorama existant, passez à l'étape 8.

1. Configurer un groupe de collecteurs.
2. Configurer le transfert des journaux vers Panorama.

STEP 8 | Vérifiez que la capacité de stockage du journal de Panorama a été augmentée.

1. Connectez-vous à l'interface Web Panorama.
2. Sélectionnez le groupe de collecteurs auquel appartient l'appareil virtuel Panorama (**Panorama** > **Collector Groups (Groupe de collecteurs)**).
3. Vérifiez que la capacité de **Log Storage (Stockage des journaux)** affiche avec précision la capacité du disque.

© 2020 Palo Alto Networks, Inc.

Ajouter un disque virtuel à Panorama sur Hyper-V

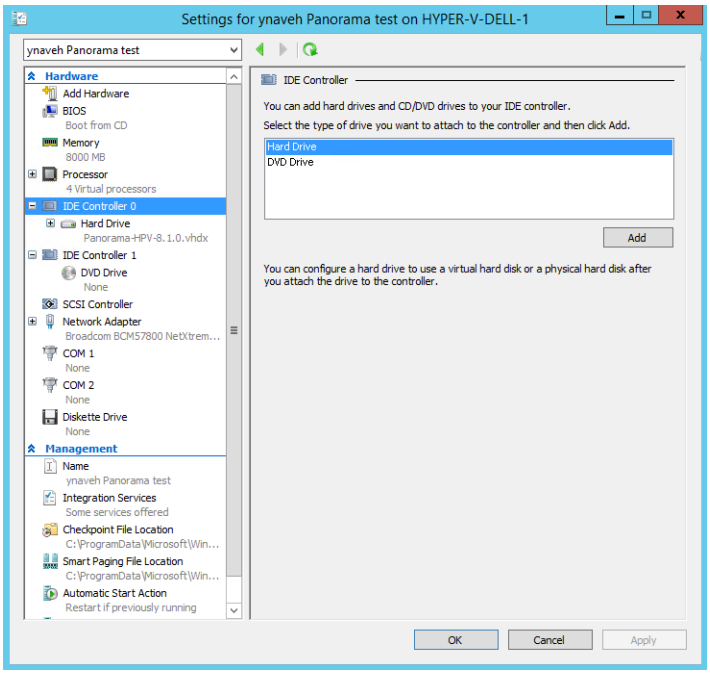
Après avoir Installer Panorama sur Hyper-V, ajoutez des disques de journalisation virtuels à l'instance de l'appareil virtuel Panorama ™ pour fournir le stockage des journaux générés par les pare-feu gérés. Vous pouvez ajouter des disques virtuels à un collecteur de journaux local pour un appareil virtuel Panorama en mode Panorama ou pour un collecteur de journaux dédié. L'appareil virtuel Panorama sur Hyper-V ne prend en charge que les disques de journalisation 2 To et prend en charge jusqu'à 24 To de stockage de journaux. Vous ne pouvez pas ajouter un disque de journalisation inférieur à 2 To ou un disque de journalisation dont la taille ne peut être divisée par 2 To, car l'appareil virtuel Panorama partitionne les disques de journalisation en partitions de 2 To. Par exemple, si vous joignez un disque de journalisation de 4 To, Panorama créera deux partitions de 2 To. Toutefois, vous ne pouvez pas ajouter un disque de journalisation de 5 To car les 1 To restants ne sont pas pris en charge en tant que partition.

STEP 1 | Mettez l'appareil virtuel Panorama hors tension.

1. Sur le gestionnaire Hyper-V, sélectionnez l'appareil virtuel Panorama dans la liste des **Virtual Machines (Machines virtuelles)**.
2. Sélectionnez **Action** > **Turn Off (Éteindre)** pour mettre l'instance de l'appareil virtuel Panorama hors tension.

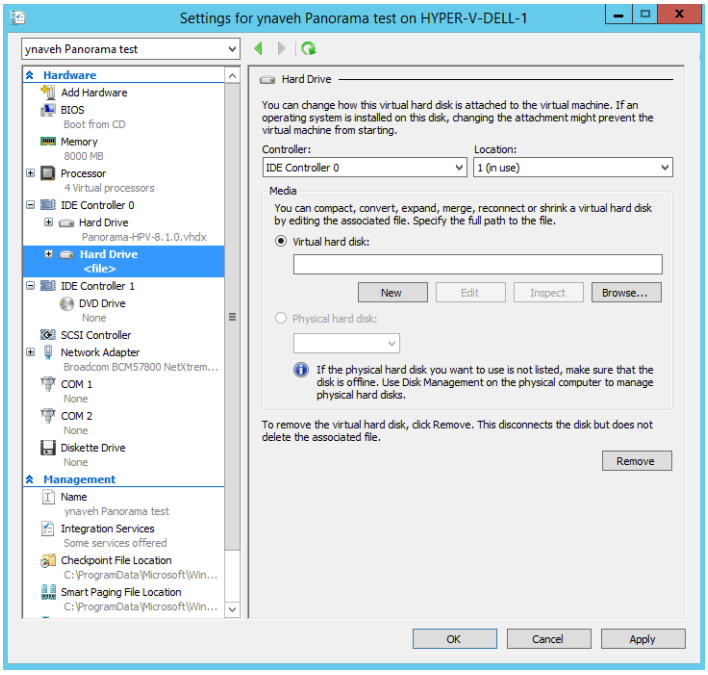
STEP 2 | Ajoutez les disques de journalisation virtuels. Répétez cette étape autant de fois que vous en avez besoin.

1. Sélectionnez l'appareil virtuel Panorama dans la liste **Virtual Machines (Machines virtuelles)**, puis sélectionnez **Action** > **Settings (Paramètres)**.
2. Dans la liste **Hardware (Matériel)**, sélectionnez **IDE Controller 0**.
3. Dans la liste des lecteurs **IDE Controller**, sélectionnez **Hard Drive (Disque dur)**, puis **Add (Ajoutez)** le nouveau disque de journalisation virtuel.



4. Sélectionnez le nouveau **Hard Drive (Disque dur)** créé sous **IDE Controller 0**.
5. Sous **Media**, ajoutez un **New (Nouveau)** disque dur.

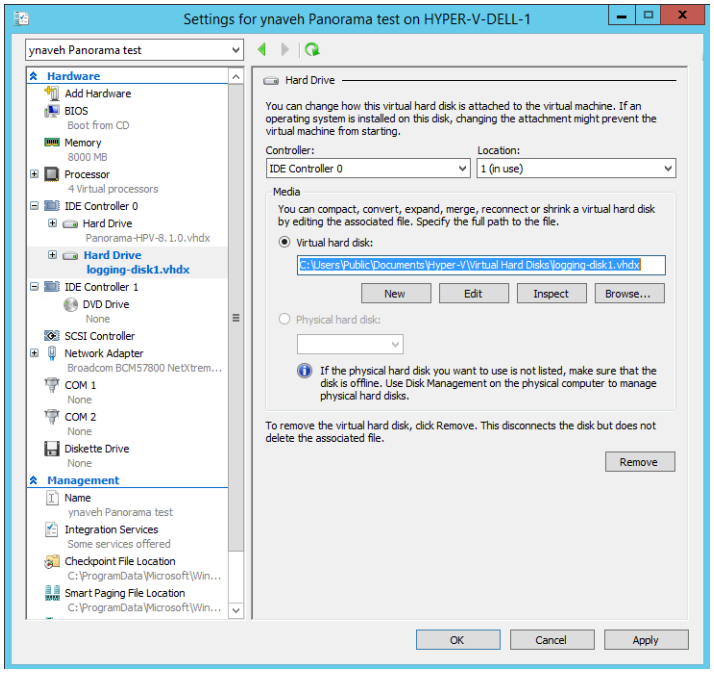
© 2020 Palo Alto Networks, Inc.



STEP 3 | Configurez le nouveau disque de journalisation virtuel.

1. Si l'invite Before You Begin (Avant de commencer) s'affiche, cliquez sur **Next (Suivant)** pour commencer l'ajout du disque de journalisation virtuel.
2. Comme format de disque, sélectionnez **VHDX**. Cliquez sur **Next (Suivant)** pour continuer
3. Comme type de disque, sélectionnez **Fixed Size (Taille fixe)** ou **Dynamically Expanding (Augmentant de manière dynamique)**, selon vos besoins. Cliquez sur **Next (Suivant)** pour continuer.
4. Précisez le **Name (Nom)** et le **Location (Emplacement)** du fichier du disque de journalisation virtuel. Cliquez sur **Next (Suivant)** pour continuer.
5. Pour configurer le disque, sélectionnez **Create a new virtual hard disk (Créer un nouveau disque dur virtuel)**, puis saisissez la taille du disque. Cliquez sur **Next (Suivant)** pour continuer.
6. Passez en revue le résumé et **Finish (Terminez)** l'ajout du disque dur de journalisation virtuel.
7. **Apply (Appliquez)** l'ajout du nouveau disque dur.

© 2020 Palo Alto Networks, Inc.



STEP 4 | Mettez l'appareil virtuel Panorama sous tension.

1. Sélectionnez l'appareil virtuel Panorama dans la liste des **Virtual Machines (Machines virtuelles)**.
2. Sélectionnez **Action** > **Start (Démarrer)** pour allumer l'instance de l'appareil virtuel Panorama.

STEP 5 | Configurez chaque disque.

L'exemple suivant utilise le disque virtuel sdc.

1. Connectez-vous à l'ILC de Panorama.
2. Entrez la commande suivante pour afficher les disques sur l'appareil virtuel Panorama :

   `show system disk details`

   L'utilisateur verra la réponse suivante :

```
 Name
: sdb
 State : Present
 Size : 2048 MB
 Status : Available
 Reason : Admin enabled
 Name : sdc
 State : Present
 Size : 2048 MB
 Status : Available
 Reason : Admin disabled
```

3. Entrez la commande suivante et confirmez la requête lorsque vous y êtes invité pour tous les disques avec la réponse `Reason : Admin disabled` (Raison : Admin désactivé) :

   `request system disk add sdc`

   *La commande **`request system disk add`** n'est pas offert sur un serveur de gestion Panorama en mode Gestion uniquementm car la journalisation n'est pas prise en charge par ce mode. Si vous ne voyez pas la commande, il suffit de Configurer un appareil virtuel Panorama en mode Panorama pour activer les disques de*

© 2020 Palo Alto Networks, Inc.

journalisation. Une fois que vous passez en mode Panorama, connecter à l'interface de ligne de commande Panorama *et passez à l'*étape 4 *pour vérifier l'ajout des disques.*

4. Saisissez la commande **`show system disk details`** pour vérifier l'état de l'ajout des disques. Passez à l'étape suivante lorsque toutes les réponses de disque nouvellement ajoutés affichent la réponse `Reason : Admin enabled`. (Raison : admin activé)

STEP 6 | Rendez les disques disponibles pour la journalisation.

1. Connectez-vous à l'interface Web Panorama.
2. Modifiez un Collecteur de journaux (**Panorama** > **Managed Collectors (Collecteurs gérés)**).
3. Sélectionnez **Disques** et **Add (Ajoutez)** chaque nouveau disque.
4. Cliquez sur **OK**.
5. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** et **Commit and Push (Validez et appliquez)** vos changements.

STEP 7 | (Nouveaux déploiements Panorama en mode Panorama uniquement) Configurez Panorama pour recevoir les journaux.

Si vous ajoutez des disques de journalisation à un appareil virtuel Panorama existant, passez à l'étape 8.

1. Configurer un groupe de collecteurs.
2. Configurer le transfert des journaux vers Panorama.

STEP 8 | Vérifiez que la capacité de stockage du journal de Panorama a été augmentée.

1. Connectez-vous à l'interface Web Panorama.
2. Sélectionnez le groupe de collecteurs auquel appartient l'appareil virtuel Panorama (**Panorama** > **Collector Groups (Groupe de collecteurs)**).
3. Vérifiez que la capacité de **Log Storage (Stockage des journaux)** affiche avec précision la capacité du disque.

Monter le serveur Panorama ESXi dans un serveur de données NFS

Lorsque l'appareil virtuel Panorama en mode hérité fonctionne sur un serveur ESXi, le montage à un magasin de données réseau (NFS) permet de se connecter à un emplacement centralisé et d'étendre la capacité de stockage du journal au-delà de ce qu'un disque virtuel prend en charge. (les versions 5.5 et ultérieures peuvent prendre en charge un disque virtuel pouvant aller jusqu'à 8 To.) Les versions antérieures d'ESXi prennent en charge un disque virtuel d'un maximum de 2 To. Avant la mise en place d'un magasin de donnée NFS dans une configuration Panorama haute disponibilité (HD), consultez Remarques sur la journalisation de Panorama en HD.



L'appareil virtuel Panorama en mode Panorama ne prend pas en charge NFS.

STEP 1 | Sélectionnez **Panorama** > **Setup (configuration)** > **Operations (Opérations)** et, dans la section Divers, cliquez sur **Storage Partition Setup (Configuration de la partition de stockage)**.

STEP 2 | Mettez la **Storage Partition (Partition de stockage)** tapez à **NFS V3**.

STEP 3 | Saisissez l'adresse IP du **Server (Serveur)** NFS.

STEP 4 | Entrez le **Log Directory (Directoire de Journaux)** chemin pour stocker les fichiers journaux. Par exemple, exportation / Panorama.

© 2020 Palo Alto Networks, Inc.

STEP 5 | Pour le **Protocol (Protocole)**, sélectionnez **TCP** ou **UDP** et entrez le **Port** pour accéder au serveur NFS.

Pour utiliser NFS sur TCP, le serveur NFS doit le prendre en charge. Les ports NFS communs portent le nom de UDP/TCP 111 pour RPC et UDP/TCP 2049 pour NFS.

STEP 6 | Pour optimiser les performances NFS, dans les**Read Size (Taille de Lecture)** et **Write Size (Taille d'écriture)** champs, préciser la taille maximale des blocs de données que le client et le serveur passent en arrière pour chaque autre. Définir une taille d'écriture / lecture optimise le volume de données et de la vitesse dans le transfert de données entre Panorama et le datastore NFS.

STEP 7 | (Facultatif) Sélectionnez **Copy On Setup (Copier lors de la configuration)** pour copier les journaux existants stockés sur Panorama au volume NFS. Si Panorama a beaucoup de journaux, cette option pourrait initier le transfert d'un grand volume de données.

STEP 8 | Cliquez **Test Logging Partition (Test de journalisation de Partition)** pour vérifier que Panorama peut accéder à la NFS **Server (Serveur)** et **Log Directory (Directoire de Journaux)**.

STEP 9 | Cliquez sur **OK** pour enregistrer vos modifications.

STEP 10 | Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements. Jusqu'à ce que vous redémarriez, l'appareil virtuel Panorama écrit les journaux sur le disque de stockage local.

STEP 11 | Sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)** et sélectionnez **Reboot Panorama (Redémarrer Panorama)** dans la section Opérations de périphérique. Après le redémarrage, Panorama commence à écrire des journaux sur le datastore NFS.

Augmenter les processeurs et la mémoire sur l'appareil virtuel Panorama

Lorsque vous effectuez la configuration initiale de l'appareil virtuel Panorama, vous spécifiez la mémoire et le nombre de processeurs selon que l'appareil est en mode Panorama ou en mode Gestion uniquement et en fonction de la capacité de stockage des journaux ou du nombre de pare-feu gérés. Si, ultérieurement, vous accroissez la capacité de stockage ou que vous ajoutez des pare-feu gérés, vous devez également augmenter la mémoire et les processeurs. Un appareil virtuel Panorama en mode collecteur de journaux doit répondre à la configuration système requise. Il n'est pas nécessaire d'augmenter le processeur et la mémoire au-delà de la configuration minimale requise. Consultez Définir la configuration requise pour l'appareil virtuel Panorama pour connaître les besoins en matière de processeur et de mémoire pour chaque mode Panorama.

- Augmentez les CPU et la mémoire pour Panorama sur un serveur ESXi
- Augmentez les CPUs et la mémoire pour panorama sur vCloud Air
- Augmenter les processeurs et la mémoire pour Panorama sur AWS
- Augmentez les CPUs et la mémoire pour Panorama sur Azure
- Augmenter les processeurs et la mémoire pour Panorama sur Google Cloud
- Augmentez les processeurs et la mémoire pour le panorama sur KVM
- Augmenter les processeurs et la mémoire pour Panorama sur Hyper-V

© 2020 Palo Alto Networks, Inc.

Augmentez les CPU et la mémoire pour Panorama sur un serveur ESXi

Pour les processeurs et la mémoire minimum requis par Panorama, consultez Augmenter les processeurs et la mémoire sur l'appareil virtuel Panorama.

STEP 1 | Accédez au client VMware vSphere et sélectionnez l'onglet **Virtual Machines (Machines virtuelles)**.

STEP 2 | Cliquez droit sur l'appareil virtuel Panorama et sélectionnez **Power (Alimentation)** > **Power Off (Mettre hors tension)**.

STEP 3 | Cliquez droit sur l'application virtuelle Panorama et sélectionnez **Edit Settings (Modifier les paramètres)**.

STEP 4 | Sélectionnez **Memory (Mémoire)** et entrez la nouvelle **Memory Size (Taille mémoire)**.

STEP 5 | Sélectionnez **CPUs (Processeurs)** et spécifiez le nombre de processeurs (le **Number of virtual sockets (Nombre de sockets virtuels)** multiplié par le **Number of cores per socket (Nombre de cœurs par socket)**).

STEP 6 | Cliquez sur **OK** pour enregistrer vos modifications.

STEP 7 | Cliquez droit sur l'appareil virtuel Panorama et sélectionnez **Power (Alimentation)** > **Power On (Mettre sous tension)**.

Augmentez les CPUs et la mémoire pour panorama sur vCloud Air

Pour les processeurs et la mémoire minimum requis par Panorama, consultez Augmenter les processeurs et la mémoire sur l'appareil virtuel Panorama.

STEP 1 | Accéder à la console Web vCloud Air et sélectionner votre **Virtual Private Cloud OnDemand (Cloud Virtuel Privé sur Demande)** région.

STEP 2 | Dans l'onglet **Virtual Machines (Machines virtuelles)**, sélectionnez la machine virtuelle Panorama et **Power Off (Mettre hors tension)**.

STEP 3 | Sélectionnez **Actions (Actions)** > **Edit Resources (Modifier les ressources)**.

STEP 4 | Définissez le **CPU (Processeur)** et la **Memory (Mémoire)**.

STEP 5 | Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.

STEP 6 | Sélectionnez la machine virtuelle Panorama et **Power On (Mettre sous tension)**.

Augmenter les processeurs et la mémoire pour Panorama sur AWS

Pour les processeurs et la mémoire minimum requis par Panorama ™, reportez-vous à la section Augmentation des processeurs et de la mémoire de l'appareil virtuel Panorama.

Un appareil virtuel Panorama en mode Collecteurs de journaux ne reste pas en mode Collecteurs de journaux si vous dimensionnez à nouveau la machine virtuelle après son déploiement et que cela peut entraîner une perte des données du journal.

STEP 1 | Connectez-vous à AWS Web Service Console et sélectionnez le tableau de bord EC2.

© 2020 Palo Alto Networks, Inc.

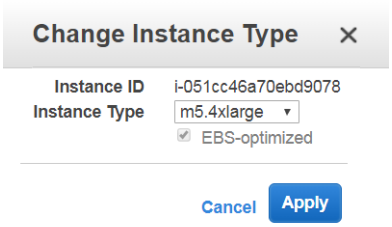
- Amazon Web Service Console
- AWS GovCloud Web Service Console

STEP 2 | Dans le tableau de bord EC2, sélectionnez **Instances** et sélectionnez l'instance de l'application virtuelle Panorama.

STEP 3 | Sélectionnez **Actions** > **Instance State (Etat de l'instance)** > **Stop (Arrêt)** pour mettre l'instance d'appareil virtuel Panorama hors tension.

STEP 4 | Sélectionnez **Actions** > **Instance Settings (Paramètres de l'instance)** > **Change Instance Type (Modifier le type d'instance)** pour changer le type d'instance de l'appareil virtuel Panorama.

STEP 5 | Sélectionnez le **Instance Type (Type d'instance)** sur lequel vous voulez effectuer une mise à jour et cliquez sur **Apply (Exécuter)**.



STEP 6 | Sélectionnez **Actions** > **Instance State (Etat de l'instance)** > **Start (Démarrer)** pour mettre l'instance d'appareil virtuel Panorama hors tension.

Augmentez les CPUs et la mémoire pour Panorama sur Azure

Pour les processeurs et la mémoire minimum requis par Panorama ™, reportez-vous à la section Augmentation des processeurs et de la mémoire de l'appareil virtuel Panorama.

Un appareil virtuel Panorama en mode Collecteurs de journaux ne reste pas en mode Collecteurs de journaux si vous dimensionnez à nouveau la machine virtuelle après son déploiement et que cela peut entraîner une perte des données du journal.

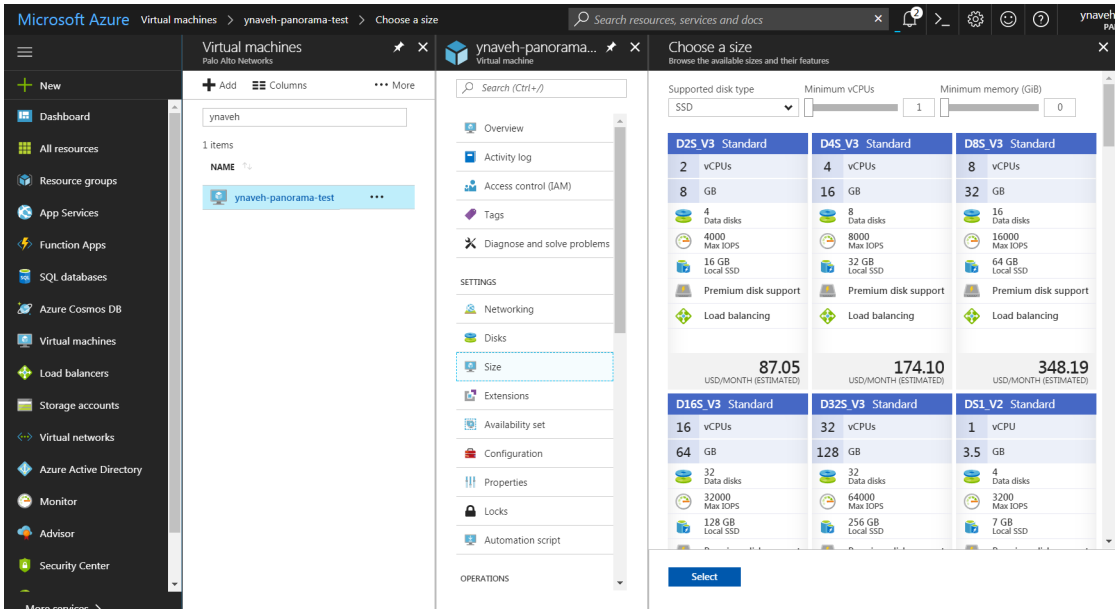
STEP 1 | Connectez-vous au Portail Microsoft Azure.

STEP 2 | Dans le tableau de bord Azure, sélectionnez **Virtual Machines (Machines virtuelles)** et sélectionnez l'instance de l'application virtuelle Panorama.

STEP 3 | Sélectionnez **Overview (Aperçu)** et **Stop (Arrêter)** l'application virtuelle Panorama.

STEP 4 | Choisissez la **taille** de la nouvelle machine virtuelle et ensuite **sélectionnez**.

© 2020 Palo Alto Networks, Inc.



STEP 5 | Sélectionnez **Overview (Aperçu)** et **Start (Démarrer)** l'application virtuelle Panorama.

Augmenter les processeurs et la mémoire pour Panorama sur Google Cloud

Pour les processeurs et la mémoire minimum requis par Panorama ™, reportez-vous à la section Augmentation des processeurs et de la mémoire de l'appareil virtuel Panorama.

Un appareil virtuel Panorama en mode Collecteurs de journaux ne reste pas en mode Collecteurs de journaux si vous dimensionnez à nouveau la machine virtuelle après son déploiement et que cela peut entraîner une perte des données du journal.

STEP 1 | Connectez-vous à Google Cloud Console.

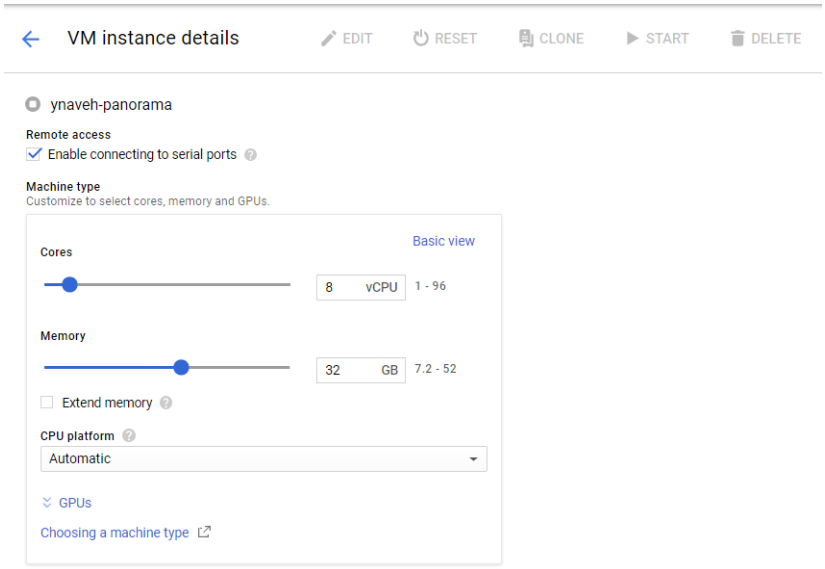
STEP 2 | Arrêtez l'instance de l'appareil virtuel Panorama.

1. Sélectionnez l'instance de l'appareil virtuel Panorama dans le menu Products & Services (Produits et Services) (**Compute Engine (Moteur de calcul)** > **VM Instances (instance de machine virtuelle)**).
2. **Stop (Arrêtez)** l'instance de l'appareil virtuel Panorama. Cela peut prendre de 2 à 3 minutes pour que l'application virtuelle Panorama s'éteigne complètement.

STEP 3 | Reconfigurez les ressources de l'application virtuelle Panorama.

1. **Edit (Modifiez)**les détails de l'instance de l'appareil virtuel Panorama.
2. Sous Type de machine, **personnalisez** les cœurs et la mémoire du processeur de l'appareil virtuel Panorama.

© 2020 Palo Alto Networks, Inc.



STEP 4 | **Save (Enregistrez)** les modifications pour mettre à jour l'instance de l'appareil virtuel Panorama.

STEP 5 | **Start (Démarrez)** l'appareil virtuel Panorama.

Augmentez les processeurs et la mémoire pour le panorama sur KVM

Pour les processeurs et la mémoire minimum requis par Panorama ™, reportez-vous à la section Augmentation des processeurs et de la mémoire de l'appareil virtuel Panorama.

Un appareil virtuel Panorama en mode Collecteurs de journaux ne reste pas en mode Collecteurs de journaux si vous dimensionnez à nouveau la machine virtuelle après son déploiement et que cela peut entraîner une perte des données du journal.

STEP 1 | **Shutdown (Arrêtez)** l'instance de l'appareil virtuel Panorama sur le Virtual Machine Manager (Gestionnaire de machine virtuelle).

STEP 2 | Double-cliquez sur l'instance de l'appareil virtuel Panorama dans le Virtual Machine Manager (Gestionnaire de machine virtuelle) et **Show virtual hardware details (Affichez les détails de la machine virtuelle)** .

STEP 3 | Modifiez les cœurs du processeur à allouer à l'appareil virtuel Panorama.

1. Éditez les **CPUs** actuellement alloués.
2. **Appliquez** l'allocation de base du processeur reconfigurée.

STEP 4 | Modifiez la mémoire de l'appareil virtuel Panorama allouée.

1. Éditez la **mémoire** actuellement allouée.
2. **Appliquez** l'allocation mémoire reconfigurée.

STEP 5 | Mettez l'appareil virtuel Panorama **Power on (sous tension)**

Augmenter les processeurs et la mémoire pour Panorama sur Hyper-V

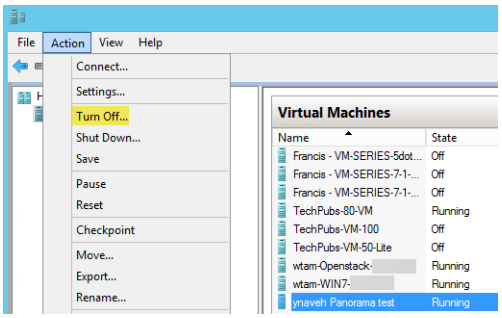
Pour les processeurs et la mémoire minimum requis par Panorama ™, reportez-vous à la section Augmentation des processeurs et de la mémoire de l'appareil virtuel Panorama.

© 2020 Palo Alto Networks, Inc.

Un appareil virtuel Panorama en mode Collecteurs de journaux ne reste pas en mode Collecteurs de journaux si vous dimensionnez à nouveau la machine virtuelle après son déploiement et que cela peut entraîner une perte des données du journal.

STEP 1 | Mettez l'appareil virtuel Panorama hors tension.

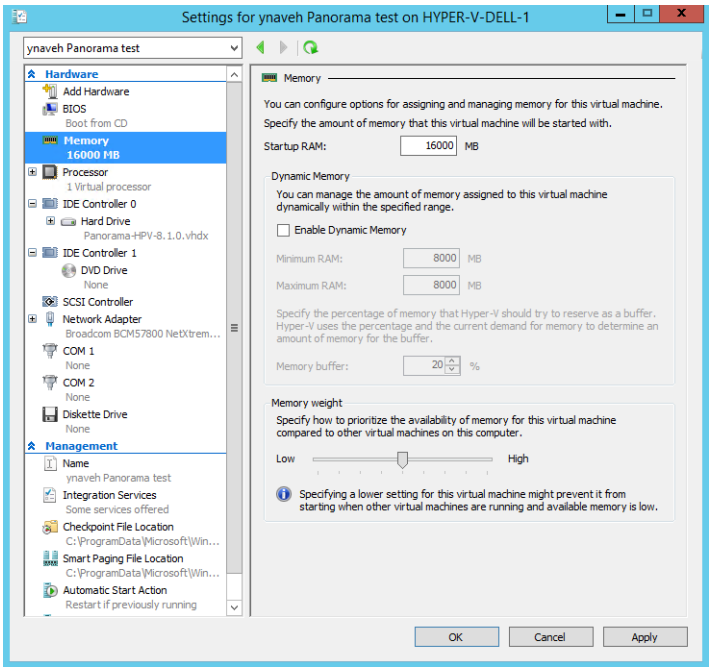
1. Sur le gestionnaire Hyper-V, sélectionnez l'appareil virtuel Panorama dans la liste des **Virtual Machines (Machines virtuelles)**.
2. Sélectionnez **Action** > **Turn Off (Éteindre)** pour mettre l'instance de l'appareil virtuel Panorama hors tension.



STEP 2 | Sur le gestionnaire Hyper-V, sélectionnez l'instance d'appareil virtuel Panorama dans la liste **Virtual Machines (Machines virtuelles)**, puis sélectionnez **Action** > **Settings (Paramètres)** pour modifier les ressources de l'appareil virtuel Panorama.

STEP 3 | Modifiez la mémoire de l'appareil virtuel Panorama allouée.

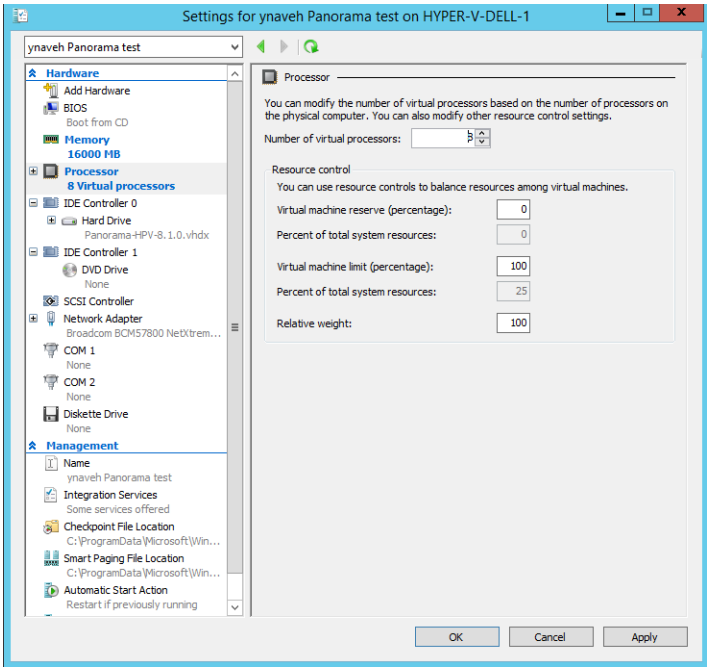
1. Dans la liste **Hardware (Matériel)**, sélectionnez **Memory (Mémoire)**.
2. Modifiez la **Startup RAM (Mémoire vive au démarrage)** actuellement allouée.



STEP 4 | Modifiez les cœurs du processeur à allouer à l'appareil virtuel Panorama.

1. Dans la liste **Hardware (Matériel)**, sélectionnez **Processor (Processus)**.
2. Modifiez le **Number of virtual processors (Nombre de processus virtuels)** actuellement alloués.

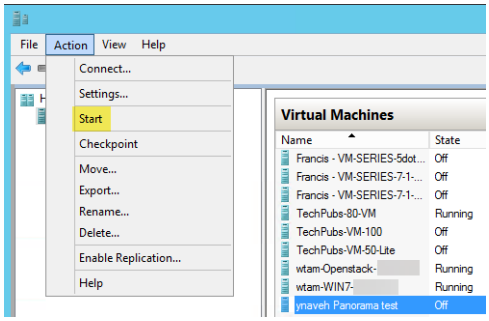
© 2020 Palo Alto Networks, Inc.



STEP 5 | **Apply (Appliquez)** la mémoire et les cœurs réalloués.

STEP 6 | Mettez l'appareil virtuel Panorama sous tension.

1. Sélectionnez l'appareil virtuel Panorama dans la liste des **Virtual Machines (Machines virtuelles)**.
2. Sélectionnez **Action** > **Start (Démarrer)** pour allumer l'instance de l'appareil virtuel Panorama.



Augmentation du disque système sur l'appareil virtuel Panorama

Augmentez la capacité du disque système à 224 Go pour l'appareil virtuel Panorama afin de prendre en charge de grands ensembles de données et de disposer d'un espace disque suffisant pour des éléments tels que les mises à jour dynamiques lorsque vous Gérer les déploiements de pare-feu à grande échelle. Par ailleurs, un disque système de 224 Go permet d'augmenter le stockage des données de surveillance et de rapport sur l'état du pare-feu géré si vous avez l'intention d'utiliser l'appareil virtuel Panorama en mode Panorama pour gérer votre déploiement SD-WAN.

- Augmentation du disque système pour Panorama sur un serveur ESXi
- Augmentation du disque système pour Panorama sur Google Cloud Platform

© 2020 Palo Alto Networks, Inc.

Augmentation du disque système pour Panorama sur un serveur ESXi

Ajoutez un disque système de 224 Go pour remplacer le disque système par défaut de 81 Go. Pour connaître les exigences minimales en matière de ressources pour l'appareil virtuel Panorama, voir la section Définir la configuration requise pour l'appareil virtuel Panorama.

La réduction du disque du système d'appareils virtuels Panorama à 81 Go n'est pas prise en charge.

STEP 1 | (Bonnes pratiques) Sauvegarde et exportation de configurations de pare-feu et de Panorama.

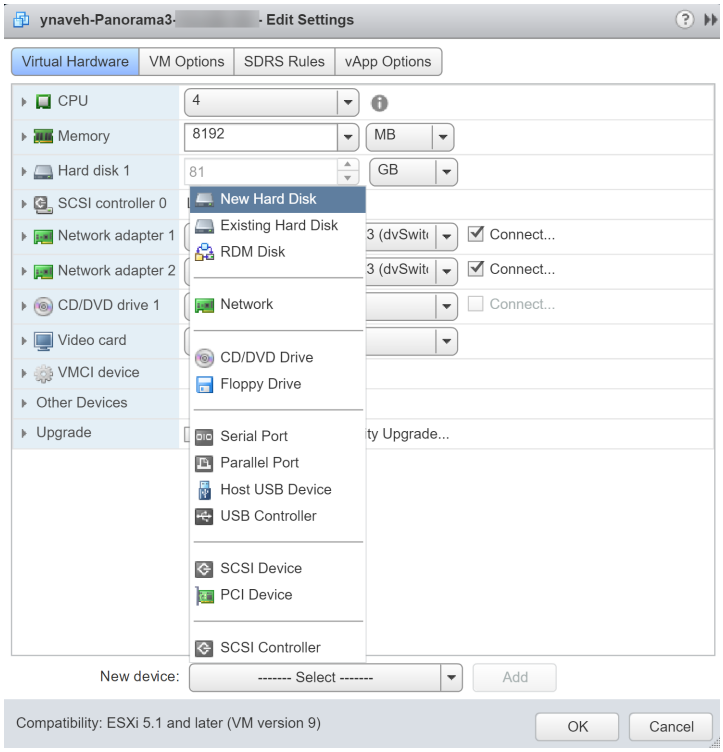
Enregistrez et exportez votre configuration de Panorama et de pare-feu pour vous assurer de pouvoir restaurer Panorama si vous rencontrez des problèmes.

STEP 2 | Accédez au client VMware vSphere et naviguez vers votre appareil virtuel Panorama.

STEP 3 | Faites un clic droit sur l'appareil virtuel Panorama et sélectionnez **Power (Alimentation)** > **Power Off (Mettre hors tension)**.

STEP 4 | Ajoutez le nouveau disque système de 224 Go.

1. Cliquez droit sur l'appareil virtuel Panorama et sélectionnez **Edit Settings (Modifier les paramètres)**.
2. Sélectionnez **New Hard Disk (Nouveau disque dur)** en tant que **New Device (Nouveau périphérique)** et **Add (Ajoutez)** le nouveau périphérique.
3. Configurez le nouveau disque dur de 224 Go et cliquez sur **OK**.



STEP 5 | Cliquez droit sur l'appareil virtuel Panorama et sélectionnez **Power (Alimentation)** > **Power On (Mettre sous tension)**.

Panorama peut prendre jusqu'à 30 minutes pour initialiser le nouveau disque système. Pendant ce temps, l'interface web Panorama et le CLI demeurent indisponibles.

© 2020 Palo Alto Networks, Inc.

STEP 6 | Migrez les données de l'ancien disque système vers le nouveau disque système.

Dans cet exemple, nous migrons vers le disque système nouvellement ajouté, appelé sdb.

1. Connectez-vous à l'ILC Panorama.
2. Saisissez la commande suivante pour afficher les disques système disponibles pour la migration :

```
admin> request system clone-system-disk target ?
```

3. Migrez les données du disque vers le nouveau disque système en utilisant la commande suivante :

```
admin> request system clone-system-disk target sdb
```

Saisissez **Y** lorsque vous êtes invité à lancer la migration du disque.

Pour commencer la migration, Panorama redémarre puis prend au moins 20 minutes pour terminer la migration du disque. Pendant ce temps, l'interface web Panorama et le CLI demeurent indisponibles.

4. Surveillez la migration des disques à partir de la console web. Passez à l'étape suivante uniquement lorsque Panorama affiche le message qui suit vous indiquant que la migration du disque est terminée.

```
==================================
Disk Cloning Utility (Version 1.0)
==================================
SOURCE - Disk sda (82944 MB)
TARGET - Disk sdb (229376 MB)

Gathering disks info
Finished gathering disks info

Preparing disks
Finished preparing disks

Copying data
Finished copying data

Making disk bootable
Finished making disk bootable

Disk cloning procedure completed. Please shutdown the sytem and switch disks..._
```

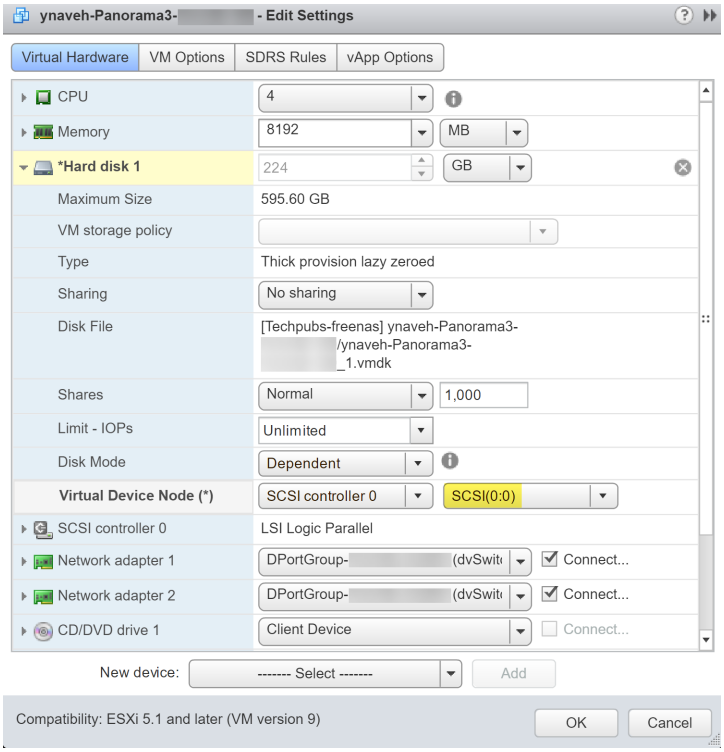
STEP 7 | Supprimez l'ancien disque système.

1. Accédez au client VMware vSphere et naviguez vers votre appareil virtuel Panorama.
2. Faites un clic droit sur l'appareil virtuel Panorama et sélectionnez **Power (Alimentation)** > **Power Off (Mettre hors tension)**.
3. Cliquez droit sur l'appareil virtuel Panorama et sélectionnez **Edit Settings (Modifier les paramètres)**.
4. Supprimez l'ancien disque système de 81 Go et cliquez sur **OK**.

STEP 8 | Modifiez le nœud de périphérique virtuel pour le nouveau disque système.

1. Développez les options de paramétrage du nouveau disque système.
2. Sélectionnez **SCSI(0:0)** comme le **nœud de périphérique virtuel**.
3. Cliquez sur **OK** pour enregistrer votre configuration.

© 2020 Palo Alto Networks, Inc.



STEP 9 | Cliquez droit sur l'appareil virtuel Panorama et sélectionnez **Power (Alimentation)** > **Power On (Mettre sous tension)**.

STEP 10 | Vérifiez que vous avez migré avec succès vers le nouveau disque système.

1. Connectez-vous à l'ILC Panorama.
2. Saisissez la commande suivante pour afficher les partitions du disque système.

   Vous devez ajouter les partitions `/dev/root`, `/dev/sda5`, `/dev/sda6`, et `/dev/sda8` pour confirmer que la taille du disque est augmentée.

```
admin> show system disk-space
```

```
admin@Panorama-Ynaveh> show system disk-space

Filesystem      Size  Used Avail Use% Mounted on
/dev/root        16G  3.4G   12G  23% /
none            4.0G   60K  4.0G   1% /dev
/dev/sda5        76G  1.8G   71G   3% /opt/pancfg
/dev/sda6        23G  5.0G   17G  24% /opt/panrepo
tmpfs           4.0G  110M  3.8G   3% /dev/shm
cgroup_root     4.0G     0  4.0G   0% /cgroup
/dev/sda8        92G   52G   35G  60% /opt/panlogs
/dev/loop0       50G  7.4G   40G  16% /opt/mongobuffer
tmpfs            12M     0   12M   0% /opt/pancfg/mgmt/ssl/private
```

Augmentation du disque système pour Panorama sur Google Cloud Platform

Ajoutez un disque système de 224 Go pour remplacer le disque système par défaut de 81 Go. Pour connaître les exigences minimales en matière de ressources pour l'appareil virtuel Panorama, voir la section Définir la configuration requise pour l'appareil virtuel Panorama.

© 2020 Palo Alto Networks, Inc.

STEP 1 | (Bonnes pratiques) Sauvegarde et exportation de configurations de pare-feu et de Panorama.

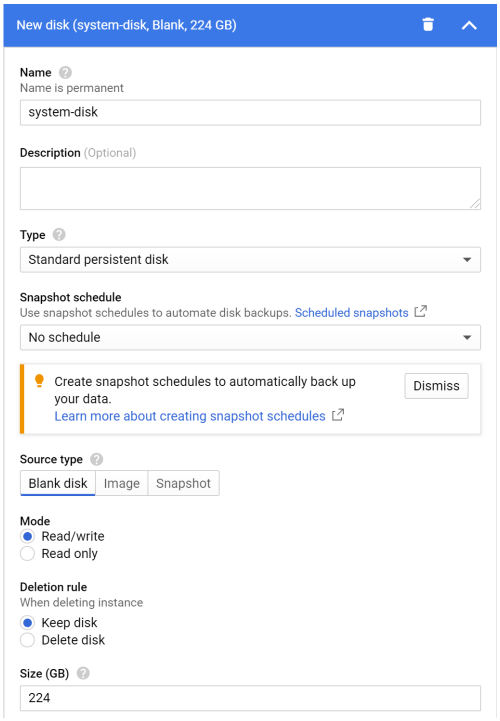
Enregistrez et exportez votre configuration de Panorama et de pare-feu pour vous assurer de pouvoir restaurer Panorama si vous rencontrez des problèmes.

STEP 2 | Connectez-vous à Google Cloud Console.

STEP 3 | Dans **VM Instances (Instances VM)**, **Stop (Arrêtez)** l'instance VM de Panorama.

STEP 4 | Ajoutez le nouveau disque système de 224 Go.

1. Sélectionnez l'instance VM de Panorama et sélectionnez **Edit (Editer)**.
2. À la section **Additional disks (Disques additionnels)**, **Add new disk (Ajoutez un nouveau disque)**.
3. Configurez le nouveau disque de 224 Go et cliquez sur **OK**.



STEP 5 | Dans **VM Instances (Instances VM)**, **Start (Lancez)** l'instance VM de Panorama.

STEP 6 | Migrez les données de l'ancien disque système vers le nouveau disque système.

Dans cet exemple, nous migrons vers le disque système nouvellement ajouté, appelé sdb.

1. Connectez-vous à l'ILC Panorama.
2. Saisissez la commande suivante pour afficher les disques système disponibles pour la migration :

```
admin> request system clone-system-disk target ?
```

3. Migrez les données du disque vers le nouveau disque système en utilisant la commande suivante :

```
admin> request system clone-system-disk target sdb
```

Saisissez **Y** lorsque vous êtes invité à lancer la migration du disque.

© 2020 Palo Alto Networks, Inc.

Pour commencer la migration, Panorama redémarre puis prend au moins 20 minutes pour terminer la migration du disque. Pendant ce temps, l'interface web Panorama et le CLI demeurent indisponibles.

4. Surveillez la migration des disques en essayant de vous connecter à la CLI Panorama. Le serveur de gestion Panorama passe en mode Maintenance une fois la migration du disque système terminée ce qui vous permettra de vous connecter à la CLI Panorama en mode Maintenance.

STEP 7 | Joignez le nouveau disque système de 224 Go.

1. Dans **VM Instances (Instances VM)**, **Stop (Arrêtez)** l'instance VM de Panorama.
2. Sélectionnez l'instance VM de Panorama et sélectionnez **Edit (Editer)**.
3. À la section **Additional disks (Disques supplémentaires)**, détachez le nouveau disque système de 224 Go.
4. À la section **Boot Disk (Disque de démarrage)** , détachez l'ancien disque système de 81 Go.
5. À la section **Boot Disk (Disque de démarrage)**, **Add item (Ajoutez un élément)** et sélectionnez le nouveau disque système de 224 Go.
6. **Save (Enregistrez)** les modifications de configuration.

STEP 8 | Dans **VM Instances (Instances VM)**, **Start (Lancez)** l'instance VM de Panorama.

STEP 9 | Vérifiez que vous avez migré avec succès vers le nouveau disque système.

1. Connectez-vous à l'ILC Panorama.
2. Saisissez la commande suivante pour afficher les partitions du disque système.

   Vous devez ajouter les partitions `/dev/root`, `/dev/sda5`, `/dev/sda6`, et `/dev/sda8` pour confirmer que la taille du disque est augmentée.

```
admin> show system disk-space
```

```
admin@Panorama-Ynaveh> show system disk-space

Filesystem      Size  Used Avail Use% Mounted on
/dev/root        16G  3.4G   12G  23% /
none            4.0G   60K  4.0G   1% /dev
/dev/sda5        76G  1.8G   71G   3% /opt/pancfg
/dev/sda6        23G  5.0G   17G  24% /opt/panrepo
tmpfs           4.0G  110M  3.8G   3% /dev/shm
cgroup_root     4.0G     0  4.0G   0% /cgroup
/dev/sda8        92G   52G   35G  60% /opt/panlogs
/dev/loop0       50G  7.4G   40G  16% /opt/mongobuffer
tmpfs            12M     0   12M   0% /opt/pancfg/mgmt/ssl/private
```

Terminer le programme d'installation de l'appareil virtuel Panorama

Après l'étape Effectuer la configuration initiale de l'appareil virtuel Panorama, poursuivez avec les tâches suivantes pour une configuration supplémentaire :

- Activer une licence d'assistance Panorama
- Activer / Récupérer une licence de gestion de pare-feu lorsque l'appareil virtuel Panorama est connectée à Internet.
- Installer les mises à jour de contenu et logicielles pour Panorama
- Accéder et naviguer dans les interfaces de gestion de Panorama
- Configurer l'accès administratif à Panorama
- Gérer les pare-feu

© 2020 Palo Alto Networks, Inc.

Configuration de l'appareil de série M

Les appareils M-600, M-500, M-200 et M-100 sont des appareils matériels haute performance que vous pouvez déployer en mode Gestionnaire uniquement (en tant que serveurs de gestion Panorama sans collection de journaux locaux), Panorama (en tant que serveurs de gestion Panorama avec collection de journaux locaux) ou en mode Collecteur de journaux (en tant que collecteurs de journaux dédiés). Les appareils fournissent plusieurs interfaces que vous pouvez affecter à divers services Panorama, tels que la gestion de pare-feu et la collecte de journaux. Avant de configurer l'appareil, examinez comment vous pouvez configurer les interfaces pour optimiser la sécurité, activer la segmentation du réseau (dans les déploiements à grande échelle) et équilibrer la charge du trafic pour les services Panorama.

- Interfaces de l'appareil de série M
- Effectuer la configuration initiale de l'appareil de série M
- Présentation de la configuration de la série M
- Configurer l'appareil de série M en tant que collecteur de journaux
- Augmenter le stockage sur l'appareil de série M
- Configurer Panorama pour l'utilisation de plusieurs interfaces

Interfaces de l'appareil de série M

Les appareils Panorama M-600, M-500, M-200 et M-100 disposent de plusieurs interfaces pour communiquer avec d'autres systèmes tels que les pare-feu gérés et les systèmes clients des administrateurs Panorama. Panorama communique avec ces systèmes pour exécuter différents services, notamment la gestion des périphériques (pare-feu, collecteurs de journaux et groupes de périphériques), la collecte de journaux, la communication avec les groupes de collecteurs et le déploiement de mises à jour de logiciels et de contenu. Par défaut, Panorama utilise son interface de gestion (MGT) pour tous ces services. Cependant, vous pouvez améliorer la sécurité en réservant l'interface MGT à l'accès administratif et en dédiant des interfaces distinctes pour les autres services. Dans un réseau à grande échelle avec plusieurs sous-réseaux et un trafic de journaux important, l'utilisation de plusieurs interfaces pour la gestion des périphériques et la collecte de journaux permet également la segmentation du réseau et l'équilibrage de charge (voir Configurer le Panorama pour utiliser plusieurs interfaces).

Lorsque vous affectez des services Panorama à différentes interfaces, gardez à l'esprit que seule l'interface MGT permet un accès administratif à Panorama pour les tâches de configuration et de surveillance. Vous pouvez affecter n'importe quelle interface aux autres services lorsque vous effectuez la configuration initiale de l'appareil M-Series. Les Guides de référence des appareils de la série M expliquent où fixer les câbles pour ces interfaces. L'appareil M-100 prend en charge un débit de 1 Gbit/s sur toutes ses interfaces : MGT, Eth1, Eth2 et Eth3. En plus de ces interfaces, l'appareil M-500 prend en charge un débit de 10 Gbit/s sur ses interfaces Eth4 et Eth5.

Les appareils de série M ne prennent pas en charge le protocole LACP (Link Aggregation Control Protocol) pour agréger les interfaces.

Interfaces prises en charge

Les interfaces peuvent être utilisées pour la gestion des périphériques, la collecte des journaux, la communication avec les groupes de collecteurs, les licences et les mises à jour logicielles. Consultez la section Configurer Panorama pour l'utilisation de plusieurs interfaces pour obtenir de plus amples renseignements sur la segmentation réseau.

© 2020 Palo Alto Networks, Inc.

Interface	Vitesse maximum	Appareil M-600	Appareil M-500	Appareil M-200
Management (MGT)	1 Gbits/s	✓	✓	✓
Ethernet 1 (Eth1)	1 Gbits/s	✓	✓	✓
Ethernet 2 (Eth2)	1 Gbits/s	✓	✓	✓
Ethernet 3 (Eth3)	1 Gbits/s	✓	✓	✓
Ethernet 4 (Eth4)	10 Gbits/s	✓	✓	—
Ethernet 5 (Eth5)	10 Gbits/s	✓	✓	—

Taux de journalisation

Passez en revue les taux de journalisation de tous les modèles d'appareils de série M. Pour atteindre les taux de journalisation indiqués ci-dessous, l'appareil M-Series doit être un collecteur de journaux unique dans un groupe de collecteurs et vous devez installer tous les disques de journalisation pour votre modèle M-Series. À titre d'exemple, pour atteindre 30 000 journaux/seconde pour l'appareil M-500, vous devez installer les 12 disques de journalisation avec des disques de 1 To ou de 2 To.

Capacités et fonctionnalités du modèle	Appareil M-600	Appareil M-500	Appareil M-200
Taux de journalisation maximum pour Panorama en mode Gestion uniquement	Le stockage des journaux locaux n'est pas pris en charge		
Taux de journalisation maximal pour Panorama en mode Panorama	25 000 journaux / seconde	20.000 journaux / seconde	10 000 journaux / seconde
Taux de journalisation maximal pour Panorama en mode Collecteur de journaux	50 000 journaux / seconde	30 000 journaux / seconde	28 000 journaux / seconde
Stockage maximum de journaux sur le modèle	48 To (12 disques RAID de 8 To)	• 24 To (24 disques RAID de 2 To) • 12 To (24 disques RAID de 1 To)	16 To (4 disques RAID de 8 To)
Stockage par défaut de journaux sur le modèle	16 To (4 disques RAID de 8 To)	4 To (4 disques RAID de 2 To)	16 To (4 disques RAID de 8 To)
Stockage SSD sur le modèle (pour les journaux que les appareils de série M génèrent)	240 Go	240 Go	240 Go

© 2020 Palo Alto Networks, Inc.

Capacités et fonctionnalités du modèle	Appareil M-600	Appareil M-500	Appareil M-200
Stockage de journaux attaché NFS	Non disponible		

Effectuer la configuration initiale de l'appareil de série M

Par défaut, Panorama a pour adresse IP 192.168.1.1 et pour nom d'utilisateur/mot de passe admin/admin. Pour des raisons de sécurité, vous devez modifier ces paramètres avant de passer aux autres tâches de configuration. Vous devez effectuer ces tâches de configuration initiales à partir de l'interface de gestion (MGT) ou à l'aide d'une connexion de port série directe au port de console sur l'appareil M-600, M-500 ou M-200.

Si vous configurez un appareil M-Series en mode Colleteur de journaux avec des interfaces de 10 Go, vous devez effectuer la totalité de cette procédure de configuration pour les interfaces de 10 GB pour qu'elles s'affichent en `Haut`.

STEP 1 | Contactez votre administrateur réseau pour obtenir les informations requises sur l'interface et le serveur.

- Rassemblez l'adresse IP, le masque réseau (pour IPv4) ou la longueur du préfixe (pour IPv6) et la passerelle par défaut pour chaque interface que vous envisagez de configurer (MGT, Eth1, Eth2, Eth3, Eth4, Eth5). Seule l'interface MGT est obligatoire.

  Palo Alto Networks vous recommande de spécifier tous ces paramètres pour l'interface MGT. Si vous omettez des valeurs pour certains de ces paramètres (comme la passerelle par défaut), vous pouvez uniquement accéder à Panorama via le port de la console pour des modifications ultérieures de la configuration. Vous ne pouvez pas valider les configurations pour d'autres interfaces, sauf si vous spécifiez tous ces paramètres.

  Si vous envisagez d'utiliser l'appareil en tant que serveur de gestion Panorama, Palo Alto Networks recommande d'utiliser l'interface MGT uniquement pour gérer Panorama et d'utiliser d'autres interfaces pour gérer les périphériques, collecter les journaux, communiquer avec les groupes de collecteurs et déployer des mises à jour (voir Interfaces de l'appareil de série M).
- Obtenez les adresses IP des serveurs DNS.

STEP 2 | Accéder l'appareil de série M à partir de votre ordinateur.

1. Connectez-vous à l'appareil de série M d'une des façons suivantes :
   - Fixer un câble série à partir d'un ordinateur au port console sur l'appareil de série M et se connecter en utilisant un logiciel d'émulation de terminal (9600-8-N-1).
   - Fixer un câble Ethernet RJ-45 depuis un ordinateur au port MGT sur Attach an RJ-45 Ethernet cable from a computer to the MGT port sur l'appareil de série M. Depuis un navigateur, accédez à https://192.168.1.1. Permettre l'accès à cette URL pourrait nécessiter de modifier l'adresse IP de l'ordinateur à une adresse dans le réseau 192.168.1.0 (par exemple, 192.168.1.2).
2. Lorsque vous êtes invité, connectez-vous à l'appareil en utilisant le nom d'utilisateur par défaut et le mot de passe (admin / admin). L'appareil démarre l'initialisation.

STEP 3 | Changez le mot de passe administrateur par défaut.

© 2020 Palo Alto Networks, Inc.

À partir de PAN-OS 9.0.4, le mot de passe de l'administrateur prédéfini par défaut (admin/admin) doit être modifié lors de la première connexion à l'appareil. Le nouveau mot de passe doit comporter au moins huit caractères et comprendre au moins une lettre minuscule et une lettre majuscule ainsi qu'un chiffre ou un caractère spécial.

Veillez à respecter les bonnes pratiques en matière de robustesse des mots de passe *pour vous assurer de créer un mot de passe fort et de revoir les* paramètres de complexité des mots de passe*.*

1. Cliquez sur le lien **admin** dans le coin inférieur gauche de la console de gestion.
2. Saisissez l'**Old Password (ancien mot de passe)**, le **New Password (Nouveau mot de passe)** et **Confirm New Password (Confirmez le nouveau mot de passe)**, puis cliquez sur **OK**. Stockez le nouveau mot de passe dans un emplacement sécurisé.

Pour vous assurer que l'interface MGT reste sécurisée, configurez les paramètres minimaux de complexité du mot de passe (sélectionnez Panorama > Setup (Configuration) > Management (Gestion)) et spécifiez l'intervalle auquel les administrateurs doivent modifier leurs mots de passe.

STEP 4 | Configurez les paramètres d'accès au réseau pour chaque interface que vous utiliserez pour gérer Panorama, gérer les périphériques, collecter les journaux, communiquer avec les groupes de collecteurs et déployer des mises à jour sur les périphériques.

1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Interfaces** et cliquez sur le nom de l'interface.
2. (Interfaces non-MGT seulement) **Enable (Activez)** l'interface.
3. Modifiez les paramètres d'accès au réseau de chaque interface utilisée par Panorama. Seule l'interface MGT est obligatoire. Les interfaces Eth1, Eth2, Eth3, Eth4 et Eth5 sont facultatives et ne s'appliquent que si vous prévoyez d'utiliser l'appareil de série M comme serveur de gestion de Panorama.
   1. Remplissez un ou les deux des ensembles de champs suivants, selon les protocoles IP de votre réseau :

      IPv4 : **Adresse publique IP**, **Adresse IP**, **Masque de réseau**, et **passerelle par défaut**

      Si votre pare-feu se connecte au serveur de gestion Panorama au moyen d'une adresse IP publique qui est traduite en une adresse IP privée (NAT), saisissez l'adresse IP publique dans le champ Public IP Address (Adresse IP publique) et l'adresse IP privée dans le champ IP Address (Adresse IP) pour transmettre les deux adresses à vos pare-feu.

      IPv6 : **IPv6 Address/Prefix Length (Longueur du préfixe / de l'adresse IPv6)** et **Default IPv6 Gateway (Passerelle IPv6 par défaut)**
   2. Sélectionnez les services de gestion de périphériques pris en charge par l'interface :

      Device Management and Device Log Collection (Gestion des périphériques et collecte des journaux de périphériques) : vous pouvez assigner une ou plusieurs interfaces.

      Collector Group Communication (Communication du groupe de collecteurs) : vous ne pouvez attribuer qu'une seule interface.

      Device Deployment (Déploiement de périphériques) (mises à jour de logiciels et de contenu) : vous ne pouvez attribuer qu'une seule interface.
   3. (Facultatif) Sélectionnez les services de connectivité réseau pris en charge par l'interface.

© 2020 Palo Alto Networks, Inc.

(Interface MGT uniquement) Désactivez Telnet et HTTP ; ces services utilisent du texte en clair et sont donc moins sécurisés que d'autres services.

4. Cliquez sur **OK** pour enregistrer vos modifications.

STEP 5 | Configurez le nom d'hôte, le fuseau horaire et les paramètres généraux.

1. Sélectionnez **Panorama (Panorama)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les Paramètres Généraux.
2. Aligner l'horloge sur Panorama et les pare-feu gérés d'utiliser le même **Time Zone (Fuseau horaire)**, Par exemple GMT ou UTC. Si vous prévoyez d'utiliser Cortex Data Lake, vous devez configurer NTP pour que Panorama puisse rester synchronisé avec Cortex Data Lake.

   Le pare-feu enregistre les horodatages lorsqu'il génère des journaux et Panorama enregistre les horodatages sur réception des journaux. Le réglage des fuseaux horaires garantit que les horodatages sont synchronisés et que le processus d'interrogation de journaux et de génération de rapports sur Panorama est harmonieux.
3. Saisissez un **Hostname (Nom d'hôte)**pour le serveur. Panorama l'utilise comme nom/intitulé d'affichage pour l'appareil. Par exemple, il s'agit du nom qui s'affiche à l'invite d'interface de ligne de commande (ILC). Il apparaît également dans le champ Nom du collecteur si vous ajoutez l'appareil comme un collecteur géré sur la page **Panorama** > **Managed Collectors (Collecteurs Gérés)**.
4. (Facultatif) Saisissez la **Latitude** et la **Longitude** pour permettre un positionnement précis de l'appareil de série M sur la carte du monde. Les cartes **App Scope (App Scope)** > **Traffic Maps (Cartes de trafic)** et **App Scope** > **Threat Maps (Cartes de menaces)** utilisent ces valeurs.
5. Cliquez sur **OK** pour enregistrer vos entrées.

STEP 6 | Configurez les serveurs DNS et le serveur de mise à jour de Palo Alto Networks.

1. Sélectionnez **Panorama (Panorama)** > **Setup Configuration)** > **Services (Services)** et modifiez les paramètres.
2. Saisissez l'adresse IP du **Primary DNS Server (Serveur DNS principal)** et, facultativement, du **Secondary DNS Server (Serveur DNS secondaire)**.
3. Saisissez l'adresse URL ou statique du **Update Server (serveur de mise à jour)** (updates.paloaltonetworks.com par défaut).

   Cochez la case Verify Update Server Identity (Vérifier l'identité du serveur de mises à jour) si vous souhaitez que Panorama vérifie si le serveur, à partir duquel il télécharge les modules logiciels ou de contenu, comporte un certificat SSL signé par une autorité approuvée. Cette option ajoute un niveau de sécurité supplémentaire à la communication entre le serveur de gestion Panorama et le serveur de mises à jour.
4. Cliquez sur **OK** pour enregistrer vos entrées.

STEP 7 | Validez vos modifications de configuration.

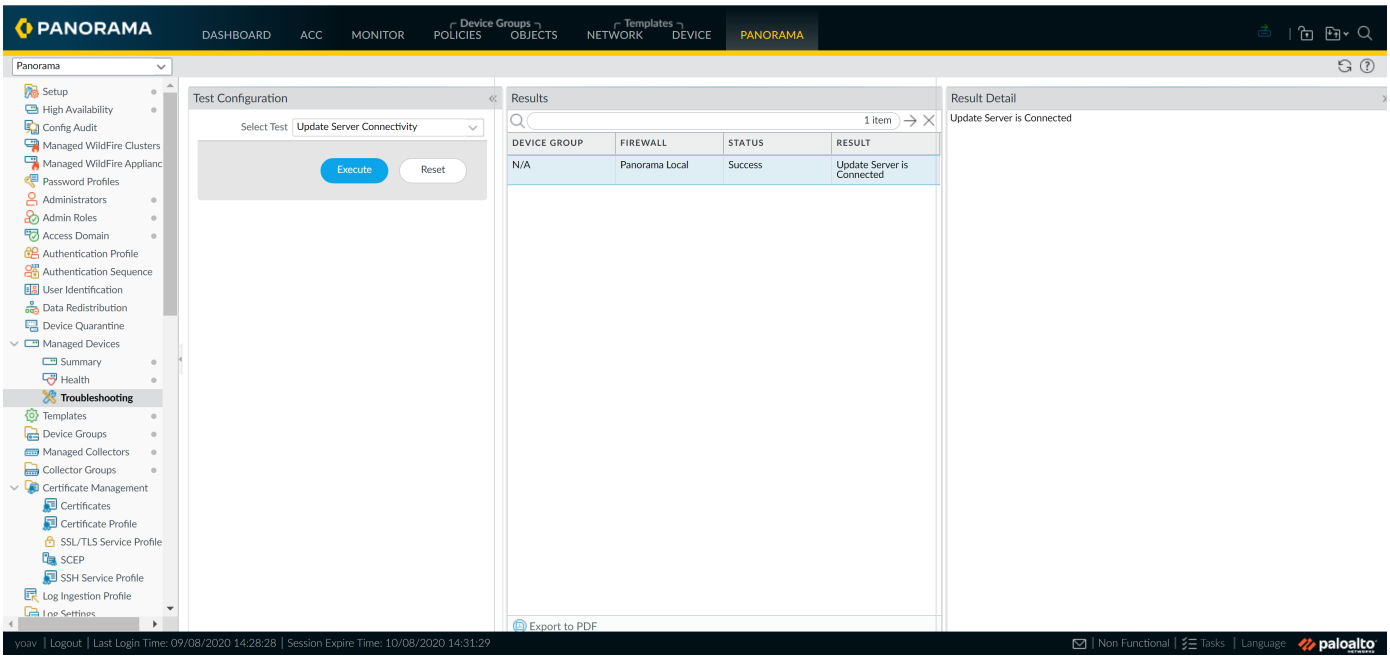
Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

Si vous prévoyez d'utiliser l'appareil de série M comme un serveur de gestion de Panorama et que vous avez configuré les interfaces autres que MGT, vous devez les assigner à la Device Log Collecte (Collecte de journaux de périphériques) ou à des fonctions de Collector Group Communication (Communication du groupe de collecteurs) lorsque vous configurez un collecteur géré. Pour rendre les interfaces opérationnelles, vous devez ensuite configurer un groupe de collecteurs pour le collecteur géré et exécuter une validation de groupe de collecteurs .

© 2020 Palo Alto Networks, Inc.

STEP 8 | Vérifiez l'accès réseau aux services externes nécessaire à la gestion de l'appareil, notamment au serveur de mises à jour de Palo Alto Networks.

1. Connectez-vous à l'appareil de série M d'une des façons suivantes :
   - Fixez un câble série à partir d'un ordinateur au port console sur l'appareil de série M. Utilisez ensuite le logiciel d'émulation de terminal (9600-8-N-1) pour vous connecter.
   - Utilisez un logiciel d'émulation de terminal tel que PuTTY pour ouvrir une session SSH à l'adresse IP que vous avez spécifiée pour l'interface MGT de l'appareil de série M lors de la configuration initiale.
2. Connectez-vous à l'ILC lorsque vous y êtes invité. Utilisez le compte admin par défaut et le mot de passe affecté lors de la configuration initiale.
3. Utilisez le test de connectivité au serveur de mises à jour pour vérifier la connectivité réseau au serveur de mises à jour de Palo Alto Networks, comme illustré dans l'exemple suivant.
   1. Sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)** > **Troubleshooting (Résolution de problèmes)**, puis sélectionnez **Updates Server Connectivity (Connectivité au serveur de mises à jour)** dans le menu déroulant Select Test (Sélectionner le test).
   2. **Execute (Lancer)** le test de connectivité au serveur de mises à jour.



4. Utilisez la commande ILC suivante pour extraire des informations sur le droit de support pour panorama à partir du serveur Update :

```
admin> request support check
```

Si vous disposez de la connectivité, le serveur de mise à jour répond avec l'état de support pour Panorama. Parce que panorama n'est pas enregistré, le serveur de mise à jour renvoie le message suivant :

```
Contact Us
https://www.paloaltonetworks.com/company/contact-us.html
Support Home
https://www.paloaltonetworks.com/support/tabs/overview.html
Device not found on this update server
```


© 2020 Palo Alto Networks, Inc.

STEP 9 | Étapes suivantes...

1. Enregistrer Panorama et installer les licences.
2. Installer les mises à jour de contenu et logicielles pour Panorama.



Le mieux est de remplacer le certificat par défaut que Panorama utilise pour sécuriser le trafic HTTPS sur l'interface de gestion.

Présentation de la configuration de la série M

Utilisez les procédures suivantes pour la configuration d'un appareil de série M :

- Configurer un appareil de série M en mode de Gestion seulement
- Configurer un appareil de série M en mode Panorama
- Configurer un appareil de série M en mode collecteur de journaux

Configurer un appareil de série M en mode de Gestion seulement

STEP 1 | Montez l'appareil de série M dans une baie. Se référer au Guide de référence du matériel de la série-M pour obtenir des instructions.

STEP 2 | Effectuer la configuration initiale de l'appareil de série M

STEP 3 | Enregistrer Panorama et Installer les licences

STEP 4 | Installer les mises à jour de contenu et logicielles pour Panorama

STEP 5 | Changez au mode de Gestion uniquement :

1. Connectez-vous à l'ILC de Panorama.
2. Passer du mode Panorama au mode Gestion uniquement :

   `request system system-mode management-only`
3. Entrez **`Y`** pour confirmer le changement de mode. Le serveur de gestion Panorama redémarre. Si le processus de redémarrage met fin à la session de votre logiciel d'émulation de terminal, reconnectez-vous au serveur de gestion Panorama pour voir l'invite de connexion Panorama.

   Si vous voyez une invite de `CMS Login`, cela signifie que le serveur de gestion Panorama n'a pas terminé le redémarrage. Appuyez sur ENTER à l'invite sans taper un nom d'utilisateur ou un mot de passe.
4. Connectez-vous à l'ILC.
5. Vérifiez que le passage en mode Gestion uniquement a réussi :

   `show system info | match system-mode`

   Si le changement de mode a réussi, la sortie affiche :

   ```
   system mode:management-only
   ```

STEP 6 | Configurer l'accès administratif à Panorama

STEP 7 | Gérer les pare-feu

STEP 8 | Gérer la collecte des journaux

Configurer un appareil de série M en mode Panorama

© 2020 Palo Alto Networks, Inc.

STEP 1 | Montez l'appareil de série M dans une baie. Se référer au Guide de référence du matériel de la série-M pour obtenir des instructions.

STEP 2 | Effectuez la configuration initiale de l'appareil de série M.

STEP 3 | Enregistrer Panorama et installer les licences.

STEP 4 | Installer les mises à jour de contenu et logicielles pour Panorama.

STEP 5 | Configurer chaque baie. Cette tâche est nécessaire pour rendre les disques RAID disponibles pour la journalisation. Vous pouvez éventuellement ajouter des disques pour augmenter la capacité de stockage sur l'appareil de série M.

STEP 6 | Configurer l'accès administratif à Panorama.

STEP 7 | Gérer les pare-feu.

STEP 8 | Gérer la collecte des journaux.

Configurer un appareil de série M en mode collecteur de journaux

STEP 1 | Montez l'appareil de série M dans une baie. Se référer au Guide de référence du matériel de la série-M pour obtenir des instructions.

STEP 2 | Effectuer la configuration initiale de l'appareil de série M

STEP 3 | Enregistrer Panorama et Installer les licences

STEP 4 | Installer les mises à jour de contenu et logicielles pour Panorama

STEP 5 | Voir les étapes Configurer chaque tableau. Cette tâche est nécessaire pour rendre les disques RAID disponibles pour la journalisation. Vous pouvez éventuellement ajouter des disques pour augmenter la capacité de stockage sur l'appareil de série M.

STEP 6 | Configurer l'appareil de série M en tant que collecteur de journaux

STEP 7 | Gérer la collecte des journaux

Configurer l'appareil de série M en tant que collecteur de journaux

Si vous voulez disposer d'un appareil dédié pour la collecte de journaux, configurez un appareil M-200, M-500 ou M-600 en mode collecteur de journaux. Pour ce faire, vous effectuez d'abord la configuration initiale de l'appareil en mode Panorama, qui comprend les licences, l'installation de logiciels et les mises à jour de contenu, et la configuration de l'interface de gestion (MGT). Vous faites ensuite passer l'appareil M-Series au mode Collecteurs de journaux et terminez la configuration des Collecteurs de journaux. En outre, si vous souhaitez utiliser des interfaces d'appareils de série M dédiées (recommandé) au lieu de l'interface de gestion pour la collecte de journaux et le groupe de collecteurs, vous devez d'abord configurer les interfaces pour le serveur de gestion Panorama, puis les configurer pour le collecteur de journaux, et effectuer une validation de Panorama suivie d'une validation du groupe de collecteurs.

Effectuez les étapes suivantes pour configurer un nouvel appareil de Série M en tant que collecteur de journaux ou pour convertir un appareil de Série M existant précédemment déployé en tant que serveur de gestion de Panorama.

© 2020 Palo Alto Networks, Inc.

Si vous configurez un appareil M-Series en mode Colleteur de journaux avec des interfaces de 10 Go, vous devez effectuer la totalité de cette procédure de configuration pour que les interfaces de 10 GB s'affichent en `Up (activées)`.

Le passage de l'appareil de série M du mode Panorama au mode collecteur de journaux redémarre l'appareil, supprime le collecteur de journaux local, supprime toutes les données existantes du journal et supprime toutes les configurations à l'exception des paramètres d'accès de gestion. La désactivation du mode ne supprime pas les licences, les mises à jour logicielles ou les mises à jour de contenu.

STEP 1 | Configurez le serveur de gestion Panorama qui gérera le collecteur de journaux si vous ne l'avez déjà fait.

Effectuez l'une des tâches suivantes :

- Configuration de l'appareil virtuel Panorama
- Configuration de l'appareil de série M

STEP 2 | Enregistrez les adresses IP de gestion du serveur de gestion Panorama.

Si vous avez déployé panorama dans une configuration haute disponibilité (HD), vous avez besoin de l'adresse IP de chaque homologue HD.

1. Connectez-vous à l'interface Web du serveur de gestion de Panorama.
2. Enregistrez l'**IP Address (Adresse IP)** du Panorama solitaire (non HD) ou actif (HD) en sélectionnant **Panorama** > **Setup (Configuration)** > **Management (Gestion)** et en vérifiant les paramètres de l'interface de gestion.
3. Pour un déploiement HD, enregistrez la **Peer HD IP Address (Adresse IP de l'homologue HD)** du Panorama passif en sélectionnant **Panorama** > **High Availability (Haute disponibilité)** et en vérifiant la section Setup (Configuration).

STEP 3 | Paramétrez l'appareil de la série M qui servira de Collecteur de Journaux dédié.

Si vous avez précédemment déployé cet appareil en tant que serveur d'administration Panorama, vous pouvez ignorer cette étape car l'interface de gestion est déjà configurée et les licences et mises à jour sont déjà installées.

L'appareil de Série M en mode collecteur de journaux n'a pas d'interface Web pour les tâches de configuration, seule une ILC. Par conséquent, avant de changer le mode de l'appareil de série M, utiliser l'interface web en mode Panorama pour :

1. Effectuez la configuration initiale de l'appareil de série M.
2. Enregistrer Panorama et installer les licences.
3. Installer les mises à jour de contenu et logicielles pour Panorama.

STEP 4 | Accédez à l'ILC de l'appareil de série M.

1. Connectez-vous à l'appareil de série M d'une des façons suivantes :
   - Fixez un câble série à partir d'un ordinateur au port console sur l'appareil de série M. Utilisez ensuite le logiciel d'émulation de terminal (9600-8-N-1) pour vous connecter.
   - Utilisez un logiciel d'émulation de terminal tel que PuTTY pour ouvrir une session SSH à l'adresse IP que vous avez spécifiée pour l'interface MGT de l'appareil de série M lors de la configuration initiale.
2. Connectez-vous à l'ILC lorsque vous y êtes invité. Utilisez le compte admin par défaut et le mot de passe affecté lors de la configuration initiale.

STEP 5 | Passez du mode Panorama au mode collecteur de journaux.

© 2020 Palo Alto Networks, Inc.

1. Pour passer à une session en mode collecteur de journaux, entrez la commande suivante :

```
> request system system-mode logger
```

2. Entrez **Y** pour confirmer le changement de mode. L'appareil de série M redémarre. Si le processus de redémarrage termine votre session du logiciel d'émulation de terminal, reconnectez à l'appareil de série M pour afficher l'invite de connexion Panorama.

   *Si vous voyez une invite de **connexion CMS**, cela signifie que le collecteur de journaux n'a pas terminé le redémarrage. Appuyez sur ENTER à l'invite sans taper un nom d'utilisateur ou un mot de passe.*

3. Connectez-vous à l'ILC.
4. Vérifiez que la bascule en mode collecteur de journaux a réussi :

```
> show system info | match system-mode
```

   Si le changement de mode a réussi, la sortie affiche :

```
system-mode: logger
```

STEP 6 | Configurez les disques de journalisation en tant que paires RAID 1.

Si vous avez précédemment déployé l'appareil en tant que serveur de gestion de panorama, vous pouvez ignorer cette étape car les paires de disques sont déjà configurées et disponibles.

Le temps requis pour configurer les lecteurs varie de plusieurs minutes à quelques heures, en fonction de la quantité de données sur les lecteurs.

1. Déterminez quelles paires de disques sont présentes pour la configuration en tant que paires RAID sur l'appareil de Série M :

```
> show system raid detail
```

   Effectuez les étapes restantes pour configurer chaque paire de disques ayant des disques `présents`. Cet exemple utilise la paire de disques A1/A2.
2. Pour ajouter le premier disque dans la paire, saisissez la commande suivante et entrez **y** lorsque vous êtes invité à confirmer la demande :

```
> request system raid add A1
```

   Attendez que le processus se termine avant d'ajouter le disque suivant dans la paire. Pour surveiller l'avancement de la configuration RAID, ré-entrer :

```
> show system raid detail
```

   Une fois le processus terminé pour le premier disque, la sortie affiche l'état de la paire de disques comme `disponible` mais `dégradée`.
3. Ajouter le deuxième disque dans la paire :

```
> request system raid add A2
```


© 2020 Palo Alto Networks, Inc.

4. Vérifiez que la configuration du disque est terminée :

```
> show system raid detail
```

Une fois le processus terminé pour le premier disque, la sortie affiche l'état de la paire de disques comme `Available` (Disponible) et `clean` (Propre) :

```
Disk Pair A      Available
Status        clean
```

STEP 7 | Activer la connectivité entre chaque collecteur de journaux et le serveur de gestion de Panorama.

Saisissez les commandes suivantes dans l'ILC du collecteur de journaux, où *<IPaddress1>* est pour l'interface de gestion du panorama solitaire (non HD) ou actif (HD) et *<IPaddress2>* est pour l'interface de gestion du panorama passif (HD), le cas échéant.

```
> configure
# set deviceconfig system panorama-server <IPaddress1> panorama-server-2
 <IPaddress2>
# commit
# exit
```

STEP 8 | Enregistrez le numéro de série du collecteur de journaux.

Vous avez besoin des numéros de série pour ajouter les collecteurs de journaux en tant que collecteurs gérés sur le serveur de gestion de Panorama.

1. Dans l'ILC du collecteur de journaux dédié, saisissez les commandes suivantes pour afficher le numéro de série :

```
> show system info | match serial
```

2. Enregistrez le numéro de série.

STEP 9 | Ajoutez le collecteur de journaux en tant que collecteur géré au serveur de gestion de Panorama.

1. Sélectionnez **Panorama (Panorama)** > **Managed Collectors (Collecteurs gérés)** et **Add (ajoutez)** le collecteur géré.
2. Dans les paramètres **General (Général)**, saisissez le numéro de série (**Collector S/N (N° de série du collecteur)**) que vous avez enregistré pour le collecteur de journaux.
3. Dans le champ **Panorama Server IP (IP du serveur Panorama)** entrez l'adresse IP ou le nom de domaine complet du Panorama solitaire (non-HD) ou primaire (HD). Pour un déploiement HD, entrez l'adresse IP ou le nom de domaine complet de l'homologue secondaire de Panorama dans le champ **Panorama Server IP 2 (Serveur Panorama IP 2)**.

   Ces adresses IP doivent spécifier une interface Panorama sont les services **Device Management and Device Log Collection (Gestion des périphériques et collecte des journaux de périphériques)** sont activés. Par défaut, ces services sont activés uniquement sur l'interface MGT. Toutefois, vous avez peut-être activé les services sur d'autres interfaces lors de l'étape Configurer l'appareil de série M qui est un serveur de gestion Panorama.
4. Sélectionnez **Interfaces**, cliquez sur **Management (Gestion)** et remplissez un ou les deux ensembles de champs suivants pour l'interface de gestion, selon les protocoles IP de votre réseau.

© 2020 Palo Alto Networks, Inc.

- IPv4 : **IP Address (Adresse IP)**, **Netmask (Masque de sous-réseau)** et **Default Gateway (Passerelle par défaut)**
- IPv6 : **IPv6 Address/Prefix Length (Longueur du préfixe / de l'adresse IPv6)** et **Default IPv6 Gateway (Passerelle IPv6 par défaut)**

5. Cliquez deux fois sur **OK** pour enregistrer les modifications au groupe de collecteurs.
6. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos modifications à la configuration Panorama.

   Cette étape est requise avant de pouvoir activer les disques de journalisation.
7. Vérifiez que la page **Panorama** > **Managed Collectors (Collecteurs gérés)** répertorie le collecteur de journaux que vous avez ajouté. La colonne Connecté affiche une icône de coche pour indiquer que le collecteur de journaux est connecté à Panorama. Vous devrez peut-être attendre quelques minutes avant que la page affiche le statut de connexion actualisée.



À ce stade, la colonne État de configuration affiche Désynchronisé et la colonne État d'exécution affiche Déconnecté. L'état passera à In sync (En synchronisation) et Connected (Connecté) après avoir configuré un groupe de collecteurs (étape Affectez le collecteur de journaux à un groupe collecteur).

STEP 10 | Activer les disques de journalisation.

1. Sélectionnez **Panorama (Panorama)** > **Managed Collectors (Collecteurs gérés)** et modifiez le collecteur de journaux.
2. Sélectionnez **Disks (disques)** et **Add (Ajoutez)** chaque paire de disques RAID.
3. Cliquez sur **OK** pour enregistrer vos modifications.
4. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos modifications à la configuration Panorama.

STEP 11 | (Recommandé) Configurez les interfaces **Ethernet1**, **Ethernet2**, **Ethernet3**, **Ethernet4**, et **Ethernet5** si le collecteur de journaux et le serveur de gestion Panorama les utiliseront pour la **Device Log Collection (Collecte de journaux de périphériques)** (réception des journaux des pare-feu) et la **Collector Group Communication (Communication du groupe de collecteurs)**.

Si vous avez précédemment déployé le collecteur de journaux en tant que serveur de gestion Panorama et configuré ces interfaces, vous devez les reconfigurer car le passage en mode collecteur de journaux (Passez du mode Panorama au mode collecteur de journaux) aurait supprimé toutes les configurations, sauf les paramètres d'accès de gestion.

1. Configurez chaque interface sur le serveur de gestion Panorama (autre que l'interface MGT) si vous n'avez pas déjà réalisé les étapes suivantes :
   1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Interfaces** et cliquez sur le nom de l'interface.
   2. Sélectionnez *<interface-name> (nom de l'interface)* pour activer l'interface.
   3. Remplissez un ou les deux des ensembles de champs suivants, selon les protocoles IP de votre réseau :

      IPv4 : **IP Address (Adresse IP)**, **Netmask (Masque de sous-réseau)** et **Default Gateway (Passerelle par défaut)**

      IPv6 : **IPv6 Address/Prefix Length (Longueur du préfixe / de l'adresse IPv6)** et **Default IPv6 Gateway (Passerelle IPv6 par défaut)**
   4. Sélectionnez les services de gestion de périphériques pris en charge par l'interface :

      Device Management and Device Log Collection (Gestion des périphériques et collecte des journaux de périphériques) : vous pouvez assigner une ou plusieurs interfaces.

© 2020 Palo Alto Networks, Inc.

Collector Group Communication (Communication du groupe de collecteurs) : vous ne pouvez attribuer qu'une seule interface.

Device Deployment (Déploiement de périphériques) (mises à jour de logiciels et de contenu) : vous ne pouvez attribuer qu'une seule interface.

5. Cliquez sur **OK** pour enregistrer vos modifications.

2. Configurez chaque interface sur le collecteur de journaux (autre que l'interface MGT) :
   1. Sélectionnez **Panorama (Panorama)** > **Managed Collectors (Collecteurs gérés)** et modifiez le collecteur de journaux.
   2. Sélectionnez **Interfaces** et cliquez sur le nom de l'interface.
   3. Sélectionnez *<interface-name> (nom de l'interface)* pour activer l'interface.
   4. Remplissez un ou les deux des ensembles de champs suivants, selon les protocoles IP de votre réseau :

      IPv4 : **IP Address (Adresse IP)**, **Netmask (Masque de sous-réseau)** et **Default Gateway (Passerelle par défaut)**

      IPv6 : **IPv6 Address/Prefix Length (Longueur du préfixe / de l'adresse IPv6)** et **Default IPv6 Gateway (Passerelle IPv6 par défaut)**
   5. Sélectionnez les services de gestion de périphériques pris en charge par l'interface :

      Device Log Collection (Collecte de journaux de périphériques) : vous pouvez assigner une ou plusieurs interfaces.

      Collector Group Communication (Communication du groupe de collecteurs) : vous ne pouvez attribuer qu'une seule interface.
   6. Cliquez sur **OK** pour enregistrer vos modifications d'interface.
3. Cliquez sur **OK** pour enregistrer les modifications au collecteur de journaux.
4. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos modifications à la configuration Panorama.

STEP 12 | (Facultatif) Si votre déploiement utilise des certificats personnalisés pour l'authentification entre Panorama et les périphériques gérés, déployez le certificat de périphérique client personnalisé. Pour plus d'informations, consultez Configurer l'authentification à l'aide de certificats personnalisés.

1. Sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificat)** et choisissez le profil de certificat dans la liste déroulante ou cliquez sur **New Certificate Profile (Nouveau profil de certificat)** pour en créer un.
2. Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** > **Add (Ajouter)** > **Communication** pour un collecteur de journaux.
3. Cochez la case **Secure Client Communication (Sécurisation des communications avec le client)**.
4. Sélectionnez le type de certificat de périphérique dans la liste déroulante Type.
   - Si vous utilisez un certificat de périphérique local, sélectionnez **Certificate (Certificat)** et **Certificate Profile (Profil de certificat)** à partir des listes déroulantes respectives.
   - Si vous utilisez SCEP comme certificat de périphérique, sélectionnez **SCEP Profile (Profil SCEP)** et **Certificate Profile (Profil de certificat)** à partir des listes déroulantes respectives.
5. Cliquez sur **OK**.

STEP 13 | (Facultatif) Configurez Secure Server Communication (Communication sécurisée avec le serveur) sur un collecteur de journaux. Pour plus d'informations, consultez Configurer l'authentification à l'aide de certificats personnalisés.

1. Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** > **Add (Ajouter)** > **Communication**

© 2020 Palo Alto Networks, Inc.

2. Vérifiez que la case **Custom Certificate Only (Certificat personnalisé uniquement)** n'est pas cochée. Cela vous permet de continuer à gérer tous les périphériques lors de la migration vers des certificats personnalisés.

   Lorsque la case Custom Certificate Only (Certificat personnalisé uniquement) est cochée, le collecteur de journaux ne s'authentifie pas et ne peut pas recevoir les journaux des périphériques à l'aide de certificats prédéfinis.
3. Sélectionnez le profil de service SSL/TLS depuis le menu déroulant **SSL/TLS Service Profile (Profil de service SSL/TLS)**. Ce profil de service SSL/TLS s'applique à toutes les connexions SSL entre le collecteur de journaux et les périphériques qu'il enregistre.
4. Sélectionnez le profil du certificat depuis la liste déroulante **Certificate Profile (Profil du certificat)**.
5. Sélectionnez **Authorize Client Based on Serial Number (Autoriser le client en fonction du numéro de série)** pour que le serveur vérifie les clients par rapport aux numéros de série des périphériques gérés. Le certificat client doit avoir le mot clé spécial $UDID défini en tant que CN à autoriser en fonction des numéros de série.
6. Dans **Disconnect Wait Time (min) (Délai d'attente de déconnexion (min))**, saisissez le nombre de minutes que Panorama doit attendre avant de mettre fin et de rétablir la connexion avec ses périphériques gérés. Ce champ est vide par défaut et la plage est comprise entre 0 et 44 640 minutes.

   Le délai d'attente de déconnexion de déconnexion ne commence pas à décompter tant que vous n'avez pas validé la nouvelle configuration.
7. (Facultatif) Configurez une liste d'autorisation.
   1. Cliquez sur **Add (Ajouter)** sous Authorization List (Liste d'autorisation).
   2. Sélectionnez **Subject (Objet)** ou **Subject Alt Name (Autre nom de l'objet)** comme type d'identifiant.
   3. Entrez un identifiant du type sélectionné.
   4. Cliquez sur **OK**.
   5. Sélectionnez **Check Authorization List (Vérifier la liste d'autorisation)** pour appliquer la liste d'autorisation.
8. Cliquez sur **OK**.
9. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)**.

STEP 14 | Affectez le Collecteur de journaux à un groupe collecteur.

1. Configurer un groupe de collecteurs. Vous devez effectuer une validation de Panorama et ensuite créer un groupe de collecteurs pour synchroniser la configuration du collecteur de journaux avec Panorama et mettre les interfaces Eth1, Eth2, Eth3, Eth4 et Eth5 (si vous les avez configurées) dans un état opérationnel sur le collecteur de journaux.

   Dans un même groupe de collecteurs, tous les collecteurs de journaux doivent être exécutés sur le même modèle Panorama : uniquement des appareils M-600, uniquement des appareils M-500, uniquement des appareils M-200 ou uniquement des appareils virtuels Panorama.

   Il est recommander d'activer l'option Enable log redundancy across collectors (Activer la redondance des journaux entre les collecteurs) si vous ajoutez plusieurs collecteurs de journaux à un seul groupe de collecteurs. Cette option nécessite que chaque collecteur de journaux ait le même nombre de disques de journalisation.
2. Sélectionnez **Panorama (Panorama)** > **Managed Collectors (Collecteurs gérés)** pour vérifier que la configuration de Collecteur de journaux est synchronisée avec Panorama.

   La colonne Configuration Status (État de configuration) doit afficher In Sync (synchronisation) et la colonne Run Time Status (État d'exécution) doit afficher Connected (Connecté).

© 2020 Palo Alto Networks, Inc.

3. Accédez à l'interface ILC du collecteur de journaux et saisissez la commande suivante pour vérifier que ses interfaces sont opérationnelles :

```
> show interface all
```

   La sortie affiche l'`État` comme `haut` pour chaque interface qui est opérationnelle.
4. Si le groupe de collecteurs possède plusieurs collecteurs de journaux, Résoudre les problèmes de connectivité aux ressources réseaux pour vérifier qu'ils peuvent communiquer entre eux en exécutant un test de connectivité Ping pour chaque interface que les collecteurs de journaux utilisent. Pour l'adresse IP `source`, précisez l'interface de l'un des collecteurs de journaux. Pour l'adresse IP de l'`hôte`, spécifiez l'interface correspondante d'un autre collecteur de journaux dans le même groupe de collecteurs.

STEP 15 | Étapes suivantes...

Pour activer le collecteur de journaux afin de recevoir les journaux du pare-feu :

1. Configurer le transfert des journaux vers Panorama.
2. Vérifier le transfert des journaux vers Panorama.

Augmenter le stockage sur l'appareil de série M

Après avoir effectué la configuration initiale de l'appareil de série M, vous pouvez augmenter la capacité de stockage de l'appareil en mettant à niveau les paires de disques existantes vers des disques de plus grande capacité ou en installant des paires de disques supplémentaires dans des baies de disques vides. Par exemple, vous pouvez choisir de mettre à niveau les disques de 1 To existants à 2 To sur un appareil M-500, ou vous pouvez ajouter des disques de 2 To aux baies de disques vides (B1 à D2).

Les appareils de série M exploitent RAID 1 pour la redondance des données en cas de panne de disque. Par conséquent, la paire de lecteurs dans une matrice RAID 1 doit être identique. Cependant, vous êtes libre de mélanger des capacités de disque entre différentes baies RAID 1. Par exemple, les lecteurs de la matrice A1/A2 RAID 1 peuvent être des lecteurs de 1 To et les lecteurs de la matrice RAID1 B1/B2 peuvent être des lecteurs de 2 To.

Le tableau suivant répertorie le nombre maximal de baies de lecteurs et les capacités de lecteur disponibles prises en charge sur les appareils de série M.

Étant donné que chaque paire de lecteurs (A1/A2 par exemple) se trouve dans une baie RAID 1, la capacité de stockage totale correspond à la moitié du nombre total de disques installés. Par exemple, si un appareil M-500 possède des disques de 2 To installés dans les baies A1/A2 et B1/B2, la baie A1/A2 fournit un stockage total de 2 To et la baie B1/B2 fournit 2 To supplémentaires pour un total de 4 To.

Appareil	Nombre de baies de disques prises en charge	Capacité de disques prise en charge
Appareil M-200	4	8 Go
Appareil M-500	24	1 To ou 2 To
Appareil M-600	12	8 Go

© 2020 Palo Alto Networks, Inc.

Avant d'étendre la capacité de stockage du journal, déterminez les exigences de stockage de journaux de Panorama. Si vous avez besoin de plus de stockage de journaux qu'un seul appareil de Série M, vous pouvez ajouter des collecteurs de journaux dédiés (voir Configurer un collecteur géré) ou vous pouvez configurer le transfert de journaux de Panorama vers des destinations extérieures.

Vous n'avez pas besoin de mettre l'appareil de série M hors ligne pour étendre le stockage lors de l'ajout de lecteurs à un appareil de série M déjà déployé. Lorsque les lecteurs supplémentaires sont configurables et disponibles, l'appareil de Série M répartit les journaux entre tous les lecteurs disponibles. Ce processus de redistribution des journaux s'exécute en arrière-plan et n'affecte pas la disponibilité de l'appareil M-100. Cependant, le processus fait diminuer la vitesse d'enregistrement maximale. La colonne État redistribution (Panorama > Collector Groups (Groupes de collecteurs)) indique l'état d'achèvement du processus en pourcentage.

- Ajouter des lecteurs supplémentaires à un appareil de la série M
- Mise à niveau des lecteurs sur les appareils de série M exécutant Panorama 7.0.8 ou une version ultérieure
- Mise à niveau des lecteurs sur les appareils de série M exécutant Panorama 7.0.7 ou une version antérieure

Ajouter des lecteurs supplémentaires à un appareil de la série M

STEP 1 | Installez les lecteurs disques dans les baies de lecteurs appropriées.

Assurez-vous d'ajouter les lecteurs séquentiellement dans l'emplacement des baies de lecteurs ouvert suivant. Par exemple, ajoutez les lecteurs à B1 et B2 avant d'ajouter les lecteurs à C1 et C2.

STEP 2 | Accédez à l'interface de ligne de commande (ILC) sur l'appareil de série M.

Connectez-vous à l'appareil de série M d'une des façons suivantes :

- Connectez un câble série de votre ordinateur au port de la console et connectez-vous à l'appareil de série M à l'aide du logiciel d'émulation de terminal (9600-8-N-1).
- Utilisez un logiciel d'émulation de terminal, tel que PuTTY, pour ouvrir une session Secure Shell (SSH) à l'adresse IP de l'appareil de série M.

STEP 3 | Lorsque vous y êtes invité, connectez-vous au périphérique.

Utilisez le compte administrateur par défaut et le mot de passe affecté.

STEP 4 | Configurez chaque baie.

Le temps nécessaire à faire une copie miroir des données du lecteur peut varier de plusieurs minutes à quelques heures, en fonction de la quantité de données présentes sur le lecteur.

Les exemples suivants utilisent les lecteurs dans les baies B1 et B2.

1. Entrez les commandes suivantes et confirmez la demande lorsque vous y êtes invité :

```
> request system raid add B1
> request system raid add B2
```

2. Pour suivre les progrès de la configuration RAID, entrez la commande suivante:

© 2020 Palo Alto Networks, Inc.

```
> show system raid detail
```

Une fois la configuration RAID terminée, la réponse suivante s'affiche :

```
Disk Pair A       Available
   Status         clean
   Disk id A1     Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : active sync
   Disk id A2     Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : active sync
Disk Pair B        Available
   Status          clean
   Disk id B1      Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : active sync
   Disk id B2     Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : active sync
```

STEP 5 | Rendez la baie disponible pour la journalisation.

Pour activer la baie pour la journalisation, vous devez d'abord ajouter l'appareil en tant que collecteur géré sur Panorama. Si vous ne l'avez pas encore ajouté, reportez-vous à la section Configurer un collecteur géré.

1. Connectez-vous à l'interface Web du serveur de gestion Panorama qui gère ce collecteur de journaux.
2. Sélectionnez **Panorama (Panorama)** > **Managed Collectors (Collecteurs gérés)** et modifiez le collecteur de journaux.
3. Sélectionnez **Disks (Disques)** et **Add (Ajoutez)** chaque baie.
4. Cliquez sur **OK** pour enregistrer vos modifications.
5. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.
6. Sélectionnez **Commit (Valider)** > **Push to Devices (Transmettre aux périphériques)**, sélectionnez le groupe de collecteurs, puis **Push (Appliquez)** vos changements.

Mise à niveau des lecteurs sur les appareils de série M exécutant Panorama 7.0.8 ou une version ultérieure

STEP 1 | Accédez à l'interface de ligne de commande (ILC) sur l'appareil de série M.

Connectez-vous à l'appareil de série M d'une des façons suivantes :

- Connectez un câble série de votre ordinateur au port de la console et connectez-vous à l'appareil de série M à l'aide du logiciel d'émulation de terminal (9600-8-N-1).
- Utilisez un logiciel d'émulation de terminal, tel que PuTTY, pour ouvrir une session Secure Shell (SSH) à l'adresse IP de l'appareil de série M.

STEP 2 | Lorsque vous y êtes invité, connectez-vous au périphérique.

© 2020 Palo Alto Networks, Inc.

Utilisez le compte administrateur par défaut et le mot de passe affecté.

STEP 3 | Vérifiez que l'état RAID 1 pour les lecteurs installés montre qu'il y a au moins deux matrices RAID 1 fonctionnant. Pendant la mise à niveau, vous allez mettre à niveau une matrice RAID 1 à la fois, et il doit y avoir au moins une autre matrice RAID 1 disponible pour l'appareil. L'appareil affichera une erreur d'abandon si vous tentez d'enlever le seul tableau fonctionnel de la configuration.

Saisissez la commande suivante pour afficher l'État RAID :

```
> show system raid detail
```

Par exemple, les résultats suivants indiquent une sortie d'un appareil M-500 avec deux tableaux disponibles (paire de disque A et paire de disque B). S'il n'y a qu'une seule matrice disponible, vous devez ajouter une deuxième matrice, tel que décrit dans Ajouter des lecteurs supplémentaires à un appareil de série M avant de mettre à niveau les lecteurs.

```
Disk Pair A                             Available
   Status                                   clean
   Disk id A1                             Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : active sync
   Disk id A2                             Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : active sync
Disk Pair B                             Available
   Status                                   clean
   Disk id B1                             Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : active sync
   Disk id B2                             Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : active sync
```

STEP 4 | Retirez le premier disque de 1 To et remplacez-le par un lecteur de 2 To.

1. Pour supprimer le premier lecteur de la configuration RAID 1 (A1 dans cet exemple), saisissez la commande suivante et entrez **y** lorsque vous êtes invité à confirmer la demande :

   ```
   > request system raid remove A1
   ```

2. Retirez physiquement le premier disque de la baie. Appuyez sur le bouton éjecteur du transporteur de la baie A1 pour relâcher la poignée d'éjection. Tirez ensuite la poignée vers vous et glissez les lecteurs hors de l'appareil.
3. Retirez un disque de 2 To de son emballage et placez le lecteur sur une table à côté du lecteur que vous venez de supprimer. Prenez note de la façon dont les lecteurs sont installés dans le transporteur parce que vous installez les lecteurs de 2 To dans ces mêmes transporteurs.
4. Retirez les quatre vis qui retiennent chaque disque dans son transporteur et retirez les disques des transporteurs.
5. Fixez le lecteur de 2 To au transporteur à l'aide des quatre mêmes vis que vous avez retirées du lecteur de 1 To, puis réinsérez le transporteur avec le lecteur de 2 To dans la baie A1.

© 2020 Palo Alto Networks, Inc.

6. Entrez la commande suivante pour vérifier que le lecteur 2 To est reconnu :

```
show system raid detail
```

Vérifiez que le disque A1 affiche le bon modèle et la bonne taille (environ 2 To). Si le modèle et la taille ne sont pas corrects, réexécutez la commande ci-dessus jusqu'à ce que le modèle et la taille corrects s'affichent.

Si le modèle et la taille incorrects sont systématiquement affichés, entrez la commande suivante :

```
request system raid remove A1
```

Attendez 30 secondes une fois que vous avez exécuté la commande ci-dessus, puis retirez le disque et réinsérez-le, et répétez la commande **`show system raid detail`** pour vérifier la taille et le modèle.

STEP 5 | Copiez les données à partir du lecteur de 1 To restant installé dans le tableau RAID 2 vers la nouvelle unité de 2 To installée dans ce tableau.

Le temps requis pour copier les données peut varier de plusieurs minutes à quelques heures, selon la quantité de données sur le lecteur.

1. Pour copier les données du lecteur de 1 To dans la baie A2 au lecteur de 2 To installé dans la baie A1, saisissez la commande suivante et entrez **`y`** lorsque vous y êtes invité :

```
> request system raid copy from A2 to A1
```

2. Pour afficher l'état du processus de copie, exécutez la commande suivante :

```
> show system raid detail
```

Continuez à exécuter cette commande pour afficher la sortie du détail du RAID jusqu'à ce que la baie (A1/A2 dans cet exemple) affiche `Available` (Disponible).

À ce stade, le lecteur A2 affichera `pas en utilisation` car il y a une incompatibilité de taille de lecteur.

STEP 6 | Mettez à niveau le deuxième lecteur dans la baie RAID 1 avec un lecteur de 2 To.

1. Supprimez le deuxième lecteur de 1 To (de la baie de disque A2 dans cet exemple) pour la configuration de la baie RAID 1 :

```
> request system raid remove A2
```

2. Insérez le support avec le disque de 2 To nouvellement installé dans la baie A2 et ajoutez-le à la configuration de la baie RAID 1 :

```
> request system raid add A2
```

Le système va copier les données de A2 à A1 pour cloner les lecteurs.

3. Pour afficher l'état du processus de copie, exécutez la commande suivante :

© 2020 Palo Alto Networks, Inc.

```
> show system raid detail
```

Continuez à exécuter cette commande pour visualiser la sortie du détail du RAID jusqu'à ce que la baie (A1/A2 dans cet exemple) affiche `Available` et que les deux disques affichent `active sync`.

```
Disk Pair A       Available
   Status         clean
   Disk id A1     Present
       model        : ST2000NX0253
       size         : 1907138 MB
       status       : active sync
Disk id A2     Present
       model        : ST2000NX0253
       size         : 1907138 MB
       status       : active sync
```

STEP 7 | Mettez à niveau les lecteurs pour des matrices RAID 1 supplémentaires si nécessaire.

Pour mettre à niveau des matrices RAID 1 supplémentaires vers des disques de 2 To, répétez cette procédure pour remplacer les indicateurs de lecteur selon le cas. Par exemple, remplacez A1 par B1 et A2 par B2 pour mettre à niveau les lecteurs dans la matrice RAID 1 B1/B2.

Mise à niveau des lecteurs sur les appareils de série M exécutant Panorama 7.0.7 ou une version antérieure

Les journaux sur les disques de 1 To ne seront pas disponibles après la mise à niveau des lecteurs sur un appareil de Série M qui exécute panorama 7.0.7 ou une version antérieure. Même si c'est acceptable, nous vous recommandons d'effectuer cette mise à niveau au cours d'une fenêtre de maintenance.

S'il est important pour vous de conserver les journaux, vous devez mettre à niveau vers Panorama 7.0.8 ou une version ultérieure, puis utiliser la procédure de Mise à niveau des lecteurs sur les appareils de série M exécutant Panorama 7.0.8 ou une version ultérieure*.*

STEP 1 | Accédez à l'interface de ligne de commande (ILC) sur l'appareil de série M.

Connectez-vous à l'appareil de série M d'une des façons suivantes :

- Connectez un câble série de votre ordinateur au port de la console et connectez-vous à l'appareil de série M à l'aide du logiciel d'émulation de terminal (9600-8-N-1).
- Utilisez un logiciel d'émulation de terminal, tel que PuTTY, pour ouvrir une session Secure Shell (SSH) à l'adresse IP de l'appareil de série M.

STEP 2 | Lorsque vous y êtes invité, connectez-vous au périphérique.

Utilisez le compte administrateur par défaut et le mot de passe affecté.

STEP 3 | Vérifiez que l'état RAID 1 pour les lecteurs installés montre qu'il y a au moins deux matrices RAID 1 fonctionnant. Pendant la mise à niveau, vous allez mettre à niveau une matrice RAID 1 à la fois, et il doit y avoir au moins une autre matrice RAID 1 disponible pour l'appareil. L'appareil affichera une erreur d'abandon si vous tentez d'enlever le seul tableau fonctionnel de la configuration.

Saisissez la commande suivante pour afficher l'État RAID :

© 2020 Palo Alto Networks, Inc.

```
> show system raid detail
```

Par exemple, les résultats suivants indiquent une sortie d'un appareil M-500 avec deux tableaux disponibles (paire de disque A et paire de disque B). S'il n'y a qu'une seule matrice disponible, vous devez ajouter une deuxième baie tel que décrit à l'étape Ajouter des lecteurs supplémentaires à un appareil de la série M avant de mettre à niveau les lecteurs.

```
Disk Pair A                             Available
   Status                                   clean
   Disk id A1                             Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : active sync
   Disk id A2                             Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : active sync
Disk Pair B                             Available
   Status                                   clean
   Disk id B1                             Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : active sync
   Disk id B2                             Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : active sync
```

STEP 4 | Retirez les deux premiers disques de 1 To de la première configuration de la baie RAID 1, puis retirez physiquement les lecteurs.

1. Pour supprimer les lecteurs de la configuration de la baie RAID 1 (A1 et A2 dans cet exemple), saisissez les commandes suivantes et entrez **y** lorsque vous êtes invité à confirmer chaque requête :

```
> request system raid remove A1
> request system raid remove A2
```

2. Retirez physiquement les disques des baies. Appuyez sur le bouton éjecteur de chaque transporteur pour libérer la poignée d'éjection. Tirez ensuite la poignée vers vous et glissez les lecteurs hors de l'appareil.
3. Retirez deux disques de 2 To de leur emballage et mettez-les sur une table à côté des lecteurs que vous venez de supprimer. Prenez note de la façon dont les lecteurs sont installés dans le transporteur parce que vous installez les lecteurs de 2 To dans ces mêmes transporteurs.
4. Retirez les quatre vis qui retiennent chaque disque dans son transporteur et retirez les disques des transporteurs.
5. Attachez les lecteurs de 2 To aux transporteurs à l'aide des mêmes vis que vous venez de supprimer, puis insérez les supports avec les lecteurs de 2 To installés récemment dans les baies de disques (A1 et A2 dans cet exemple).

STEP 5 | Créez une nouvelle matrice RAID 1 pour les lecteurs de 2 To installés et assurez-vous que les deux lecteurs sont dans la nouvelle matrice.

1. Pour créer un nouveau tableau comprenant le lecteur dans la baie A1, saisissez la commande suivante :

© 2020 Palo Alto Networks, Inc.

```
> request system raid add A1
```

2. Pour visualiser et confirmer l'état de la nouvelle configuration du tableau RAID 1, saisissez la commande suivante :

```
> show system raid detail
```

La sortie suivante montre que le tableau `paire de disques A` est `disponible`.



À ce stade, le lecteur A2 affichera `pas en cours d'utilisation`.

```
Disk Pair A       Available
   Status         clean, degraded
   Disk id A1     Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : active sync
   Disk id A2       Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : not in use
```

3. Ajoutez le deuxième disque au nouveau tableau. Dans cet exemple, ajoutez A2 :

```
> request system raid add A2
```

4. Continuez à exécuter la commande **`show System RAID detail`** pour visualiser la sortie RAID jusqu'à ce que l'état de la paire de disques affiche `Clean` et les deux disques affichent `Active Sync`.

STEP 6 | Mettez à niveau les lecteurs pour des matrices RAID 1 supplémentaires si nécessaire.

Pour mettre à niveau des matrices RAID 1 supplémentaires vers des disques de 2 To, répétez cette procédure pour remplacer les indicateurs de lecteur selon le cas. Par exemple, remplacez A1 par B1 et A2 par B2 pour mettre à niveau les lecteurs dans la matrice RAID 1 B1/B2.

Configurer Panorama pour l'utilisation de plusieurs interfaces

Dans un réseau à grande échelle, vous pouvez améliorer la sécurité et réduire la congestion en implémentant la segmentation du réseau, ce qui implique de séparer les sous-réseaux en fonction de l'utilisation des ressources, des rôles utilisateur et des exigences de sécurité. Panorama prend en charge la segmentation du réseau en vous permettant d'utiliser plusieurs Interfaces de l'appareil de série M pour la gestion des périphériques (pare-feu, collecteurs de journaux et appareils WildFire et clusters d'appareils) et la collecte des journaux ; vous pouvez affecter des interfaces distinctes aux périphériques sur des sous-réseaux distincts.

L'utilisation de plusieurs interfaces pour collecter les journaux offre également l'avantage d'équilibrer la charge, ce qui est particulièrement utile dans les environnements où les pare-feu transmettent les journaux à un débit élevé vers les collecteurs de journaux. Si vous activez le paramètre **forward to all Log Collectors (transférer à tous les collecteurs de journaux)** dans la liste de préférence de transfert de journaux du Groupe de collecteurs, les journaux sont envoyés sur toutes les interfaces configurées. Autrement, les journaux sont transférés via une seule interface, et si cette interface tombe en panne, le transfert des journaux se poursuit via l'interface configurée suivante. Par exemple, vous configurez Eth1/1, Eth1/2, et

© 2020 Palo Alto Networks, Inc.

Eth1/3 pour le transfert des journaux. Si l'interface Eth1/1 tombe en panne, le transfert des journaux se poursuit sur Eth1/2.

Étant donné que les administrateurs accèdent à Panorama et le gèrent via l'interface MGT, la sécurisation de cette interface est particulièrement importante. Une méthode pour améliorer la sécurité de l'interface MGT consiste à décharger les services Panorama sur d'autres interfaces. Outre la gestion des périphériques et la collecte des journaux, vous pouvez également décharger la communication du groupe de collecteurs et le déploiement des mises à jour logicielles et de contenu sur les pare-feu, les collecteurs de journaux, les appareils WildFire et les clusters d'appareils. En déchargeant ces services, vous pouvez réserver l'interface MGT pour le trafic administratif et l'affecter à un sous-réseau sécurisé qui est séparé des sous-réseaux où résident vos pare-feu, collecteurs de journaux et dispositifs WildFire et clusters d'appareils.

- Exemple d'interfaces multiples pour la segmentation du réseau
- Configurer Panorama pour la segmentation du réseau

Exemple d'interfaces multiples pour la segmentation du réseau

Figure 10: Interfaces Panorama multiples illustre un déploiement utilisant plusieurs interfaces sur des appareils M-500 en mode Panorama et en mode collecteur de journaux. Dans cet exemple, les interfaces prennent en charge la segmentation du réseau comme suit :

- **Réseau de gestion Panorama** : pour protéger l'interface Web Panorama, la CLI et l'API XML contre les accès non autorisés, l'interface MGT sur Panorama se connecte à un sous-réseau auquel seuls les administrateurs peuvent accéder.
- **Internet** : Panorama utilise l'interface MGT pour communiquer avec des services externes tels que le serveur de mise à jour Palo Alto Networks.
- **Passerelle de périmètre** et **Centre de données** : Panorama utilise une paire d'interfaces distincte pour gérer les pare-feu et les collecteurs de journaux dans chacun de ces sous-réseaux. La gestion des pare-feu génère généralement moins de trafic que l'interrogation des collecteurs de journaux pour les informations de rapport. Par conséquent, Panorama utilise des interfaces de 1 Gbit/s (Eth1 et Eth2) pour gérer les pare-feu et utilise des interfaces de 10 Gbit/s (Eth4 et Eth5) pour interroger et gérer les collecteurs de journaux. Chaque collecteur de journaux utilise son interface MGT pour répondre aux requêtes, mais utilise ses interfaces Eth4 et Eth5 pour le trafic plus important associé à la collecte de journaux à partir des pare-feu.
- **Mises à jour logicielles** : les pare-feu et les collecteurs de journaux des deux sous-réseaux récupèrent les mises à jour logicielles et de contenu sur l'interface Eth3 sur Panorama.

© 2020 Palo Alto Networks, Inc.

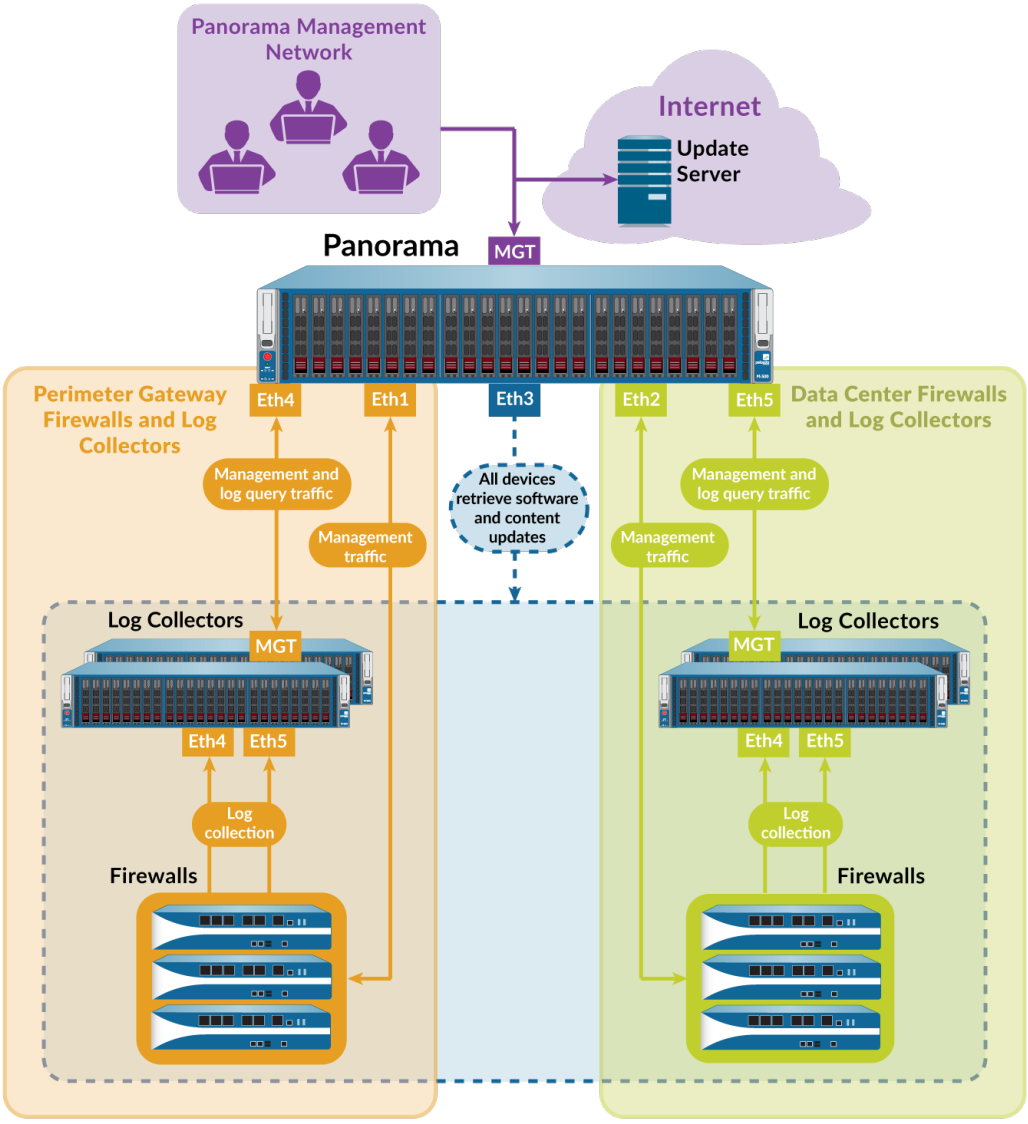


Figure 10: Interfaces Panorama multiples

Configurer Panorama pour la segmentation du réseau

Pour décharger les services Panorama de l'interface MGT vers d'autres interfaces, commencez par configurer les interfaces sur le serveur de gestion Panorama. Si le trafic de votre réseau est important, n'oubliez pas que les interfaces Eth4 et Eth5 de l'appareil M-500 prennent en charge un débit plus élevé (10 Gbit/s) que les autres interfaces (1 Gbit/s). Configurez ensuite les collecteurs de journaux dans chaque sous-réseau pour qu'ils se connectent à des interfaces spécifiques sur Panorama. Pour chaque collecteur de journaux, vous sélectionnez également une interface à utiliser pour la communication du groupe de collecteurs et une ou plusieurs interfaces à utiliser pour la collecte des journaux à partir des pare-feu. Enfin, configurez les pare-feu dans chaque sous-réseau pour la connexion aux interfaces sur Panorama.

Si vous configurez un appareil M-Series en mode Colleteur de journaux avec des interfaces de 10 Go, vous devez effectuer la totalité de cette procédure de configuration pour les interfaces de 10 GB pour qu'elles s'affichent en `Haut`*.*

© 2020 Palo Alto Networks, Inc.

Palo Alto Networks recommande de spécifier l'adresse IP, le masque réseau (pour IPv4) ou la longueur de préfixe (pour IPv6), ainsi que la passerelle par défaut pour l'interface MGT. Si vous omettez l'un de ces paramètres (comme la passerelle par défaut), vous pouvez uniquement accéder à l'appareil de série M via le port de la console pour les modifications de configuration futures.

Effectuez les étapes suivantes pour configurer Panorama et les collecteurs de journaux dédiés pour utiliser plusieurs interfaces :

STEP 1 | Vérifiez que les appareils Panorama et les pare-feu prennent en charge plusieurs interfaces et qu'ils possèdent les versions et configurations logicielles requises.

- Les appareils de série M doivent exécuter Panorama 8.0 ou une version ultérieure pour utiliser une interface distincte pour le déploiement des mises à jour et pour utiliser plusieurs interfaces pour la gestion des périphériques et la collecte des journaux. Les appareils M-200 et M-600 doivent exécuter Panorama 8.1 ou une version ultérieure. Les appareils Panorama déployés sur ESXi, vCloud, Air, Hyper-V et KVM doivent exécuter Panorama 8.1 ou toute version ultérieure.
- Si vous avez déployé un collecteur de journaux ou un Panorama en tant qu'appareil virtuel, vérifiez les interfaces prises en charge pour l'appareil virtuel Panorama.
- Les appareils de série M doivent exécuter Panorama 6.1 ou une version ultérieure pour utiliser des interfaces distinctes pour la collecte de journaux ou la communication de groupe de collecteurs.
- La configuration initiale de chaque serveur de gestion Panorama est terminée. Cela inclut la configuration de l'interface MGT.
- Les collecteurs de journaux et les groupes de collecteurs sont configurés. Cela inclut la configuration de l'interface MGT sur les collecteurs de journaux.
- La configuration initiale des pare-feu est terminée, vous avez ajouté les pare-feu à Panorama en tant que périphériques gérés, et les pare-feu de chaque sous-réseau sont affectés à un modèle distinct.
- La configuration initiale des appareils WildFire est terminée et vous avez ajouté des appareils WildFire à Panorama en tant que dispositifs gérés.

STEP 2 | Configurez les interfaces sur le serveur de gestion Panorama solitaire (non-HD) ou actif (HD).

Comme l'interface MGT a été configurée lors de la configuration initiale de Panorama, il n'est pas nécessaire de la configurer à nouveau.

Répétez ces étapes pour chaque interface :

1. Configurez les interfaces sur le serveur de gestion Panorama solitaire (non-HD) ou actif (HD).
2. Sélectionnez **Panorama** > **Setup (Configuration)** > **Interfaces**.
3. Cliquez sur un nom d'interface pour modifier l'interface.
4. Sélectionnez *<interface-name> (nom de l'interface)* pour activer l'interface.
5. Configurez un ou les deux champs selon les protocoles IP de votre réseau :
   - IPv4 : **IP Address (Adresse IP)**, **Netmask (Masque de sous-réseau)** et **Default Gateway (Passerelle par défaut)**
   - IPv6 : **IPv6 Address/Prefix Length (Longueur du préfixe / de l'adresse IPv6)** et **Default IPv6 Gateway (Passerelle IPv6 par défaut)**
6. Sélectionnez les services pris en charge par l'interface :
   - **Device Management and Device Log Collection (Gestion des périphériques et collecte des journaux de périphériques)** : gérez les pare-feu, les collecteurs de journaux, les appareils et les clusters d'appareils WildFire, collectez les journaux générés par les collecteurs de journaux et interrogez les collecteurs de journaux pour obtenir des informations sur les rapports. Pour prendre en charge un réseau segmenté, vous pouvez activer ces services sur plusieurs interfaces.

© 2020 Palo Alto Networks, Inc.

- **Collector Group Communication (Communication du groupe de collecteurs)** : communiquez avec les groupes de collecteurs que Panorama gère dans tous les sous-réseaux.
- **Device Deployment (Déploiement de périphériques)** : déployez des mises à jour logicielles et de contenu sur les pare-feu gérés, les collecteurs de journaux, les appareils WildFire et les clusters d'appareils sur tous les sous-réseaux.

7. Cliquez sur **OK** pour enregistrer vos modifications d'interface.
8. Cliquez sur **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.
9. Cliquez sur **Commit (Valider)** > **Push to Devices (Transmettre aux périphériques)** et transmettez les modifications au groupe de collecteurs qui contient les collecteurs de journaux que vous avez modifiés.

STEP 3 | (HA uniquement) Configurez les interfaces Web du serveur de gestion du Panorama passif.

1. Se connecter à l'interface Web Panorama du serveur de gestion Panorama actif.
2. Sélectionnez **Panorama (Panorama)** > **Managed Collectors (Collecteurs gérés)**, puis sélectionnez l'homologue HA passif.
3. Sélectionnez **Interfaces**, puis cliquez sur un nom d'interface à modifier.
4. Cochez la case **Enable Interface (Activer l'interface)** pour activer l'interface.
5. Configurez un ou les deux champs selon les protocoles IP de votre réseau :

   - IPv4 : **IP Address (Adresse IP)**, **Netmask (Masque de sous-réseau)** et **Default Gateway (Passerelle par défaut)**
   - IPv6 : **IPv6 Address/Prefix Length (Longueur du préfixe / de l'adresse IPv6)** et **Default IPv6 Gateway (Passerelle IPv6 par défaut)**

6. Sélectionnez les services pris en charge par l'interface :

   - **Device Management and Device Log Collection (Gestion des périphériques et collecte des journaux de périphériques)** : gérez les pare-feu, les collecteurs de journaux, les appareils et les clusters d'appareils WildFire, collectez les journaux générés par les collecteurs de journaux et interrogez les collecteurs de journaux pour obtenir des informations sur les rapports. Pour prendre en charge un réseau segmenté, vous pouvez activer ces services sur plusieurs interfaces.
   - **Collector Group Communication (Communication du groupe de collecteurs)** : communiquez avec les groupes de collecteurs que Panorama gère dans tous les sous-réseaux.
   - **Device Deployment (Déploiement de périphériques)** : déployez des mises à jour logicielles et de contenu sur les pare-feu gérés, les collecteurs de journaux, les appareils WildFire et les clusters d'appareils sur tous les sous-réseaux.

7. Cliquez sur **OK** pour enregistrer vos modifications d'interface.
8. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** pour valider vos modifications dans Panorama et pour appliquer les modifications aux groupes de collecteurs contenant l'homologue HA passif que vous avez modifié.

STEP 4 | Configurez chaque collecteur de journaux pour qu'il se connecte à une interface Panorama.

Pour prendre en charge un réseau segmenté, vous pouvez connecter les collecteurs de journaux dans chaque sous-réseau pour séparer les interfaces Panorama. Les interfaces doivent avoir **Device Management and Device Log Collection (Gestion des périphériques et collecte des journaux de périphériques)** activé, comme décrit à l'étape précédente.

1. Configurez les interfaces sur le serveur de gestion Panorama solitaire (non-HD) ou actif (HD).
2. Sélectionnez **Panorama (Panorama)** > **Managed Collectors (Collecteurs gérés)** et modifiez le collecteur de journaux.
3. Dans le champ **Panorama Server IP (IP du serveur Panorama)**, entrez l'adresse IP d'une interface sur le Panorama solitaire (non-HD) ou actif (HD).

© 2020 Palo Alto Networks, Inc.

4. (HD uniquement) Dans le champ **Panorama Server IP 2 (IP serveur Panorama 2)**, entrez l'adresse IP d'une interface sur le Panorama passif qui prendra en charge **Device Management and Device Log Collection (Gestion des périphériques et collecte des journaux de périphériques)** si le basculement se produit sur le Panorama actif.
5. Cliquez sur **OK** pour enregistrer vos modifications.
6. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** pour valider vos modifications dans Panorama et pour appliquer les modifications aux groupes de collecteurs contenant le collecteur de journaux que vous avez modifié.
7. Effectuez les étapes suivantes sur chaque collecteur de journaux dédié :
    1. Accédez à la CLI du collecteur de journaux en utilisant un logiciel d'émulation tel que PuTTY pour ouvrir une session SSH sur le collecteur de journaux à l'aide de l'adresse IP de son interface MGT. Lorsque vous y êtes invité, connectez-vous à l'aide des informations d'identification de l'administrateur Panorama.
    2. Exécutez les commandes suivantes, où *<IPaddress1>* (Adresse IP 1) est pour le Panorama solitaire (non-HD) ou actif (HD) et *<IPaddress2>* (adresse IP 2) est pour le Panorama passif (le cas échéant).

```
> configure
# set deviceconfig system panorama-server <IPaddress1> panorama-
server-2 <IPaddress2>
# commit
```

STEP 5 | (HD uniquement) Configurez une interface sur le serveur de gestion du Panorama passif pour déployer des mises à jour en cas de basculement du Panorama actif.

1. Se connecter à l'interface Web Panorama du serveur de gestion Panorama passif.
2. Sélectionnez **Panorama** > **Setup (Configuration)** > **Interfaces**.
3. Cliquez sur un nom d'interface pour modifier l'interface.
4. Sélectionnez *<interface-name> (nom de l'interface)* pour activer l'interface.
5. Configurez un ou les deux champs selon les protocoles IP de votre réseau :
    - IPv4 : **IP Address (Adresse IP)**, **Netmask (Masque de sous-réseau)** et **Default Gateway (Passerelle par défaut)**
    - IPv6 : **IPv6 Address/Prefix Length (Longueur du préfixe / de l'adresse IPv6)** et **Default IPv6 Gateway (Passerelle IPv6 par défaut)**
6. Sélectionnez **Device Deployment (Déploiement de périphériques)**.
7. Cliquez sur **OK** pour enregistrer vos modifications.
8. Cliquez sur **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

STEP 6 | Configurez les interfaces que les collecteurs de journaux utiliseront pour collecter les journaux des pare-feu et communiquer avec les autres collecteurs de journaux.

Étant donné que l'interface MGT a été configurée lors de la configuration initiale des collecteurs de journaux, il n'est pas nécessaire de le configurer à nouveau.

1. Configurez les interfaces sur le serveur de gestion Panorama solitaire (non-HD) ou actif (HD).
2. Sélectionnez **Panorama (Panorama)** > **Managed Collectors (Collecteurs gérés)** et modifiez le collecteur de journaux.
3. Sélectionnez **Interfaces** et effectuez les étapes suivantes pour chaque interface :
    1. Cliquez sur un nom d'interface pour modifier cette interface.
    2. Sélectionnez *<interface-name> (nom de l'interface)* pour activer l'interface.

© 2020 Palo Alto Networks, Inc.

3. Configurez un ou les deux des ensembles de champs suivants selon les protocoles IP de votre réseau.

   IPv4 : **IP Address (Adresse IP)**, **Netmask (Masque de sous-réseau)** et **Default Gateway (Passerelle par défaut)**

   IPv6 : **IPv6 Address/Prefix Length (Longueur du préfixe / de l'adresse IPv6)** et **Default IPv6 Gateway (Passerelle IPv6 par défaut)**
4. Sélectionnez les fonctions prises en charge par l'interface :

   Device Log Collection (Collecte de journaux de périphériques) : collectez des journaux à partir de pare-feu. Vous pouvez équilibrer le trafic de journalisation en permettant à plusieurs interfaces d'exécuter cette fonction.

   Collector Group Communication (Communication du groupe de collecteurs) : communiquez avec d'autres collecteurs de journaux dans le groupe de collecteurs.
5. Cliquez sur **OK** pour enregistrer vos modifications d'interface.

4. Cliquez sur **OK** pour enregistrer les modifications au collecteur de journaux.
5. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** pour valider vos modifications dans Panorama et pour appliquer les modifications aux groupes de collecteurs contenant les collecteurs de journaux que vous avez modifiés.
6. Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** pour vérifier que les collecteurs de journaux sont synchronisés et connectés à Panorama.

   La colonne Configuration Status (État de configuration) doit afficher `InSync` (synchronisation) et la colonne Run Time Status (État d'exécution) doit afficher `connected` (Connecté).

STEP 7 | Configurez les pare-feu pour qu'ils se connectent à une interface Panorama.

Pour prendre en charge un réseau segmenté, vous pouvez connecter les pare-feu dans chaque sous-réseau pour séparer les interfaces Panorama. Les interfaces doivent avoir **Device Management and Device Log Collection (Gestion des périphériques et collecte des journaux de périphériques)** activé. Cette étape suppose que vous utilisez des modèles distincts pour configurer les pare-feu dans des sous-réseaux distincts.



Dans cet exemple de déploiement, Panorama utilise ces interfaces pour gérer les pare-feu, mais pas pour collecter les journaux des pare-feu. Vous spécifiez les collecteurs de journaux dédiés qui collectent les journaux de pare-feu lorsque vous configurez les groupes de collecteurs*.*

1. Configurez les interfaces sur le serveur de gestion Panorama solitaire (non-HD) ou actif (HD).
2. Sur Panorama, sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)**, sélectionnez **Template (Modèle)** et modifiez les paramètres de Panorama.
3. Dans le premier champ **Panorama Servers (Serveurs Panorama)**, entrez l'adresse IP d'une interface sur le Panorama solitaire (non-HD) ou actif (HD).
4. (HD uniquement) Dans le deuxième champ **Panorama Servers (Serveurs Panorama)**, entrez l'adresse IP d'une interface sur le Panorama passif qui prendra en charge la gestion des périphériques en cas de basculement.
5. Cliquez sur **OK** pour enregistrer vos modifications.
6. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** pour valider vos modifications dans Panorama et appliquer les modifications de modèle aux pare-feu.
7. Sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)** pour vérifier que les pare-feu sont synchronisés et connectés à Panorama.

   La colonne Device State (État du périphérique) doit s'afficher `Connected (Connecté)`. Les colonnes Shared Policy (Politique partagée) et Template (Modèle) doivent s'afficher `In Sync`.

© 2020 Palo Alto Networks, Inc.

Enregistrer Panorama et Installer les licences

Avant de pouvoir utiliser Panorama pour la gestion, la journalisation et la génération de rapports centralisées, vous devez enregistrer, activer et récupérer les licences de gestion et de support des appareils Panorama. Chaque instance de Panorama exige des licences valides qui vous donnent droit à gérer les pare-feux et à obtenir un soutien. La licence de gestion du pare-feu impose le nombre maximum de pare-feu que Panorama puisse gérer. Cette licence est basée sur les numéros de série de pare-feu, et non pas sur le nombre de systèmes virtuels sur chaque pare-feu. La licence de support permet les mises à jour logicielles et des mises à jour de contenu dynamique de Panorama (pour les dernières applications et les signatures de menaces, à titre d'exemple). De plus, les appareils virtuels Panorama sur AWS et Azure doivent être achetées auprès de Palo Alto Networks et ne peuvent être achetées sur les places de marché AWS ou Azure.

Après avoir mis à niveau votre appareil virtuel Panorama vers PAN-OS 8.1, vous êtes invité à indiquer si une licence de capacité n'a pas été installée avec succès ou si le nombre total de pare-feu gérés par Panorama dépasse la licence de gestion des appareils. Vous disposez de 180 jours à compter de la date de mise à niveau pour installer une licence de gestion de périphérique valide si aucune licence n'a été installée. Si le nombre de pare-feu gérés dépasse la licence de gestion des périphériques, vous disposez de 180 jours pour supprimer les pare-feu afin de répondre aux exigences de licence de gestion des périphériques ou mettre à niveau votre licence de gestion des périphériques. Toutes les validations vont échouer si une licence de gestion de périphérique valide n'est pas installée ou si la limite de licence de gestion de périphérique existante n'est pas atteinte, dans les 180 jours suivant la mise à niveau. Pour acheter une licence de gestion de périphérique, contactez votre représentant commercial ou votre revendeur agréé chez Palo Alto Networks.

Si vous voulez utiliser Cortex Data Lake basé sur le cloud, vous avez besoin d'une licence Cortex Data Lake, en plus de la licence de gestion de pare-feu et de la licence de support premium. Pour acheter des licences, contactez votre ingénieur ou revendeur Palo Alto Networks Systems

Si vous exécutez une licence d'évaluation pour la gestion de pare-feu sur votre appareil virtuel panorama et que vous souhaitiez appliquer une licence panorama que vous avez achetée, effectuez les tâches Enregistrer Panorama *et* activez/récupérez une licence de gestion du pare-feu sur l'appareil virtuel Panorama*.*

- Enregistrer Panorama
- Activer une licence d'assistance Panorama
- Activer / Récupérer une licence de gestion de pare-feu lorsque l'appareil virtuel Panorama est connectée à Internet.
- Activer / Récupérer une licence de gestion de pare-feu lorsque l'appareil virtuel Panorama n'est pas connecté à Internet
- Activer / récupérer une licence de gestion de pare-feu sur l'appareil de la série M

Enregistrer Panorama

STEP 1 | Notez le numéro de série Panorama ou code d'authentification et enregistrez votre numéro de commande, de vente, ou de client.

Pour le code d'authentification des commandes, numéro de commande, de vente, ou de client, voir l'email que Service Clients de Palo Alto Networks vous a envoyé lorsque vous avez passé votre commande de Panorama.

Pour le numéro de série, l'emplacement dépend du modèle :

© 2020 Palo Alto Networks, Inc.

- Appareil de série M-Connectez-vous à l'interface Web Panorama et enregistrer le **Serial # (numéro de série)** La valeur de l' **Dashboard (Tableau de bord)** onglet, section Informations générales.
- Appareil virtuel Panorama : consultez le courrier électronique d'exécution de la commande.

STEP 2 | Enregistrer Panorama. Les étapes varient selon que vous ayez déjà une connexion au site de support.

- Si c'est le premier appareil Palo Alto Networks que vous enregistrez et que vous n'avez pas encore de connexion :
  1. Connectez-vous au site web de support de Palo Alto Networks.
  2. Cliquez sur **Register (Enregistrer)** au bas de la page (**Overview (Vue d'ensemble)** > **Get Help (Obtenir de l'aide)** > **Register (Enregistrer)**), entrez votre **Email Address (Adresse e-mail)**, entrez le code affiché sur la page et cliquez sur **Submit (Soumettre)**.
  3. Renseignez les champs de la section **Create Contact Details (Créer des détails de contact)**.
  4. Saisissez un **Display Name (Nom d'affichage)**, **Confirm Email Address (Confirmer l'adresse électronique)** et un **Password/Confirm Password (Mot de passe/Confirmer le mot de passe)**.
  5. Saisissez le **Device Serial Number** (Numéro de série du périphérique) ou **Auth Code** (Code d'autorisation) Panorama.
  6. Saisissez votre **Sales Order Number (Numéro de commande)** ou **Customer ID (Identifiant client)**.
  7. Cliquez sur **Submit (Envoyer)**.
- Si vous disposez déjà d'un compte de support :
  1. Connectez-vous au site web de support de Palo Alto Networks.
  2. Cliquez sur **Assets (Ressources)** > **Device (Périphérique)** > **Register New Device (Enregistrer un nouveau périphérique)**.
  3. Sélectionnez **Register device using Serial Number or Authorization Code (Enregistrer un périphérique au moyen d'un numéro de série ou d'un code d'autorisation)** et cliquez sur **Submit (Soumettre)**.
  4. Si le serveur de gestion Panorama n'est pas connecté à Internet, cochez la case **Device will be used offline (Périphérique utilisé hors ligne)** et sélectionnez la version du **OS Release (système d'exploitation)**.
  5. Saisissez le **Serial Number (Numéro de série)** Panorama.
  6. Entrez les informations de localisation requises (comme indiqué par les astérisques) si vous avez acheté le RMA 4 heures.
  7. **Agree and Submit (Accepter et soumettre)** le EULA.

     Après avoir vu le message d'enregistrement terminé, fermez la boîte de dialogue Device Registration (Enregistrement du périphérique).

Activer une licence d'assistance Panorama

Avant d'activer une licence de support Panorama sur un appareil Panorama de série M ou une application virtuelle Panorama, vous devez Enregistrer Panorama.

Si la licence de support expire, Panorama peut encore gérer les pare-feu et recueillir les journaux, mais les mises à jour de logiciels et de contenus ne seront plus disponibles. Les versions de logiciels et de contenus sur Panorama doivent être les mêmes ou ultérieures aux versions sur les pare-feu gérés, sinon des erreurs pourraient survenir. Pour plus d'informations, consultez la section Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire .

© 2020 Palo Alto Networks, Inc.

STEP 1 | Connectez-vous au portail d'assistance client de Palo Alto Networks pour activer le code d'authentification.

1. Sélectionnez **Assets (Ressources)** > **Devices (Périphériques)** et entrez votre numéro de série Panorama pour filtrer par **Serial Number (Numéro de série)**.
2. Sélectionnez l'icône en forme de crayon dans la colonne Action, sélectionnez **Activate Auth-Code (Activer le code d'autorisation)**, entrez votre **Authorization Code (Code d'autorisation)** de licence d'assistance et cliquez sur **Agree and Submit (Accepter et soumettre)**.

STEP 2 | Connectez-vous à l'interface Web Panorama et sélectionnez **Panorama** > **Support (Assistance)** > **Activate feature using authorization code (Activer la fonctionnalité à l'aide du code d'autorisation)**.

STEP 3 | Saisissez le **Authorization Code (Code d'autorisation)**, puis cliquez sur **OK**.

STEP 4 | Vérifiez que l'abonnement est activé. Vérifiez les détails (par exemple, la **Expiry Date (Date d'expiration)**, le **Level (Niveau)** de support et la **Description**) dans la section Support (Assistance) de la page.

Activer / Récupérer une licence de gestion de pare-feu lorsque l'appareil virtuel Panorama est connectée à Internet.

Pour gérer les appareils sur Panorama, vous devez activer une licence de gestion de pare-feu générée par PAN-OS. La licence de gestion de périphérique que vous activez détermine le nombre de périphériques que Panorama peut gérer. Les collecteurs de journaux et les appareils WildFire ne sont pas traités comme des périphériques gérés et ne seront pas comptabilisés dans le nombre d'appareils alloués par la licence de gestion de périphériques.

Avant d'activer et de récupérer une licence de gestion de périphérique sur l'appareil virtuel Panorama, vous devez Enregistrer Panorama. Si vous vous servez d'une licence d'évaluation et que vous souhaitiez appliquer une licence que vous avez achetée, vous devez toujours enregistrer et activer/récupérer la licence achetée. De même, vous devez changer le numéro de série de Panorama en le faisant passer du numéro de série d'évaluation au numéro de série de production.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Sélectionnez **Panorama (Panorama)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les Paramètres Généraux.

STEP 3 | Saisissez le **Serial Number (Numéro de série)** de Panorama (fourni dans l'e-mail de confirmation de commande), puis cliquez sur **OK**.

STEP 4 | Sélectionnez **Panorama** > **Licenses (Licences)**pour activer ou récupérer la licence de gestion du pare-feu :

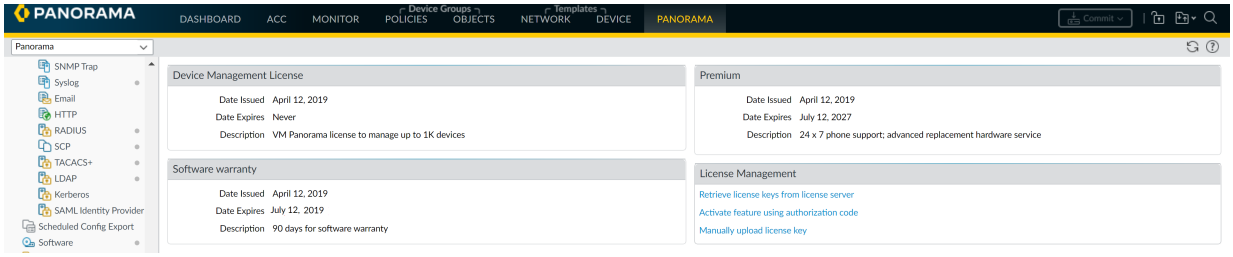
- **Retrieve license keys from license server (Récupérer les clés de la licence du serveur de licence)** : Panorama récupère et active automatiquement la licence de gestion du pare-feu du service de mise à jour de Panorama.
- **Activate feature using authorization code (Activer la fonctionnalité à l'aide du code d'autorisation)** : saisissez le code d'autorisation de la licence de gestion du pare-feu, puis cliquez sur **OK** pour activer la licence. On peut obtenir le code d'autorisation dans le courriel d'exécution de l'ordre ou en se connectant au site Web d'assistance client de Palo Alto Networks et en cherchant le serveur de gestion de Panorama.

© 2020 Palo Alto Networks, Inc.

- **Manually upload license key (Charger manuellement la clé de la licence)** : connectez-vous au site web de support de Palo Alto Networks., trouvez votre serveur de gestion Panorama et téléchargez la clé de la licence de gestion du pare-feu sur votre périphérique local. Après avoir téléchargé la clé de la licence, cliquez sur **Choose File (Choisir le fichier)** pour sélectionner la clé de la licence et cliquez sur **OK**.

STEP 5 | Vérifiez que la licence de gestion du pare-feu est activée.

La section Device Management License (Licence de gestion du périphérique) apparaît et affiche la date d'émission de la licence, la date d'expiration de la licence et une description de la licence de gestion du pare-feu.



Activer / Récupérer une licence de gestion de pare-feu lorsque l'appareil virtuel Panorama n'est pas connecté à Internet

Avant d'activer et de récupérer une licence de gestion de périphérique sur l'appareil virtuel Panorama, vous devez Enregistrer Panorama. Pour gérer les appareils sur Panorama, vous devez activer une licence de gestion de périphérique. La licence de gestion de périphérique que vous activez détermine le nombre de périphériques que Panorama peut gérer. Les collecteurs de journaux et les appareils WildFire ne sont pas traités comme des périphériques gérés et ne seront pas comptabilisés dans le nombre d'appareils alloués par la licence de gestion de périphériques. Si vous vous servez d'une licence d'évaluation et que vous souhaitiez appliquer une licence que vous avez achetée, vous devez toujours enregistrer et activer/récupérer la licence achetée.

Après la mise à niveau vers PAN-OS 8.1, vous serez invité à récupérer une licence de gestion Panorama valide lorsque vous vous connecterez pour la première fois à l'interface Web Panorama une fois le redémarrage terminé. Pour activer ou récupérer la licence de gestion valide si l'appareil virtuel Panorama est hors connexion ou ne parvient pas à atteindre le serveur de mise à jour de Palo Alto Networks, vous devez obtenir les informations d'appareils correspondantes pour l'appareil virtuel Panorama et les télécharger sur le site Web du support à la clientèle.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | (Déploiement initial seulement) Entrez le **Serial Number (Numéro de série)** de Panorama.

1. Sélectionnez **Panorama (Panorama)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les Paramètres Généraux.
2. Saisissez le **Serial Number (Numéro de série)** de Panorama (fourni dans l'e-mail de confirmation de commande), puis cliquez sur **OK**.
3. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

STEP 3 | Téléchargez les informations de l'appareil virtuel Panorama sur le site Web du support client.

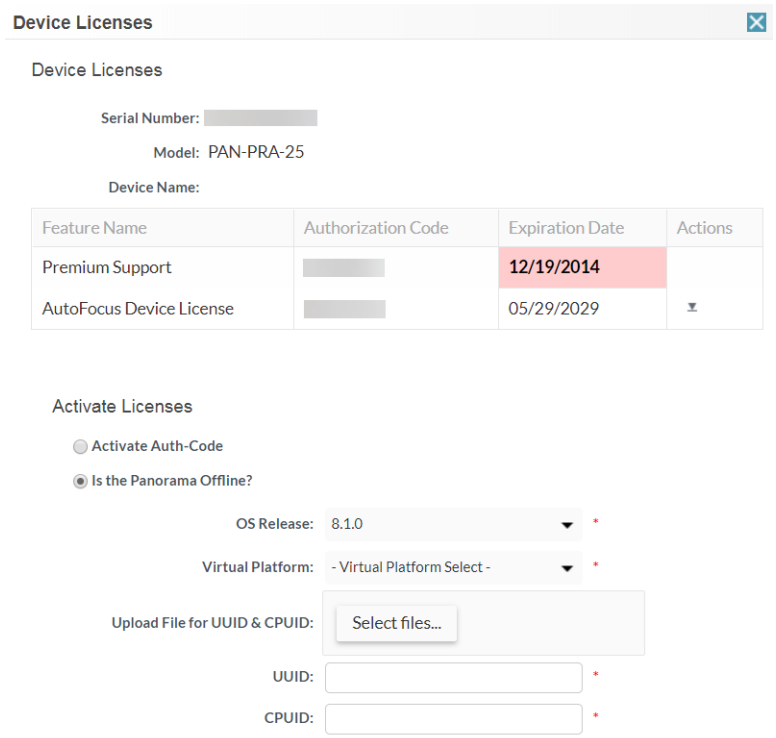
1. Dans la boîte de dialogue Retrieve Management License (Récupérer la licence de gestion), cliquez sur le lien **ici** pour regrouper les informations UUID, CPUID, Panorama et sur la plateforme

© 2020 Palo Alto Networks, Inc.

virtuelle. Cliquez sur **Download Link (Lien de téléchargement)** pour télécharger un fichier XML des informations Panorama requises pouvant être téléchargées sur le portail de support client.

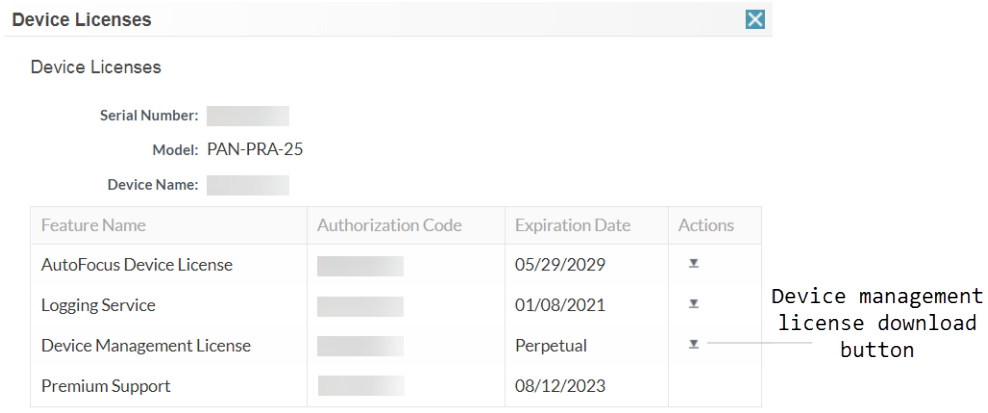
Lors du déploiement initial, vous devrez peut-être vous déconnecter et revenir à l'interface Web pour voir le dialogue.

2. Connectez-vous au site web de support de Palo Alto Networks.
3. Cliquez sur **Get Support (Soutien technique)** dans le coin supérieur droit.
4. Sélectionnez **Assets (Ressources)** > **Devices (Périphériques)**, trouvez votre appareil virtuel Panorama et, dans la colonne Action, cliquez sur l'icône de modification ( ).
5. Sélectionnez **Is the Panorama Offline? (Panorama est-il hors ligne?)** et entrez les informations Panorama collectées à l'étape 2 ou cliquez sur **Select files... (Sélectionner les fichiers ...)** pour télécharger le fichier XML téléchargé.
6. **Agree and Submit (Accepter et soumettre)** le EULA.



STEP 4 | Activer la licence de gestion de périphérique.

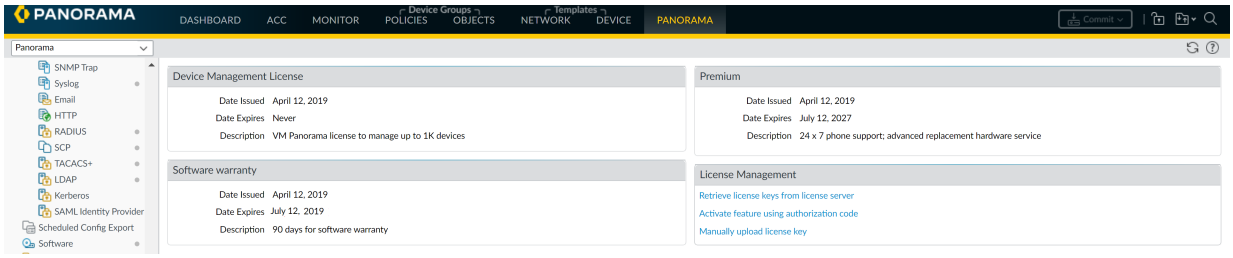
1. Dans la colonne Actions, téléchargez la licence de gestion de périphérique.



© 2020 Palo Alto Networks, Inc.

2. Dans l'interface web de Panorama, sélectionnez **Panorama** > **Licenses (Licences)**, cliquez sur **Manually upload license key (Charger manuellement la clé de licence)**.
3. Cliquez sur **Choose file (Choisir le fichier)**, localisez la clé de licence de gestion de périphérique téléchargée et cliquez sur **OK**.

STEP 5 | Confirmez que la licence de gestion de périphérique a été téléchargée avec succès en vérifiant que la licence de gestion de périphérique s'affiche avec les informations de licence.



Activer / récupérer une licence de gestion de pare-feu sur l'appareil de la série M

Pour pouvoir gérer des appareils sur Panorama, vous devez activer une licence de capacité. La licence de capacité détermine le nombre de périphériques que Panorama peut gérer. Les collecteurs de journaux et les dispositifs WildFire ne sont pas traités comme des périphériques gérés et ne sont pas comptabilisés dans le nombre de périphériques attribués par la licence de capacité.

Avant d'activer et de récupérer une licence de gestion de pare-feu Panorama sur l'appareil de série M :

- Enregistrez Panorama.
- Localisez les codes d'authentification pour le produit / abonnement que vous avez acheté. Lorsque vous avez passé votre commande, le service à la clientèle de Palo Alto Networks vous a envoyé un courriel indiquant le code d'authentification associé à l'achat. Si vous ne trouvez pas ce e-mail, contactez le Support Client Palo Alto Networks pour obtenir vos codes avant de poursuivre.

Après avoir activé et récupéré la licence, la page **Panorama** > **Licenses (Licences)** indique la date d'émission, la date d'expiration associée et le nombre de périphériques que Panorama peut gérer via la licence.

Les options d'activation et de récupération de la licence sont les suivantes :

- Utilisez l'interface web pour activer et récupérer la licence.

  Sélectionnez cette option si Panorama est prêt pour une connexion au serveur de mises à jour Palo Alto Networks (vous avez effectué la tâche Exécuter la configuration initiale de l'appareil de Série M) mais que vous n'avez pas activé la licence sur le site Web de Support Client de Palo Alto Networks.

  1. Sélectionnez **Panorama** > **Licenses (Licences)** et cliquez sur **Activate feature using authorization code (Activer la fonction à l'aide du code d'autorisation)**.
  2. Saisissez le **Authorization Code (Code d'autorisation)**, puis cliquez sur **OK**. Panorama récupère et active la licence.

- Récupérer la clé de licence à partir du serveur de licence.

  Si Panorama est pas prêt à se connecter au serveur de mise à jour (par exemple, vous n'avez pas terminé la configuration initiale de l'appareil de série M), vous pouvez activer la licence sur le site Web de support de telle sorte que, lorsque Panorama est prêt à vous connecter, vous pouvez alors utiliser l'interface web pour récupérer la licence activée. Le processus de récupération d'une licence activée est plus rapide que le processus de récupération et d'activation à la fois.

© 2020 Palo Alto Networks, Inc.

1. Activez la licence sur le site web de Support Client de Palo Alto Networks.
    1. Sur un hôte doté d'un accès Internet, utilisez un navigateur web pour accéder au site web de Support Client de Palo Alto Networks et connectez-vous.
    2. Sélectionnez **Assets (Ressources)** > **Devices (Périphériques)**, trouvez votre appareil de série M et, dans la colonne Action, cliquez sur l'icône de modification ( ).
    3. Sélectionnez **Activate Auth-Code (Activer le code d'autorisation)**, saisissez le **Authorization Code (Code d'autorisation)**, puis cliquez sur **Agree and Submit (Activer et soumettre)** pour activer la licence.
2. Configurez panorama pour vous connecter au serveur de mise à jour : reportez-vous à la Configuration Initiale de l'Appareil de Série M.
3. Sélectionnez **Panorama** > **Licenses(Licences)**, puis cliquez sur **Retrieve license keys from the license server (Récupérer les clés de licence auprès du serveur de licences)**. Panorama récupère la licence activée.

- Charger manuellement la licence d'un hôte sur Panorama. Panorama doit avoir accès à cet hôte.

  Si Panorama est configuré (vous avez effectué la tâche Effectuer la configuration initiale de l'appareil de Série M) mais qu'il ne dispose pas d'une connexion au serveur de mises à jour, activez la licence sur le site web de Support, téléchargez-la sur l'hôte connecté au serveur de mises à jour, puis téléchargez-la sur Panorama.

  1. Activez et téléchargez la licence sur le site web de Support de Palo Alto Networks.
      1. Sur un hôte doté d'un accès Internet, utilisez un navigateur web pour accéder au site web de Support Client de Palo Alto Networks et connectez-vous.
      2. Sélectionnez **Assets (Ressources)** > **Devices (Périphériques)**, trouvez votre appareil de série M et, dans la colonne Action, cliquez sur l'icône de modification ( ).
      3. Sélectionnez **Activate Auth-Code (Activer le code d'autorisation)**, saisissez le **Authorization Code (Code d'autorisation)**, puis cliquez sur **Agree and Submit (Activer et soumettre)** pour activer la licence.
      4. Dans la colonne Action, cliquez sur l'icône de téléchargement et enregistrez le fichier de clé de licence sur l'hôte.
  2. Dans l'interface web de Panorama, sélectionnez **Panorama** > **Licenses (Licences)**, cliquez sur **Manually upload license key (Charger manuellement la clé de licence)**, puis cliquez sur **Browse (Parcourir)**.
  3. Sélectionnez le fichier de clé que vous avez téléchargé sur l'hôte, puis cliquez sur **Open (Ouvrir)**.
  4. Cliquez sur **OK** pour charger la clé de licence activée.

© 2020 Palo Alto Networks, Inc.

Installation du certificat du périphérique Panorama

Dans PAN-OS 9.1.3 et les versions ultérieures, vous devez installer le certificat du périphérique sur le serveur de gestion Panorama™ pour réussir à authentifier Panorama auprès du portail de support client (CSP) de Palo Alto Networks et exploiter des services cloud comme Zero Touch Provisioning (ZTP), Device Telemetry, IoT et Entreprise Data Loss Prevention (prévention des pertes de données - DLP). Panorama doit avoir accès à Internet pour installer avec succès le certificat du périphérique.



Si vous exploitez le plug-in Cloud Services, vous devez avoir le plug-in Cloud Services 1.5 ou une version ultérieure *installée afin de réussir l'installation du certificat du périphérique Panorama.*

STEP 1 | Enregistrer PanoramaConnectez-vous au portail de support client (CSP) de Palo Alto Networks.

STEP 2 | Configurez le serveur Network Time Protocol (protocole d'heure réseau - NTP).

Un serveur NTP est nécessaire pour valider la date d'expiration de la certification du périphérique, s'assurer que le certificat du périphérique n'expire pas prématurément ou ne devienne pas invalide.

1. Se connecter à l'interface Web Panorama.
2. Sélectionnez **Panorama** > **Setup (Configuration)** > **Services**.
3. Sélectionnez **NTP** et saisissez le nom d'hôte `pool.ntp.org` comme **serveur NTP primaire** ou saisissez l'adresse IP de votre serveur NTP primaire.
4. (Facultatif) Saisissez une **Secondary NTP Server (adresse IP de serveur DNS Secondary (Secondaire))**.
5. (Facultatif Pour authentifier les mises à jour de temps à partir du (des) serveur (s) NTP, pour le **Authentification Type (Type d'authentification)**, sélectionnez l'un des éléments suivants pour chaque serveur.
   - **None (Aucun)** (Par défaut) : Désactive l'authentification NTP.
   - **Symmetric Key (Clé symétrique)**: Le pare-feu utilise l'échange de clés symétrique (secrets partagés) pour authentifier les mises à jour de temps.
     - **Key ID (ID de clé)** : Saisissez l'ID de la clé (1-65534).
     - **Algorithm (Algorithme)** : Sélectionnez l'algorithme à utiliser lors de l'authentification NTP (**MDS** or **SHA1**)
6. Cliquez sur **OK** pour enregistrer votre configuration.
7. Sélectionnez **Commit (Valider)** et **Commit to Panorama (Validez sur Panorama)**.

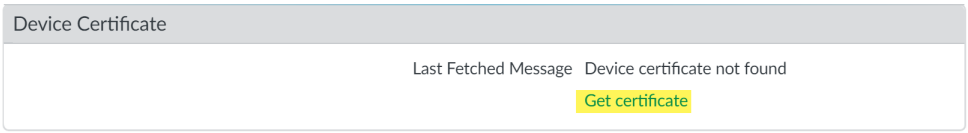
STEP 3 | Générer le One-Time Password (mot de passe à usage unique ; OTP).

1. Ouvrez une session dans le portail de support client.
2. Sélectionnez **Assets (Ressources)** > **Device Certificates (Certificats de périphériques)** et **Generate OTP (Générer un OTP)**.
3. Pour le **Device Type (Type de périphérique)**, sélectionnez **Generate OTP for Panorama (Générer un OTP pour Panorama)** et **Generate OTP (Générer un OTP)**.
4. Sélectionnez le numéro de série du **Panorama Device (Périphérique Panorama)**.
5. **Generate OTP (Générez un OTP)** puis copiez-le.

STEP 4 | Se connecter à l'interface Web Panorama en tant qu'utilisateur admin.

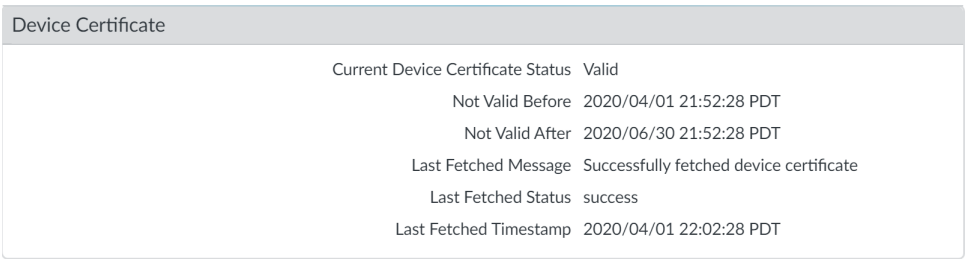
© 2020 Palo Alto Networks, Inc.

STEP 5 | Sélectionnez **Panorama** > **Setup (Configuration)** > **Management (Gestion)** > **Device Certificate Settings (Paramètres du certificat du périphérique)** et **Get certificate (Obtenir le certificat)**.



STEP 6 | Saisissez le **One-Time Password (mot de passe à usage unique - OTP)** que vous avez généré puis cliquez sur **OK**.

STEP 7 | Le certificat est récupéré et installé avec succès par Panorama.



© 2020 Palo Alto Networks, Inc.

Installer les mises à jour de contenu et logicielles pour Panorama

Un abonnement de support valide permet d'accéder à l'image du logiciel et aux notes de version Panorama. Pour profiter des dernières corrections et améliorations de la sécurité, passez à la dernière mise à jour de logiciel et de contenu que votre revendeur ou un ingénieur système de Palo Alto Networks® recommande pour votre déploiement. La procédure d'installation des mises à jour de logiciel et de contenu dépend de si Panorama dispose d'une connexion directe à Internet et d'une configuration haute disponibilité (HD).

- Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire
- Installer les mises à jour pour Panorama dans une configuration HD
- Installer des mises à jour pour Panorama avec une connexion Internet
- Installer des mises à jour de Panorama sans connexion Internet
- Installer des mises à jour de Panorama sans connexion Internet
- Migrer les journaux de Panorama vers le nouveau format de journal

Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire

Pour de meilleurs résultats, respectez les consignes de compatibilité Panorama™ suivantes :

- Installez la même version de Panorama sur le serveur de gestion Panorama et sur les collecteurs de journaux dédiés.
- Panorama doit exécuter la même version ou une version ultérieure de PAN-OS que du pare-feu qu'il gère. Avant de mettre à niveau les pare-feux vers PAN-OS 10.0, vous devez d'abord mettre à niveau Panorama vers la version 10.0.

  Cependant, Panorama 6.1 et les versions ultérieures ne peuvent pas appliquer des configurations de pare-feu exécutant PAN-OS à 6.0.0 à 6.0.3.
- Panorama exécutant PAN-OS 10.0 peut gérer les appareils et les clusters d'appareils WildFire® qui exécutent la même version ou une version antérieure de PAN-OS 10.0. Il est recommandé que le serveur de gestion Panorama, les appareils WildFire et les clusters d'appareils WildFire exécutent la même version de PAN-OS.
- La version de contenu sur le serveur de gestion Panorama doit être identique (ou antérieure) à celle des collecteurs de journaux dédiés ou des pare-feu gérés.

  Palo Alto Networks® vous recommande d'installer la même version de la base de données des applications sur Panorama que celle des collecteurs de journaux dédiés et ses pare-feu.

  Indépendamment de si vos abonnements incluent la base de données des applications ou des applications et des menaces, Panorama n'installe que la base de données des applications. Panorama et les collecteurs de journaux dédiés n'appliquent pas les règles de stratégie et n'ont donc pas besoin des signatures de menaces de la base de données des menaces. La base de données des applications contient des métadonnées de menace (telles que les ID de menace et les noms) que vous utilisez sur Panorama et les collecteurs de journaux dédiés lors de la définition des règles de stratégie pour insérer vers les pare-feu gérés et lors de l'interprétation des informations de menace dans les journaux et les rapports. Cependant, les pare-feu requièrent la base de données complète des applications et des menaces pour faire correspondre les identifiants enregistrés dans les journaux avec les noms de menace, d'URL, ou d'application correspondants. Consultez les Notes de publication pour la version de contenu minimale que vous devez installer pour une version de Panorama.

© 2020 Palo Alto Networks, Inc.

Installer les mises à jour pour Panorama dans une configuration HD

Pour assurer un basculement transparent lorsque vous mettez à jour le logiciel Panorama dans une configuration haute disponibilité (HD), les homologues Panorama actifs et passifs doivent exécuter la même version Panorama avec la même version de la base de données Applications. L'exemple suivant décrit comment mettre à jour une paire HD (l'homologue actif est nommé Primaire_A et l'homologue passif est nommé Secondaire_B).

Avant de mettre à jour Panorama, reportez-vous aux Notes de version pour la version de contenu minimum requise pour PAN-OS 10.0.

STEP 1 | Mettez à niveau le logiciel Panorama sur l'homologue Secondaire_B (passif).

Effectuez l'une des tâches suivantes sur l'homologue Secondaire_B :

- Installer des mises à jour pour Panorama avec une connexion Internet
- Installer des mises à jour pour Panorama lorsqu'il n'est pas connecté à Internet

Après la mise à niveau, ce Panorama passera à un état non fonctionnel car les homologues n'exécutent plus la même version de logiciel.

STEP 2 | Suspendez l'homologue Primaire_A pour forcer un basculement.

Sur l'homologue Primaire_A :

1. Dans la section Operational Commands (Commandes opérationnelles) (PanoramaHigh Availability (Haute disponibilité)), cliquez sur le lien Suspend local Panorama (Suspendre le Panorama local).
2. Vérifiez que l'état est `suspended` (suspendu) (affiché dans le coin inférieur droit de l'interface Web).

   Le basculement qui en résulte devrait provoquer la transition de l'homologue Secondaire_B vers l'état `active` (actif).

STEP 3 | Mettez à niveau le logiciel Panorama sur l'homologue Primaire_A (actuellement passif).

Effectuez l'une des tâches suivantes sur l'homologue Primaire_A :

- Installer des mises à jour pour Panorama avec une connexion Internet
- Installer des mises à jour pour Panorama lorsqu'il n'est pas connecté à Internet

Après le redémarrage, l'homologue Primaire_A est initialement toujours à l'état passif. Ensuite, si la préemption est activée (par défaut), l'homologue Primaire_A passe automatiquement à l'état actif et l'homologue Secondaire_B revient à l'état passif.

Si vous désactivez la préemption, restaurez manuellement le panorama principal à l'état actif.

STEP 4 | Vérifiez que les deux homologues exécutent maintenant les versions de mise à jour de contenu nouvellement installées et la version Panorama nouvellement installée.

Sur le **Dashboard (Tableau de bord)** de chaque homologue Panorama, vérifiez la version du logiciel Panorama et la version de l'application, et confirmez qu'elles sont identiques sur les deux homologues et que la configuration en cours est synchronisée.

STEP 5 | (Collecteurs de journaux locaux dans un groupe de collecteurs uniquement) Mettez à niveau les collecteurs de journaux restants dans le groupe de collecteurs.

- Mettre à niveau les collecteurs de journaux lorsque Panorama est connecté à Internet
- Mettre à niveau les collecteurs de journaux lorsque Panorama n'est pas connecté à Internet

© 2020 Palo Alto Networks, Inc.

Installer des mises à jour pour Panorama avec une connexion Internet

Si Panorama™ dispose d'une connexion directe à Internet, suivez les étapes suivantes pour installer les mises à jour du logiciel Panorama et du contenu au besoin. Si Panorama est exécuté dans une configuration haute disponibilité (HD), mettez à niveau le logiciel Panorama sur chaque homologue (voir Installer les mises à jour pour Panorama dans une configuration HD).

La mise à niveau du logiciel sur l'appareil virtuel Panorama ne modifie pas le mode du système ; le passage en mode Panorama ou en mode de Gestion est une tâche manuelle qui nécessite des paramètres supplémentaires tels que décrits lorsque vous configurez l'appareil virtuel Panorama avec le collecteur de journaux local.

PAN-OS® 9.0 a intégré un nouveau format de données de journaux pour les collecteurs de journaux dédiés et locaux. Lorsque vous passez à PAN-OS 10.0, les données de journaux existantes sont automatiquement converties au nouveau format lors de la mise à niveau de PAN-OS 10.0. Lors du reformatage, les données des journaux ne sont pas visibles dans les onglets **ACC** ou **Monitor (Surveillance)**. De plus, les nouvelles données des journaux ne sont pas transférées aux collecteurs de journaux avant que le reformatage a été effectué. Lors du reformatage, de nouveaux journaux sont rédigés sur le disque système du pare-feu et après que la procédure a terminé avec succès, les nouveaux journaux sont transmis au collecteur de journaux appropriée.

Vous devez mettre à niveau tous les collecteurs de journaux d'un groupe de collecteurs en même temps afin d'éviter de perdre des données de journal. Aucun transfert de journaux ou collecte de journaux ne se produit si les collecteurs de journaux d'un groupe de collecteurs n'utilisent pas tous la même version de PAN-OS. De plus, les données des journaux des collecteurs de journaux du groupe de collecteur ne sont pas visibles dans les onglets **ACC** ou **Monitor (Surveillance)** jusqu'à ce que tous les collecteurs de journaux exécutent la même version PAN-OS. Par exemple, si vous disposez de trois collecteurs de journaux dans un groupe de collecteurs et que vous mettez à niveau deux d'entre eux, aucun journal n'est alors transmis aux collecteurs de journaux du groupe de collecteurs.

Avant de mettre à jour Panorama, reportez-vous aux Notes de version pour la version de contenu minimum requise pour PAN-OS 10.0.

Pour Panorama sur Azure, vous devez exécuter quelques étapes supplémentaires avant de mettre à jour la version logicielle avec succès. Pour procéder à la mise à niveau, vous devez exporter la configuration de Panorama, mettre à niveau les versions de contenu et les versions logicielles, puis importez la configuration vers le serveur de gestion de Panorama une fois la mise à niveau réussie.

STEP 1 | Vérifiez que les mises à jour que vous prévoyez d'installer sont appropriées pour votre déploiement Panorama.

- Consultez les Notes de version pour la version de contenu minimum requise pour une version de logiciel Panorama. Si vous souhaitez mettre à niveau des pare-feu et des collecteurs de journaux vers une version particulière, vous devez d'abord mettre à niveau Panorama à cette version (ou à une version ultérieure).
- Pour un appareil virtuel Panorama qui fonctionne sur un hyperviseur, assurez-vous que l'instance respecte la configuration prérequise pour l'appareil virtuel Panorama.

STEP 2 | Enregistrez une sauvegarde du fichier de configuration Panorama en cours que vous pouvez utiliser pour restaurer la configuration si vous rencontrez des problèmes avec la mise à niveau.

Bien que Panorama crée automatiquement une sauvegarde de la configuration, l'idéal consiste à créer et à stocker à l'extérieur une sauvegarde avant la mise à niveau.

© 2020 Palo Alto Networks, Inc.

1. Cliquez sur **Save named Panorama configuration snapshot (Enregistrer un instantané de configuration nommé Panorama)** (**Panorama** > **Setup (Configuration)** > **Operations (Opérations)**), entrez un **Name (Nom)** pour la configuration et cliquez sur **OK**.
2. Cliquez sur **Export named Panorama configuration snapshot (Exporter l'instantané de configuration nommé Panorama)**, sélectionnez le **Name (Nom)** de la configuration que vous venez d'enregistrer, cliquez sur **OK**, et enregistrez le fichier exporté à un emplacement qui est externe à Panorama.

STEP 3 | (Au besoin) Installez les mises à jour de contenu.

Si Panorama n'exécute pas les versions de contenu minimum requises pour la version Panorama vers laquelle vous souhaitez effectuer la mise à niveau, vous devez mettre à jour les versions de contenu vers les versions minimales (ou ultérieures) avant d'installer les mises à jour logicielles. Consultez les Notes de version *pour la version de contenu minimale pour une version de Panorama.*

Palo Alto Networks® recommande fortement que Panorama, les collecteurs de journaux et tous les pare-feu gérés exécutent la même version de contenu. De plus, nous vous recommandons de planifier des mises à jour automatiques et récurrentes afin que vous exécutiez toujours les dernières versions de contenu (reportez-vous à 9).

1. **Check Now (Vérifier maintenant)** (**Panorama** > **Dynamic Updates (Mises à jour dynamiques)**) les dernières mises à jour. Si la valeur dans la colonne Action est **Download (Télécharger)**, une mise à jour est disponible.

   Assurez-vous que Panorama exécute la même version de contenu, mais pas une version ultérieure à celle exécutée sur les pare-feu gérés et les collecteurs de journaux.
2. (Au besoin) Avant de mettre à jour la version du contenu sur Panorama, assurez-vous de mettre à niveau les pare-feu gérés puis les collecteurs de journaux (voir Mettre à niveau les collecteurs de journaux lorsque Panorama est connecté à Internet) à la même version de contenu (ou une version ultérieure).

   Si vous n'avez pas besoin d'installer de mises à jour de contenu pour le moment, passez directement à la prochaine étape.
3. Installez les mises à jour de contenu restantes en fonction des besoins. Lorsque l'installation est terminée, la colonne Currently Installed (Actuellement installé) affiche une coche.
   1. **Download (Téléchargez)** et **Install (installez)** les applications ou les applications et mises à jour des menaces. Indépendamment de votre abonnement, Panorama installe et n'a besoin que de la mise à jour de contenu des applications, et non du contenu des menaces. Pour plus d'informations, consultez la section Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire .
   2. **Download (Téléchargez)** et **Install (Installez)** toutes les autres mises à jour (antivirus, WildFire® ou filtrage d'URL) une à la fois, dans n'importe quel ordre.

STEP 4 | Déterminer le chemin de mise à niveau vers PAN-OS 10.0.

Vous ne pouvez pas sauter l'installation de versions majeures (avec de nouvelles fonctionnalités) dans le chemin de mise à jour de la version PAN-OS en cours vers PAN-OS 10.0. Passez en revue les problèmes connus et les modifications du comportement par défaut dans les Notes de version et les considérations de mise à niveau vers une version supérieure ou antérieure dans le Guide des nouvelles fonctionnalités de chaque version à travers laquelle vous passez dans le cadre de votre chemin de mise à niveau.

(Requis si vous faites une mise à niveau à partir de la version 7.1 ou antérieure) PAN-OS 8.0 a lancé un nouveau format de stockage des journaux. Après avoir effectué la mise à niveau vers PAN-OS 8.0, vous

© 2020 Palo Alto Networks, Inc.

devez Migrer les journaux de Panorama vers le nouveau format de journal avant de continuer la mise à niveau. La migration de journaux est une tâche ponctuelle. Si vous avez déjà migré les journaux sur le collecteur de journaux pour une mise à niveau vers PAN-OS 8.0, vous n'avez pas besoin de les migrer à nouveau lorsque vous passez à PAN-OS 8.1.



Si vous mettez à niveau plusieurs collecteurs de journaux, rationalisez le processus en déterminant les chemins de mise à niveau pour tous les collecteurs de journaux que vous avez l'intention de mettre à niveau avant de commencer à télécharger des images.

STEP 5 | Installez Panorama 10.0.

1. Cliquez sur **Check Now (Vérifier maintenant)** (**Panorama** > **Software (Logiciel)**) pour rechercher les dernières mises à jour. Si une version logicielle est disponible, la colonne Action affiche **Download (Télécharger)**.
2. Localisez et **Download (Téléchargez)** le fichier spécifique au modèle pour la version finale vers laquelle vous effectuez la mise à niveau. Par exemple, pour mettre à niveau un appareil de série M vers Panorama 10.0.0, téléchargez l'image `Panorama_m-10.0.0`. Pour mettre à niveau un appareil virtuel Panorama vers Panorama 10.0.0, `téléchargez l'image Panorama_pc-10.0.0`. Après un téléchargement réussi, la colonne Action passe de **Download (Télécharger)** à **Install (Installer)** pour l'image téléchargée.
3. (Vous ne pouvez pas sauter l'installation de versions de fonctions dans le chemin de la version PAN-OS en cours vers PAN-OS 10.0.0.) Installez l'image téléchargée et redémarrez.
   1. Installez l'image.
   2. Une fois l'installation terminée, redémarrez en utilisant l'une des méthodes suivantes :
      - Si vous êtes invité à redémarrer, cliquez sur **Yes (Oui)**. Si une invite CMS Login s'affiche, appuyez sur Entrée sans saisir de nom d'utilisateur ou de mot de passe. Lorsque l'invite de connexion Panorama s'affiche, saisissez le nom d'utilisateur et le mot de passe que vous avez spécifiés lors de la configuration initiale.
      - Si vous n'êtes pas invité à redémarrer, cliquez sur **Reboot Panorama (Redémarrer Panorama)** dans la section Device Operations (Opérations de périphérique) (**Panorama** > **Setup (Configuration)** > **Operations (Opérations)**).
4. (Requis uniquement lors d'une mise à niveau vers PAN-OS 9.1.1 ou une version ultérieure) Après avoir effectué les étapes ci-dessus pour l'image de base PAN-OS 10.0, répétez les étapes 1 à 3 pour passer à la version de maintenance cible.

STEP 6 | Vérifiez l'état de la migration du format des journaux après la réussite d'une mise à niveau vers PAN-OS 10.0.

1. Connectez-vous à l'ILC Panorama du collecteur de journaux.
2. Exécutez la commande suivante pour vérifier l'état de la migration du formation des journaux :

```
admin> debug logdb show-es-upgrade-time
```

Réponse type lorsque la migration du format des journaux est toujours en cours :

```
Response
from logger 23456212: 50.98% of indices upgraded complete. Approximately
less than a minute remaining until migration is complete. Once the
log migration is complete, please run the 'show log-collector-es-cluster
health' command to check the ElasticSearch cluster status to verify
logging and reporting functionality is restored.
```

Réponse lorsque la migration du format des journaux est terminée :

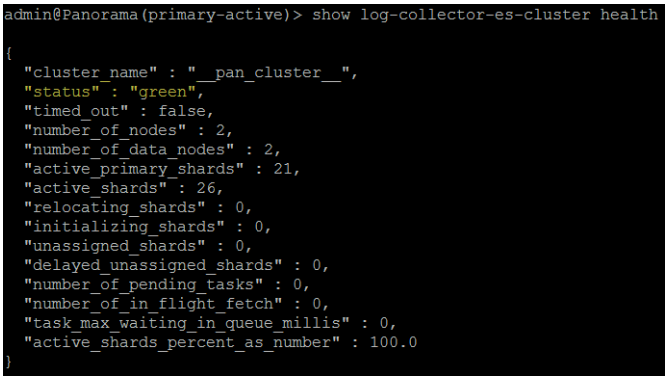
© 2020 Palo Alto Networks, Inc.

```
Response
from logger 23456212: 100% of indices complete. Please run the 'show
log-collector-es-cluster health' command to check the ElasticSearch
cluster status to verify logging and reporting functionality is
restored.
```

3. Une fois la migration du format des journaux est terminé, exécutez la commande suivante pour vérifier l'état du cluster ElasticSearch avant de passer à l'étape suivante :

```
admin> show log-collector-es-cluster health
```

Passez à l'étape suivante lorsque l'état de santé (`"status"`) du cluster ElasticSearch indique `"green"` :



STEP 7 | (Panorama sur Azure uniquement) Chargez la configuration de Panorama que vous avez exportée à l'étape 2.

1. **Import named Panorama configuration snapshot (Importez un instantané de configuration nommé Panorama)** (**Panorama** > **Setup (Configuration)** > **Operations (Opérations)**), **Browse (Cherchez)** et sélectionnez le fichier de configuration Panorama, puis cliquez sur **OK**.
2. **Load named Panorama configuration snapshot (Chargez un instantané de configuration nommé Panorama)**, sélectionnez le **Name (Nom)** de la configuration que vous venez d'importer, saisissez la **Decryption Key (Clé de décryptage)** au besoin, puis cliquez sur OK.
3. Connectez-vous à l'ILC Panorama.
4. Validez la configuration de Panorama en entrant les commandes suivantes :

```
admin> configure
```

```
admin> commit force
```

STEP 8 | (Si le collecteur de journaux locaux dans un groupe de collecteurs uniquement) Mettez à niveau les collecteurs de journaux restants dans le groupe de collecteurs.

- Mettre à niveau les collecteurs de journaux lorsque Panorama est connecté à Internet
- Mettre à niveau les collecteurs de journaux lorsque Panorama n'est pas connecté à Internet

STEP 9 | (Recommandé) Programmez les mises à jour automatiques de contenu.

Panorama ne synchronise pas les calendriers de mise à jour de contenu dans les paires HD. Vous devez effectuer cette tâche à la fois sur le panorama actif et passif.

© 2020 Palo Alto Networks, Inc.

Dans la ligne d'en-tête pour chaque type (**Panorama** > **Dynamic Updates (Mises à jour dynamiques)**), le **Schedule (Calendrier)** est initialement défini sur **None (Aucune)**. Effectuez les étapes suivantes pour chaque type de journal.

1. Cliquez sur **None (Aucune)** et sélectionnez la fréquence de mise à jour (**Recurrence (récurrence)**). Les options de fréquence disponibles dépendent du type de la mise à jour.
2. Sélectionnez l'action de planification :
   - **Download And Install (Téléchargez et installez)** (recommandé) : Panorama installe automatiquement les mises à jour après les avoir téléchargées.
   - **Download Only (Télécharger uniquement)** : vous devez installer manuellement les mises à jour après que panorama les télécharge.
3. En fonction des meilleures pratiques pour la posture de sécurité de votre organisation, configurez un délai (**Threshold (Seuil)**) après qu'une mise à jour devient disponible avant que Panorama ne télécharge la mise à jour.
4. Cliquez sur **OK** pour enregistrer vos modifications.
5. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

Installer des mises à jour pour Panorama lorsqu'il n'est pas connecté à Internet

Si Panorama™ ne dispose pas d'une connexion directe à Internet, suivez les étapes suivantes pour installer le logiciel Panorama et les mises à jour logicielles et de contenu au besoin. Si Panorama est déployé dans une configuration haute disponibilité (HD), vous devez mettre à niveau chaque homologue (voir Installer les mises à jour pour Panorama dans une configuration HD).

La mise à niveau du logiciel sur l'appareil virtuel Panorama ne modifie pas le mode du système ; le passage en mode Panorama ou en mode de Gestion est une tâche manuelle qui nécessite des paramètres supplémentaires tels que décrits lorsque vous configurez l'appareil virtuel Panorama avec le collecteur de journaux local.

PAN-OS® 9.0 intègre un nouveau format de données de journaux pour les collecteurs de journaux dédiés et locaux. Lorsque vous passez à PAN-OS 10.0, les données de journaux existantes sont automatiquement converties au nouveau format lors de la mise à niveau de PAN-OS 10.0. Lors du reformatage, les données des journaux ne sont pas visibles dans les onglets **ACC** ou **Monitor (Surveillance)**. De plus, les nouvelles données des journaux ne sont pas transférées aux collecteurs de journaux avant que le reformatage a été effectué. Lors du reformatage, de nouveaux journaux sont rédigés sur le disque système du pare-feu et après que la procédure a terminé avec succès, les nouveaux journaux sont transmis au collecteur de journaux appropriée.

Vous devez mettre à niveau tous les collecteurs de journaux d'un groupe de collecteurs en même temps afin d'éviter de perdre des données de journal. Aucun transfert de journaux ou collecte de journaux ne se produit si les collecteurs de journaux d'un groupe de collecteurs n'utilisent pas tous la même version de PAN-OS. De plus, les données des journaux des collecteurs de journaux du groupe de collecteur ne sont pas visibles dans les onglets **ACC** ou **Monitor (Surveillance)** jusqu'à ce que tous les collecteurs de journaux exécutent la même version PAN-OS. Par exemple, si vous disposez de trois collecteurs de journaux dans un groupe de collecteurs et que vous mettez à niveau deux d'entre eux, aucun journal n'est alors transmis aux collecteurs de journaux du groupe de collecteurs.

Avant de mettre à jour Panorama, reportez-vous aux Notes de version pour la version de contenu minimum requise pour PAN-OS® 10.0.

© 2020 Palo Alto Networks, Inc.

Pour Panorama sur Azure, vous devez exécuter quelques étapes supplémentaires avant de mettre à jour la version logicielle avec succès. Pour procéder à la mise à niveau, vous devez exporter la configuration de Panorama, mettre à niveau les versions de contenu et les versions logicielles, puis importez la configuration vers le serveur de gestion de Panorama une fois la mise à niveau réussie.

STEP 1 | Vérifiez que les mises à jour que vous prévoyez d'installer sont appropriées pour votre déploiement Panorama.

- Consultez les Notes de version pour la version minimale du contenu que vous devez installer pour une version de Panorama. Si vous souhaitez mettre à niveau des pare-feu et des collecteurs de journaux vers une version particulière, vous devez d'abord mettre à niveau Panorama à cette version (ou à une version ultérieure).
- Pour un appareil virtuel Panorama, assurez-vous que l'instance respecte la configuration prérequise pour l'appareil virtuel Panorama.

STEP 2 | Enregistrez une sauvegarde du fichier de configuration Panorama en cours que vous pouvez utiliser pour restaurer la configuration si vous rencontrez des problèmes avec la mise à niveau.

Bien que Panorama crée automatiquement une sauvegarde de la configuration, l'idéal consiste à créer et à stocker à l'extérieur une sauvegarde avant la mise à niveau.

1. Cliquez sur **Save named Panorama configuration snapshot (Enregistrer un instantané de configuration nommé Panorama)** (**Panorama** > **Setup (Configuration)** > **Operations (Opérations)**), entrez un **Name (Nom)** pour la configuration et cliquez sur **OK**.
2. Cliquez sur **Export named Panorama configuration snapshot (Exporter l'instantané de configuration nommé Panorama)**, sélectionnez le **Name (Nom)** de la configuration que vous venez d'enregistrer, cliquez sur **OK**, et enregistrez le fichier exporté à un emplacement qui est externe à Panorama.

STEP 3 | Déterminez les mises à jour de contenu à installer.

Palo Alto Networks recommande fortement que Panorama, les collecteurs de journaux et tous les pare-feu gérés exécutent la même version de contenu.

1. Pour chaque mise à jour de contenu, déterminez si vous avez besoin de mises à jour et quelles mises à jour de contenu doivent être téléchargées à la prochaine étape.

   Assurez-vous que Panorama exécute la même version de contenu, mais pas une version ultérieure à celle exécutée sur les pare-feu gérés et les collecteurs de journaux.
2. (Au besoin) Avant de mettre à jour la version du contenu sur Panorama, assurez-vous de mettre à niveau les pare-feu gérés puis les collecteurs de journaux (voir Mettre à niveau les collecteurs de journaux lorsque Panorama est connecté à Internet) à la même version de contenu (ou une version ultérieure).

STEP 4 | Déterminer le chemin de mise à niveau vers PAN-OS 10.0.

Vous ne pouvez pas sauter l'installation de versions majeures (avec de nouvelles fonctionnalités) dans le chemin de mise à jour depuis la version PAN-OS en cours vers PAN-OS 10.0. Passez en revue les problèmes connus et les modifications du comportement par défaut dans les Notes de version et les considérations de mise à niveau vers une version supérieure ou antérieure dans le Guide des nouvelles fonctionnalités de chaque version à travers laquelle vous passez dans le cadre de votre chemin de mise à niveau.

(Requis si vous faites une mise à niveau à partir de la version 7.1 ou antérieure) PAN-OS 8.0 a lancé un nouveau format de stockage des journaux. Après avoir effectué la mise à niveau vers PAN-OS 8.0, vous

© 2020 Palo Alto Networks, Inc.

devez Migrer les journaux de Panorama vers le nouveau format de journal avant de continuer la mise à niveau. La migration de journaux est une tâche ponctuelle. Si vous avez déjà migré les journaux sur le collecteur de journaux pour une mise à niveau vers PAN-OS 8.0, vous n'avez pas besoin de les migrer à nouveau lorsque vous passez à PAN-OS 8.1.

Si vous mettez à niveau plusieurs collecteurs de journaux, rationalisez le processus en déterminant les chemins de mise à niveau pour tous les collecteurs de journaux que vous avez l'intention de mettre à niveau avant de commencer à télécharger des images.

STEP 5 | (Au besoin) Téléchargez des mises à jour de contenu vers un hôte qui peut se connecter et chargez le contenu sur Panorama via SCP ou HTTPS.

Si vous n'avez pas besoin d'installer de mises à jour de contenu pour le moment, passez directement à l'étape 6.

1. Utilisez un hôte qui dispose d'un accès à Internet pour ouvrir une session sur le site Web d'assistance client de Palo Alto Networks.
2. Téléchargez les mises à jour de contenu au besoin :
    1. Cliquez sur **Updates (Mises à jour)** > **Dynamic Updates (Mises à jour dynamiques)** dans la section Ressources.
    2. **Download (Téléchargez)** les mises à jour de contenu appropriées et enregistrez les fichiers sur l'hôte. Effectuez cette étape pour chaque type de contenu que vous devez mettre à jour.

STEP 6 | Installez les mises à jour de contenu en fonction des besoins.

Vous devez installer les mises à jour de contenu et vous devez premièrement Mettre à niveau les pare-feu et ensuite Mettre à jour les collecteurs de journaux avant de les installer sur le serveur de gestion Panorama.

Installez d'abord les mises à jour des applications ou des applications et menaces, puis installez toutes les autres mises à jour (Antivirus, WildFire® ou Filtrage d'URL) une à la fois dans n'importe quel ordre.

Peu importe si votre abonnement comprend le contenu Applications et Menaces, Panorama installe et n'a besoin que du contenu Applications. Pour plus d'informations, consultez la section Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire .

Dans Panorama (**Panorama** > **Dynamic Updates (Mises à jour dynamiques)**), effectuez les étapes suivantes pour chaque type de contenu :

1. Cliquez sur **Download (Télécharger)**, sélectionnez le **Type** de contenu, **Browse (Recherchez)** l'emplacement sur l'hôte sur lequel vous avez téléchargé la mise à jour, sélectionnez la mise à jour, puis cliquez sur **OK**.
2. Cliquez sur **Install From File (Installer depuis le fichier)**, sélectionnez le **Package Type (Type de package)** et cliquez **OK**.

STEP 7 | Téléchargez les mises à jour logicielles sur un hôte qui peut se connecter et charger du contenu sur Panorama via SCP ou HTTPS.

1. Utilisez un hôte avec accès à Internet pour ouvrir une session sur le site Web d'assistance client de Palo Alto Networks.
2. Télécharger les mises à jour logicielles :
    1. Sur la page principale du site d'assistance client de Palo Alto Networks, cliquez sur **Updates (Mises à jour)** > **Software Updates (Mises à jour logicielles)**.

© 2020 Palo Alto Networks, Inc.

2. Pour la première (ou prochaine) version de Panorama dans votre chemin de mise à niveau, identifiez le fichier spécifique au modèle. Par exemple, pour mettre à niveau un appareil de série M vers Panorama 10.0.0, téléchargez l'image `Panorama_m-10.0.0`. Pour mettre à niveau un appareil virtuel Panorama vers Panorama 10.0.0, téléchargez l'image `Panorama_pc-10.0.0`.

   Vous pouvez rapidement localiser les images de Panorama en sélectionnant Panorama M Images (Images M Panorama) (appareils de série M) ou Panorama Updates (Mises à jour de Panorama) (appareils virtuels) du menu déroulant Filter By (Filtrer par).
3. Cliquez sur le nom du fichier et enregistrez le fichier sur l'hôte.
4. Répétez la sous-étape 2 ci-dessus pour toutes les versions supplémentaires dans votre chemin de mise à niveau, comme déterminé à l'étape 4.

STEP 8 | Installez Panorama 10.0.

Pour chaque version de votre chemin de mise à niveau (en commençant par la première), procédez comme suit :

1. Cliquez sur Download (Télécharger) (**Panorama** > **Software (Logiciel)**).
2. **Browse (Naviguez)** vers l'emplacement de l'hôte sur lequel vous avez téléchargé la mise à jour, sélectionnez la mise à jour, **Sync to peer (Synchronisez avec l'homologue)** si Panorama est dans une configuration HD (pour appliquer l'image du logicielle à l'homologue secondaire), puis cliquez sur **OK**.
3. Installez l'image du logiciel et redémarrez.

   Pour une configuration HD, installez les mises à jour pour Panorama dans une configuration haute disponibilité ; sinon :

   1. Installez l'image téléchargée.
   2. Après avoir terminé l'installation avec succès, redémarrez en utilisant l'une des méthodes suivantes :
      - Si vous êtes invité à redémarrer, cliquez sur **Yes (Oui)**. Si une invite CMS Login s'affiche, appuyez sur Entrée sans saisir de nom d'utilisateur ou de mot de passe. Lorsque l'invite de connexion Panorama s'affiche, saisissez le nom d'utilisateur et le mot de passe que vous avez spécifiés lors de la configuration initiale.
      - Si vous n'êtes pas invité à redémarrer, cliquez sur **Reboot Panorama (Redémarrer Panorama)** dans la section Device Operations (Opérations de périphérique) (**Panorama** > **Setup (Configuration)** > **Operations (Opérations)**).
4. Répétez les sous-étapes 1 à 3 ci-dessus pour chaque version de votre chemin, au besoin.

STEP 9 | Vérifiez l'état de la migration du format des journaux après la réussite d'une mise à niveau vers PAN-OS 10.0.

1. Connectez-vous à l'ILC Panorama du collecteur de journaux.
2. Exécutez la commande suivante pour vérifier l'état de la migration du formation des journaux :

```
admin> debug logdb show-es-upgrade-time
```

Réponse type lorsque la migration du format des journaux est toujours en cours :

```
Response from logger 23456212: 50.98% of indices upgraded complete.
 Approximately less than a minute remaining until migration is complete.
 Once the log migration is complete, please run the 'show log-collector-
es-cluster health' command to check the ElasticSearch cluster status to
 verify logging and reporting functionality is restored.
```


© 2020 Palo Alto Networks, Inc.

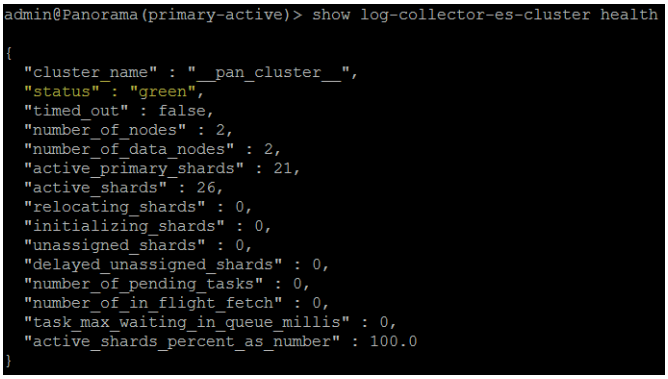
Réponse lorsque la migration du format des journaux est terminée :

```
Response from logger 23456212: 100% of indices complete. Please run the
 'show log-collector-es-cluster health' command to check the ElasticSearch
 cluster status to verify logging and reporting functionality is restored.
```

3. Une fois la migration du format des journaux est terminé, exécutez la commande suivante pour vérifier l'état du cluster ElasticSearch avant de passer à l'étape suivante :

```
admin> show log-collector-es-cluster health
```

Passez à l'étape suivante lorsque l'état de santé (`"status"`) du cluster ElasticSearch indique `"green"` :



STEP 10 | (Panorama sur Azure uniquement) Chargez la configuration de Panorama que vous avez exportée à l'étape 2.

1. **Import named Panorama configuration snapshot (Importez un instantané de configuration nommé Panorama)** (**Panorama** > **Setup (Configuration)** > **Operations (Opérations)**), **Browse (Cherchez)** et sélectionnez le fichier de configuration Panorama, puis cliquez sur **OK**.
2. **Load named Panorama configuration snapshot (Chargez un instantané de configuration nommé Panorama)**, sélectionnez le **Name (Nom)** de la configuration que vous venez d'importer, saisissez la **Decryption Key (Clé de décryptage)** au besoin, puis cliquez sur OK.
3. Connectez-vous à l'ILC Panorama.
4. Validez la configuration de Panorama en entrant les commandes suivantes :

```
admin> configure
```

```
admin> commit force
```

STEP 11 | (Si le collecteur de journaux locaux dans un groupe de collecteurs uniquement) Mettez à niveau les collecteurs de journaux restants dans le groupe de collecteurs.

- Mettre à niveau les collecteurs de journaux lorsque Panorama est connecté à Internet
- Mettre à niveau les collecteurs de journaux lorsque Panorama n'est pas connecté à Internet

Installer des mises à jour de Panorama sans connexion Internet

Téléchargez automatiquement des mises à jour dynamiques vers les pare-feux, les Collecteurs de journaux et les appareil WildFire® sur les réseaux à air gap lorsque le serveur de gestion Panorama™, les pare-

© 2020 Palo Alto Networks, Inc.

feux gérés, les Collecteurs de journaux et les appareils WildFire ne sont pas connectés à Internet. Afin de faire cela, vous devez déployer un Panorama supplémentaire avec un accès internet et un serveur SCP. Après avoir déployé le Panorama avec un accès internet, vous configurez le Panorama connecté à internet afin qu'il télécharge automatiquement les mises à jour dynamiques sur le serveur SCP. Depuis le serveur SCP, la Panorama à air gap est configuré afin de télécharger et installer automatiquement les mises à jour dynamiques selon votre programme de mises à jour dynamiques. Panorama génère un journal système lorsque le Panorama avec un accès à internet télécharge des mises à jour dynamiques sur le serveur SCP ou lorsque le Panorama à air gap télécharge et installe les mises à jour dynamiques depuis le serveur SCP.

Seuls les programmes de mises à jour dynamiques suivants depuis un Panorama connecté à internet vers un Panorama sans connexion internet sont possibles :

Ne manipulez pas et ne modifiez pas le nom du fichier de mise à jour dynamique après l'avoir téléchargé sur le serveur SCP. Panorama ne peut pas télécharger et installer des mises à jour dynamiques ayant des noms de fichiers modifiés. Par ailleurs, pour que la mise à jour dynamique réussisse, vous devez vous assurer qu'il y a assez d'espace disque sur le serveur SCP, que le serveur SCP fonctionne lorsqu'un téléchargement est sur le point de commencer et que les deux Panoramas sont alimentés et non au milieu d'un redémarrage.

Le présent exemple montre comment configurer les mises à jour de contenu automatiques pour les mises à jour dynamiques des Applications et des Menaces.

STEP 1 | Déployer un serveur SCP.

Les mises à jour dynamiques pare-feux gérés, Collecteurs de journaux et appareils WildFire sont téléchargées depuis le Panorama connecté à internet. Le Panorama air gap télécharge les mises à jour dynamiques depuis le serveur SCP et les installe sur les pare-feux gérés, les appareils WildFire et les Collecteurs de journaux.

Lorsque vous créez le répertoire de dossiers pour des mises à jour dynamiques, les bonnes pratiques consistent à créer un dossier pour chaque type de mise à jour dynamique. C'est l'inconvénient de gérer un gros volume de mises à jour dynamiques et cela réduit la possibilité de supprimer des mises à jour dynamiques qui ne devraient pas être supprimées du serveur SCP.

STEP 2 | Déployez le Panorama connecté à internet.

Ce Panorama communique avec le serveur de mises à jour Palo Alto Networks et télécharge les mises à jour dynamiques sur le serveur SCP.

1. Configurez le serveur de gestion Panorama.
   - Configuration de l'appareil de série M
   - Configuration de l'appareil virtuel Panorama
2. Appliquez la configuration Panorama initiale.
   - Effectuer la configuration initiale de l'appareil de série M
   - Effectuer la configuration initiale de l'appareil virtuel Panorama

STEP 3 | Installez le Panorama sans connexion Internet.

Ce Panorama communique avec le serveur SCP pour télécharger et installer les mises à jour dynamiques sur les pare-feux gérés, les Collecteurs de journaux et les appareils WildFire.

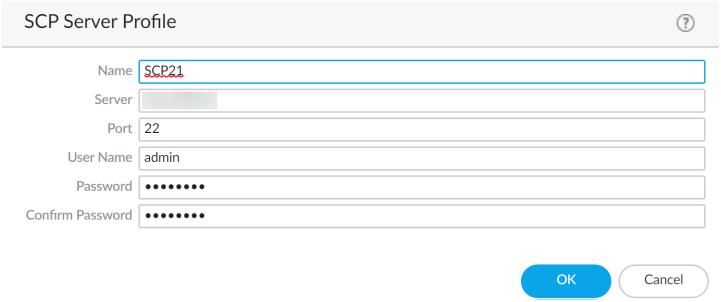
1. Configurez le serveur de gestion Panorama.
   - Configuration de l'appareil de série M
   - Configuration de l'appareil virtuel Panorama

© 2020 Palo Alto Networks, Inc.

2. Appliquez la configuration Panorama initiale.
   - Effectuer la configuration initiale de l'appareil de série M
   - Effectuer la configuration initiale de l'appareil virtuel Panorama
3. Ajoutez vos pare-feux gérés, Collecteurs de journaux et appareils WildFire.
   - Ajouter un pare-feu en tant que périphérique géré
   - Configurer un collecteur géré
   - Ajouter des appareils WildFire autonomes à gérer avec Panorama

STEP 4 | Configurez le Panorama connecté à internet pour télécharger les mises à jour dynamiques sur votre serveur SCP.

1. Se connecter à l'interface Web Panorama.
2. Créez un profil de serveur SCP.
   1. Sélectionnez **Panorama** > **Server Profiles (Profils de serveur)** > **SCP** et **Add (Ajoutez)** un nouveau profil de serveur SCP.
   2. Saisissez un **Name (Nom)** descriptif pour le profil de serveur SCP.
   3. Saisissez l'adresse IP du **Server (serveur)** SCP.
   4. Saisissez le **Port**.
   5. Saisissez le**User Name (Nom d'utilisateur)** du serveur SCP.
   6. Saisissez le **Password (Mot de passe)** du serveur SCP et **Confirm Password (Confirmez le mot de passe)**.
   7. Cliquez sur **OK** pour enregistrer vos modifications.



3. Créez un programme de mises à jour dynamiques afin de télécharger des mises à jour dynamiques sur le serveur SCP.

   Vous devez créer un programme pour chaque type de mise à jour dynamique que vous avez l'intention de télécharger et installer sur vos pare-feux gérés, Collecteurs de journaux et appareils WildFire.

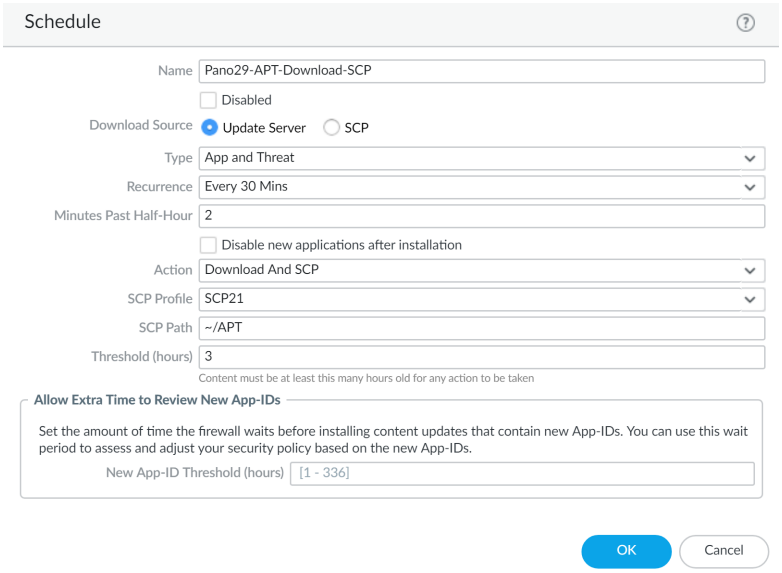
   1. Sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Dynamic Updates (Mises à jour dynamiques)**, sélectionnez **Schedules (Programmes)** et **Add (Ajoutez)** un programme de mise à jour dynamique.
   2. Saisissez un **Name (Nom)** descriptif pour le programme de mises à jour dynamiques.
   3. Pour la **Download Source (Source de téléchargement)**, sélectionnez**Update Server (Serveur de mise à jour)**.
   4. Sélectionnez le **Type** de mise à jour dynamique.
   5. Sélectionnez la **Recurrence (Récurrence)** pour définir l'intervalle selon lequel Panorama recherchera de nouvelles mises à jour dynamiques sur le serveur de mises à jour Palo Alto Networks.

      Pour configurer un programme de récurrence plus précis, saisissez le nombre de minutes à côté de l'intervalle de récurrence sélectionné. Si vous avez plusieurs

© 2020 Palo Alto Networks, Inc.

mises à jour dynamiques programmées pour un téléchargement en utilisant le même intervalle de récurrence, échelonnez les afin d'éviter de surcharger le Panorama et le serveur SCP.

6. Pour l'**Action**, sélectionnez **Télécharger et SCP**.
7. Sélectionnez le **SCP Profile (Profil SCP)** que vous avez configuré au cours des étapes antérieures.
8. Saisissez le **SCP Path (chemin d'accès SCP)** du type des mises à jour dynamiques.
9. (En option) saisissez le **Threshold (Seuil)**, en heures, pour les mises à jour dynamiques. Panorama ne télécharge que les mises à jour dynamiques qui existent depuis le nombre d'heures indiqué (ou plus anciennes)
10. Cliquez sur **OK** pour enregistrer vos modifications.

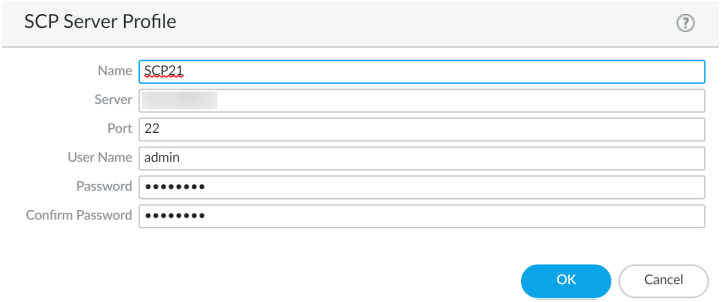


4. **Commit (Validez)** vos modifications.

STEP 5 | Configurez le Panorama air gap pour qu'il télécharge les mises à jour dynamiques depuis le serveur SCP et les installe sur les pare-feux gérés, les Collecteurs de journaux et les appareils WildFire.

1. Se connecter à l'interface Web Panorama.
2. Créez un profil de serveur SCP.
   1. Sélectionnez **Panorama** > **Server Profiles (Profils de serveur)** > **SCP** et **Add (Ajoutez)** un nouveau profil de serveur SCP.
   2. Saisissez un **Name (Nom)** descriptif pour le profil de serveur SCP.
   3. Saisissez l'adresse IP du **Server (serveur)** SCP.
   4. Saisissez le **Port**.
   5. Saisissez le**User Name (Nom d'utilisateur)** du serveur SCP.
   6. Saisissez le **Password (Mot de passe)** du serveur SCP et **Confirm Password (Confirmez le mot de passe)**.
   7. Cliquez sur **OK** pour enregistrer vos modifications.

© 2020 Palo Alto Networks, Inc.



3. Créez un programme de mises à jour dynamiques afin de télécharger et d'installer régulièrement des mises à jour dynamiques depuis le serveur SCP.

   Vous devez créer un programme pour chaque type de mise à jour dynamique que vous avez l'intention de télécharger et installer sur vos pare-feux gérés, Collecteurs de journaux et appareils WildFire.

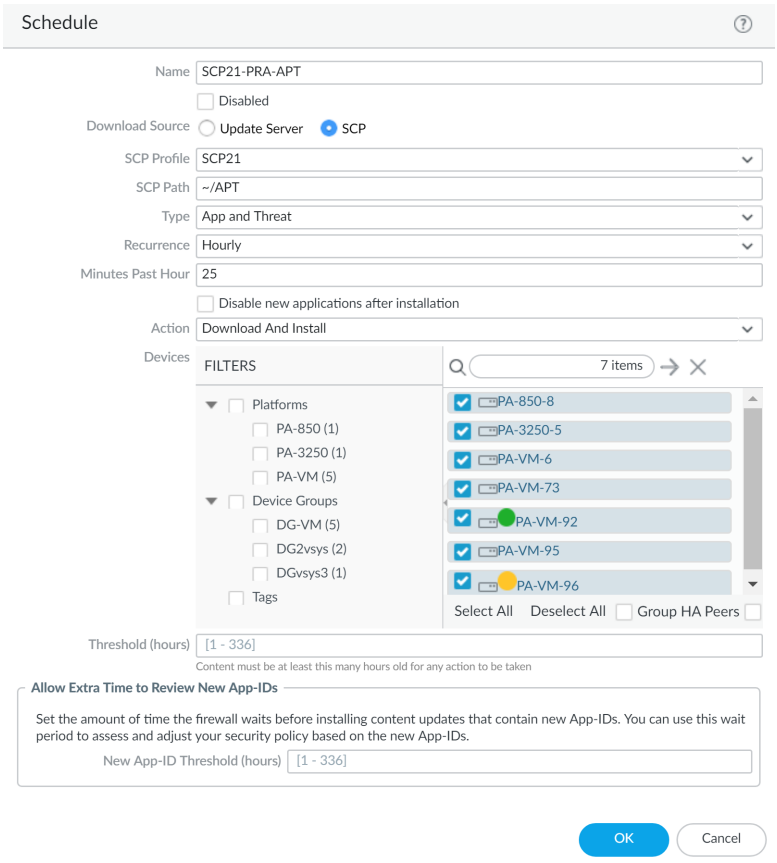
   1. Sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Dynamic Updates (Mises à jour dynamiques)**, sélectionnez **Schedules (Programmes)** et **Add (Ajoutez)** un programme de mise à jour dynamique.
   2. Saisissez un **Name (Nom)** descriptif pour le programme de mises à jour dynamiques.
   3. Pour la **Download Source (Source de téléchargement)**, sélectionnez**SCP**.
   4. Sélectionnez le **SCP Profile (Profil SCP)** que vous avez configuré au cours des étapes antérieures.
   5. Saisissez le **SCP Path (chemin d'accès SCP)** du type des mises à jour dynamiques.
   6. Sélectionnez le **Type** de mise à jour dynamique.
   7. Sélectionnez la **Recurrence (Récurrence)** pour définir l'intervalle selon lequel Panorama recherchera de nouvelles mises à jour dynamiques sur le serveur de mises à jour Palo Alto Networks.

      Pour configurer un programme de récurrence plus précis, saisissez le nombre de minutes à côté de l'intervalle de récurrence sélectionné. Si vous avez plusieurs mises à jour dynamiques programmées pour un téléchargement en utilisant le même intervalle de récurrence, échelonnez les afin d'éviter de surcharger le Panorama et le serveur SCP.
   8. Pour **Action**, sélectionnez**Download (Télécharger)** ou **Download And Install (télécharger et installer)**.

      Seuls Download (Télécharger) et Download and Install (télécharger et installer) sont possibles lorsque la Download Source (Source de téléchargement) est SCP.

      Si vous sélectionnez Download (Télécharger), vous devez lancer manuellement l'installation de la mise à jour dynamique sur vos pare-feux gérés.
   9. Sélectionnez les **Devices (Périphériques)** sur lesquels installer les mises à jour dynamiques.
   10. (En option) saisissez le **Threshold (Seuil)**, en heures, pour les mises à jour dynamiques. Panorama ne télécharge que les mises à jour dynamiques qui existent depuis le nombre d'heures indiqué (ou plus anciennes)
   11. Cliquez sur **OK** pour enregistrer vos modifications.

© 2020 Palo Alto Networks, Inc.



4. **Commit (Validez)** vos modifications.

Migrer les journaux de Panorama vers le nouveau format de journal

Après la mise à niveau vers une version Panorama 8.0 (ou ultérieure), le collecteur de journaux de Panorama utilise un nouveau format de stockage de journaux. Panorama ne pouvant pas générer de rapports ou de données ACC à partir de journaux dans le format de journal antérieur à la version 8.0, vous devez migrer les journaux existants dès la mise à niveau de Panorama et de ses collecteurs de journaux de puis une version de PAN-OS® 7.1 ou antérieure vers une version PAN-OS 8.0 ou ultérieure, et vous devez le faire avant de mettre à niveau vos pare-feu gérés. Panorama continuera à collecter les journaux des périphériques gérés pendant la migration des journaux, mais stockera les journaux entrants dans le nouveau format de journal après la mise à niveau vers PAN-OS 8.0 ou une version ultérieure. Pour cette raison, vous ne verrez que des données partielles dans l'ACC et dans les rapports tant que Panorama n'a pas terminé le processus de migration des journaux.

La migration du journal vers le nouveau format est une tâche ponctuelle que vous devez effectuer lorsque vous effectuez une mise à niveau vers la version PAN-OS 8.0 ou une version ultérieure (ou lorsque vous effectuez une mise à niveau vers la version PAN-OS 8.0 dans le cadre de votre chemin de mise à niveau) ; vous n'avez plus besoin d'effectuer cette migration lorsque vous effectuez une mise à niveau vers une version ultérieure de PAN-OS.

Le temps nécessaire à Panorama pour terminer le processus de migration des journaux dépend du volume des nouveaux journaux écrits dans Panorama et de la taille de la base de données de journaux que vous migrez. Étant donné que la migration de journaux est un processus gourmand en ressources

© 2020 Palo Alto Networks, Inc.

processeur, commencez la migration à un moment où le taux de journalisation est inférieur. Vous pouvez toujours arrêter la migration pendant les périodes de pointe si vous remarquez que les taux d'utilisation du processeur sont élevés et reprendre la migration lorsque le débit de journalisation entrant est inférieur.

Après la Installer les mises à jour de contenu et de logiciel pour Panorama et pour la mise à niveau des collecteurs de journaux, migrez les journaux comme suit :

- Affichez le taux de journalisation entrant.

  Pour de meilleurs résultats, démarrez la migration des journaux lorsque le taux de journalisation entrant est faible. Pour vérifier le débit, exécutez la commande suivante depuis la CLI du collecteur de journaux :

```
admin@FC-M500-1> debug log-collector log-collection-stats show incoming-logs
```

  Une utilisation élevée du processeur (proche de 100 %) pendant la migration des journaux est attendue et les opérations continueront à fonctionner normalement. La migration des journaux est limitée en faveur des journaux entrants et d'autres processus en cas de conflit de ressources.

- Commencez à migrer les journaux sur chaque collecteur de journaux au nouveau format.

  Pour commencer la migration, entrez la commande suivante depuis la CLI de chaque collecteur de journaux :

```
admin@FC-M500-1> request logdb migrate lc serial-number <ser_num> start
```

- Consultez l'état de la migration des journaux pour estimer le temps nécessaire à la migration de tous les journaux existants vers le nouveau format.

```
admin@FC-M500-1> request logdb migrate lc serial-number <ser_num> status
 Slot: all
Migration State: In Progress
Percent Complete: 0.04
Estimated Time Remaining: 451 hour(s) 47 min(s)
```

- Arrêtez le processus de migration des journaux.

  Pour arrêter temporairement le processus de migration des journaux, entrez la commande suivante depuis la CLI du collecteur de journaux :

```
admin@FC-M500-1 request logdb migrate lc serial-number <ser_num> stop
```


© 2020 Palo Alto Networks, Inc.

Transition vers un modèle Panorama différent

Lorsque vos besoins de réseau changent (par exemple, le taux d'enregistrement augmente), vous pouvez migrer les serveurs de gestion Panorama et collecteurs de journaux dédiés vers les Modèles Panorama pour mieux soutenir ces exigences.

- Migrer à partir d'un appareil virtuel Panorama vers un appareil de série M
- Migrer un appareil virtuel Panorama vers un autre hyperviseur
- Migrer d'un appareil de série M à un appareil virtuel Panorama
- Migrer d'un appareil M-100 à un appareil M-500

Migrer à partir d'un appareil virtuel Panorama vers un appareil de série M

Vous pouvez migrer la configuration Panorama à partir d'un appareil virtuel Panorama à un appareil de série M en mode Panorama. Cependant, vous ne pouvez pas migrer les journaux parce que le format de journal sur l'appareil virtuel Panorama est incompatible avec celui sur les appareils de série M. Par conséquent, si vous voulez maintenir l'accès aux anciens journaux stockés sur l'appareil virtuel Panorama, vous devez continuer à exécuter appareil virtuel Panorama après la migration. L'appareil de série M recueillera les nouveaux journaux que les pare-feu transfèrent après la migration. Après la pré-migration, les journaux expirent ou deviennent sans importance en raison du vieillissement, vous pouvez éteindre l'appareil virtuel Panorama.

Le mode hérité n'est plus pris en charge dans PAN-OS 8.1 ou les versions ultérieures. Si le vieil appareil virtuel Panorama est en mode hérité, vous devez le faire passer au mode Panorama avant de le migrer vers le nouvel hyperviseur afin de préserver les paramètres des journaux et les configurations de transfert du collecteur de journaux. L'importation de la configuration du vieux Panorama en mode Hérité vers un nouveau Panorama en mode Panorama entraîne la suppression de tous les paramètres des journaux et de transfert des journaux.

Vous ne pouvez migrer les journaux entre les hyperviseurs. Par conséquent, si vous voulez maintenir l'accès aux journaux stockés sur l'ancien appareil virtuel Panorama, vous devez continuer à exécuter appareil virtuel Panorama après la migration et l'ajouter en tant que collecteur de journaux géré sur le nouvel appareil virtuel Panorama. Cela permet au nouvel appareil virtuel Panorama de collecter les journaux que les pare-feu transfèrent après la migration, tout en préservant l'accès aux données des anciens journaux. Après la pré-migration, les journaux expirent ou deviennent sans importance en raison du vieillissement, vous pouvez éteindre l'appareil virtuel Panorama.

Si vous stockez des journaux de pare-feu sur les collecteurs de journaux dédiés (appareils de la série M en mode collecteur de journaux) au lieu de l'appareil virtuel Panorama, vous pouvez accéder aux journaux en migrant les collecteurs de journaux dédiés vers l'appareil de la série M en mode Panorama.

STEP 1 | Planifier la migration.

- ❑ La mise à niveau du logiciel sur l'appareil virtuel Panorama avant la migration si l'appareil de série M nécessite une version ultérieure du logiciel actuel (l'appareil M-500 nécessite Panorama 7.0 ou une version ultérieure). L'appareil M-600 et M-200 nécessitent Panorama 8.1 ou une version ultérieure). Pour des informations importantes sur les versions logicielles, voir Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire.

© 2020 Palo Alto Networks, Inc.

- Programmer une fenêtre de maintenance pour la migration. Bien que les pare-feu puissent tamponner les journaux après que l'appareil virtuel Panorama se déconnecte puis transférer les journaux une fois que l'appareil de série M est en ligne, le fait de compléter la migration au cours d'une fenêtre de maintenance minimise le risque que les journaux dépassent les capacités de mémoire tampon et soient perdus au cours de la transition entre les modèles Panorama.
- Examiner l'opportunité de maintenir l'accès à l'appareil virtuel Panorama après la migration pour accéder aux journaux existants. L'approche la plus efficace consiste à attribuer une nouvelle adresse IP à l'appareil virtuel Panorama et réutiliser son ancienne adresse IP pour l'appareil de série M. Cela garantit que l'appareil virtuel Panorama reste accessible et que les pare-feux peuvent pointer vers l'appareil de série M sans devoir reconfigurer l'adresse IP Panorama sur chaque pare-feu.

STEP 2 | Achetez le nouvel appareil M-Series et migrez vos abonnements vers le nouvel appareil.

1. Achetez le nouvel appareil M-Series.
2. Achetez la nouvelle licence de support et la licence de migration.
3. Au moment de l'achat du nouvel appareil M-Series, indiquez à votre représentant des ventes le numéro de série et le code d'autorisation de gestion des périphériques de l'appareil virtuel Panorama que vous retirez progressivement ainsi que la date de migration des licences que vous avez choisie. Lorsque vous recevez votre appareil M-Series, enregistrez l'appareil et activez les licences de soutien et de gestion des périphériques à l'aide des codes d'autorisation du soutien et de la migration fournis par Palo Alto Networks. À la date de migration, la licence de gestion des périphériques sur l'appareil virtuel Panorama est mise hors service, et vous ne pouvez plus gérer les périphériques ou collecter les journaux à l'aide de l'appareil virtuel Panorama. Cependant, la licence de soutien est conservée et l'appareil Panorama continue à bénéficier du soutien. Vous pouvez terminer la migration après la date d'entrée en vigueur, mais vous n'êtes pas en mesure de valider les changements de configuration sur l'appareil virtuel Panorama qui est désormais hors service.

STEP 3 | (Mode Hérité uniquement) Sur le vieil appareil virtuel Panorama, passez en mode Panorama.

Cette étape est requise pour préserver les données des journaux, les paramètres et la configuration du transfert des journaux de l'appareil virtuel Panorama. Si vous exportez la configuration Panorama en mode Hérité, ces paramètres sont perdus. Vous devez effectuer l'étape 9 si vous ne faites pas passer Panorama en mode Panorama avant de poursuivre.

Passez à l'étape suivante si l'appareil virtuel Panorama est déjà en mode Panorama ou en mode Gestion uniquement.

1. Configurer un appareil virtuel Panorama en mode Panorama.
2. Migrer les journaux de Panorama vers le nouveau format de journal si vous souhaitez préserver les données des journaux existants sur le vieil appareil virtuel Panorama.

STEP 4 | Exportez la configuration Panorama de l'appareil virtuel Panorama.

1. Connectez-vous à l'appareil virtuel et sélectionnez **Panorama (Panorama)** > **Setup (Configuration)** > **Operations (Opérations)**.
2. Cliquez sur **Save named Panorama configuration snapshot (Enregistrer un instantané de configuration nommé Panorama)**, entrez un **Name (Nom)** pour identifier la configuration et cliquez **sur OK**.
3. Cliquez sur **Export named Panorama configuration snapshot (Exporter l'instantané de configuration nommé Panorama),** sélectionnez le **Name (Nom)** de la configuration que vous venez d'enregistrer et cliquez sur **OK** . Panorama exporte la configuration de votre système client sous forme de fichier XML.

© 2020 Palo Alto Networks, Inc.

STEP 5 | Mise hors tension de l'appareil virtuel Panorama si vous n'avez pas besoin d'y accéder après la migration ou attribuer une nouvelle adresse IP à son interface de gestion (MGT) si vous aurez besoin d'y accéder.

Pour éteindre l'appareil virtuel Panorama, reportez-vous à la documentation de votre produit VMware.

Pour modifier l'adresse IP sur l'appareil virtuel Panorama :

1. Sélectionnez **Panorama (Panorama)** > **Setup (Configuration)** > **Management (Gestion)**, puis modifiez les paramètres d'interface de gestion.
2. Entrez la nouvelle **IP Address (Adresse IP)** et cliquez sur **OK**.
3. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

STEP 6 | Effectuez la configuration initiale de l'appareil de série M.

1. Montez l'appareil de série M dans une baie. Se référer au Guide de référence du matériel de la série-M pour obtenir des instructions.
2. Effectuez la configuration initiale de l'appareil de Série M pour définir les connexions réseau requises pour activer les licences et installer les mises à jour.
3. Enregistrez Panorama.
4. Activer une licence d'assistance Panorama.
5. Activer / Récupérer une Licence de Gestion de Pare-feu sur l'appareil de série M. Utilisez le code d'authentification associé à la licence de migration.
6. Installer les mises à jour de contenu et logicielles pour Panorama. Installez les mêmes versions que celles sur l'appareil virtuel Panorama.

STEP 7 | Charger le snapshot de configuration Panorama que vous avez exporté à partir de l'appareil virtuel Panorama dans l'appareil de série M.

1. Sur l'appareil M-Series, sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)**.
2. Cliquez sur **Import named Panorama configuration snapshot (Importer un instantané de configuration nommé Panorama)**, **Browse (Rechercher)** le fichier de configuration Panorama vous avez exporté depuis l'appareil virtuel Panorama, et cliquez sur **OK**.
3. Cliquez sur **Load named Panorama configuration snapshot (Charger un instantané de configuration nommé Panorama)**, sélectionnez le **Name (Nom)** de la configuration que vous venez d'importer, sélectionnez une **Decryption Key (Clé de décryptage)** (la clé maître pour Panorama), et cliquez sur **OK**. Panorama écrase sa configuration candidate actuelle avec la configuration chargée. Panorama affiche toutes les erreurs qui se produisent lors du chargement du fichier de configuration.
4. Si des erreurs se produisent, enregistrez-les dans un fichier local. Résolvez chaque erreur pour vous assurer que la configuration migrée est valide.

STEP 8 | Modifier la configuration de l'appareil de série M.

Requis si l'appareil de série M utilise des valeurs différentes que l'appareil virtuel Panorama. Si vous maintenez l'accès à l'appareil virtuel Panorama pour accéder à ses journaux, utilisez un nom d'hôte différent et l'adresse IP de l'appareil de série M.

1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Management (Gestion)**.
2. Modifier les paramètres généraux, modifier le **Hostname (nom d'hôte)** et cliquez **OK**.
3. Modifier les paramètres de l'interface de gestion, modifiez les valeurs selon les besoins, puis cliquez sur **OK**.

STEP 9 | Ajouter le collecteur géré par défaut et Groupe Collecteur en retour à l'appareil de série M.

Le chargement de la configuration depuis l'appareil virtuel Panorama (étape 7) supprime le collecteur géré par défaut et le groupe de collecteurs qui sont prédéfinis sur chaque appareil M-Series.

© 2020 Palo Alto Networks, Inc.

1. Configurez un collecteur géré qui est local à l'appareil de série M.
2. Configurez un groupe de collecteurs pour le collecteur géré par défaut.
3. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos modifications à la configuration Panorama.

STEP 10 | Synchroniser l'appareil de série M avec les pare-feux pour reprendre la gestion de pare-feu.

Terminez cette étape lors d'une fenêtre de maintenance pour minimiser les perturbations du réseau.

1. Sur l'appareil M-Series, sélectionnez **Panorama** > **Managed Devices (périphériques gérés)** et vérifiez que la colonne Device State (État du périphérique) affiche **Connected (Connecté)** pour les pare-feu.

   À ce stade, la politique partagée (groupes de périphériques) et colonnes Modèle affichent **Out of sync (Désynchronisés)** pour les pare-feu.
2. Appliquez vos modifications aux groupes de périphériques et aux modèles :
   1. Sélectionnez **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)** et **Edit Selections (Modifier les sélections)**.
   2. Sélectionnez **Device Groups (Groupes de périphériques)**, sélectionnez chaque groupe de périphériques, **Include Device and Network Templates (Inclure les modèles de périphérique et de réseau)** et cliquez **OK**.
   3. **Push (Appliquez)** vos changements.
3. Sur la page **Panorama** > **Managed Devices (Périphériques gérés)**, vérifiez que les colonnes Shared Policy (Politique partagée) et Template (Modèle) affichent **In sync (En synchronisation)** pour les pare-feu.

Migrer un appareil virtuel Panorama vers un autre hyperviseur

Migrez la configuration Panorama d'un appareil virtuel Panorama d'un hyperviseur pris en charge vers un autre hyberviseur pris en charge en mode Gestion uniquement ou en mode Panorama. Avant de migrer l'appareil virtuel Panorama vers un nouvel hyperviseur, passez en revue les Modèles Panorama pour vous assurer que le nouvel hyperviseur vous lequel vous effectuez la migration est pris en charge. De plus, si votre configuration Panorama comporte une configuration de plusieurs interface pour la gestion des périphériques, la collecte des journaux, la communication avec les groupes de collecteurs, les licences et les mises à jour logicielles, passez en revue la rubrique Définir la configuration requise pour l'appareil virtuel Panorama pour vérifier que l'hyperviseur vers lequel vous effectuez la migration prend en charge plusieurs interfaces.

Le mode hérité n'est plus pris en charge dans PAN-OS 8.1 ou les versions ultérieures. Si le vieil appareil virtuel Panorama est en mode hérité, vous devez le faire passer au mode Panorama avant de le migrer vers le nouvel hyperviseur afin de préserver les paramètres des journaux et les configurations de transfert du collecteur de journaux. L'importation de la configuration du vieux Panorama en mode Hérité vers un nouveau Panorama en mode Panorama entraîne la suppression de tous les paramètres des journaux et de transfert des journaux.

Vous ne pouvez pas faire migrer des journaux depuis un appareil virtuel Panorama. Par conséquent, si vous voulez maintenir l'accès aux journaux stockés sur l'ancien appareil virtuel Panorama, vous devez continuer à exécuter appareil virtuel Panorama en mode Collecteur de journaux après la migration et l'ajouter en tant que collecteur de journaux géré sur le nouvel appareil virtuel Panorama. Cela permet au nouvel appareil virtuel Panorama de collecter les journaux que les pare-feu transfèrent après la migration, tout en préservant l'accès aux données des anciens journaux. Après la pré-migration, les journaux expirent ou deviennent sans importance en raison du vieillissement, vous pouvez éteindre l'appareil virtuel Panorama.

© 2020 Palo Alto Networks, Inc.

Si vous stockez des journaux de pare-feu sur les collecteurs de journaux dédiés (appareil virtuel Panorama en mode Collecteur de journaux) au lieu de l'appareil virtuel Panorama, vous pouvez accéder aux journaux en migrant les collecteurs de journaux dédiés vers le nouvel appareil virtuel Panorama en mode Panorama.

STEP 1 | Planifier la migration.

- Mettez à niveau le logiciel sur l'appareil virtuel Panorama avant la migration, si le nouvel appareil virtuel Panorama exige une version ultérieure du logiciel actuel. Sur AWS et Microsoft Azure, Panorama doit utiliser la version 8.1 ou une version ultérieure, sur Google Cloud Platform (GCP), la version 8.1.1 ou une version ultérieure, sur KVM et AWS GovCloud, la version 8.1.2 ou une version ultérieure et sur Hyper-V, la version 8.1.3 ou une version ultérieure. Pour des informations importantes sur les versions logicielles, voir Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire.
- Programmer une fenêtre de maintenance pour la migration. Bien que les pare-feu puissent tamponner les journaux après que l'appareil virtuel Panorama se déconnecte puis transférer les journaux une fois que l'appareil de série M est en ligne, le fait de compléter la migration au cours d'une fenêtre de maintenance minimise le risque que les journaux dépassent les capacités de mémoire tampon et soient perdus au cours de la transition entre les modèles Panorama.
- Examinez l'opportunité de maintenir l'accès à l'ancien appareil virtuel Panorama après la migration pour accéder aux journaux existants. L'approche la plus efficace consiste à attribuer une nouvelle adresse IP à l'ancien appareil virtuel Panorama et réutiliser son ancienne adresse IP pour l'appareil virtuel Panorama. Cela garantit que l'ancien appareil virtuel Panorama reste accessible et que les pare-feu peuvent pointer vers le nouvel appareil virtuel Panorama sans devoir reconfigurer l'adresse IP Panorama sur chaque pare-feu.

STEP 2 | Achetez le nouvel appareil virtuel Panorama et migrez vos abonnements vers l'appareil virtuel.

1. Achetez la licence du nouvel appareil virtuel Panorama.
2. Achetez la nouvelle licence de support et la licence de migration.
3. Au moment de l'achat de la licence du nouvel appareil virtuel Panorama, indiquez à votre représentant des ventes le numéro de série et le code d'autorisation de gestion des périphériques de l'appareil virtuel Panorama que vous retirez progressivement ainsi que la date de migration des licences que vous avez choisie. Après avoir déployé le nouvel appareil virtuel Panorama, enregistrez l'appareil et activez les licences de soutien et de gestion des périphériques à l'aide des codes d'autorisation du soutien et de la migration fournis par Palo Alto Networks. À la date de migration, la licence de gestion des périphériques sur l'ancien appareil virtuel Panorama est mise hors service, et vous ne pouvez plus gérer les périphériques ou collecter les journaux à l'aide de l'ancien appareil virtuel Panorama. Cependant, la licence de soutien est conservée et l'appareil Panorama continue à bénéficier du soutien. Vous pouvez terminer la migration après la date d'entrée en vigueur, mais vous n'êtes pas en mesure de valider les changements de configuration sur l'appareil virtuel Panorama qui est désormais hors service.

STEP 3 | (Mode Hérité uniquement) Sur le vieil appareil virtuel Panorama, passez en mode Panorama.

Cette étape est requise pour préserver les données des journaux, les paramètres et la configuration du transfert des journaux de l'appareil virtuel Panorama. Si vous exportez la configuration Panorama en mode Hérité, ces paramètres sont perdus. Vous devez effectuer l'étape 10 si vous ne faites pas passer Panorama en mode Panorama avant de poursuivre.

Passez à l'étape suivante si l'appareil virtuel Panorama est déjà en mode Panorama ou en mode Gestion uniquement.

1. Configurer un appareil virtuel Panorama en mode Panorama.

© 2020 Palo Alto Networks, Inc.

2. Migrer les journaux de Panorama vers le nouveau format de journal si vous souhaitez préserver les données des journaux existants sur le vieil appareil virtuel Panorama.

STEP 4 | Exportez la configuration Panorama de l'ancien appareil virtuel Panorama.

1. Se connecter à l'interface Web Panorama.
2. Sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)**.
3. Cliquez sur **Save named Panorama configuration snapshot (Enregistrer un instantané de configuration nommé Panorama)**, entrez un **Name (Nom)** pour identifier la configuration et cliquez **sur OK**.
4. Cliquez sur **Export named Panorama configuration snapshot (Exporter l'instantané de configuration nommé Panorama),** sélectionnez le **Name (Nom)** de la configuration que vous venez d'enregistrer et cliquez sur **OK** . Panorama exporte la configuration de votre système client sous forme de fichier XML.

STEP 5 | Mise hors tension de l'ancien appareil virtuel Panorama si vous n'avez pas besoin d'y accéder après la migration ou attribuer une nouvelle adresse IP à son interface de gestion (MGT) si vous aurez besoin d'y accéder.

Pour mettre l'appareil virtuel Panorama hors tension, voir la documentation prise en charge pour l'hyperviseur sur lequel l'ancien appareil virtuel Panorama a été déployé.

Pour modifier l'adresse IP sur l'appareil virtuel Panorama :

1. Sur l'interface Web de l'ancien appareil virtuel Panorama, sélectionnez **Panorama** > **Setup (Configuration)** > **Management (Gestion)**, et modifiez les Management Interface Settings (Paramètres de l'interface de gestion).
2. Entrez la nouvelle **IP Address (Adresse IP)** et cliquez sur **OK**.
3. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

STEP 6 | Effectuez la configuration initiale du nouvel appareil virtuel Panorama.

1. Configuration de l'appareil virtuel Panorama.
2. Effectuer la configuration initiale de l'appareil virtuel Panorama pour définir les connexions réseau requises pour activer les licences et installer les mises à jour.
3. Enregistrez Panorama.
4. Activer une licence d'assistance Panorama.
5. Activer / Récupérer une licence de gestion de pare-feu lorsque l'appareil virtuel Panorama est connectée à Internet.. Utilisez le code d'authentification associé à la licence de migration.
6. Installer les mises à jour de contenu et logicielles pour Panorama. Installez les mêmes versions que celles sur l'ancien appareil virtuel Panorama.

STEP 7 | Chargez l'instantané de configuration Panorama que vous avez exporté depuis l'ancien appareil virtuel Panorama vers le nouvel appareil virtuel Panorama.

1. Se connecter à l'interface Web Panorama du nouvel appareil virtuel Panorama.
2. Sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)**.
3. Cliquez sur **Import named Panorama configuration snapshot (Importer un instantané de configuration nommé Panorama)**, **Browse (Rechercher)** le fichier de configuration Panorama vous avez exporté depuis l'appareil virtuel Panorama, et cliquez sur **OK**.
4. Cliquez sur **Load named Panorama configuration snapshot (Charger un instantané de configuration nommé Panorama)**, sélectionnez le **Name (Nom)** de la configuration que vous venez d'importer, laissez la **Decryption Key (Clé de décryptage)** vide, puis cliquez sur OK. Panorama écrase sa configuration candidate actuelle avec la configuration chargée. Panorama affiche toutes les erreurs qui se produisent lors du chargement du fichier de configuration.

© 2020 Palo Alto Networks, Inc.

5. Si des erreurs se produisent, enregistrez-les dans un fichier local. Résolvez chaque erreur pour vous assurer que la configuration migrée est valide.

STEP 8 | Modifiez la configuration du nouvel appareil virtuel Panorama.

Requis si le nouvel appareil virtuel Panorama utilise des valeurs qui diffèrent de celles de l'ancien appareil virtuel Panorama. Si vous maintenez l'accès à l'ancien appareil virtuel Panorama pour accéder à ses journaux, utilisez un nom d'hôte différent et l'adresse IP du nouvel appareil virtuel Panorama,

Les configurations de plusieurs interfaces ne sont pas prises en charge lorsque Panorama est déployé sur AWS, AWS GovCloud, Microsoft Azure et GCP. Vous devez reconfigurer la gestion des périphériques, la collecte de journaux, la communication avec les groupes de collecteurs, les licences et les mises à jour logicielles pour un fonctionnement sur l'interface MGT si vous effectuez une migration vers l'un de ces hyperviseurs.

1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Management (Gestion)**.
2. Modifier les paramètres généraux, modifier le **Hostname (nom d'hôte)** et cliquez **OK**.
3. Modifier les paramètres de l'interface de gestion, modifiez les valeurs selon les besoins, puis cliquez sur **OK**.

STEP 9 | Ajouter le collecteur géré par défaut et Groupe Collecteur au nouvel appareil virtuel Panorama.

Le chargement de la configuration depuis l'appareil virtuel Panorama (étape 7) supprime le collecteur géré par défaut et le groupe de collecteurs qui sont prédéfinis sur chaque appareil virtuel Panorama en mode Panorama.

1. Configurez un collecteur géré qui est local à l'appareil virtuel Panorama.
2. Configurez un groupe de collecteurs pour le collecteur géré par défaut.
3. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos modifications à la configuration Panorama.

STEP 10 | (Mode Hérité uniquement) Si vous avez exporté la configuration de Panorama à partir d'un appareil virtuel Panorama en mode hérité, Configurer le transfert des journaux vers Panorama.

STEP 11 | Synchronisez le nouvel appareil virtuel Panorama avec les pare-feu pour reprendre la gestion de pare-feu.

Terminez cette étape lors d'une fenêtre de maintenance pour minimiser les perturbations du réseau.

1. Sur le nouvel appareil virtuel Panorama, sélectionnez **Panorama** > **Managed Devices (périphériques gérés)** et vérifiez que la colonne Device State (État du périphérique) affiche **Connected (Connecté)** pour les pare-feu.

   À ce stade, la politique partagée (groupes de périphériques) et colonnes Modèle affichent **Out of sync (Désynchronisés)** pour les pare-feu.
2. Appliquez vos modifications aux groupes de périphériques et aux modèles :
   1. Sélectionnez **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)** et **Edit Selections (Modifier les sélections)**.
   2. Sélectionnez **Device Groups (Groupes de périphériques)**, sélectionnez chaque groupe de périphériques, **Include Device and Network Templates (Inclure les modèles de périphérique et de réseau)** et cliquez **OK**.
   3. **Push (Appliquez)** vos changements.

© 2020 Palo Alto Networks, Inc.

3. Sur la page **Panorama** > **Managed Devices (Périphériques gérés)**, vérifiez que les colonnes Shared Policy (Politique partagée) et Template (Modèle) affichent **In sync (En synchronisation)** pour les pare-feu.

Migrer d'un appareil de série M à un appareil virtuel Panorama

Vous pouvez faire migrer la configuration Panorama d'un appareil M-100, M-200, M-500, M-600 vers un appareil virtuel Panorama en mode Panorama. Cependant, vous ne pouvez pas migrer les journaux parce que le format de journal sur l'appareil de série M est incompatible avec celui sur les appareils virtuels Panorama . Par conséquent, si vous souhaitez conserver l'accès aux anciens journaux stockés sur l'appareil de série M, vous devez continuer à exécuter l'appareil de série M en tant que collecteur de journaux dédié après la migration et l'ajouter à l'appareil virtuel Panorama en tant que collecteur géré.

Si votre serveur de gestion Panorama fait partie d'une configuration à haute disponibilité, vous devez déployer un deuxième appareil virtuel Panorama du même environnement d'hyperviseur ou de cloud et acheter les licences de gestion et de soutien requises. Référez-vous à Conditions préalables HA Panorama pour obtenir la liste complète des exigences HA.

STEP 1 | Planifier la migration.

- Mettez à niveau l'appareil M-Series vers PAN-OS 10.0 ou une version ultérieure avant la migration vers l'appareil virtuel Panorama. Pour faire une mise-à-jour de Panorama, référez-vous à Installer les mises à jour de contenu et logicielles pour Panorama. Pour des informations importantes sur les versions logicielles, voir Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire.
- Programmer une fenêtre de maintenance pour la migration. Bien que les pare-feu puissent mettre les journaux en mémoire tampon après la déconnexion de l'appareil M-Series, puis transférer les journaux une fois que l'appareil virtuel Panorama est en ligne, l'achèvement de la migration au cours des heures de maintenance réduit le risque que les journaux dépassent les capacités de la mémoire tampon pendant la transition vers un autre modèle Panorama.

STEP 2 | Achetez des licences de gestion et de support pour le nouvel appareil virtuel Panorama.

1. Contactez votre représentant commercial pour acheter les nouvelles licences de gestion et de support des appareils.
2. Indiquez à votre représentant commercial le numéro de série de l'appareil M-Series que vous prévoyez de retirer, le numéro de série et le code d'authentification du support que vous avez reçus lors de l'achat du nouvel appareil virtuel Panorama, ainsi que la date à laquelle vous pensez que la migration de l'ancien appareil vers le nouvel appareil virtuel sera finalisée. Avant la date de migration, enregistrez le numéro de série et activez le code d'autorisation du support sur le nouvel appareil virtuel afin de pouvoir commencer votre migration. Le code d'autorisation de capacité sur l'ancien appareil M-Series est automatiquement supprimé à la date prévue de fin de migration que vous avez indiquée.

STEP 3 | Effectuez la configuration initiale de l'appareil virtuel Panorama.

1. Configurez l'appareil virtuel Panorama.
2. Effectuez la configuration initiale de l'appareil virtuel Panorama pour définir les connexions réseau requises pour activer les licences et installer les mises à jour.
3. Enregistrez Panorama.
4. Activer une licence d'assistance Panorama.
5. Activer / Récupérer une licence de gestion de pare-feu lorsque l'appareil virtuel Panorama est connectée à Internet.
6. Installer les mises à jour de contenu et logicielles pour Panorama. Installez les mêmes versions que celles de l'appareil de série M.

© 2020 Palo Alto Networks, Inc.

STEP 4 | Modifiez la configuration de l'interface Panorama de l'appareil M-Series pour utiliser uniquement l'interface de gestion.

L'appareil virtuel Panorama ne prend en charge que l'interface de gestion pour la gestion des périphériques et la collecte des journaux.

1. Connectez-vous à l'interface Web Panorama de l'appareil M-Series.
2. Sélectionnez **Panorama** > **Setup (Configuration)** > **Management (Gestion)**.
3. Modifier les paramètres généraux, modifier le **Hostname (nom d'hôte)** et cliquez **OK**.
4. Sélectionnez**interface** et modifiez l'interface de **Management (Gestion)** pour activer les services requis.
5. Désactiver les services pour les interfaces restantes.
6. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)**.

STEP 5 | Ajouter l'adresse IP sur l'appareil virtuel Panorama.

Sur l'appareil M-Series, ajoutez l'adresse IP publique de l'appareil virtuel Panorama en tant que deuxième serveur Panorama pour gérer les périphériques à partir du nouveau serveur d'administration Panorama. Si l'appareil virtuel Panorama est déployé sur AWS, Azure ou Google™ Cloud Platform, utilisez l'adresse IP publique.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)**.
2. Dans la liste déroulante contextuelle Modèle, sélectionnez le modèle ou la pile de modèles contenant la configuration du serveur Panorama.
3. Modifiez les paramètres de Panorama.
4. Entrez l'adresse publique de l'appareil virtuel Panorama et cliquez sur **OK**.
5. Sélectionnez **Commit (valider)** > **Commit and Push (Valider et appliquer)**.

STEP 6 | Exportez la configuration de l'appareil de série M.

1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)**.
2. Cliquez sur **Save named Panorama configuration snapshot (Enregistrer un instantané de configuration nommé Panorama)**, entrez un **Name (Nom)** pour identifier la configuration et cliquez **sur OK**.
3. Cliquez sur **Export named Panorama configuration snapshot (Exporter l'instantané de configuration nommé Panorama),** sélectionnez le **Name (Nom)** de la configuration que vous venez d'enregistrer et cliquez sur **OK** . Panorama exporte la configuration de votre système client sous forme de fichier XML. Enregistrez la configuration dans un emplacement externe à l'appareil Panorama.

STEP 7 | Éteignez l'appareil M-Series ou attribuez une nouvelle adresse IP à l'interface de gestion (MGT).

Si l'appareil M-Series est en mode Panorama et que des journaux sont stockés sur le collecteur de journaux local auquel vous devez accéder sur le nouvel appareil virtuel Panorama, vous devez modifier l'adresse IP sur l'appareil M-Series pour pouvoir l'ajouter à l'appareil virtuel Panorama en tant que collecteur de journaux géré.

- **Pour mettre l'appareil de série M hors tension :**

1. Connectez-vous à l'interface Web Panorama.
2. Sélectionnez **Panorama** > **Setup (configuration)** > **Operations (Opérations)** et, sous Device Operations (Opérations de périphérique), cliquez sur **Shutdown Panorama (Arrêter Panorama)**. Cliquez sur **Yes (Oui)** pour confirmer l'arrêt.

- **Pour modifier l'adresse IP sur l'appareil virtuel Panorama :**

1. Connectez-vous à l'interface Web Panorama.

© 2020 Palo Alto Networks, Inc.

2. Sélectionnez **Panorama (Panorama)** > **Setup (Paramétrage)** > **Management (Gestion)**, puis modifiez les paramètres d'interface de gestion.
3. Entrez la nouvelle **IP Address (Adresse IP)** et cliquez sur **OK**.
4. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

STEP 8 | Chargez l'instantané de configuration Panorama que vous avez exporté depuis l'appareil de série M vers l'appareil virtuel Panorama.

1. Connectez-vous à l'interface Web Panorama de l'appareil virtuel Panorama et sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)**.
2. Cliquez sur **Import named Panorama configuration snapshot (Importer un instantané de configuration nommé Panorama)**, **Browse (Rechercher)** le fichier de configuration Panorama vous avez exporté depuis l'appareil de série M, et cliquez sur **OK**.
3. Cliquez sur **Load named Panorama configuration snapshot (Charger un instantané de configuration nommé Panorama)**, sélectionnez le **Name (Nom)** de la configuration que vous venez d'importer, sélectionnez une **Decryption Key (Clé de décryptage)** (la clé maître pour Panorama), et cliquez sur **OK**. Panorama écrase sa configuration candidate actuelle avec la configuration chargée. Panorama affiche toutes les erreurs qui se produisent lors du chargement du fichier de configuration.

Si des erreurs se produisent, enregistrez-les dans un fichier local. Résolvez chaque erreur pour vous assurer que la configuration migrée est valide. La configuration a été chargée une fois la validation réussie.

STEP 9 | Faites passer l'appareil M-Series en mode Log Collector pour conserver les données de journal existantes.

La journalisation des données est effacée si vous passez en mode Log Collector alors que les disques de journalisation sont toujours insérés dans l'appareil M-Series. Les disques de journalisation doivent être supprimés avant de changer de mode pour éviter la perte des données contenues dans les journaux.

La génération des métadonnées de chaque paire de disques recrée les index. Par conséquent, selon le volume de données, ce processus peut prendre beaucoup de temps. Afin d'accélérer le processus, vous pouvez lancer plusieurs sessions ILC et exécuter la commande de régénération des métadonnées dans chaque session pour terminer le processus simultanément pour chaque paire. Pour plus d'informations, consultez régénération des métadonnées pour les paires RAID des unités de Série M.

1. Supprimez les disques RAID de l'appareil de la série M.
   1. Mettez l'appareil M-Series hors tension en appuyant sur le bouton d'alimentation jusqu'à ce que le système s'éteigne.
   2. Retirez les paires de disques. Pour plus d'informations, reportez-vous à la procédure de remplacement dans le Guide de Référence des appareils de la série-M.
2. Mettez l'appareil M-Series sous tension en appuyant sur le bouton d'alimentation.
3. Configurer un `compte d'administrateur super-utilisateur` admin

   Si un compte d'administrateur `admin` est déjà créé, passez à l'étape suivante.

   Vous devez créer un compte `admin` avec des privilèges de super-utilisateur avant de passer en mode Collecteur de journaux, sous peine de perdre l'accès à l'appareil M-Series après le changement de mode.
4. Connectez-vous au Panorama CLI sur l'ancien appareil de la série-M.
5. Passez du mode Panorama au mode collecteur de journaux.

© 2020 Palo Alto Networks, Inc.

- Pour passer à une session en mode collecteur de journaux, entrez la commande suivante :

```
> request system system-mode logger
```

- Entrez **Y** pour confirmer le changement de mode. L'appareil de série M redémarre. Si le processus de redémarrage termine votre session du logiciel d'émulation de terminal, reconnectez à l'appareil de série M pour afficher l'invite de connexion Panorama.

  *Si vous voyez une invite de **connexion CMS**, cela signifie que le collecteur de journaux n'a pas terminé le redémarrage. Appuyez sur ENTER à l'invite sans taper un nom d'utilisateur ou un mot de passe.*

- Connectez-vous à l'ILC.
- Vérifiez que la bascule en mode collecteur de journaux a réussi :

```
> show system info | match system-mode
```

  Si le changement de mode a réussi, la sortie affiche :

```
> system-mode: logger
```

6. Réinsérez les disques dans l'ancien appareil M-Series. Pour plus d'informations, reportez-vous à la procédure de remplacement dans le Guide de Référence des appareils de la série-M.

   Vous devez maintenir la liaison de paire de disques. Bien que vous puissiez placer une paire de disques de l'emplacement A1 / A2 sur l'emplacement dans B1 / B2, vous devez conserver les disques ensemble dans le même emplacement; dans le cas contraire, Panorama risque de ne pas restaurer les données correctement.
7. Activez les paires de disques en exécutant la commande ILC suivante pour chaque paire :

```
> request system raid add <slot> force no-format
```

   Par exemple :

```
> request system raid add A1 force no-format
> request system raid add A2 force no-format
```

   Les arguments **forçage**et **non-formatage** sont requis. L'argument **forçage** associe la paire de disques au nouvel appareil. L'argument **non-formatage** empêche le reformatage des disques et conserve les journaux stockés sur les disques.
8. Générez les métadonnées pour chaque paire de disques.

```
> request metadata-regenerate slot <slot_number>
```

   Par exemple :

```
> request metadata-regenerate slot 1
```

9. Activer la connectivité entre chaque collecteur de journaux et le serveur de gestion de Panorama.

   Saisissez les commandes suivantes dans l'ILC du collecteur de journaux, où *<IPaddress1>* est pour l'interface de gestion du panorama solitaire (non HD) ou actif (HD) et *<IPaddress2>* est pour l'interface de gestion du panorama passif (HD), le cas échéant.

© 2020 Palo Alto Networks, Inc.

```
> configure
# set deviceconfig system panorama-server <IPaddress1> panorama-server-2
 <IPaddress2>
# commit
# exit
```

STEP 10 | Synchronisez l'appareil virtuel Panorama avec les pare-feu pour reprendre la gestion de pare-feu.

Terminez cette étape lors d'une fenêtre de maintenance pour minimiser les perturbations du réseau.

1. Sur l'appareil virtuel Panorama, sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)** et vérifiez que la colonne Device State (État du périphérique) pour les pare-feu affiche **Connected (Connecté)**.

   À ce stade, la politique partagée (groupes de périphériques) et colonnes Modèle affichent **Out of sync (Désynchronisés)** pour les pare-feu.
2. Appliquez vos modifications aux groupes de périphériques et aux modèles :
   1. Sélectionnez **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)** et **Edit Selections (Modifier les sélections)**.
   2. Sélectionnez **Device Groups (Groupe de périphériques)**, sélectionnez tous les périphériques du groupe et **Inclure les modèles de périphérique et de réseau**.
   3. Sélectionnez **Collector Groups (Groupe de collecteurs)**, sélectionnez tous les collecteurs du groupe et cliquez sur **OK**.
   4. **Push (Appliquez)** vos changements.
3. Sur la page **Panorama** > **Managed Devices (Périphériques gérés)**, vérifiez que les colonnes Shared Policy (Politique partagée) et Template (Modèle) affichent **In sync (En synchronisation)** pour les pare-feu.

STEP 11 | (HA seulement) Configurez la paire HA Panorama.

Si les serveurs de gestion Panorama sont dans une configuration à haute disponibilité, effectuez les étapes ci-dessous sur l'homologue HA.

1. Effectuez la configuration initiale de l'appareil virtuel Panorama.
2. Modifiez la configuration de l'interface Panorama de l'appareil M-Series pour utiliser uniquement l'interface de gestion.
3. Ajouter l'adresse IP sur l'appareil virtuel Panorama.
4. Éteignez l'appareil M-Series ou attribuez une nouvelle adresse IP à l'interface de gestion (MGT).
5. Faites passer l'appareil M-Series en mode Log Collector pour conserver les données de journal existantes.

STEP 12 | (HA seulement) Modifiez la configuration de paire HA de l'appareil virtuelle Panorama.

1. Sur une paire HA, connectez-vous à l'interface Web Panorama, sélectionnez **Panorama** > **High Availability (haute disponibilité)** et modifiez la **Setup (Configuration)**.
2. Dans le champ **Peer HA IP Address (Adresse IP de l'homologue HA)**, entrez la nouvelle adresse IP de l'homologue HA et cliquez sur **OK**.
3. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.
4. Répétez ces étapes sur l'autre homologue dans l'homologue HA.

© 2020 Palo Alto Networks, Inc.

STEP 13 | (HA seulement) Synchronisez la paire Panorama HA.

1. Accédez au **Tableau de bord** sur l'un des homologues HA et sélectionnez **Widgets** > **System (Système)** > **High Availability (Haute disponibilité)** et affichez le widget HA.
2. **Sync to peer (Synchroniser avec l'homologue)**, cliquez sur **Yes (Oui)** et attendez que **Running config (Configuration actuelle)** affiche **Synchronized (Synchronisé)**.
3. Accédez au **tableau de bord** sur l'homologue HA restant et sélectionnez **Widgets** > **System (Système)** > **High Availability (Haute disponibilité)** et affichez le widget HA.
4. Vérifiez que **Running config (Configuration actuelle)** affiche **Synchronized (Synchronisé)**.

Migrer d'un appareil M-100 à un appareil M-500

Vous pouvez migrer la configuration Panorama et les journaux de pare-feu d'un appareil M-100 à un appareil M-500 en mode Panorama (serveur de gestion Panorama). Vous pouvez également migrer les journaux de pare-feu à partir d'un appareil M-100 à un appareil M-500 en mode Collecteur de Journaux (collecteur de journaux dédié). Étant donné que tous les collecteurs de journaux d'un groupe de collecteurs doivent être du même modèle Panorama , vous devez migrer tous ou aucun des appareils M-100 dans un groupe de collecteurs.

Dans la procédure suivante, le serveur de gestion Panorama est déployé dans une configuration active/passive haute disponibilité (HD), vous allez migrer et la configuration et les journaux, et les appareils M-500 réutiliseront les adresses IP des appareils M-100.



Cette procédure suppose que vous n'utilisez plus l'appareil M-100 pour la gestion des périphériques ou la collecte des journaux. Si vous prévoyez d'utiliser l'appareil M-100 hors service comme collecteur de journaux dédié, une licence de gestion des périphériques doit être installée sur l'appareil M-100. Sans une licence de gestion des périphériques, vous n'arrivez pas à utiliser l'appareil M-100 en tant que collecteur de journaux.

Si vous ne prévoyez pas d'utiliser l'appareil M-100 en tant que collecteur de journaux dédié, mais que l'appareil M-100 contient les données des journaux auxquels vous devez accéder ultérieurement, vous pourrez tout de même effectuer des interrogations et générer des rapports à l'aide des données des journaux existantes. Palo Alto Networks recommande de passer en revue la politique de conservation des journaux avant de mettre hors service l'appareil M-100.



Si vous migrez uniquement les journaux et non la configuration Panorama, effectuez la migration des journaux vers un nouvel appareil de Série M en mode collecteur de journaux *ou* migrez les journaux vers un nouvel appareil de Série M en mode Panorama*.*

Si vous migrez vers un nouveau serveur de gestion Panorama qui n'est pas déployé dans une configuration HD et que le nouveau Panorama doive accéder aux journaux sur les collecteurs de journaux dédiés existants, effectuez la migration des collecteurs de journaux après défaillance/RMA du Panorama non-HD*.*

STEP 1 | Planifier la migration.

- Mise à niveau du logiciel sur l'appareil M-100 si sa version actuelle est antérieure à 7.0 ; l'appareil M-500 nécessite Panorama 7.0 ou une version ultérieure. Pour des informations importantes sur les versions logicielles, voir Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire.
- Transférez le système et les journaux de configuration que Panorama et les collecteurs de journaux génèrent à une destination externe avant la migration si vous souhaitez conserver ces journaux. L'appareil de série M en mode Panorama stocke ces types de journaux sur son SSD, que vous ne

© 2020 Palo Alto Networks, Inc.

pouvez pas déplacer entre les modèles. Vous pouvez déplacer uniquement les disques RAID, qui stockent les journaux de pare-feu.

- Programmer une fenêtre de maintenance pour la migration. Bien que les pare-feu peuvent tamponner les journaux après que l'appareil M-100 se déconnecte puis transférer les journaux une fois que l'appareil M-500 est en ligne, le fait de compléter la migration au cours d'une fenêtre de maintenance minimise le risque que les journaux dépassent les capacités de mémoire tampon et soient perdus au cours de la transition entre les modèles Panorama.

STEP 2 | Achetez le nouvel appareil M-500 et migrez vos abonnements vers le nouvel appareil.

1. Achetez le nouvel appareil M-500.
2. Achetez la nouvelle licence de support et la licence de migration.
3. Au moment de l'achat du nouvel appareil M-500, indiquez à votre représentant des ventes le numéro de série et le code d'autorisation de gestion des périphériques de l'appareil M-100 que vous retirez progressivement ainsi que la date de migration des licences que vous avez choisie. Lorsque vous recevez votre appareil M-500, enregistrez l'appareil et activez les licences de soutien et de gestion des périphériques à l'aide des codes d'autorisation du soutien et de la migration fournis par Palo Alto Networks. À la date de migration, la licence de gestion des périphériques sur l'appareil M-100 est mise hors service, et vous ne pouvez plus gérer les périphériques ou collecter les journaux à l'aide de l'appareil M-100. Cependant, la licence de soutien est conservée et l'appareil Panorama continue à bénéficier du soutien. Vous pouvez terminer la migration après la date d'entrée en vigueur, mais vous n'êtes pas en mesure de valider les changements de configuration sur l'appareil M-100 qui est désormais hors service.

STEP 3 | Exportez la configuration Panorama de chaque appareil M-100 en mode Panorama.

Effectuez cette tâche sur chaque paire HD de l'appareil M-100 :

1. Connectez-vous à l'appareil M-100 et sélectionnez **Panorama** > **Setup (configuration)** > **Operations (Opérations)**.
2. Cliquez sur **Save named Panorama configuration snapshot (Enregistrer un instantané de configuration nommé Panorama)**, entrez un **Name (Nom)** pour identifier la configuration et cliquez **sur OK**.
3. Cliquez sur **Export named Panorama configuration snapshot (Exporter l'instantané de configuration nommé Panorama),** sélectionnez le **Name (Nom)** de la configuration que vous venez d'enregistrer et cliquez sur **OK** . Panorama exporte la configuration de votre système client sous forme de fichier XML.

STEP 4 | Mise hors tension de chaque appareil M-100 en mode Panorama.

1. Se connecter à la paire HD de l'appareil M-100 que vous éteignez.
2. Sélectionnez **Panorama** > **Setup (configuration)** > **Operations (Opérations)**, puis cliquez sur **Shutdown Panorama (Arrêter Panorama)**.

STEP 5 | Effectuer la configuration initiale de chaque appareil M-500.

1. Montage en rack des appareils M-500. Se référer au Guide de référence du matériel M-500 pour obtenir des instructions.
2. Effectuez la configuration initiale de l'appareil de Série M pour définir les connexions réseau requises pour activer les licences et installer les mises à jour.
3. Enregistrez Panorama.
4. Activer une licence d'assistance Panorama.
5. Activer une licence de gestion de périphérique. Utilisez le code d'authentification associé à la licence de migration.
6. Installer les mises à jour de contenu et logicielles pour Panorama. Installez les mêmes versions que celles de l'appareil M-100.

© 2020 Palo Alto Networks, Inc.

7. (Collecteur de journaux dédié uniquement) Configurez l'appareil de série M en tant que collecteur de journaux.

STEP 6 | Charger le snapshot de configuration Panorama que vous avez exporté à partir de chaque appareil M-100 dans chaque appareil M-500 en mode Panorama (les deux homologues HD).

Effectuez cette tâche sur chaque paire HD de l'appareil M-500 :

1. Connectez-vous à l'appareil M-500 et sélectionnez **Panorama** > **Setup (configuration)** > **Operations (Opérations)**.
2. Cliquez **Import named Panorama configuration snapshot (Importation nommée Panorama configuration instantané)**, **Browse (Feuilleter)** dans le fichier de configuration que vous avez exporté à partir de l'appareil M-100 qui a la même priorité HD (primaire ou secondaire) que l'appareil M-500 aura, et cliquez sur **OK**.
3. Cliquez sur **Load named Panorama configuration snapshot (Charger un instantané de configuration nommé Panorama)**, sélectionnez le **Name (Nom)** de la configuration que vous venez d'importer, sélectionnez une **Decryption Key (Clé de décryptage)** (la clé maître pour Panorama), et cliquez sur **OK**. Panorama écrase sa configuration candidate actuelle avec la configuration chargée. Panorama affiche toutes les erreurs qui se produisent lors du chargement du fichier de configuration. Si des erreurs se produisent, enregistrez-les dans un fichier local. Résolvez chaque erreur pour vous assurer que la configuration migrée est valide.
4. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Validate Commit (Confirmer la validation)**. Résolvez les erreurs avant de poursuivre.
5. **Commit (Validez)** vos modifications dans la configuration de Panorama.

STEP 7 | Synchroniser la configuration entre les paires HD des appareils M-500 en mode Panorama.

1. Sur l'appareil M-500 actif, sélectionnez la **Dashboard (Tableau de bord)** onglet et, dans le widget de haute disponibilité, cliquez sur **Sync to peer (Synchroniser les homologues)**.
2. Dans le widget Haute Disponibilité, vérifiez que le **Local (locale)** (Appareil M-500 primaire) est **active (actif)**, la **Peer (Paire)** est passive, et **Running Config (Configuration actuelle)** est **synchronized (synchronisée)**.

STEP 8 | Déplacez les disques RAID de chaque appareil M-100 à son appareil de remplacement M-500 pour migrer les journaux collectés à partir des pare-feux.

Dans les tâches suivantes, sauter toutes les étapes que vous avez déjà effectuées sur l'appareil M-500.

- Migrer les journaux vers un nouvel appareil de la série M en Mode Collecteur de Journaux. Migrer les journaux de l'appareil M-100 seulement s'il utilise un collecteur géré par défaut pour la collecte des journaux.
- Migrer les journaux vers un nouvel appareil de la série M en Mode Collecteur de Journaux.

STEP 9 | Synchroniser l'appareil M-500 actif en mode Panorama avec les pare-feux pour reprendre la gestion des pare-feu.

Terminez cette étape lors d'une fenêtre de maintenance pour minimiser les perturbations du réseau.

1. Sur l'appareil M-500 actif, sélectionnez **Panorama** > **Managed Devices (périphériques gérés)** et vérifiez que la colonne Device State (Etat du périphérique) affiche **Connected (Connecté)** pour les pare-feu.

   À ce stade, la politique partagée (groupes de périphériques) et colonnes Modèle affichent **Out of sync (Désynchronisés)** pour les pare-feu.
2. Appliquez vos modifications aux groupes de périphériques et aux modèles :

© 2020 Palo Alto Networks, Inc.

1. Sélectionnez **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)** et **Edit Selections (Modifier les sélections)**.
2. Sélectionnez **Device Groups (Groupes de périphériques)**, sélectionnez chaque groupe de périphériques, **Include Device and Network Templates (Inclure les modèles de périphérique et de réseau)** et cliquez **OK**.
3. **Push (Appliquez)** vos changements.

3. Sur la page **Panorama** > **Managed Devices (Périphériques gérés)**, vérifiez que les colonnes Shared Policy (Politique partagée) et Template (Modèle) affichent **In sync (En synchronisation)** pour les pare-feu.

© 2020 Palo Alto Networks, Inc.

Accéder et naviguer dans les interfaces de gestion de Panorama

Panorama propose trois interfaces de gestion :

- **Interface web** - L'interface web de Panorama est volontairement conçue avec un aspect similaire à l'interface web du pare-feu. Si vous êtes familiarisé avec cette dernière, vous pouvez facilement naviguer, effectuer des tâches administratives et générer des rapports à partir de l'interface Web Panorama. Cette interface graphique vous permet d'accéder à Panorama en utilisant le protocole HTTPS et c'est la meilleure façon d'effectuer des tâches administratives. Reportez-vous aux sections Se connecter à l'interface Web Panorama et Naviguer dans l'interface Web Panorama. Si vous avez besoin d'activer l'accès HTTP à Panorama, modifiez les paramètres de l'interface de gestion sur l'onglet **Panorama (Panorama)** > **Setup (Configuration)** > **Management (Gestion)**.
- **Interface de la ligne de commande (ILC)** : l'ILC est une interface sans fioritures qui vous permet de taper les commandes en succession rapide pour effectuer une série de tâches. L'ILC prend en charge deux modes de commandes - opérationnel et de configuration - et chaque mode a sa propre hiérarchie de commandes et d'instructions. Lorsque vous êtes familiarisé avec la structure d'imbrication et la syntaxe pour les commandes, l'ICL permet des temps de réponse rapides et une efficacité administrative. Reportez-vous à la section Connectez-vous à l'ILC Panorama.
- **API XML** : l'API XML est fournie en tant que service Web implémenté à l'aide de demandes et de réponses HTTP/HTTPS. Il vous permet de simplifier vos opérations et d'intégrer avec des applications existantes et des référentiels développés en interne. Pour plus d'informations sur l'utilisation de l'API Panorama, reportez-vous au Guide d'utilisation de l'API PAN-OS et Panorama XML.

Se connecter à l'interface Web Panorama

STEP 1 | Lancez un navigateur Internet et saisissez l'adresse IP de Panorama à l'aide d'une connexion sécurisée (https://<IP address="">).

STEP 2 | Connectez-vous à Panorama en fonction du type d'authentification utilisé pour votre compte. Si vous vous connectez à Panorama pour la première fois, utilisez la valeur **admin** par défaut pour votre nom d'utilisateur et votre mot de passe.

- **SAML** : cliquez sur **Use Single Sign-On (Utiliser l'ouverture de session unique)**. Si Panorama exécute l'autorisation (attribution de rôle) pour les administrateurs, entrez votre **Username (Nom d'utilisateur)** et **Continue (Continuez)**. Si le fournisseur d'identité (IdP) SAML effectue l'autorisation, **Continue (Continuez)** sans entrer de **Username (Nom d'utilisateur)**. Dans les deux cas, Panorama vous redirige vers l'IdP, qui vous invite à entrer un nom d'utilisateur et un mot de passe. Après vous être authentifié auprès de l'IdP, l'interface Web de Panorama s'affiche.
- **Tout autre type d'authentification** : entrez votre **Name (Nom)** d'utilisateur et votre **Password (Mot de passe)**. Lisez la bannière de connexion et sélectionnez **I Accept and Acknowledge the Statement Below (J'accepte et accuse réception de l'énoncé ci-dessous)** si la page de connexion dispose de la bannière et de la case à cocher. Cliquez ensuite sur **Login (Connexion)**.

STEP 3 | Lisez et **Close (fermer)** tous les messages de la journée.

Naviguer dans l'interface Web Panorama

Utilisez l'interface Web Panorama pour configurer Panorama, gérer et surveiller les pare-feu et les collecteurs de journaux et les appareils et clusters d'appareils WildFire, et accédez à l'interface Web de chaque pare-feu via le menu déroulant **Context (Contexte)**. Reportez-vous à l'aide en ligne de Panorama

© 2020 Palo Alto Networks, Inc.

pour plus d'informations sur les options et les champs dans chaque onglet de l'interface Web. Voici un aperçu des onglets :

Onglet	Description
Tableau de bord	Affichez des informations générales sur le modèle et les paramètres d'accès réseau Panorama. Cet onglet inclut des widgets qui fournissent des informations sur les applications, les journaux, les ressources système et les paramètres système.
ACC	Consultez le niveau global de risque et de menace sur le réseau, en fonction des informations recueillies par Panorama à partir des pare-feu gérés.
surveiller	Affichez et gérez les journaux et les rapports.
Device Groups (Groupes de périphériques) > Policies (Politiques)	Créer des règles de stratégie centralisées et appliquez-les à plusieurs pare-feu/groupes de périphériques. Vous devez Ajouter un groupe de périphériques pour que cet onglet s'affiche.
Device Groups (Groupes de périphériques) > Objects (Objets)	Définir la stratégie des objets que les règles de stratégie qui peuvent faire référence et que les pare-feu gérés / groupes de périphériques peuvent partager. Vous devez Ajouter un groupe de périphériques pour que cet onglet s'affiche.
Templates (Modèles) > Network (Réseau)	Configurez les paramètre réseau, tel que les profils réseau et les appliquez à plusieurs pare-feux. Vous devez Ajouter un modèle pour que cet onglet s'affiche.
Templates (Modèles) > Device (Périphérique)	Configurez les paramètres du périphérique, tels que les profils serveur et les rôles Admin, et appliquez-les à plusieurs pare-feux. Vous devez Ajouter un modèle pour que cet onglet s'affiche.
Panorama	Configurer Panorama, gérer les licences, mettre en place une haute disponibilité, accéder à des mises à jour de logiciels et des alertes de sécurité, gérer l'accès administratif et gérer les pare-feu déployés, les collecteurs de journaux et les appareils et clusters d'appareils WildFire.

Connectez-vous à l'ILC Panorama

Vous pouvez vous connecter à l'ILC Panorama en utilisant une connexion de port série ou l'accès à distance en utilisant un Shell (SSH) Secure.

- Utilisez SSH pour vous connecter à l'ILC Panorama

  Les mêmes instructions sont valables pour un appareil de série M en mode collecteur de journaux.

© 2020 Palo Alto Networks, Inc.

Vous pouvez éventuellement Configurer un administrateur avec une clé d'authentification SSH basée sur l'ILC.

1. Vérifiez que les conditions suivantes sont remplies :
   - Vous avez un ordinateur avec un accès au réseau Panorama
   - Vous connaissez l'adresse IP panorama.
   - L'interface de gestion prend en charge SSH, qui est le paramètre par défaut. Si un administrateur a désactivé SSH et que vous voulez le réactiver, sélectionnez **Panorama** > **Setup (Configuration)** > **Interfaces**, cliquez sur **Management (Gestion)**, sélectionnez **SSH**, cliquez sur **OK**, sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)**, et **Commit (Validez)** vos modifications à la configuration Panorama.
2. Pour accéder à l'ILC en utilisant SSH :
   1. Saisissez l'adresse IP Panorama dans le client SSH et utilisez le port 22.
   2. Saisissez vos informations d'accès administratif à l'invite. Après avoir connecté, le message du jour s'affiche, suivi de l'invite ILC en mode opérationnel. Par exemple :

      ```
      admin@ABC_Sydney>
      ```

- Utilisez un port série pour vous connecter à l'interface de ligne de commande Panorama.
  1. Assurez-vous que vous disposez des éléments suivants :
     - Un câble série pour modem relie Panorama à un ordinateur avec un port série DB-9
     - Un programme d'émulation de terminal s'exécutant sur l'ordinateur
  2. Utilisez les paramètres suivants dans le logiciel d'émulation de terminal pour vous connecter : 9600 bauds; 8 bits de données; 1 bit d'arrêt; Pas de parité; Pas de contrôle de flux matériel.
  3. Saisissez vos informations d'accès administratif à l'invite. Après avoir connecté, le message du jour s'affiche, suivi de l'invite ILC en mode opérationnel.

- Passez en mode de configuration.

  Pour passer en mode de configuration, entrez la commande suivante à l'invite :

  ```
  admin@ABC_Sydney> configure
  ```

  L'invite devient `admin@ABC_Sydney#`.

© 2020 Palo Alto Networks, Inc.

Configurer l'accès administratif à Panorama

Outils Panorama Contrôle d'accès basé sur les rôles (RBAC) pour vous permettre de spécifier les privilèges et les responsabilités des administrateurs. Les rubriques suivantes décrivent comment créer des rôles d'administrateur, domaines d'accès, et les comptes pour accéder à l'interface Web et l'interface ligne de commande Panorama (ILC) :

- Configuration d'un profil de rôle administrateur
- Configurer un domaine d'accès
- Configurer l'authentification et les comptes administrateurs

Configuration d'un profil de rôle administrateur

Les profils d'administration de rôle sont personnalisés Rôles d'administrateur qui vous permettent de définir des privilèges d'accès granulaires administratifs pour assurer la protection des informations sensibles de l'entreprise et la vie privée pour les utilisateurs finaux. L'idéal est de créer des profils de rôle d'administrateur qui permettent aux administrateurs d'accéder uniquement aux zones des interfaces de gestion nécessaires pour effectuer leur travail.

STEP 1 | Configurez un admin role profile (profil de rôle admin) de pare-feu.

Vous devez créer un profil de rôle admin pour le pare-feu et l'attribuer au profil de rôle admin du serveur de gestion Panorama pour permettre aux administrateurs de basculer en contexte (context switch) entre les interfaces web Panorama et pare-feu géré.

STEP 2 | Sélectionnez les **Panorama** > **Admin Roles (rôles administrateur)** et cliquez sur **Add (Ajouter)**.

STEP 3 | Entrez un **Name (Nom)** pour le profil et sélectionnez le type de **Role (Rôle)** : **Panorama** ou **Device Group and Template (Groupe de périphériques et modèle)**.

STEP 4 | Configurez les privilèges d'accès à chaque domaine fonctionnel de Panorama (**Web UI (Interface utilisateur Web))** et pare-feu (**Context Switch UI (Interface utilisateur de commutation de contexte))** en activant les icônes sur la valeur souhaitée : Activer (lecture-écriture), lecture seule, ou Désactiver.

Si les administrateurs ayant des rôles personnalisés valideront un groupe d'appareils ou des changements au modèle des pare-feux gérés, vous devez donner à ces rôles un accès en lecture-écriture Panorama > Device Groups (Groupes de périphériques) et Panorama > Templates (Modèles). Si vous mettez à niveau à partir d'une version antérieure de Panorama, le processus de mise à niveau fournit des accès en lecture seule à ces noeuds.

Vous ne pouvez pas gérer l'accès à l'ILC de pare-feu ou l'API XML grâce à des privilèges de contexte de commutation dans les rôles Panorama.

STEP 5 | Si le type de **Role (Rôle)** est **Panorama**, configurez l'accès à la **XML API (API XML)** en basculant l'icône Activé / Désactivé pour chaque domaine fonctionnel.

STEP 6 | Si le type de **Role (Rôle)** est **Panorama**, sélectionnez un niveau d'accès pour l'interface **Command Line (Ligne de commande)** : **None (Aucun)** (par défaut), **superuser (super-utilisateur)**, **superreader (super-lecteur)**, ou **panorama-admin (admin panorama)**.

© 2020 Palo Alto Networks, Inc.

STEP 7 | Afin d'activer le basculement de contexte, sélectionnez le **Device Admin Role (Rôle admin du périphérique)** que vous avez créé à l'Étape 1.

STEP 8 | Cliquez sur **OK** pour enregistrer le profil.

Configurer un domaine d'accès

Utilisez Domaines d'accès pour définir l'accès pour les groupes de périphériques et les modèles administrateurs pour les groupes et les modèles de périphériques spécifiques, et aussi pour contrôler la capacité de ces administrateurs à changer de contexte sur l'interface Web de pare-feu gérés. Panorama prend en charge jusqu'à 4 000 domaines d'accès.

STEP 1 | Sélectionnez le **Panorama** > **Access Domain (Domaine d'accès)** et cliquez sur **Add (Ajouter)**.

STEP 2 | Entrez **Name (Nom)** pour identifier le domaine d'accès.

STEP 3 | Sélectionnez un privilège d'accès pour **Shared Objects (Objets partagés)** :

- **write (écrire)** : les administrateurs peuvent effectuer toutes les opérations sur les objets partagés. Il s'agit de la valeur par défaut.
- **read (lire)** : les administrateurs peuvent afficher et cloner, mais ne peuvent pas effectuer d'autres opérations sur les objets partagés. Lors de l'ajout d'objets non partagés ou du clonage d'objets partagés, la destination doit être un groupe de périphériques dans le domaine d'accès, pas l'emplacement partagé.
- **shared-only (partagé uniquement)** : les administrateurs peuvent ajouter des objets seulement à l'emplacement partagé. Les administrateurs peuvent afficher, modifier et supprimer des objets partagés, mais ne peuvent pas les déplacer ou cloner.

Une conséquence de cette option est que les administrateurs ne peuvent effectuer aucune opération sur les objets non-partagés autrement que pour les afficher. Un exemple de la raison pour laquelle vous pouvez sélectionner cette option est une organisation qui exige que tous les objets soient dans un référentiel unique et global.

STEP 4 | Basculer les icônes dans l'onglet **Device Groups (Groupes de périphériques)** pour activer l'accès en lecture-écriture ou en lecture seule des groupes de périphériques dans le domaine d'accès.

Si vous définissez l'accès Shared Objects (Objets partagés) sur shared-only (partagé uniquement), Panorama applique accès en lecture seule aux objets dans des groupes de périphériques pour lesquels vous spécifiez un accès en lecture-écriture.

STEP 5 | Sélectionnez l'onglet **Templates (Modèles)** et **Add (Ajouter)** chaque modèle que vous souhaitez attribuer au domaine d'accès.

STEP 6 | Sélectionnez l'onglet **Device Context (Contexte du périphérique)**, sélectionnez les pare-feu à attribuer au domaine d'accès, puis cliquez sur **OK**. Les administrateurs peuvent accéder à l'interface web de ces pare-feu en utilisant le menu déroulant **Context (Contexte)** de Panorama.

Configurer l'authentification et les comptes administrateurs

Si vous avez déjà configuré un profil d'authentification ou que vous n'en avez pas besoin pour authentifier les administrateurs, vous êtes prêt à Configuration du compte administrateur Panorama. Sinon, effectuez

© 2020 Palo Alto Networks, Inc.

l'une des autres procédures énumérées ci-dessous pour configurer les comptes administrateurs pour des types spécifiques d'authentification.

- Configuration du compte administrateur Panorama
- Configuration de l'authentification locale ou externe des administrateurs de Panorama
- Configurer un administrateur Panorama avec authentification basée sur les certificats pour l'interface Web
- Configurer un administrateur avec une clé d'authentification SSH basée sur l'ILC
- Configurer l'authentification RADIUS pour les administrateurs de Panorama
- Configurer l'authentification TACACS pour les administrateurs de Panorama
- Configurer l'authentification SAML pour les administrateurs de Panorama

Configuration du compte administrateur Panorama

Les comptes administrateurs précisent les rôles administrateurs et l'authentification des administrateurs Panorama. C'est le service que vous utilisez pour affecter des rôles et effectuer l'authentification qui vous permet de déterminer si vous devez ajouter les comptes sur Panorama, sur un serveur externe, ou sur les deux (reportez-vous à la section Authentification administrateur). Pour un service d'authentification externe, vous devez configurer un profil d'authentification avant d'ajouter un compte administrateur (reportez-vous à la section Configuration de l'authentification et des comptes administrateurs). Si vous avez déjà configuré le profil d'authentification ou si vous utiliserez le mécanisme d'authentification local à Panorama, procédez comme suit pour ajouter un compte administrateur sur Panorama.



Vous ne pouvez ajouter un compte administrateur à un collecteur de journaux dédié (appareil de série M en mode collecteur de journaux). Seul le compte administrateur prédéfini avec le nom d'utilisateur par défaut (admin) est disponible sur les collecteurs de journaux dédiés.

STEP 1 | Sélectionnez **Panorama** > **Administrators (Administrateurs)** et **Add (Ajoutez)** un compte.

STEP 2 | Saisissez un **Name (Nom)** d'utilisateur pour l'administrateur.

STEP 3 | Sélectionnez une séquence ou un **Authentication Profile (Profil d'authentification)** si vous avez configuré l'un ou l'autre pour l'administrateur.

Cela est requis si Panorama utilisera Kerberos SSO ou un service externe pour l'authentification.

Si Panorama utilisera l'authentification locale, définissez le **Authentication Profile (profil d'authentification)** sur **None (Aucun)** et entrez un **Password (Mot de passe)** puis **Confirm Password (Confirmez le mot de passe)**.

STEP 4 | Sélectionnez l'**Administrator Type (Type d'administrateur)** :

- **Dynamic (Dynamique)** : sélectionnez un rôle d'administrateur prédéfini.
- **Custom Panorama Admin (Admin Panorama personnalisé)** : sélectionnez le **Profile (Profil)** du rôle administrateur que vous avez créé pour cet administrateur (voir Configurer un profil de rôle administrateur).
- **Device Group and Template Admin (Admin groupe de périphériques et modèle)** : mappez les domaines d'accès aux rôles administrateurs comme décrit à l'étape suivante.

STEP 5 | (Admin groupe de périphériques et modèle uniquement) Dans la section Access Domain to Administrator Role (Domaine d'accès au rôle administrateur), cliquez sur **Ajouter**, sélectionnez un domaine d'accès dans la liste déroulante (voir Configurer un domaine d'accès), cliquez

© 2020 Palo Alto Networks, Inc.

sur la cellule Admin Role (Rôle administrateur) adjacente et sélectionnez un profil de rôle administrateur.

STEP 6 | Cliquez sur **OK** pour enregistrer vos modifications.

STEP 7 | Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

Configuration de l'authentification locale ou externe des administrateurs de Panorama

Vous pouvez utiliser un service d'authentification externe ou le service qui est local à Panorama pour authentifier les administrateurs qui accèdent à Panorama. Ces méthodes d'authentification invitent les administrateurs à répondre à une ou plusieurs demandes d'authentification, par exemple, une page d'ouverture de session où ils doivent saisir un nom d'utilisateur et un mot de passe.

Si vous utilisez un service externe pour gérer l'authentification et l'autorisation (affectations des rôles et des domaines d'accès), reportez-vous aux sections suivantes :

- Configurer l'authentification RADIUS pour les administrateurs de Panorama
- Configurer l'authentification TACACS pour les administrateurs de Panorama
- Configurer l'authentification SAML pour les administrateurs de Panorama

Pour authentifier les administrateurs sans un mécanisme de demande/réponse, vous pouvez configurer un administrateur Panorama avec authentification basée sur les certificats pour l'interface Web *et* configurer un administrateur avec une clé d'authentification SSH basée sur l'ILC*.*

STEP 1 | (Authentification externe uniquement) Autorisez Panorama à se connecter à un serveur externe pour authentifier les administrateurs.

1. Sélectionnez **Panorama** > **Server Profiles (Profils de serveur)** , sélectionnez le type de service (**RADIUS**, **TACACS+**, **SAML**, **LDAP** ou **Kerberos**), et configurez le profil de serveur :

   - Configurer l'authentification RADIUS pour les administrateurs de Panorama.

     Vous pouvez utiliser un serveur RADIUS pour prendre en charge les services d'authentification RADIUS ou les services d'authentification multifacteur*.*

   - Configurer l'authentification TACACS pour les administrateurs de Panorama.
   - Ajoutez un profil de serveur d'IDP en SAML. Vous ne pouvez combiner l'ouverture de session unique (SSO) Kerberos à la SSO SAML ; vous ne pouvez utiliser qu'un seul type de service SSO.
   - Ajouter un profil de serveur Kerberos.
   - Ajouter un profil de serveur LDAP.

STEP 2 | (Facultatif) Définissez les paramètres de complexité et d'expiration du mot de passe si Panorama utilise l'authentification locale.

Ces paramètres protègent Panorama d'un accès non autorisé, car ils font en sorte qu'il soit plus difficile pour les pirates de deviner les mots de passe.

1. Définissez les paramètres de complexité des mots de passe et d'expiration globaux qui s'appliquent à tous les administrateurs locaux.

© 2020 Palo Alto Networks, Inc.

1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Management (Gestion)** et modifiez la section de complexité minimale de mot de passe.
2. Sélectionnez **Enabled (Activé)**.
3. Définissez les paramètres de mot de passe et cliquez sur **OK**.

2. Définissez un profil de mot de passe.

   Vous affectez le profil aux comptes administrateur pour lesquels vous souhaitez remplacer les paramètres d'expiration des mots de passe globaux.

   1. Sélectionnez **Panorama** > **Password Profiles (Profils de mots de passe)** et **Add (Ajoutez)** un profil.
   2. Saisissez un **Name (Nom)** pour identifier le profil.
   3. Définissez les paramètres d'expiration des mots de passe et cliquez sur **OK**.

STEP 3 | (SSO Kerberos uniquement) Créez un keytab Kerberos.

Un keytab est un fichier qui contient des informations concernant le compte Kerberos de Panorama. Pour prendre en charge la SSO Kerberos, votre réseau doit être doté d'une infrastructure Kerberos.

STEP 4 | Configurez un profil d'authentification.



Si vos comptes administrateurs sont stockés dans de multiples types de serveurs, vous pouvez créer un profil d'authentification pour chaque type et ajouter tous les profils à une séquence d'authentification.

Dans le profil d'authentification, indiquez le **Type** de service d'authentification et les paramètres connexes :

- **Service externe** : sélectionnez le **Type** de service externe et sélectionnez le **Server Profile (Profil de serveur)** que vous avez créé pour celui-ci.
- **Authentification locale** : définissez le **Type** sur **None (Aucun)**.
- **Kerberos SSO (SSO Kerberos)** : spécifiez la **Kerberos Realm (Partition Kerberos)** et **Import (Importez)** le **Kerberos Keytab (Keytab Kerberos)** que vous avez créé.

STEP 5 | (Administrateurs de groupes de périphériques et de modèles uniquement) Configurez un domaine d'accès.

Configurez un ou plusieurs domaines d'accès.

STEP 6 | (Rôles personnalisés uniquement) Configurez un profil de rôle administrateur.

Configurez un ou plusieurs profils de rôle administrateur.

Pour les administrateurs de Panorama personnalisés, le profil définit les privilèges d'accès pour le compte. Pour les administrateurs de groupes de périphériques et de modèles, le profil définit les privilèges d'accès pour un ou plusieurs domaines d'accès associés au compte.

STEP 7 | Configurez un administrateur.

1. Configurez un compte administrateur Panorama.
   - Affectez le **Authentication Profile (Profil d'authentification)** ou la séquence d'authentification que vous avez configuré.
   - (Admin groupe de périphériques et modèle uniquement uniquement) Mappez les domaines d'accès aux profils de rôle administrateur.
   - (Authentification locale uniquement) Sélectionnez un **Password Profile (Profil de mot de passe)** si vous en avez configuré un.
2. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

© 2020 Palo Alto Networks, Inc.

3. (Facultatif) Procédez à la Vérification de la connectivité du serveur d'authentification pour vérifier que le pare-feu peut utiliser le profil d'authentification pour authentifier les administrateurs.

Configurer un administrateur Panorama avec authentification basée sur les certificats pour l'interface Web

Comme alternative plus sûre à l'authentification par mot de passe à l'interface Web Panorama, vous pouvez configurer l'authentification basée sur les certificats pour les comptes locaux d'administrateur sur Panorama. L'authentification basée sur les certificats implique l'échange et la vérification d'une signature numérique à la place d'un mot de passe.

Configurer l'authentification basée sur les certificats pour tout administrateur désactive les connexions nom d'utilisateur / mot de passe pour tous les administrateurs sur Panorama et tous les administrateurs exigent ensuite le certificat pour se connecter.

STEP 1 | Générer un certificat autorité de certification (CA) sur Panorama.

Vous utiliserez ce certificat CA pour signer le certificat client de chaque administrateur.

Créer un certificat racine CA auto-signé.

Alternativement, vous pouvez importer un certificat *de votre CA d'entreprise.*

STEP 2 | Configurez un profil de certificat pour sécuriser l'accès à l'interface web.

1. Sélectionnez **Panorama** > **Certificate Management (Gestion de certificat)** > **Certificate Profile (Profil de certificat)** et cliquez sur **Add (Ajouter)**.
2. Entrez un **Name (Nom)** pour le profil de certificat et définissez le champ **Username (Nom d'utilisateur)** sur **Subject (Objet)**.
3. Sélectionnez **Add (Ajouter)** dans la section des certificats CA et sélectionnez le **CA Certificate (Certificat CA)** que vous venez de créer.
4. Cliquez sur **OK** pour enregistrer le profil.

STEP 3 | Configurer Panorama pour utiliser le profil de certificat pour authentifier les administrateurs.

1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les Paramètres Généraux.
2. Sélectionnez le **Certificate Profile (Profil de certificat)** que vous venez de créer et cliquez sur **OK**.

STEP 4 | Configurez les comptes administrateurs pour utiliser l'authentification du certificat client.

Configuration du compte administrateur Panorama pour chaque administrateur qui aura accès à l'interface Web Panorama. Cochez la case **Use only client certificate authentication (Web) (Utiliser uniquement l'authentification du certificat client (Web))**.

Si vous avez déjà déployé des certificats client générés par votre CA d'entreprise, passez à l'étape 8. Sinon, passez à l'étape 5.

STEP 5 | Générez un certificat client pour chaque administrateur.

Générez un certificat sur Panorama. Dans le menu déroulant **Signed By (Signé par)**, sélectionnez le certificat CA que vous avez créé.

STEP 6 | Exportez les certificats clients.

1. Exportez les certificats.

© 2020 Palo Alto Networks, Inc.

2. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

   Panorama redémarre et met fin à votre session de connexion. Par la suite, les administrateurs peuvent accéder à l'interface web uniquement depuis des systèmes clients qui ont le certificat client que vous avez généré.

STEP 7 | Importez le certificat client dans le système client de chaque administrateur qui accédera à l'interface web.

Reportez-vous à la documentation de votre navigateur web si nécessaire pour terminer cette étape.

STEP 8 | Vérifiez que les administrateurs peuvent accéder à l'interface web.

1. Ouvrez l'adresse IP de Panorama dans un navigateur sur l'ordinateur qui a le certificat client.
2. Lorsque vous y êtes invité, sélectionnez le certificat que vous avez importé et cliquez sur **OK**. Le navigateur affiche un avertissement de certificat.
3. Ajoutez le certificat à la liste des exceptions du navigateur.
4. Cliquez sur **Login (Connexion)**. L'interface Web doit apparaître sans vous inviter à saisir de nom d'utilisateur ni de mot de passe.

Configurer un administrateur avec une clé d'authentification SSH basée sur l'ILC

Pour les administrateurs qui utilisent Secure Shell (SSH) pour accéder à l'ILC Panorama, les clés SSH fournissent une méthode d'authentification plus sécurisée que les mots de passe. Les clés SSH éliminent pratiquement le risque d'attaques par force brute, permettent l'authentification à deux facteurs (clé privée et phrase secrète) et n'envoient pas de mots de passe sur le réseau. Les clés SSH permettent également des scripts automatisés pour accéder à l'ILC.

STEP 1 | Utilisez un outil de génération de clé SSH pour créer une paire de clés asymétriques sur le système de l'administrateur du client.

Les formats de clés pris en charge sont IETF SECSH et OpenSSH. Les algorithmes pris en charge sont DSA (1024 bits) et RSA (768-4096 bits).

Pour les commandes pour générer la paire de clés, reportez-vous à la documentation de votre client SSH.

La clé publique et la clé privée sont des fichiers distincts. Enregistrer les deux à un endroit auquel Panorama peut accéder Pour plus de sécurité, entrez un mot de passe pour chiffrer la clé privée. Panorama invite l'administrateur pour ce mot de passe lors de la connexion.

STEP 2 | Configurez le compte administrateur pour utiliser l'authentification de clé publique.

1. Configuration du compte administrateur Panorama.
   - Configurez l'une des deux méthodes d'authentification à utiliser comme solution de repli si l'authentification par clé SSH échoue :

     Service d'authentification externe : sélectionnez un **Authentication Profile (Profil d'authentification)**.

     Authentification locale : définissez **Authentication Profile (Profil d'authentification)** sur **None (Aucun)** et entrez un **Password (Mot de passe)**, puis **Confirm Password (Confirmez le mot de passe)**.
   - Cochez la case **Use Public Key Authentication (SSH) (Utiliser l'authentification par clé publique (SSH))**, cliquez sur **Import Key (Importer la clé)**, **Browse (Naviguez)** vers la clé publique que vous venez de générer, et cliquez sur **OK**.
2. Cliquez sur **OK** pour enregistrer le compte administrateur.

© 2020 Palo Alto Networks, Inc.

3. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

STEP 3 | Configurez le client SSH pour qu'il utilise la clé privée pour authentifier Panorama.

Effectuez cette tâche sur le système client de l'administrateur. Reportez-vous à la documentation de votre client SSH si nécessaire pour terminer cette étape.

STEP 4 | Vérifiez que l'administrateur peut accéder à l'ILC Panorama en utilisant l'authentification par clé SSH.

1. Utilisez un navigateur sur le système de l'administrateur du client pour accéder à l'adresse IP Panorama.
2. Connectez-vous à l'ILC Panorama en tant qu'administrateur. Après avoir saisi un nom d'utilisateur, vous verrez la sortie suivante (la valeur de clé est un exemple) :

```
Authenticating with public key "dsa-key-20130415"
```

3. À l'invite, saisissez la phrase secrète que vous avez définie lors de la création des clés.

Configurer l'authentification RADIUS pour les administrateurs de Panorama

Vous pouvez utiliser un serveur RADIUS pour authentifier l'accès administratif à l'interface Web Panorama. Vous pouvez également définir des attributs spécifiques au fournisseur (VSA) sur le serveur RADIUS pour gérer l'autorisation de l'administrateur. L'utilisation de VSA vous permet de changer les rôles rapidement, d'accéder aux domaines et aux groupes d'utilisateurs à travers votre service d'annuaire au lieu de reconfigurer les réglages dans Panorama.



Vous pouvez utiliser un serveur RADIUS pour authentifier l'accès administratif à l'interface Web Panorama. Vous pouvez également définir des attributs spécifiques au fournisseur (VSA) sur le serveur RADIUS pour gérer l'autorisation de l'administrateur. L'utilisation de VSA vous permet de changer les rôles rapidement, d'accéder aux domaines et aux groupes d'utilisateurs à travers votre service d'annuaire au lieu de reconfigurer les réglages dans Panorama.

Vous pouvez importer le dictionnaire RADIUS de Palo Alto Networks dans le serveur RADIUS pour définir les attributs d'authentification nécessaires pour la communication entre Panorama et le serveur RADIUS.

Vous pouvez également utiliser un serveur RADIUS pour mettre en œuvre l'authentification multifacteur (MFA) pour les administrateurs.

STEP 1 | Ajoutez un profil de serveur RADIUS.

Le profil définit comment Panorama se connecte au serveur RADIUS.

1. Sélectionnez **Panorama** > **Server Profiles (Profils de serveur)** > **RADIUS** et **Add (Ajoutez)** un profil.
2. Saisissez un **Profile Name (Nom de profil)** pour identifier le profil de serveur.
3. Saisissez l'intervalle du **Timeout (Délai d'expiration)**, en secondes, après lequel une requête d'authentification arrive à expiration (plage de 1 à 20 ; par défaut 3).



Si vous utilisez le profil de serveur pour intégrer Panorama à un service MFA, indiquez un intervalle qui donne aux administrateurs suffisamment de temps pour répondre à la demande d'authentification. Par exemple, si le service MFA demande un mot de passe à usage unique (OTP), les administrateurs ont besoin de temps pour visualiser l'OTP sur leur périphérique final, puis pour saisir l'OTP sur la page de connexion MFA.

© 2020 Palo Alto Networks, Inc.

4. Sélectionnez l'**Authentication Protocol (Protocole d'authentification)** (par défaut, **CHAP**) que Panorama utilise pour s'authentifier au serveur RADIUS.

   Sélectionnez CHAP si le serveur RADIUS prend en charge ce protocole ; il est plus sécuritaire que PAP.

5. **Add (Ajoutez)** chaque serveur RADIUS et saisissez les renseignements suivants :
   - Le **Name (Nom)** qui permet d'identifier le serveur.
   - L'adresse IP ou le FQDN du **RADIUS Server (Serveur RADIUS)**.
   - Le **Secret** / **Confirm Secret (Phrase secrète / Confirmer une phrase secrète)**, une clé pour chiffrer les noms d'utilisateur et les mots de passe.
   - Le **Port** du serveur pour les demandes d'authentification (1812 par défaut).
6. Cliquez sur **OK** pour enregistrer le profil de serveur.

STEP 2 | Affectez le profil de serveur RADIUS à un profil d'authentification.

Le profil d'authentification définit les paramètres d'authentification qui sont communs à un ensemble d'administrateurs.

1. Sélectionnez **Panorama** > **Authentication Profile (Profil d'authentification)** et **Add (Ajoutez)** un profil.
2. Entrez un **Name (Nom)** pour identifier le profil d'authentification.
3. Définissez le **Type** sur **RADIUS**.
4. Sélectionnez le **Server Profile (Profil de serveur)** que vous avez créé.
5. Sélectionnez **Retrieve user group from RADIUS (Récupérer le groupe d'utilisateurs auprès de TACACS+)** pour recueillir de l'information sur le groupe d'utilisateurs auprès des VSA définis sur le serveur TACACS+.

   Panorama fait correspondre l'information sur le groupe avec les groupes que vous avez spécifiés dans la liste d'autorisation du profil d'authentification.
6. Sélectionnez **Advanced (Avancé)** et, dans la liste d'autorisation, **Add (Ajoutez)** les administrateurs qui sont autorisés à s'authentifier avec ce profil d'authentification.
7. Cliquez sur **OK** pour enregistrer le profil d'authentification.

STEP 3 | Configurez Panorama pour utiliser le profil d'authentification pour tous les administrateurs.

1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les paramètres d'authentification.
2. Sélectionnez l'**Authentication Profile (Profil d'authentification)** que vous avez configuré et cliquez sur **OK**.

STEP 4 | Configurez les rôles et les domaines d'accès qui définissent les paramètres d'autorisation pour les administrateurs.

1. Configurez un profil de rôle Administrateur si l'administrateur utilise un rôle personnalisé plutôt qu'un rôle prédéfini (dynamique).
2. Configurez un domaine d'accès si l'administrateur utilise un groupe de périphériques et le rôle de modèle.

STEP 5 | Validez vos modifications.

Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

STEP 6 | Configurez le serveur RADIUS.

Reportez-vous à vos documents sur le serveur RADIUS pour obtenir les directives particulières à suivre pour effectuer ces étapes :

© 2020 Palo Alto Networks, Inc.

1. Ajoutez l'adresse IP ou le nom d'hôte du client RADIUS.
2. Ajoutez les comptes utilisateur.

   Si le profil de serveur RADIUS indique CHAP en tant que Authentication Protocol (Protocole d'authentification), vous devez définir les comptes en utilisant le chiffrement de mots de passe réversible. Sinon, l'authentification CHAP échouera.
3. Définissez le code fournisseur de Panorama (25461) et définissez les VSA RADIUS du rôle, du domaine d'accès et du groupe d'utilisateurs incombant à chaque administrateur.

   Lorsque vous définissez des rôles administrateur dynamiques pour les utilisateurs, utilisez des lettres minuscules pour préciser le rôle (par exemple, saisissez **`superuser`**, et nons pas **`SuperUser`**).

STEP 7 | Vérifiez que le serveur RADIUS authentifie et autorise les administrateurs.

1. Connectez-vous à l'interface Web Panorama à l'aide d'un compte administrateur que vous avez ajouté au serveur RADIUS.
2. Vérifiez que vous pouvez accéder uniquement aux pages de l'interface Web qui sont autorisées pour le rôle que vous avez associé à l'administrateur.
3. Aux onglets **Monitor (Surveillance)**, **Policies (Politiques)** et **Objects (Objets)**, vérifiez que vous pouvez accéder uniquement aux groupes de périphériques qui sont autorisés pour le domaine d'accès que vous avez associé à l'administrateur.

Configurer l'authentification TACACS pour les administrateurs de Panorama

Vous pouvez utiliser un serveur TACACS pour authentifier l'accès administratif à l'interface Web Panorama. Vous pouvez également définir des attributs spécifiques au fournisseur (VSA) sur le serveur TACACS + pour gérer l'autorisation de l'administrateur. L'utilisation de VSA vous permet de changer les rôles rapidement, d'accéder aux domaines et aux groupes d'utilisateurs à travers votre service d'annuaire au lieu de reconfigurer les réglages dans Panorama.

STEP 1 | Ajoutez un profil de serveur TACACS+.

Le profil définit comment Panorama se connecte au serveur TACACS+.

1. Sélectionnez **Panorama** > **Server Profiles (Profils de serveur)** > **TACACS+** et **Add (Ajoutez)** un profil.
2. Saisissez un **Profile Name (Nom de profil)** pour identifier le profil de serveur.
3. Saisissez l'intervalle du **Timeout (Délai d'expiration)**, en secondes, après lequel une requête d'authentification arrive à expiration (plage de 1 à 20 ; par défaut 3).
4. Sélectionnez l'**Authentication Protocol (Protocole d'authentification)** (par défaut, **CHAP**) que Panorama utilise pour s'authentifier au serveur TACACS+.

   Sélectionnez CHAP si le serveur TACACS+ prend en charge ce protocole ; il est plus sécuritaire que PAP.
5. **Add (Ajoutez)** chaque serveur TACACS+ et saisissez les renseignements suivants :
   - Le **Name (Nom)** qui permet d'identifier le serveur.
   - L'adresse IP ou le FQDN du **TACACS+ Server (Serveur TACACS+)**.
   - Le **Secret** / **Confirm Secret (Phrase secrète / Confirmer une phrase secrète)**, une clé pour chiffrer les noms d'utilisateur et les mots de passe.
   - Le **Port** du serveur pour les demandes d'authentification (49 par défaut).
6. Cliquez sur **OK** pour enregistrer le profil de serveur.

STEP 2 | Affectez le profil de serveur TACACS+ à un profil d'authentification.

© 2020 Palo Alto Networks, Inc.

Le profil d'authentification définit les paramètres d'authentification qui sont communs à un ensemble d'administrateurs.

1. Sélectionnez **Panorama** > **Authentication Profile (Profil d'authentification)** et **Add (Ajoutez)** un profil.
2. Saisissez un **Name (Nom)** pour identifier le profil.
3. Définissez le **Type** sur **TACACS+**.
4. Sélectionnez le **Server Profile (Profil de serveur)** que vous avez créé.
5. Sélectionnez **Retrieve user group from TACACS+ (Récupérer le groupe d'utilisateurs auprès de TACACS+)** pour recueillir de l'information sur le groupe d'utilisateurs auprès des VSA définis sur le serveur TACACS+.

   Panorama fait correspondre l'information sur le groupe avec les groupes que vous avez spécifiés dans la liste d'autorisation du profil d'authentification.
6. Sélectionnez **Advanced (Avancé)** et, dans la liste d'autorisation, **Add (Ajoutez)** les administrateurs qui sont autorisés à s'authentifier avec ce profil d'authentification.
7. Cliquez sur **OK** pour enregistrer le profil d'authentification.

STEP 3 | Configurez Panorama pour utiliser le profil d'authentification pour tous les administrateurs.

1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les paramètres d'authentification.
2. Sélectionnez l'**Authentication Profile (Profil d'authentification)** que vous avez configuré et cliquez sur **OK**.

STEP 4 | Configurez les rôles et les domaines d'accès qui définissent les paramètres d'autorisation pour les administrateurs.

1. Configurez un profil de rôle Administrateur si l'administrateur utilisera un rôle personnalisé plutôt qu'un rôle prédéfini (dynamique).
2. Configurez un domaine d'accès si l'administrateur utilise un groupe de périphériques et le rôle de modèle.

STEP 5 | Validez vos modifications.

Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

STEP 6 | Configurez le serveur TACACS+ pour l'authentification et l'autorisation des administrateurs.

Reportez-vous à vos documents sur le serveur TACACS+ pour obtenir les directives particulières à suivre pour effectuer ces étapes :

1. Ajoutez l'adresse IP ou le nom d'hôte du client TACACS+.
2. Ajoutez les comptes utilisateur.

   Si vous avez sélectionné CHAP en tant que Authentication Protocol (Protocole d'authentification), vous devez définir les comptes en utilisant le chiffrement de mots de passe réversible. Sinon, l'authentification CHAP échouera.
3. Définissez les VSA de TACACS+ pour les rôles, le domaine d'accès et le groupe d'utilisateurs de chaque administrateur.

   Lorsque vous définissez des rôles administrateur dynamiques pour les utilisateurs, utilisez des lettres minuscules pour préciser le rôle (par exemple, saisissez ***`superuser`****, et nons pas* ***`SuperUser`****).*

STEP 7 | Vérifiez que le serveur TACACS+ authentifie et autorise les administrateurs.

© 2020 Palo Alto Networks, Inc.

1. Connectez-vous à l'interface Web Panorama à l'aide d'un compte administrateur que vous avez ajouté au serveur TACACS+.
2. Vérifiez que vous pouvez accéder uniquement aux pages de l'interface Web qui sont autorisées pour le rôle que vous avez associé à l'administrateur.
3. Aux onglets **Monitor (Surveillance)**, **Policies (Politiques)** et **Objects (Objets)**, vérifiez que vous pouvez accéder uniquement aux systèmes virtuels qui sont autorisés pour le domaine d'accès que vous avez associé à l'administrateur.

Configurer l'authentification SAML pour les administrateurs de Panorama

Vous pouvez utiliser SAML (Security Assertion Markup Language) 2.0 pour l'accès administratif à l'interface Web Panorama (mais pas à la CLI). Vous pouvez également utiliser les attributs SAML pour gérer les autorisations d'administrateur. Les attributs SAML vous permettent de changer les rôles rapidement, d'accéder aux domaines et aux groupes d'utilisateurs à travers votre service d'annuaire au lieu de configurer à nouveau les réglages dans Panorama.

Pour configurer l'ouverture de session unique (SSO) et la déconnexion unique (SLO) SAML, vous devez enregistrer Panorama auprès de l'identity provider (fournisseur d'identité ; IdP), et vice-versa, pour permettre la communication entre eux. Si l'IdP fournit un fichier de métadonnées qui contient les informations d'enregistrement, vous pouvez l'importer sur Panorama pour y enregistrer l'IdP et pour créer un profil de serveur IdP. Le profil de serveur définit comment se connecter à l'IdP et indique le certificat que l'IdP utilise pour signer les messages SAML. Vous pouvez également utiliser un certificat pour la signature des messages SAML par Panorama. L'utilisation de certificats est facultative, mais recommandée, pour sécuriser les communications entre Panorama et l'IdP.

STEP 1 | (Recommandé) Obtenez les certificats que l'IdP et Panorama utiliseront pour signer les messages SAML.

Si les certificats ne précisent pas les attributs d'utilisation des clés, toutes les utilisations sont autorisées par défaut, y compris la signature des messages. Dans ce cas, vous pouvez obtenir les certificats en utilisant la méthode de votre choix.

Si les certificats énumèrent les attributs d'utilisation des clés, l'un des attributs doit être la Signature numérique, qui n'est pas disponible dans les certificats que vous générez sur Panorama. Dans ce cas, vous devez importer les certificats :

- **Certificat que le Panorama utilise pour signer des messages SAML** : importez le certificat de votre autorité de certification (CA) d'entreprise ou d'une CA tierce.
- **Certificat que l'IdP utilise pour signer les messages SAML** : importez un fichier de métadonnées qui contient le certificat de l'IdP (voir l'étape suivante). Le certificat IdP se limite aux algorithmes suivants :
  - **Algorithmes à clé publique** : RSA (1 024 bits ou plus) et ECDSA (toutes les tailles).
  - **Algorithmes de signature** : SHA1, SHA256, SHA384 et SHA512.

STEP 2 | Ajoutez un profil de serveur d'IDP en SAML.

Le profil de serveur enregistre l'IdP auprès de Panorama et définit leur connexion.

Dans cet exemple, vous importez un fichier de métadonnées SAML de l'IdP, pour que Panorama puisse automatiquement créer un profil de serveur et renseigner les informations de connexion, d'enregistrement et de certificat IdP.

Si l'IdP ne fournit pas de fichier de métadonnées, sélectionnez Panorama > Server Profiles (Profils de serveur) > SAML Identity Provider (Fournisseur d'identité SAML), Add (Ajoutez) le profil de serveur et saisissez manuellement les informations (consultez votre administrateur IdP pour connaître les valeurs).

© 2020 Palo Alto Networks, Inc.

1. Exportez le fichier de métadonnées SAML de l'IdP vers un système client auquel Panorama peut accéder.

   Le certificat indiqué dans le fichier doit répondre aux exigences énumérées à l'étape précédente. Consultez votre documentation sur l'IdP pour connaître les instructions relatives à l'exportation du fichier.
2. Sélectionnez **Panorama** > **Server Profiles (Profils de serveur)** > **SAML Identity Provider (Fournisseur d'identité SAML)** et **Import (Importez)** le fichier de métadonnées sur Panorama.
3. Saisissez un **Profile Name (Nom de profil)** pour identifier le profil de serveur.
4. **Browse (Accédez)** au fichier **Identity Provider Metadata (De métadonnées du fournisseur d'identité)**.
5. (Recommandé) Sélectionnez **Validate Identity Provider Certificate (Valider le certificat du fournisseur d'identité)** (par défaut) pour que Panorama valide le **Identity Provider Certificate (Certificat du fournisseur d'identité)**.

   La validation se produit uniquement après avoir affecté le profil de serveur à un profil d'authentification et après avoir cliqué sur **Commit (Valider)**. Panorama utilise le **Certificate Profile (Profil de certificat)** qui se trouve dans le profil d'authentification pour valider le certificat.

   Il est recommandé de valider le certificat pour accroître la sécurité.
6. Saisissez le **Maximum Clock Skew (Décalage d'horloge maximum)**, c'est-à-dire l'écart en secondes permis entre l'heure système de l'IdP et de Panorama au moment où Panorama valide les messages IdP (par défaut : 60 ; plage comprise entre 1 et 900). Si l'écart est supérieur à cette valeur, l'authentification échoue.
7. Cliquez sur **OK** pour enregistrer le profil de serveur.
8. Cliquez sur le nom du profil de serveur pour afficher les paramètres du profil. Vérifiez que les informations importées sont justes et modifiez-les, au besoin.

STEP 3 | Configurez un profil d'authentification.

Le profil d'authentification spécifie un profil de serveur IdP en SAML et définit les options pour le processus d'authentification, telles que SLO.

1. Sélectionnez **Panorama** > **Authentication Profile (Profil d'authentification)** et **Add (Ajoutez)** un profil.
2. Saisissez un **Name (Nom)** pour identifier le profil.
3. Définissez le **Type** sur **SAML**.
4. Sélectionnez le **IdP Server Profile (Profil de serveur IdP)** que vous avez créé.
5. Sélectionnez **Certificate for Signing Requests (Certificat de signature des demandes)**.

   Panorama utilise ce certificat pour signer les messages qu'il envoie à l'IdP.
6. (Facultatif) **Enable Single Logout (Activer la déconnexion unique)** (désactivée par défaut).
7. Sélectionnez le **Certificate Profile (Profil de certificat)** que Panorama utilise pour valider l'**Identity Provider Certificate (Certificat de fournisseur d'identité)**.
8. Entrez le **Username Attribute (Attribut du nom d'utilisateur)** que les messages IdP utilisent pour identifier les utilisateurs (**`username`** par défaut).

   *Lorsque vous définissez des rôles administrateur dynamiques pour les utilisateurs, utilisez des lettres minuscules pour préciser le rôle (par exemple, saisissez **`superuser`**, et nons pas **`SuperUser`**). Si vous gérez l'autorisation des administrateurs dans l'annuaire d'identités IdP, indiquez également le Admin Role Attribute (Attribut du rôle administrateur) et le Access Domain Attribute (Attribut du domaine d'accès).*
9. Sélectionnez **Advanced (Avancé)** et **Add (Ajoutez)** les administrateurs qui peuvent s'authentifier en utilisant ce profil d'authentification.

© 2020 Palo Alto Networks, Inc.

10. Cliquez sur **OK** pour enregistrer le profil d'authentification.

STEP 4 | Configurez Panorama pour utiliser le profil d'authentification pour tous les administrateurs.

1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Management (Gestion)**, modifiez les Authentication Settings (Paramètres d'authentification), puis sélectionnez le **Authentication Profile (Profil d'authentification)** que vous avez configuré.
2. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** pour activer vos modifications sur Panorama et valider l'**Identity Provider Certificate (Certificat du fournisseur d'identité)** que vous avez affecté au profil du serveur d'identification SAML.

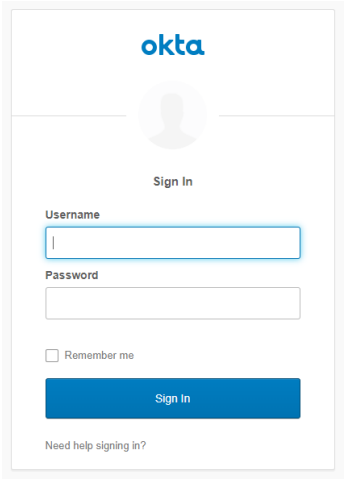
STEP 5 | Créez un fichier de métadonnées SAML pour enregistrer Panorama sur l'IdP.

1. Sélectionnez **Panorama** > **Authentication Profile (Profil d'authentification)**, puis, dans la colonne Authentication (Authentification) associée au profil d'authentification que vous avez configuré, cliquez sur **Metadata (Métadonnées)**.
2. Définissez le **Management Choice (Choix de gestion)** sur **Interface** (le paramètre par défaut est sélectionné) et sélectionnez l'interface de gestion (MGT).
3. Cliquez sur **OK** pour enregistrer le fichier de métadonnées sur votre système client.
4. Importez le fichier de métadonnées sur le serveur IdP pour enregistrer Panorama. Pour obtenir des instructions, reportez-vous à la documentation sur IdP.

STEP 6 | Vérifiez que les administrateurs peuvent s'authentifier au moyen de la SSO SAML.

1. Rendez-vous à l'URL de l'interface Web Panorama.
2. Cliquez sur **Use Single Sign-On (Ouverture de session unique)**.
3. Cliquez sur **Continue (Continuer)**.

   Panorama vous redirige pour vous demander de vous authentifier à l'IdP, qui présente une page de connexion. Par exemple :



4. Connectez-vous à l'aide de votre nom d'utilisateur et de votre mot de passe SSO.

   Une fois que vous vous serez authentifié à l'IdP, vous serez redirigé vers Panorama, où l'interface Web s'affichera.
5. Utilisez votre compte administrateur Panorama pour demander l'accès à une autre application SSO.

   Un accès réussi indique que l'authentification SSO SAML a fonctionné.

© 2020 Palo Alto Networks, Inc.

Configurer l’authentification à l’aide de certificats personnalisés

Par défaut, les appareils Palo Alto Networks utilisent des certificats prédéfinis pour l'authentification mutuelle afin d'établir les connexions SSL utilisées pour l'accès de gestion et la communication entre appareils. Cependant, vous pouvez configurer l’authentification à l’aide de certificats personnalisés. En outre, vous pouvez utiliser des certificats personnalisés pour sécuriser les connexions haute disponibilité (HD) entre les homologues HD Panorama. Les certificats personnalisés vous permettent d’établir une chaîne de confiance unique pour assurer une authentification mutuelle entre Panorama et les pare-feu gérés et les collecteurs de journaux. Consultez Gestion des certificats pour obtenir des informations détaillées sur les certificats et pour savoir comment les déployer sur Panorama, les collecteurs de journaux et les pare-feu.

Les rubriques suivantes décrivent comment configurer et gérer des certificats personnalisés à l'aide de Panorama.

- Comment les connexions SSL/TLS sont-elles mutuellement authentifiées ?
- Configurer l'authentification à l'aide de certificats personnalisés sur Panorama
- Configurer l'authentification à l'aide de certificats personnalisés sur les périphériques gérés
- Ajouter de nouveaux périphériques clients
- Modifier les certificats

Comment les connexions SSL/TLS sont-elles mutuellement authentifiées ?

Dans une connexion SSL normale, seul le serveur doit s’identifier auprès du client en présentant son certificat. Cependant, dans l’authentification SSL mutuelle, le client présente également son certificat au serveur. Panorama, l'homologue HA Panorama principal, les collecteurs de journaux, les dispositifs WildFire et les dispositifs PAN-DB peuvent servir de serveur. Les pare-feu, les collecteurs de journaux, les dispositifs WildFire et l’homologue HD du Panorama secondaire peuvent agir en tant que client. Le rôle d’un périphérique dépend du déploiement. Par exemple, dans le diagramme ci-dessous, Panorama gère un certain nombre de pare-feu et un groupe de collecteurs, et joue le rôle de serveur pour les pare-feu et les collecteurs de journaux. Le collecteur de journaux agit en tant que serveur pour les pare-feu qui lui envoient des journaux.

Pour déployer des certificats personnalisés pour l’authentification mutuelle dans votre déploiement, vous avez besoin de ce qui suit :

- **Profil de service SSL/TLS** : un profil de service SSL/TLS définit la sécurité des connexions en référençant votre certificat personnalisé et en établissant les versions du protocole SSL / TLS utilisées par le périphérique serveur pour communiquer avec les périphériques clients.
- **Certificat de serveur et profil** : Les périphériques du rôle de serveur requièrent un certificat et un profil de certificat pour s'identifier auprès des périphériques clients. Vous pouvez déployer ce certificat à partir de votre infrastructure à clé publique d’entreprise (PKI) ; achetez-en une auprès d’une autorité de certification tierce approuvée ou générez localement un certificat auto-signé. Le certificat de serveur doit inclure l'adresse IP ou le nom de domaine complet (FQDN) de l'interface de gestion du périphérique dans le nom commun du certificat (CN) ou le nom de l'attribut du sujet. Le pare-feu client ou le collecteur de journaux correspond au CN ou à l’autre nom de l’objet dans le certificat que le serveur présente par rapport à l’adresse IP ou au FQDN du serveur pour vérifier l’identité du serveur.

  En outre, utilisez le profil de certificat pour définir le statut de révocation de certificat (OCSP/CRL) et les actions prises en fonction du statut de révocation.

© 2020 Palo Alto Networks, Inc.

- **Certificats clients et profil** : chaque appareil géré nécessite un certificat client et un profil de certificat. Le périphérique client utilise son certificat pour s'identifier auprès du périphérique serveur. Vous pouvez déployer des certificats à partir de votre infrastructure à clé publique d'entreprise à l'aide du protocole SCEP (Simple Certificate Enrollment Protocol) ; achetez-en un auprès d'une autorité de certification tierce approuvée ou générez localement un certificat auto-signé.

  Les certificats personnalisés peuvent être uniques à chaque périphérique client ou communs à tous les périphériques. Les certificats de périphérique uniques utilisent un hachage du numéro de série du périphérique géré et du CN. Le serveur fait correspondre le nom commun ou l'autre nom du sujet avec les numéros de série configurés des périphériques clients. Pour que la validation du certificat client basée sur le CN se produise, le nom d'utilisateur doit être défini sur Subject common-name. Le comportement du certificat client s'applique également aux connexions des homologues HD Panorama.

  Vous pouvez configurer le certificat client et le profil de certificat sur chaque périphérique client ou transférer la configuration de Panorama vers chaque périphérique dans le cadre d'un modèle.

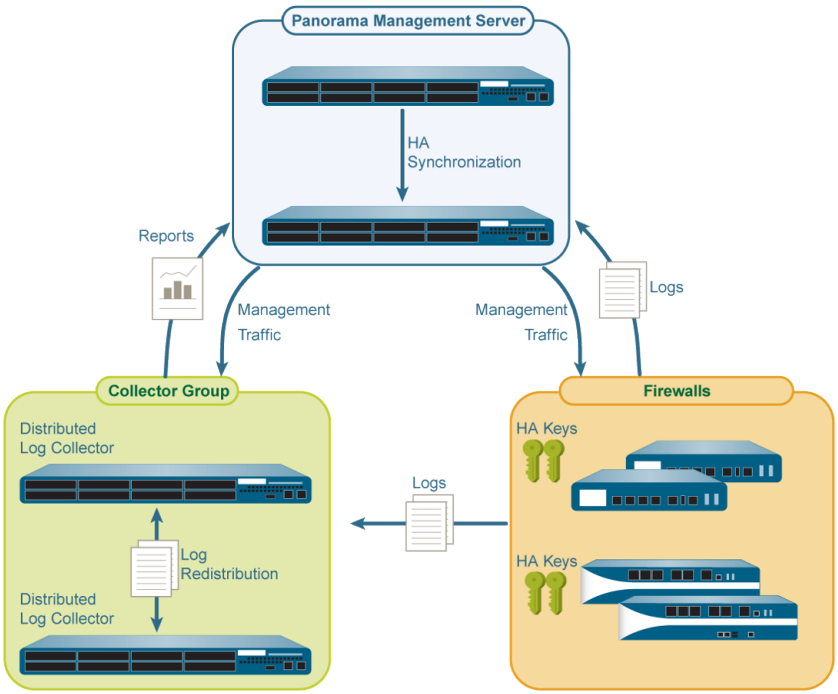


Figure 11: Authentification SSL/TLS

Configurer l'authentification à l'aide de certificats personnalisés sur Panorama

Effectuez la procédure suivante pour configurer le côté serveur (Panorama) pour utiliser des certificats personnalisés au lieu de certificats prédéfinis pour l'authentification mutuelle avec les périphériques gérés dans votre déploiement. Consultez la section Configurer l'authentification à l'aide de certificats personnalisés entre homologues HD pour configurer des certificats personnalisés sur une paire Panorama HD.

STEP 1 | Déployez le certificat de serveur.

Vous pouvez déployer des certificats sur Panorama ou sur un collecteur de journaux en générant un certificat auto-signé sur Panorama ou en obtenant un certificat de votre autorité de certification (CA) d'entreprise ou d'une autorité de certification tierce approuvée.

© 2020 Palo Alto Networks, Inc.

STEP 2 | Dans Panorama, configurez un profil de certificat. Ce profil de certificat définit le certificat à utiliser et le champ de certificat à rechercher dans l'adresse IP ou le nom de domaine complet.

1. Sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificats)**.
2. Configurez un profil de certificat.

Si vous configurez une autorité de certification intermédiaire dans le cadre du profil de certificat, vous devez également inclure l'autorité de certification racine.

STEP 3 | Configurez un profil de service SSL/TLS.

1. Sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **SSL/TLS Service Profile (Profil de service SSL/TLS)**.
2. Configurez un profil SSL/TLS pour définir le certificat et le protocole que Panorama et ses périphériques gérés utilisent pour les services SSL/TLS.

STEP 4 | Configurez Secure Server Communication (Communication sécurisée avec le serveur) sur Panorama ou un collecteur de journaux dans le rôle de serveur.

1. Sélectionnez l'un des chemins de navigation suivants :
   - Pour Panorama : **Panorama (Panorama)** > **Setup (Paramétrage)** > **Management (Gestion)** et **Edit (Modifiez)** les paramètres de communication sécurisée.
   - Pour un collecteur de journaux : **Panorama** > **Managed Collectors (Collecteurs gérés)** > **Add (Ajouter)** > **Communication**
2. Sélectionnez l'option **Customize Secure Server Communication (Personnaliser la communication sécurisée avec le serveur)**.
3. Vérifiez que la case **Allow Custom Certificates Only (Autoriser les certificats personnalisés uniquement)** n'est pas cochée. Cela vous permet de continuer à gérer tous les périphériques lors de la migration vers des certificats personnalisés.

   Lorsque la case Custom Certificate Only (Certificat personnalisé uniquement) est cochée, Panorama ne s'authentifie pas et ne peut pas gérer les périphériques à l'aide de certificats prédéfinis.
4. Sélectionnez le **SSL/TLS Service Profile (Profil de service SSL/TLS)**. Ce profil de service SSL/TLS s'applique à toutes les connexions SSL entre Panorama, les pare-feu, les collecteurs de journaux et les homologues HD de Panorama.
5. Sélectionnez le **Certificate Profile (Profil de certificat)** qui identifie le certificat à utiliser pour établir une communication sécurisée avec les clients, tels que les pare-feu.
6. (Facultatif) Configurez une liste d'autorisation. La liste d'autorisation ajoute une couche de sécurité supplémentaire au-delà de l'authentification par certificat. La liste d'autorisation vérifie l'objet ou l'autre nom de l'objet du certificat client. Si l'objet ou l'autre nom de l'objet présenté avec le certificat client ne correspond pas à un identificateur de la liste d'autorisation, l'authentification est refusée.

   Vous pouvez également autoriser les périphériques clients en fonction de leur numéro de série.

   1. **Add (Ajoutez)** une liste d'autorisation.
   2. Sélectionnez le **Subject (Objet)** ou **Subject Alt Name (Autre nom de l'objet)** configuré dans le profil de certificat en tant que type d'identifiant.
   3. Entrez le nom commun si l'identifiant est Subject (Objet) et l'adresse IP, le nom d'hôte ou l'e-mail si l'identificateur est Subject Alt Name (Autre nom de l'objet).
   4. Cliquez sur **OK**.
   5. Sélectionnez **Check Authorization List (Vérifier la liste d'autorisation)** pour appliquer la liste d'autorisation.
7. Sélectionnez **Authorize Client Based on Serial Number (Autoriser le client en fonction du numéro de série)** pour que le serveur authentifie le client en fonction des numéros de série des périphériques

© 2020 Palo Alto Networks, Inc.

gérés. Le CN ou le subject (objet) dans le certificat client doit avoir le mot-clé spécial $UDID pour activer ce type d'authentification.

8. Sélectionnez l'option **Data Redistribution (Redistribution de données)** dans la partie **Customize Communication (Personnaliser la communication)** pour utiliser un certificat personnalisé pour sécuriser la communication sortante avec les clients de redistribution de données.
9. Dans **Disconnect Wait Time (min) (Délai d'attente de déconnexion (min))**, indiquez la période pendant laquelle Panorama doit attendre avant de mettre fin à la session en cours et de rétablir la connexion avec ses périphériques gérés. Ce champ est vide par défaut et la plage est comprise entre 0 et 44 640 minutes. Laisser ce champ vide revient à le définir sur 0.

   Le délai d'attente de déconnexion de déconnexion ne commence pas à décompter tant que vous n'avez pas validé la nouvelle configuration.

10. Cliquez sur **OK**.
11. **Commit (Validez)** vos modifications.

Configurer l'authentification à l'aide de certificats personnalisés sur les périphériques gérés

Effectuez la procédure suivante pour configurer le côté client (pare-feu ou collecteur de journaux) pour utiliser des certificats personnalisés au lieu de certificats prédéfinis pour l'authentification mutuelle avec les périphériques gérés dans votre déploiement.

STEP 1 | Mettez à niveau chaque pare-feu géré ou collecteur de journaux. Tous les périphériques gérés doivent exécuter PAN-OS 8.0 ou une version ultérieure pour appliquer l'authentification par certificat personnalisé.

Upgrade the firewall (Mettre le pare-feu à jour). Après la mise à niveau, chaque pare-feu se connecte à Panorama en utilisant les certificats prédéfinis par défaut.

STEP 2 | Obtenez ou générez le certificat de périphérique.

Vous pouvez déployer des certificats sur Panorama ou sur un collecteur de journaux de serveur en générant un certificat auto-signé sur Panorama ou en obtenant un certificat de votre autorité de certification (CA) d'entreprise ou d'une autorité de certification tierce approuvée.

Définissez le nom commun sur $UDID ou l'objet sur CN=$UDID (dans le profil SCEP) si vous autorisez des périphériques clients en fonction du numéro de série.

- Vous pouvez générer un certificat auto-signé sur Panorama ou obtenir un certificat auprès de votre autorité de certification d'entreprise ou d'une autorité de certification tierce approuvée.
- Si vous utilisez SCEP pour le certificat de périphérique, configurez un profil SCEP. SCEP vous permet de déployer automatiquement des certificats sur des périphériques gérés. Lorsqu'un nouveau périphérique client avec un profil SCEP tente de s'authentifier avec Panorama, le certificat est envoyé par le serveur SCEP au périphérique.

STEP 3 | Configurez le profil du certificat du périphérique client.

Vous pouvez le configurer sur chaque périphérique client individuellement ou vous pouvez envoyer cette configuration au périphérique géré dans le cadre d'un modèle.

1. Sélectionnez l'un des chemins de navigation suivants :
   - Pour les pare-feu : sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificats)**.
   - Pour les collecteurs de journaux : sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificats)**.

© 2020 Palo Alto Networks, Inc.

2. Configurez un profil de certificat.

STEP 4 | Déployez des certificats personnalisés sur chaque pare-feu ou collecteur de journaux.

1. Sélectionnez l'un des chemins de navigation suivants :
   - Pour les pare-feu : Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et **Edit (Modifiez)** les paramètres de Panorama.
   - Pour les collecteurs de journaux : Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** et **Add (Ajoutez)** un nouveau collecteur de journaux ou sélectionnez un collecteur existant. Sélectionnez **Communication**.
2. Cochez la case **Secure Client Communication (Sécurisation des communications avec le client)** (pare-feu uniquement).
3. Sélectionnez le **Certificate Type (Type de certificat)**.
   - Si vous utilisez un certificat de périphérique local, sélectionnez **Certificate (Certificat)** et **Certificate Profile (Profil de certificat)**.
   - Si vous utilisez SCEP pour déployer le certificat de périphérique, sélectionnez **SCEP Profile (Profil SCEP)** et **Certificate Profile (Profil de certificat)**.
   - Si vous utilisez le certificat Panorama par défaut, sélectionnez **Predefined (Prédéfini)**.
4. (Facultatif) Activez **Check Server Identity (Vérifier l'identité du serveur)**. Le pare-feu ou le collecteur de journaux compare le CN dans le certificat du serveur à l'adresse IP ou au nom de domaine complet de Panorama pour vérifier son identité.
5. Cliquez sur **OK**.
6. **Commit (Validez)** vos modifications.

   Après avoir validé vos modifications, le périphérique géré ne termine pas sa session en cours avec Panorama tant que le délai d'attente de déconnexion n'est pas terminé.

STEP 5 | Sélectionnez les types de communication entrants pour lesquels vous voulez utiliser un certificat personnalisé :

- **HA Communication (Communication HA)**
- **WildFire Communication (Communication WildFire)**
- **Data Redistribution (Redistribution des données)**

STEP 6 | Après avoir déployé des certificats personnalisés sur tous les périphériques gérés, appliquez l'authentification à l'aide de certificats personnalisés.

L'appareil WildFire ne prend actuellement pas en charge les certificats personnalisés. Si votre Panorama gère un appareil WildFire, ne sélectionnez pas Allow Custom Certificates Only (Autoriser les certificats personnalisés uniquement).

1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Management (Gestion)** et **Edit (Modifiez)** les paramètres de Panorama.
2. Cochez **Allow Custom Certificates Only (Autoriser les certificats personnalisés uniquement)**.
3. Cliquez sur **OK**.
4. **Commit (Validez)** vos modifications.

   Une fois cette modification validée, tous les périphériques gérés par Panorama doivent utiliser des certificats personnalisés. Si ce n'est pas le cas, l'authentification entre Panorama et le périphérique échoue.

© 2020 Palo Alto Networks, Inc.

Ajouter de nouveaux périphériques clients

Lors de l'ajout d'un nouveau pare-feu ou d'un collecteur de journaux à Panorama, le flux de travail dépend de la configuration ou non de ces périphériques pour utiliser des certificats personnalisés uniquement pour l'authentification mutuelle.

- Si Custom Certificates Only (Certificats personnalisés uniquement) n'est pas sélectionné dans Panorama, vous pouvez ajouter le périphérique à Panorama, puis déployer le certificat personnalisé en suivant le processus commençant à l'étape Configurer l'authentification à l'aide de certificats personnalisés sur les périphériques gérés.
- Si Custom Certificates Only (Certificats personnalisés uniquement) est sélectionné dans Panorama, vous devez déployer les certificats personnalisés sur le pare-feu avant de les ajouter à Panorama. Sinon, le périphérique géré ne pourra pas s'authentifier auprès de Panorama. Cela peut être fait manuellement via l'interface Web du pare-feu ou via l'amorçage dans le cadre du fichier bootstrap.xml.

Modifier les certificats

Si un certificat personnalisé dans votre déploiement a expiré ou a été révoqué et doit être remplacé, vous pouvez effectuer l'une des tâches ci-dessous.

- Modifier un certificat de serveur
- Modifier un certificat de client
- Modifier un certificat d'autorité de certification racine ou intermédiaire

Modifier un certificat de serveur

Effectuez la tâche suivante pour remplacer un certificat de serveur.

STEP 1 | Déployez le nouveau certificat de serveur.

Vous pouvez déployer des certificats sur Panorama ou sur un collecteur de journaux de serveur en générant un certificat auto-signé sur Panorama ou en obtenant un certificat de votre autorité de certification d'entreprise ou d'une autorité de certification tierce approuvée.

STEP 2 | Changez le certificat dans le profil de service SSL/TLS.

1. Sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **SSL/TLS Service Profile (Profil de service SSL/TLS)** et sélectionnez le profil de service SSL/TLS.
2. Sélectionnez le **Certificate (Certificat)**.
3. Cliquez sur **OK**.

STEP 3 | Rétablissez la connexion entre le serveur (Panorama ou un collecteur de journaux) et les périphériques clients.

1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Management (Gestion)** et **Edit (Modifiez)** les paramètres Panorama pour Panorama ou sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** > **Add (Ajouter)** > **Communication** pour un collecteur de journaux.
2. Définissez le **Disconnect Wait Time (Délai d'attente de déconnexion)**.
3. Cliquez sur **OK**.
4. **Commit (Validez)** vos modifications.

Modifier un certificat de client

Effectuez la tâche suivante pour remplacer un certificat de client.

STEP 1 | Obtenez ou générez le certificat de périphérique.

© 2020 Palo Alto Networks, Inc.

Vous pouvez déployer des certificats sur Panorama ou sur un collecteur de journaux de serveur en générant un certificat auto-signé sur Panorama ou en obtenant un certificat de votre autorité de certification d'entreprise ou d'une autorité de certification tierce approuvée.

Définissez le nom commun sur $UDID ou l'objet sur CN=$UDID (dans le profil SCEP) si vous autorisez des périphériques clients en fonction du numéro de série.

- Vous pouvez générer un certificat auto-signé sur Panorama ou obtenir un certificat auprès de votre autorité de certification d'entreprise ou d'une autorité de certification tierce approuvée.
- Si vous utilisez SCEP pour le certificat de périphérique, configurez un profil SCEP. SCEP vous permet de déployer automatiquement des certificats sur des périphériques gérés. Lorsqu'un nouveau périphérique client avec un profil SCEP tente de s'authentifier avec Panorama, le certificat est envoyé par le serveur SCEP au périphérique.

STEP 2 | Changez le certificat dans le profil de certificat.

1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates Profile (Profil de certificat)** et sélectionnez le profil de certificat.
2. Sous les certificats CA, **Add (Ajouter)** le nouveau certificat à affecter au profil de certificat.
3. Cliquez sur **OK**.
4. **Commit (Validez)** vos modifications.

Modifier un certificat d'autorité de certification racine ou intermédiaire

Effectuez la tâche suivante pour remplacer un certificat d'autorité de certification racine ou intermédiaire.

STEP 1 | Configurez le serveur pour l'acceptation des certificats prédéfinis des clients.

1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Management (Gestion)** et **Edit (Modifiez)** les paramètres de Panorama.
2. Décochez **Custom Certificate Only (Certificat personnalisé uniquement)**.
3. Sélectionnez **Aucun** dans la liste déroulante Certificate Profile (Profil de certificat).
4. Cliquez sur **OK**.
5. **Commit (Validez)** vos modifications.

STEP 2 | Déployez le nouveau certificat d'autorité de certification racine ou intermédiaire.

Vous pouvez déployer des certificats sur Panorama ou sur un collecteur de journaux de serveur en générant un certificat auto-signé sur Panorama ou en obtenant un certificat de votre autorité de certification d'entreprise ou d'une autorité de certification tierce approuvée.

STEP 3 | Mettez à jour le certificat de l'autorité de certification dans le profil de certificat du serveur.

1. Sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **Certificates Profile (Profil de certificat)** et sélectionnez le profil de certificat à mettre à jour.
2. **Delete (Supprimez)** l'ancien certificat CA.
3. **Add (Ajoutez)** le nouveau certificat CA.
4. Cliquez sur **OK**.

STEP 4 | Générez ou importez le nouveau certificat client.

1. Sélectionnnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)**.
2. Créez un certificat racine CA auto-signé ou importez un certificat de votre CA d'entreprise.

STEP 5 | Mettez à jour le certificat d'autorité de certification dans le profil de certificat client.

© 2020 Palo Alto Networks, Inc.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et cliquez sur l'icône **Edit (Modifier)** dans les paramètres de Panorama pour un pare-feu ou sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** > **Add (Ajouter)** > **Communication** pour un collecteur de journaux et sélectionnez le profil de certificat à mettre à jour.
2. **Delete (Supprimez)** l'ancien certificat CA.
3. **Add (Ajoutez)** le nouveau certificat CA.
4. Cliquez sur **OK**.

STEP 6 | Après la mise à jour des certificats CA sur tous les périphériques gérés, appliquez l'authentification par certificat personnalisé.

1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Management (Gestion)** et **Edit (Modifiez)** les paramètres de Panorama.
2. Cochez **Custom Certificate Only (Certificat personnalisé uniquement)**.
3. Cliquez sur **OK**.
4. **Commit (Validez)** vos modifications.

   Une fois cette modification validée, tous les périphériques gérés par Panorama doivent utiliser des certificats personnalisés. Si ce n'est pas le cas, l'authentification entre Panorama et le périphérique échoue.

Gérer les pare-feu

Pour utiliser le serveur de gestion Panorama™ pour la gestion des pare-feu de Palo Alto Networks, vous devez ajouter les pare-feu comme des périphériques gérés, puis assignez-les aux groupes de volumes et à des modèles ou des piles de modèles. Les tâches suivantes sont mieux adaptées à un déploiement de pare-feu pour la première utilisation. Avant de procéder, révisez planifier votre déploiement Panorama pour comprendre les options de déploiement.

- Ajouter un pare-feu en tant que périphérique géré
- Installation du certificat de périphérique pour les pare-feux gérés
- Configurer Zero Touch Provisioning
- Gérer des groupes de périphériques
- Gérer les modèles et les piles de modèle
- Gérer la clé principale de Panorama
- Redistribuer les données vers les pare-feux gérés.
- Configurer Entreprise Data Loss Prevention (prévention des pertes de données - DLP)
- Transition d'un pare-feu à une gestion Panorama
- Surveillance de périphériques sur Panorama
- Cas d'utilisation : Configurer des pare-feu en utilisant Panorama

Pour afficher les onglets des **Objects (objets)** et des **Policies (politiques)** sur l'interface web de Panorama, vous devez d'abord créer au moins un groupe de périphériques. Pour afficher les onglets **Network (Réseau)** et **Device (Périphérique)**, vous devez créer au moins un modèle. Ces onglets contiennent les options avec lesquelles vous configurez et gérez les pare-feux de votre réseau.

© 2020 Palo Alto Networks, Inc.

Ajouter un pare-feu en tant que périphérique géré

Pour utiliser Panorama pour gérer vos pare-feu, vous devez activer une connexion entre le pare-feu et Panorama. Une connexion réussie exige que vous saisissiez l'adresse IP de Panorama sur chaque pare-feu que Panorama gérera, et que vous saisissiez également le numéro de série de chaque pare-feu sur Panorama. Lorsque vous ajoutez un pare-feu en tant que périphérique géré, vous pouvez associer le nouveau pare-feu à un groupe de périphériques, à une pile de modèles, à un groupe de collecteurs et à un collecteur de journaux lors du déploiement initial. De plus, vous avez l'option de transmettre automatiquement la configuration à votre pare-feu nouvellement ajouté lorsque le pare-feu se connecte pour la première fois à Panorama, ce qui garantit que les pare-feu sont immédiatement configurés et prêts à sécuriser votre réseau.



Vous pouvez uniquement importer en masse les pare-feu d'un seul système virtuel qui doivent être gérés par Panorama.

Le pare-feu utilise l'adresse IP du serveur Panorama pour configurer une connexion SSL pour l'enregistrement auprès de Panorama. Panorama et le pare-feu s'authentifient mutuellement à l'aide de certificats 2 048 bits et de connexions SSL chiffrées AES-256 pour la gestion de la configuration et la collecte des journaux. Préparez Panorama et chaque pare-feu comme suit :

STEP 1 | Configurez le pare-feu pour communiquer avec Panorama.

Répétez cette étape pour chaque pare-feu que Panorama surveillera.

1. Effectuez la configuration initiale sur le pare-feu afin qu'il soit accessible et puisse communiquer avec Panorama sur le réseau.
2. Configurez chaque interface de données que vous prévoyez utiliser sur le pare-feu et associez-le à une zone de sécurité, de façon à pouvoir diffuser la configuration et la stratégie depuis Panorama.
3. Ajoutez l'adresse IP de Panorama au pare-feu.
    1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et Edit (Modifiez) les paramètres de Panorama.
    2. Saisissez l'adresse IP de Panorama dans le premier champ.

    Panorama émet une adresse IP uniquement pour la gestion des périphériques, la collecte des journaux, la production de rapports et les mises à jour dynamiques. Saisissez l'adresse IP externe Internet pour veiller à ce que Panorama puisse accéder aux périphériques gérés existants et nouveaux et aux collecteurs de journaux. Si une adresse IP Panorama interne est configurée, vous pourriez ne pas être en mesure de gérer certains périphériques. Par exemple, si vous Installer Panorama sur AWS et saisissez l'adresse IP interne, Panorama n'arrive pas à gérer les périphériques ou les collecteurs de journaux à l'extérieur du gorupe de sécurité AWS.

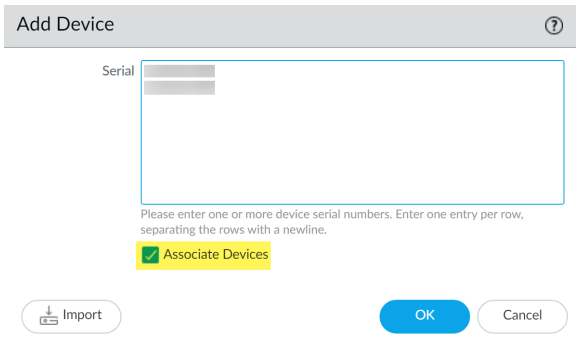
    3. (Facultatif) Si vous avez configuré une paire haute disponibilité dans Panorama, entrez l'adresse IP du Panorama secondaire dans le deuxième champ.
    4. Cliquez sur **OK**.
    5. Sélectionnez **Commit (Valider)** et **Commit (Valider)** pour enregistrer vos modifications.

STEP 2 | Ajoutez un ou plusieurs pare-feu à Panorama.

- Ajoutez un ou plusieurs pare-feu.

© 2020 Palo Alto Networks, Inc.

1. Ajoutez un nouveau périphérique géré (**Panorama** > **Managed Devices (Périphériques gérés)** > **Summary (Récapitulatif)**).
2. Saisissez le numéro **Serial (De série)** du pare-feu. Si vous ajoutez plusieurs pare-feu, entrez chaque numéro de série une ligne distincte. Si vous souhaitez associer les nouveaux pare-feu à un groupe de périphériques, à une pile de modèles, à un groupe de collecteurs ou au collecteur de journaux pour le déploiement initial, passez à l'étape suivante. Pour affecter manuellement chaque pare-feu, cliquez sur **OK** et passez à l'étape 3.
3. Cochez la case **Associate Devices (Associer les périphériques)**, puis cliquez sur **OK**.

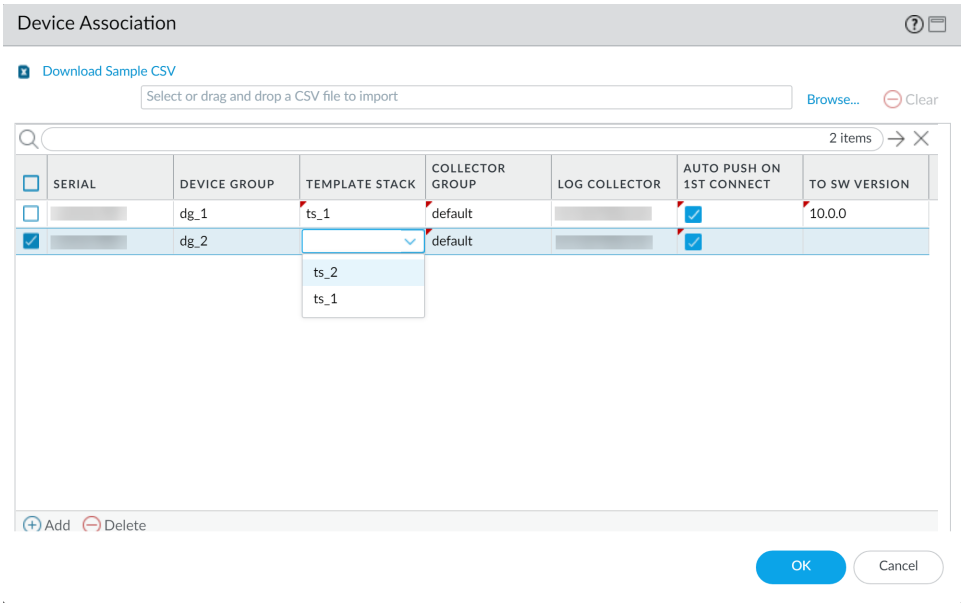


4. Affectez le **Device Group (Groupe de périphériques)**, la **Template Stack (Pile de modèles)**, le **Collector Group (Groupe de collecteurs)** et le **Log Collector (Collecteur de journaux)** selon les besoins dans la liste déroulante de chaque colonne.
5. Activez la case **Auto Push on 1st connect (Transmettre automatiquement lors de la première connexion)** pour transmettre automatiquement la configuration du groupe de périphériques et de la piles de modèles aux nouveaux périphériques lorsqu'ils se connectent avec succès à Panorama.

   L'option Auto Push on 1st Connect (Transmettre automatiquement lors de la première connexion) est prise en charge uniquement sur les pare-feu exécutant les versions 8.1 ou ultérieures de PAN-OS. La tâche `commit all` *exécute de Panorama aux périphériques gérés exécutant PAN-OS 8.1 et les versions ultérieures.*
6. (En option) Sélectionnez un version de PAN-OS dans la colonne **To SW Version (Vers la version logicielle)** pour commencer automatiquement à mettre à jour la version de PAN-OS dès la connexion à Panorama.

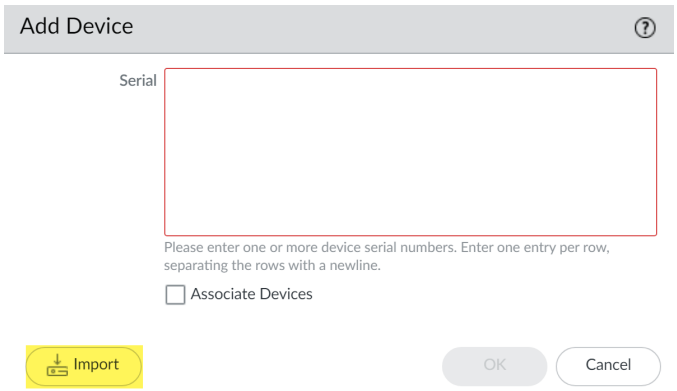
   Laissez cette colonne vide si vous ne voulez pas effectuer de mise à jour automatique du pare-feu géré.
7. Cliquez sur **OK** pour ajouter les périphériques.

© 2020 Palo Alto Networks, Inc.



- Importez les pare-feu en masse en utilisant un fichier Comma-Separated Values (valeurs séparées par des virgules ; CSV).

  1. Ajoutez un nouveau périphérique géré (**Panorama** > **Managed Devices (Périphériques gérés)** > **Summary (Récapitulatif)**).
  2. Cliquez sur **Import (Importer)**.

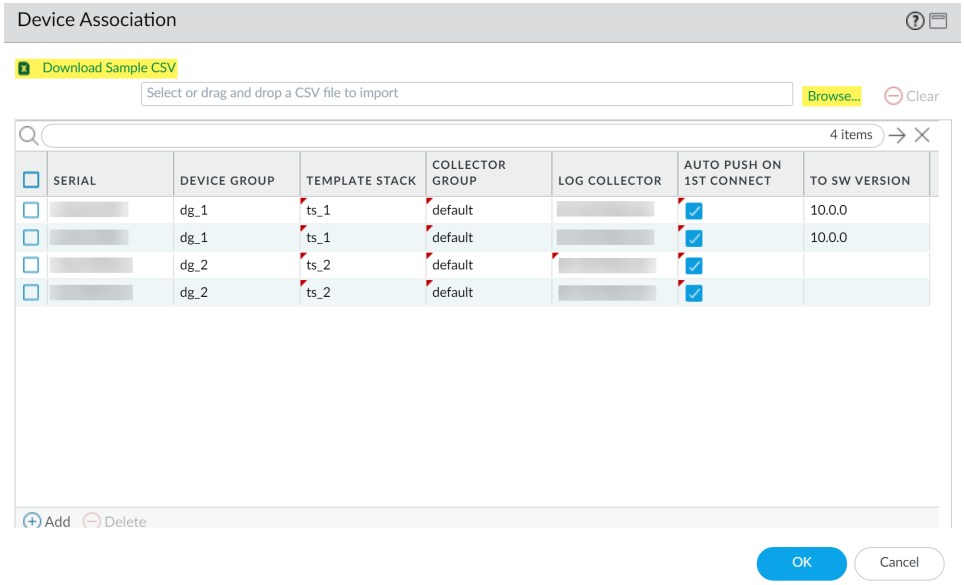


  3. **Download Sample CSV (Télécharger le fichier CSV)** et modifiez le fichier CSV téléchargé avec les pare-feu que vous ajoutez. Vous pouvez choisir d'affecter les pare-feu à un groupe de périphériques, à une pile de modèles, à un groupe de collecteurs et à un collecteur de journaux du CSV ou de saisir uniquement les numéros de série du pare-feu et de les affecter à l'interface Web. Enregistrez le fichier CSV après avoir fini de le modifier.
  4. **Browse (Parcourez)** et sélectionnez le fichier CSV que vous avez modifié à l'étape précédente.
  5. S'ils ne sont pas déjà affectés dans le fichier CSV, affectez aux pare-feux un **Device Group (Groupe de périphériques)**, une **Template Stack (Pile de modèles)**, un **Collector Group (Groupe de collecteurs)** et un **Log Collector (Collecteur de journaux)** selon les besoins dans la liste déroulante de chaque colonne.
  6. Si elle n'est pas déjà activée dans le fichier CSV, activez la case **Auto Push on 1st connect (Transmettre automatiquement lors de la première connexion)** pour transmettre automatiquement la configuration du groupe de périphériques et de la piles de modèles aux nouveaux périphériques lorsqu'ils se connectent avec succès à Panorama.

© 2020 Palo Alto Networks, Inc.

7. (En option) Sélectionnez un version de PAN-OS dans la colonne **To SW Version (Vers la version logicielle)** pour commencer automatiquement à mettre à jour la version de PAN-OS dès la connexion à Panorama.

   Laissez cette colonne vide si vous ne voulez pas effectuer de mise à jour automatique du pare-feu géré.
8. Cliquez sur **OK** pour ajouter les périphériques.



STEP 3 | (Facultatif) Ajoutez un **Tag (Balise)**. Les balises facilitent la détection d'un pare-feu dans une longue liste ; elles vous permettent de filtrer de manière dynamique et d'affiner la liste des pare-feu qui s'affiche. Par exemple, si vous ajoutez une balise libellée Filiale, vous pouvez définir un filtre pour tous les pare-feu des filiales de votre réseau.

1. Sélectionnez chaque pare-feu et cliquez sur **Tag (Balise)**.
2. Cliquez sur **Add (Ajouter)**, saisissez une chaîne de texte de 31 caractères maximum (sans espace vide), puis cliquez sur **OK**.

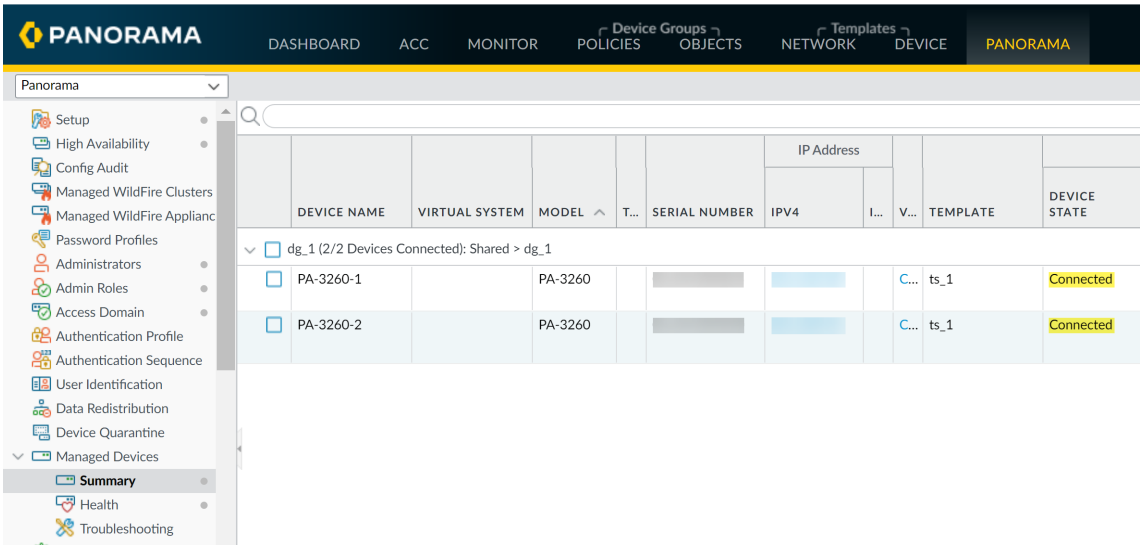
STEP 4 | Si votre déploiement utilise des certificats personnalisés pour l'authentification entre Panorama et les périphériques gérés, déployez le certificat de périphérique client personnalisé. Pour plus d'informations, reportez-vous aux sections Configurer l'authentification à l'aide de certificats personnalisés et Ajouter de nouveaux périphériques clients.

STEP 5 | Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

STEP 6 | Vérifiez que le pare-feu est connecté à Panorama.

1. Cliquez sur **Panorama** > **Managed Devices (Périphériques gérés)** > **Summary (Récapitulatif)**.
2. Vérifiez que le **Device State (État du périphérique)** du nouveau périphérique est `Connected`.

© 2020 Palo Alto Networks, Inc.



© 2020 Palo Alto Networks, Inc.

Installation du certificat de périphérique pour les pare-feux gérés

Dans PAN-OS 10.0 et les versions ultérieures, vous devez installer le certificat de périphérique sur vos pare-feux gérés afin d'authentifier avec succès vos pare-feux gérés pour exploiter les services cloud Palo Alto Networks tels que Device Telemetry, IoT et Entreprise Data Loss Prevention (prévention des pertes de données - DLP). Vous pouvez installer le certificat du périphérique pour un seul pare-feu géré ou plusieurs pare-feux gérés à la fois.



Voir Device Certificates (Certificats de périphérique) *pour installer localement le certificat de périphérique du pare-feu.*

- Installation du certificat de périphérique pour un pare-feu géré
- Installation du certificat de périphérique pour plusieurs pare-feux gérés

Installation du certificat de périphérique pour un pare-feu géré

Dans PAN-OS 10.0 et les versions ultérieures, vous devez installer le certificat de périphérique pour un pare-feu géré à partir du serveur de gestion Panorama. Le pare-feu géré doit avoir accès à Internet pour installer avec succès le certificat du périphérique.

STEP 1 | Enregistrer Panorama et managed firewalls (pare-feu gérés) avec le portail de support client (CSP) de Palo Alto Networks.

STEP 2 | Se connecter à l'interface Web Panorama en tant qu'utilisateur admin.

STEP 3 | Configurez le serveur Network Time Protocol (protocole d'heure réseau - NTP).

Un serveur NTP est nécessaire pour valider la date d'expiration de la certification du périphérique, s'assurer que le certificat du périphérique n'expire pas prématurément ou ne devienne pas invalide.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Services** et sélectionnez le **Template (Modèle)**.
2. Sélectionnez l'une des options suivantes en fonction de votre plate-forme :
   - Pour les platesformes de système multi-virtuelles, sélectionnez **Global (Global)** et modifiez la section Services.
   - Pour les platesformes de système virtuel unique, modifiez la section Services.
3. Sélectionnez **NTP** et saisissez le nom d'hôte **`pool.ntp.org`** comme **serveur NTP primaire** ou saisissez l'adresse IP de votre serveur NTP primaire.
4. (Facultatif) Saisissez une **Secondary NTP Server (adresse IP de serveur DNS Secondary (Secondaire))**.
5. (Facultatif Pour authentifier les mises à jour de temps à partir du (des) serveur (s) NTP, pour le **Authentification Type (Type d'authentification)**, sélectionnez l'un des éléments suivants pour chaque serveur.
   - **None (Aucun)** (Par défaut) : Désactive l'authentification NTP.
   - **Symmetric Key (Clé symétrique)**: Le pare-feu utilise l'échange de clés symétrique (secrets partagés) pour authentifier les mises à jour de temps.
     - **Key ID (ID de clé)** : Saisissez l'ID de la clé (1-65534).
     - **Algorithm (Algorithme)** : Sélectionnez l'algorithme à utiliser lors de l'authentification NTP (**MDS** or **SHA1**)

© 2020 Palo Alto Networks, Inc.

6. Cliquez sur **OK** pour enregistrer votre configuration.
7. Cliquez sur **Commit (Valider)** et **Commit and Push (Validez et appliquez)** vos modifications aux pare-feu que vous gérez.

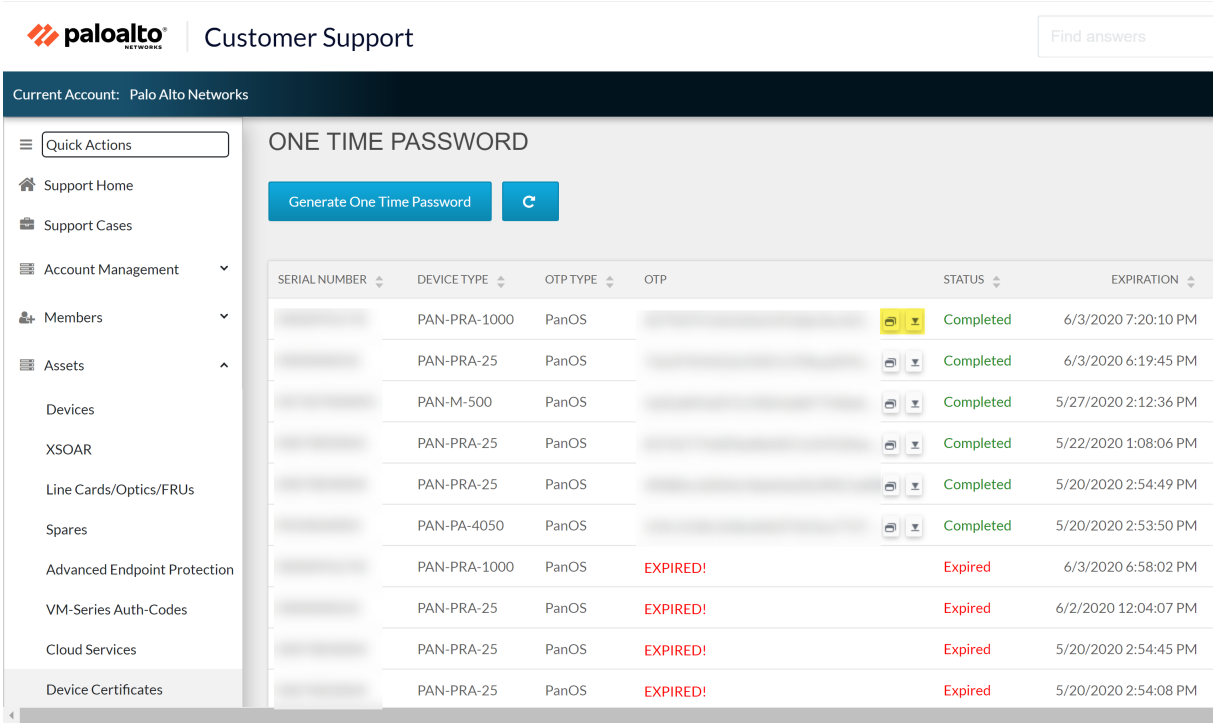
STEP 4 | Sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)** > **Summary (Résumé)** et sélectionnez un pare-feu géré.

STEP 5 | Sélectionnez **Request OTP From CSP (Demander un OTP auprès du CSP)** > **Custom selected devices (Personnaliser les périphériques sélectionnés)**.

STEP 6 | Copiez le jeton de demande OTP dans son intégralité.

STEP 7 | Générez le One-Time Password (mot de passe à usage unique ; OTP) pour les pare-feux gérés.

1. Ouvrez une session dans le portail de support client.
2. Sélectionnez **Assets (Ressources)** > **Device Certificates (Certificats de périphériques)** et **Generate OTP (Générer un OTP)**.
3. Pour le **Device Type (Type de périphérique)**, sélectionnez **Generate OTP for Panorama managed firewalls (Générer un OTP pour les pare-feux gérés de Panorama)**.
4. Collez la demande de l'OTP que vous avez copiée lors de l'étape précédente et **Generate OTP (Générer OTP)**.
5. Cliquez sur **Done (Terminé)** et patientez quelques minutes pour que l'OTP soit généré. Vous pouvez actualiser la page si le nouvel OTP n'est pas affiché.
6. **Copy to Clipboard (Copiez dans le presse-papier)** ou **Download (Téléchargez)** l'OTP.



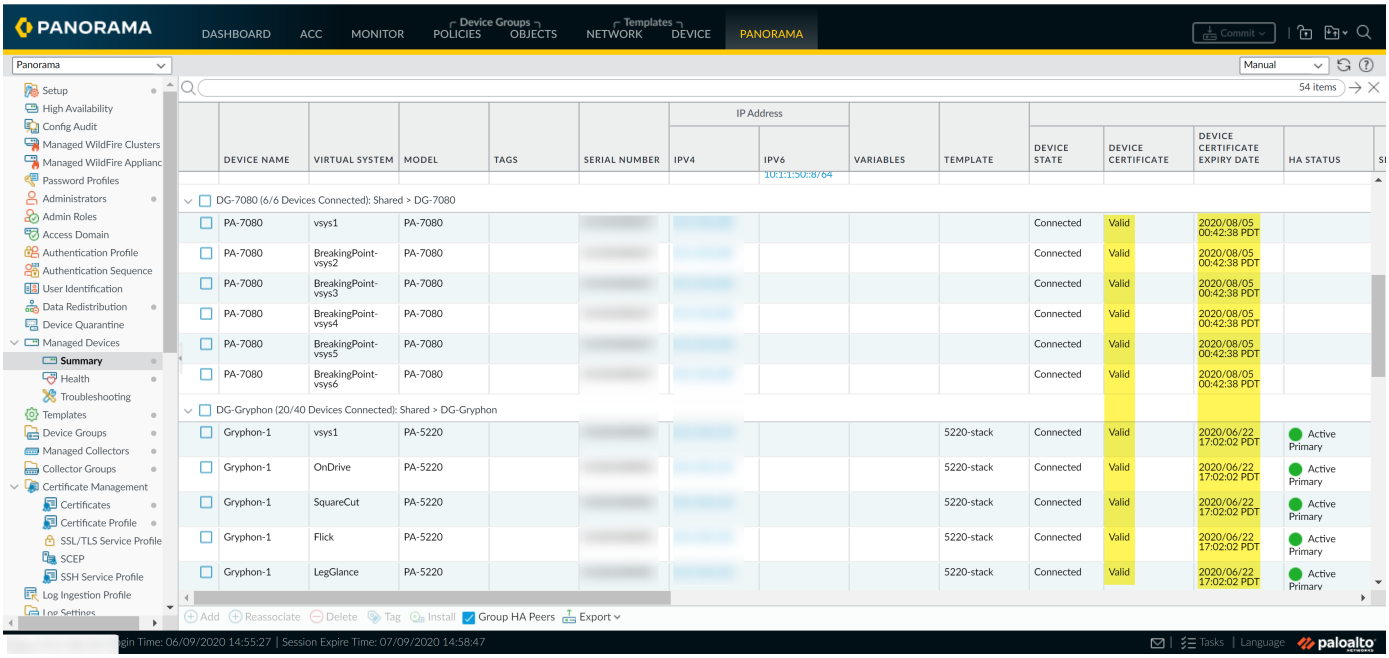
STEP 8 | Se connecter à l'interface Web Panorama en tant qu'utilisateur admin.

STEP 9 | Sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)** > **Summary (Récapitulatif)** et **Upload OTP** (Télécharger un OTP).

STEP 10 | Copiez l'OTP que vous avez généré et cliquez sur **Upload (Télécharger)**.

© 2020 Palo Alto Networks, Inc.

STEP 11 | Vérifiez que la colonne **Device Certificate (Certificat de périphérique)** indique **`Valid (Valide)`** et que la **Device Certificate Expiry Date (date d'expiration du certificat de périphérique)** indique une date d'expiration.



Installation du certificat de périphérique pour plusieurs pare-feux gérés

Dans PAN-OS 10.0 et les versions ultérieures, vous devez installer le certificat de périphérique pour les pare-feux gérés à partir du serveur de gestion Panorama. Les pare-feux gérés doivent avoir accès à Internet pour installer avec succès le certificat du périphérique.

STEP 1 | Enregistrer Panorama et managed firewalls (pare-feu gérés) avec le portail de support client (CSP) de Palo Alto Networks.

STEP 2 | Se connecter à l'interface Web Panorama en tant qu'utilisateur admin.

STEP 3 | Configurez le serveur Network Time Protocol (protocole d'heure réseau - NTP).

Un serveur NTP est nécessaire pour valider la date d'expiration de la certification du périphérique, s'assurer que le certificat du périphérique n'expire pas prématurément ou ne devienne pas invalide.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Services** et sélectionnez le **Template (Modèle)**.
2. Sélectionnez l'une des options suivantes en fonction de votre plate-forme :
   - Pour les plateformes multi virtual-systems, sélectionnez **Global (Global)** et modifiez la section Services.
   - Pour les plateformes multi virtual-systems, modifiez la section Services.
3. Sélectionnez **NTP** et saisissez le nom d'hôte **`pool.ntp.org`** comme **serveur NTP primaire** ou saisissez l'adresse IP de votre serveur NTP primaire.
4. (Facultatif) Saisissez une **Secondary NTP Server (adresse IP de serveur DNS Secondary (Secondaire))**.
5. (Facultatif Pour authentifier les mises à jour de temps à partir du (des) serveur (s) NTP, pour le **Authentification Type (Type d'authentification)**, sélectionnez l'un des éléments suivants pour chaque serveur.

© 2020 Palo Alto Networks, Inc.

- **None (Aucun)** (Par défaut) : Désactive l'authentification NTP.
- **Symmetric Key (Clé symétrique)**: Le pare-feu utilise l'échange de clés symétrique (secrets partagés) pour authentifier les mises à jour de temps.
  - **Key ID (ID de clé)** : Saisissez l'ID de la clé (1-65534).
  - **Algorithm (Algorithme)** : Sélectionnez l'algorithme à utiliser lors de l'authentification NTP (**MDS** or **SHA1**)

6. Cliquez sur **OK** pour enregistrer votre configuration.
7. Cliquez sur **Commit (Valider)** et **Commit and Push (Validez et appliquez)** vos modifications aux pare-feu que vous gérez.

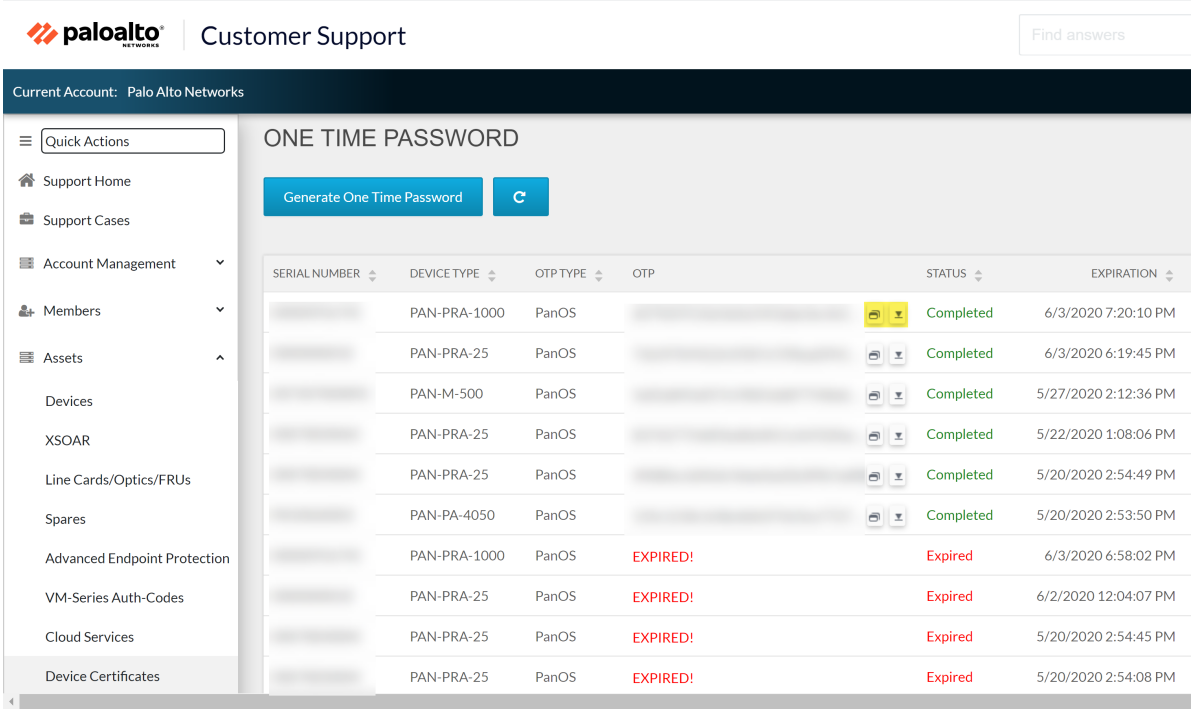
STEP 4 | Sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)** > **Summary (Récapitulatif)**.

STEP 5 | Sélectionnez **Request OTP From CSP (Demande OTP auprès du CSP)** > **Sélectionnez tous les périphériques sans certificat .**

STEP 6 | Copiez le jeton de demande OTP dans son intégralité.

STEP 7 | Générez le One-Time Password (mot de passe à usage unique ; OTP) pour les pare-feux gérés.

1. Ouvrez une session dans le portail de support client.
2. Sélectionnez **Assets (Ressources)** > **Device Certificates (Certificats de périphériques)** et **Generate OTP (Générer un OTP)**.
3. Pour le **Device Type (Type de périphérique)**, sélectionnez **Generate OTP for Panorama managed firewalls (Générer un OTP pour les pare-feux gérés de Panorama)**.
4. Collez la demande de l'OTP que vous avez copiée lors de l'étape précédente et **Generate OTP (Générer OTP)**.
5. Cliquez sur **Done (Terminé)** et patientez quelques minutes pour que l'OTP soit généré. Vous pouvez actualiser la page si le nouvel OTP n'est pas affiché.
6. **Copy to Clipboard (Copier dans le presse-papier)** ou **Download (Télécharger)** l'OTP.



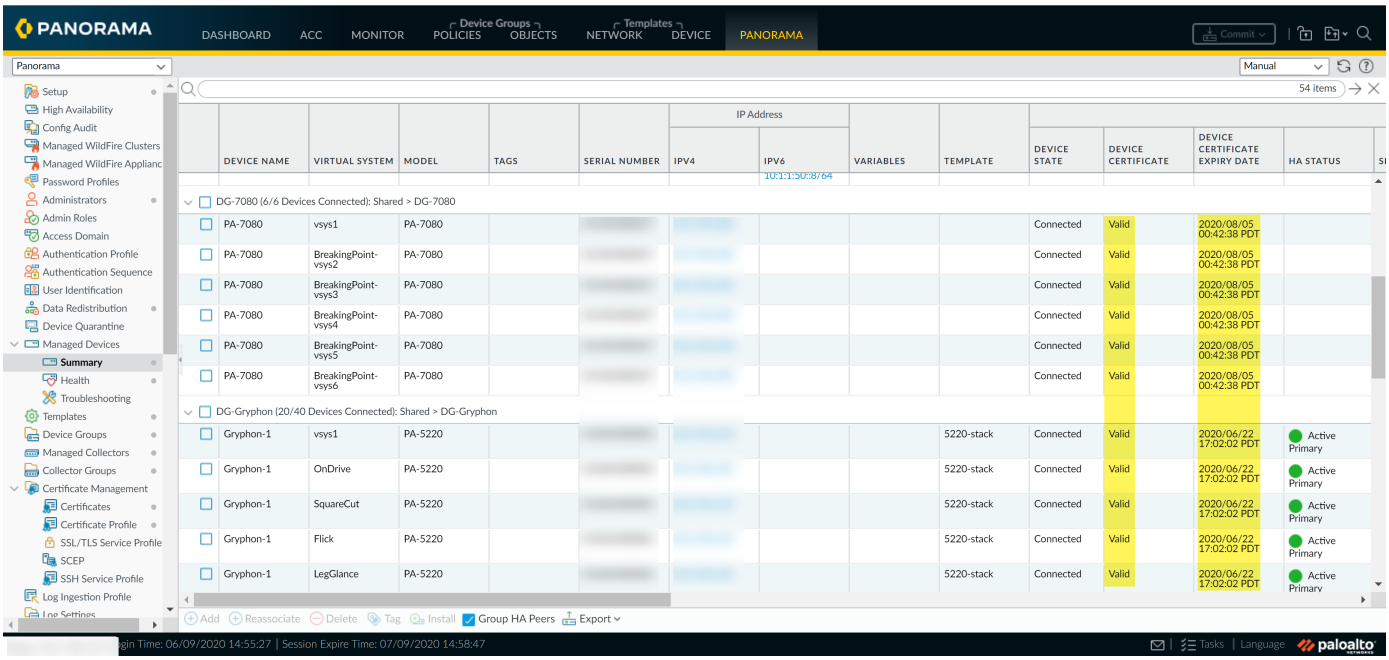
STEP 8 | Se connecter à l'interface Web Panorama en tant qu'utilisateur admin.

© 2020 Palo Alto Networks, Inc.

STEP 9 | Sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)** > **Summary (Récapitulatif)** et **Upload OTP** (Télécharger un OTP).

STEP 10 | Copiez l'OTP que vous avez généré et cliquez sur **Upload (Télécharger)**.

STEP 11 | Vérifiez que la colonne **Device Certificate (Certificat de périphérique)** indique **`Valid (Valide)`** et que la **Device Certificate Expiry Date (date d'expiration du certificat de périphérique)** indique une date d'expiration.



© 2020 Palo Alto Networks, Inc.

Configurer Zero Touch Provisioning

Configurez Zero Touch Provisioning (ZTP) pour simplifier et rationaliser les déploiements initiaux du pare-feux en automatisant l'intégration du nouveau pare-feu géré sans que les administrateurs de réseau aient besoin de l'approvisionner manuellement.

Pour bien exploiter le service ZTP, intégrez vos pare-feux ZTP avec la version PAN-OS d'usine par défaut avant de mettre à jour vers la version PAN-OS 10.0.0 ou une version ultérieure.

Le ZTP est pris en charge par la version PAN-OS 10.0.1 et toute version ultérieure.

- Présentation de ZTP
- Installation du plug-in ZTP
- Configuration du compte administrateur de l'installateur ZTP
- Importation de pare-feu ZTP sur Panorama
- Utiliser le CLI pour les tâches ZTP
- Désinstaller le plug-in ZTP

Présentation de ZTP

En savoir plus sur le plug-in ZTP (Zero Touch Provisioning) et ses éléments de configuration.

- À propos de ZTP
- Éléments de configuration de ZTP

À propos de ZTP

Le Zero Touch Provisioning (ZTP) est conçu pour simplifier et automatiser l'intégration de nouveaux pare-feux au serveur de gestion Panorama™. ZTP rationalise le processus de déploiement initial du pare-feu en permettant aux administrateurs réseau d'envoyer les pare-feux gérés directement à leurs succursales et d'ajouter automatiquement le pare-feu au serveur de gestion Panorama™ après que le pare-feu ZTP se soit connecté avec succès au service ZTP de Palo Alto Networks. Cela permet aux entreprises d'économiser du temps et des ressources lors du déploiement de nouveaux pare-feux dans les succursales en évitant aux administrateurs informatiques de devoir approvisionner manuellement le nouveau pare-feu géré. Une fois l'intégration réussie, Panorama fournit les moyens de configurer et de gérer votre configuration ZTP et vos pare-feux.

Examinez et abonnez-vous aux événements ZTP Service Status (statut de service ZTP) qui seront annoncés au sujet des fenêtres de maintenance planifiées, des coupures de service et des solutions de contournement.

ZTP est pris en charge par les pare-feux ZTP énumérés ci-dessous fonctionnant sous PAN-OS 9.1.3 et les versions ultérieures :

- PA-220-ZTP et PA-220R-ZTP
- PA-820-ZTP et PA-850-ZTP
- PA-3220-ZTP, PA-3250-ZTP, et PA-3260-ZTP

Éléments de configuration de ZTP

Les éléments suivants fonctionnent ensemble pour vous permettre d'intégrer rapidement les pare-feux ZTP nouvellement déployés en les ajoutant automatiquement au serveur de gestion Panorama en utilisant le service ZTP.

© 2020 Palo Alto Networks, Inc.

- **ZTP Plugin** : le plug-in ZTP permet à Panorama de se connecter au service ZTP et de réclamer un pare-feu ZTP pour une intégration simplifiée.
- **Customer Support Portal (Portail de support client, CSP)** : Le portail de support client de Palo Alto Networks est utilisé pour enregistrer votre Panorama afin qu'il se connecte au CSP pour enregistrer automatiquement les pare-feux ZTP nouvellement ajoutés.
- **One-Time Password (mot de passe à usage unique - OTP)** : Un mot de passe à usage unique fourni par Palo Alto Networks utilisé pour récupérer et installer un certificat sur Panorama afin qu'il communique avec le CSP et le service ZTP.
- **Programme d'installation** : Un utilisateur administrateur créé à l'aide du rôle admin `installeradmin` pour l'intégration du pare-feu ZTP. L'utilisateur admin jouit d'un accès limité à l'interface web de Panorama, ne permettant de saisir que le numéro de série du pare-feu ZTP et la clé de réclamation (Claim Key) pour enregistrer les pare-feux sur le CSP et Panorama. L'utilisateur installeradmin peut être créé sur Panorama ou en utilisant une authentification à distance comme RADIUS, SAML, ou TACACS+.
- **Claim Key (Clé de réclamation)** : Clé numérique à huit chiffres physiquement attachée au pare-feu ZTP utilisée pour enregistrer le pare-feu ZTP auprès du CSP.
- **To-SW-Version** : Désigne la version logicielle PAN-OS du pare-feu ZTP (**Panorama** > **Managed Devices (Périphériques gérés)** > **Summary (Résumé)**). Sélectionnez la version PAN-OS cible. Si le pare-feu exécute une version antérieure à la version indiquée, celui-ci démarre une boucle de mise à niveau jusqu'à ce que la version cible soit installée avec succès.



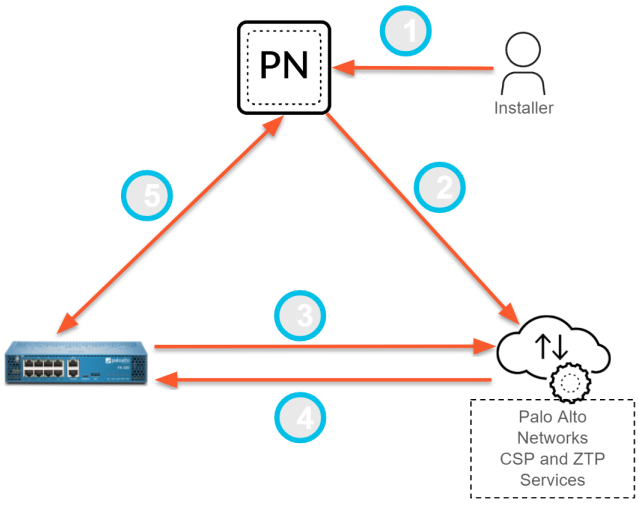
Panorama ne peut gérer que les pare-feux exécutant une version de PAN-OS égale ou inférieure à celle installée sur Panorama.

Après avoir installé le plug-in ZTP sur Panorama et inscrit Panorama au service ZTP, la procédure d'intégration ZTP continue comme suit :

1. L'installateur ou l'administrateur informatiqueenregistre les pare-feux ZTP en les ajoutant à Panorama à l'aide du numéro de série du pare-feu et de la clé de réclamation.
2. Panorama enregistre les pare-feux dans le CSP. Une fois que les pare-feux sont correctement enregistrés, le pare-feu est associé à la même instance (tenant) ZTP que le Panorama dans le service ZTP.

   Les pare-feux ZTP correctement enregistrés dans le service ZTP sont automatiquement enregistrés en tant que pare-feux gérés (**Panorama** > **Managed Devices (Périphériques gérés par Panorama)**) dans Panorama.
3. Lorsque le pare-feu se connecte à Internet, le pare-feu ZTP demande un certificat de périphérique (device certificate) au CSP afin de se connecter au service ZTP.
4. Le service ZTP envoie l'IP de Panorama ou le FQDN vers les pare-feux ZTP.
5. Les pare-feux ZTP se connectent à Panorama et les configurations de groupe de périphériques (device-group) ainsi de modèle (template) sont envoyées depuis Panorama vers les pare-feux ZTP.

© 2020 Palo Alto Networks, Inc.



Installation du plug-in ZTP

Installez le plug-in ZTP sur votre serveur de gestion Panorama™ pour enregistrer Panorama auprès du service ZTP afin de déclarer des pare-feux ZTP pour une intégration simplifiée.

Si votre Panorama est dans une configuration haute disponibilité (HA), installez le plug-in ZTP et enregistrez les deux homologues HA de Panorama au service ZTP.

- Installation du plug-in ZTP sur Panorama
- Enregistrer Panorama auprès du service ZTP

Installation du plug-in ZTP sur Panorama

Simplifiez l'intégration et la gestion des pare-feux ZTP en installant le plug-in ZTP sur votre serveur de gestion Panorama.

STEP 1 | Installation du certificat du périphérique Panorama.

STEP 2 | Connectez vous à l'interface web de Panorama en tant que super-utilisateur ou administrateur Panorama ayant accès aux plug-ins Panorama (**Panorama** > **Plugins (Plug-ins)**).

STEP 3 | Sélectionnez **Panorama** > **Plugins (Plug-ins)**, puis cherchez le plug-in `ztp`.

STEP 4 | **Téléchargez** et **installez** la version la plus récente du plug-in ZTP.

Enregistrer Panorama auprès du service ZTP

Enregistrer le serveur de gestion Panorama™ auprès du service ZTP pour les nouveaux déploiements ZTP et ceux existants.

- Enregistrer Panorama auprès du service ZTP pour les nouveaux déploiements
- Enregistrer Panorama auprès du service ZTP pour les déploiements existants

Enregistrer Panorama auprès du service ZTP pour les nouveaux déploiements

Après avoir installé le plug-in ZTP sur le serveur de gestion Panorama™, vous devez enregistrer le Panorama auprès du service ZTP pour permettre au service ZTP d'y associer des pare-feux. Dans le cadre du processus d'enregistrement pour un nouveau déploiement ZTP, générez automatiquement les configurations des groupes d'appareils et des modèles nécessaires pour connecter vos pare-feux ZTP au service ZTP. Une fois que le groupe d'appareils et le modèle sont générés automatiquement, vous devez

© 2020 Palo Alto Networks, Inc.

ajouter vos pare-feux ZTP au groupe d'appareils et au modèle afin qu'ils puissent se connecter au service ZTP après leur première connexion à Panorama.

STEP 1 | Installation du certificat du périphérique Panorama.

STEP 2 | Connectez-vous au Customer Support Portal (Portail Support Client) de Palo Alto Networks.

STEP 3 | Associez votre Panorama au service ZTP sur le CSP de Palo Alto Networks.

Le service ZTP permet d'associer jusqu'à deux Panoramas uniquement s'ils sont dans une configuration High Availability (haute disponibilité - HA). Si Panorama n'est pas dans une configuration HA, un seul Panorama peut être associé.

1. Sélectionnez **Assets (Ressources)** > **ZTP Service (Service ZTP)** et **Associate Panorama(s) (Associer Panorama(s))**.
2. Sélectionnez le numéro de série de Panorama qui gère vos pare-feux ZTP.
3. (HA uniquement) Sélectionnez le numéro de série de l'homologue HA Panorama.
4. Cliquez sur **OK**.

STEP 4 | Se connecter à l'interface Web Panorama.

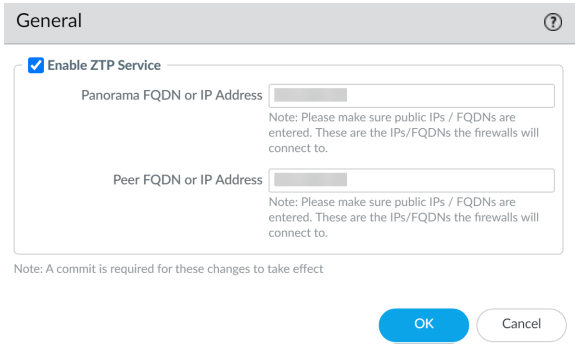
STEP 5 | Sélectionnez **Panorama** > **Zero Touch Provisioning** > **Setup (Configuration)** et modifiez les paramètres **General (Généraux)** ZTP.

STEP 6 | Enregistrez Panorama auprès du service ZTP.

1. **Activez le service ZTP**.
2. Saisissez **le FQDN ou l'adresse IP** Panorama.

   Il s'agit du FQDN ou de l'adresse IP publique de Panorama sur lequel le plug-in ZTP est installé vers lequel le CSP envoie les pare-feux ZTP.
3. (HA uniquement) Saisissez **le FQDN homologue ou l'adresse IP**.

   Il s'agit du FQDN ou de l'adresse IP publique de l'homologue Panorama sur lequel le plug-in ZTP est installé vers lequel le CSP envoie les pare-feux ZTP en cas de basculement.
4. Cliquez sur **OK** pour enregistrer les modifications de votre configuration.



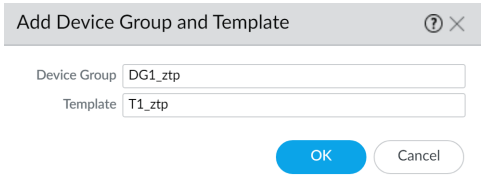
STEP 7 | Créez le groupe d'appareils et le modèle par défaut afin de générer automatiquement la configuration requise pour connecter vos pare-feux ZTP à Panorama.

L'ajout du groupe d'appareils et du modèle génère automatiquement un nouveau groupe d'appareils et un modèle qui contiennent la configuration par défaut pour connecter Panorama et les pare-feux ZTP.

1. **Ajoutez le groupe d'appareils et le modèle**.
2. Saisissez le nom du **Device Group (Groupe d'appareils)**.
3. Saisissez le nom du **Template (Modèle)**.

© 2020 Palo Alto Networks, Inc.

4. Cliquez sur **OK** pour enregistrer les modifications de votre configuration.



STEP 8 | Ajoutez vos pare-feux ZTP au groupe d'appareils et au modèle spécifiés à l'étape précédente.

1. Sélectionnez **Panorama** > **Device Groups (Groupes d'appareils)** et sélectionnez le groupe d'appareils qui a été créé automatiquement.
2. Sélectionnez les **Devices (Périphériques)** ZTP.
3. Cliquez sur **OK** pour enregistrer les modifications de votre configuration.
4. Sélectionnez **Panorama** > **Templates (Modèles)** et cliquez sur **Add Stack (Ajouter une pile)**.
5. Dans la section **Templates (Modèles)**, **ajoutez** le modèle qui a été généré automatiquement.
6. Sélectionnez les **Devices (Périphériques)** ZTP.
7. Cliquez sur **OK** pour enregistrer les modifications de votre configuration.

STEP 9 | Vérifiez que les configurations des groupes d'appareils et les modèles requis ont été générées avec succès.

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet** puis sélectionnez le **Template (Modèle)** que vous avez créé à l'étape précédente.
2. Vérifiez que `ethernet1/1` est configuré avec une adresse IP, un routeur virtuel et une zone de sécurité.
3. Sélectionnez **Network (Réseau)** > **Interfaces** > **Loopback** puis sélectionnez le **Template (Modèle)** que vous avez créé à l'étape précédente.
4. Vérifiez que l'interface `loopback.900` a été correctement créée.
5. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** > **Pre Rules (Règles avant)** et sélectionnez le **Device Group (Groupe d'appareils)** que vous avez créé à l'étape précédente.
6. Vérifiez que la `règle1` a été correctement créée.
7. Sélectionnez **Policies (Politiques)** > **NAT** > **Pre Rules (Règles avant)** et sélectionnez le **Device Group (Groupe d'appareils)** que vous avez créé à l'étape précédente.
8. Vérifiez que `ztp-nat` a été correctement créé.

STEP 10 | Modifiez vos groupes d'appareils et vos modèles selon vos besoins.

Créez et configurez des groupes d'appareils et des modèles nouveaux ou existants pour compléter votre déploiement.

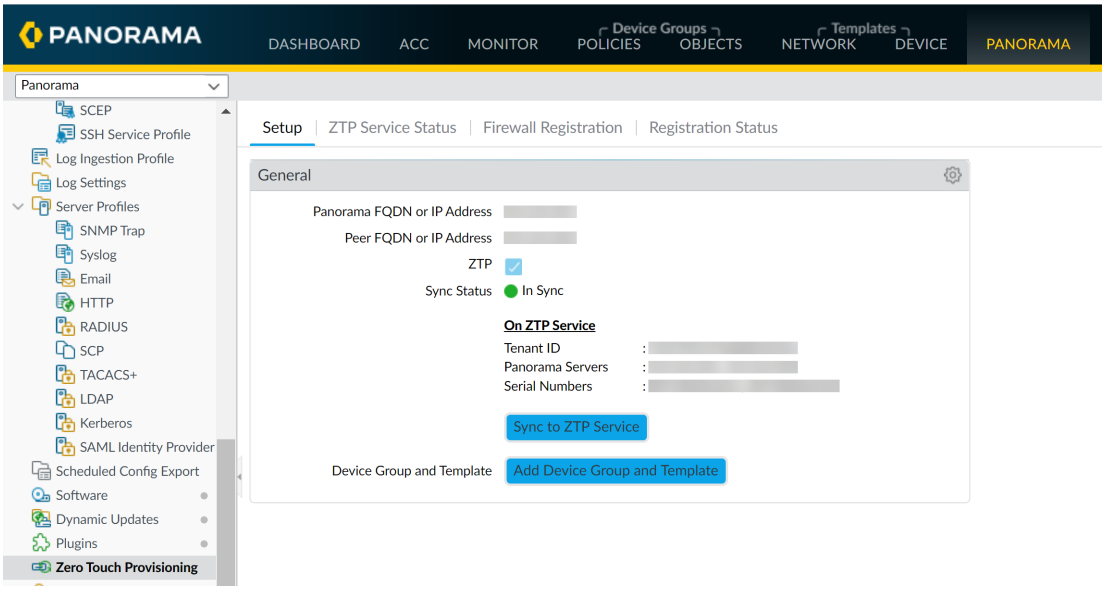
Lorsque vous examinez la hiérarchie des groupes d'appareils et la priorité des modèles dans votre pile de modèles, assurez-vous que le groupe d'appareils et le modèle contenant la configuration ZTP requise qui permet au pare-feux ZTP et à Panorama de communiquer ont la priorité de sorte que la configuration ne soit pas annulée en cas de conflit de configurations.

Ne modifiez pas l'adresse IP, le routeur virtuel et la zone de sécurité de l'interface `ethernet1/1`, de l'interface `loopback.900`, de la `règle1` de la politique de sécurité ou de la règle de la politique NAT `ztp-nat`. Ces configurations sont nécessaires pour connecter votre pare-feu ZTP à Panorama.

STEP 11 | Sélectionnez **Commit (Valider)** et **Commit to Panorama (Validez sur Panorama)**.

STEP 12 | **Synchronisez avec le service ZTP** et vérifiez que l'état de la synchronisation de Panorama s'affiche comme **`In Sync`**.

© 2020 Palo Alto Networks, Inc.



Enregistrer Panorama auprès du service ZTP pour les déploiements existants

Après avoir installé le plug-in ZTP sur le serveur de gestion Panorama™, vous devez enregistrer Panorama auprès du service ZTP pour permettre au service ZTP d'y associer des pare-feux. Dans le cadre de la procédure d'enregistrement, ajoutez vos pare-feux ZTP à un groupe d'appareils et à un modèle qui contiennent la configuration ZTP requise pour connecter vos pare-feux ZTP au service ZTP après leur première connexion à Panorama.

STEP 1 | Installation du certificat du périphérique Panorama.

STEP 2 | Connectez-vous au Customer Support Portal (Portail Support Client) de Palo Alto Networks.

STEP 3 | Associez votre Panorama au service ZTP sur le CSP de Palo Alto Networks.

Le service ZTP permet d'associer jusqu'à deux Panoramas uniquement s'ils sont dans une configuration High Availability (haute disponibilité - HA). Si Panorama n'est pas dans une configuration HA, un seul Panorama peut être associé.

1. Sélectionnez **Assets (Ressources)** > **ZTP Service (Service ZTP)** et **Modify Association (Modifier une association)**.
2. Sélectionnez le numéro de série de Panorama qui gère vos pare-feux ZTP.
3. (HA uniquement) Sélectionnez le numéro de série de l'homologue HA Panorama.
4. Cliquez sur **OK**.

STEP 4 | Se connecter à l'interface Web Panorama.

STEP 5 | Sélectionnez **Panorama** > **Zero Touch Provisioning** > **Setup (Configuration)** et modifiez les paramètres **General (Généraux)** ZTP.

STEP 6 | Enregistrez Panorama auprès du service ZTP.

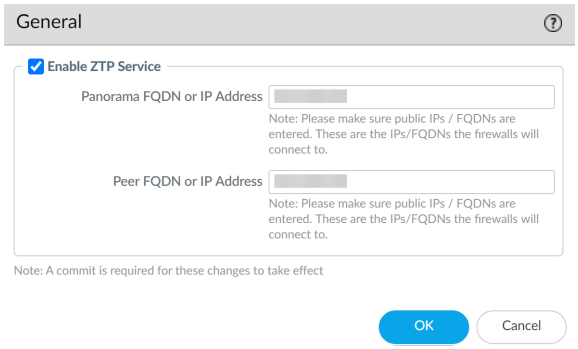
1. **Activez le service ZTP**.
2. Saisissez **le FQDN ou l'adresse IP** Panorama.

   Il s'agit du FQDN ou de l'adresse IP publique de Panorama sur lequel le plug-in ZTP est installé et vers lequel le CSP envoie les pare-feux ZTP.
3. (HA uniquement) Saisissez **le FQDN homologue ou l'adresse IP**.

© 2020 Palo Alto Networks, Inc.

Il s'agit du FQDN ou de l'adresse IP publique de l'homologue Panorama sur lequel le plug-in ZTP est installé vers lequel le CSP envoie les pare-feux ZTP en cas de basculement.

4. Cliquez sur **OK** pour enregistrer les modifications de votre configuration.



STEP 7 | Ajoutez vos pare-feux ZTP au groupe d'appareils et au modèle qui contiendra la configuration ZTP requise.

1. Sélectionnez **Panorama** > **Device Groups (Groupes de Périphériques)** et sélectionnez le groupe d'appareils qui contiendra la configuration ZTP requise.
2. Sélectionnez les **Devices (Périphériques)** ZTP.
3. Cliquez sur **OK** pour enregistrer les modifications de votre configuration.
4. Sélectionnez **Panorama** > **Templates (Modèles)** et choisissez la pile de modèles qui contient le modèle qui aura la configuration ZTP requise.
5. Sélectionnez les **Devices (Périphériques)** ZTP.
6. Cliquez sur **OK** pour enregistrer les modifications de votre configuration.

STEP 8 | Modifiez vos groupes d'appareils et vos modèles selon vos besoins.

Lorsque vous examinez la hiérarchie des groupes d'appareils et la priorité des modèles dans votre pile de modèles, assurez-vous que le groupe d'appareils et le modèle contenant la configuration ZTP requise qui permet au pare-feux ZTP et à Panorama de communiquer ont la priorité de sorte que la configuration ne soit pas annulée en cas de conflit de configurations.

1. Configurez l'interface Ethernet1/1.
   1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**, sélectionnez un **Template (Modèle)** pour contenir votre configuration ZTP puis sélectionnez **ethernet1/1**.
   2. Sous **Interface Type (Type d'interface)**, sélectionnez **Layer3 (Couche 3)**.
   3. Sélectionnez **Config (Configurer)** et configurez un**Virtual Router (routeur virtuel - VR)** et paramétrez **Security Zone (Zone de sécurité)** sur **Untrust (Non approuvée)**.
   4. Sélectionnez **IPv4** et pour le **Type**, sélectionnez**DHCP Client (client DHCP)**.

      Un client DHCP est nécessaire pour que les pare-feux ZTP puissent communiquer avec le service ZTP.
   5. Cliquez sur **OK** pour enregistrer votre configuration.
2. Créez l'interface en boucle
   1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Loopback (En boucle)**, sélectionnez un **Template (Modèle)** pour contenir votre configuration ZTP et **ajoutez** une interface en boucle.
   2. Pour le **Interface Name (Nom de l'interface)**, saisissez **`loopback (En boucle)`** puis saisissez le suffixe **`900`**.
   3. Sélectionnez **Config (Configurer)** puis **Virtual Router (routeur virtuel - VR)** et paramétrez **Security Zone (Zone de sécurité)** sur **Trust (Approuvée)**.

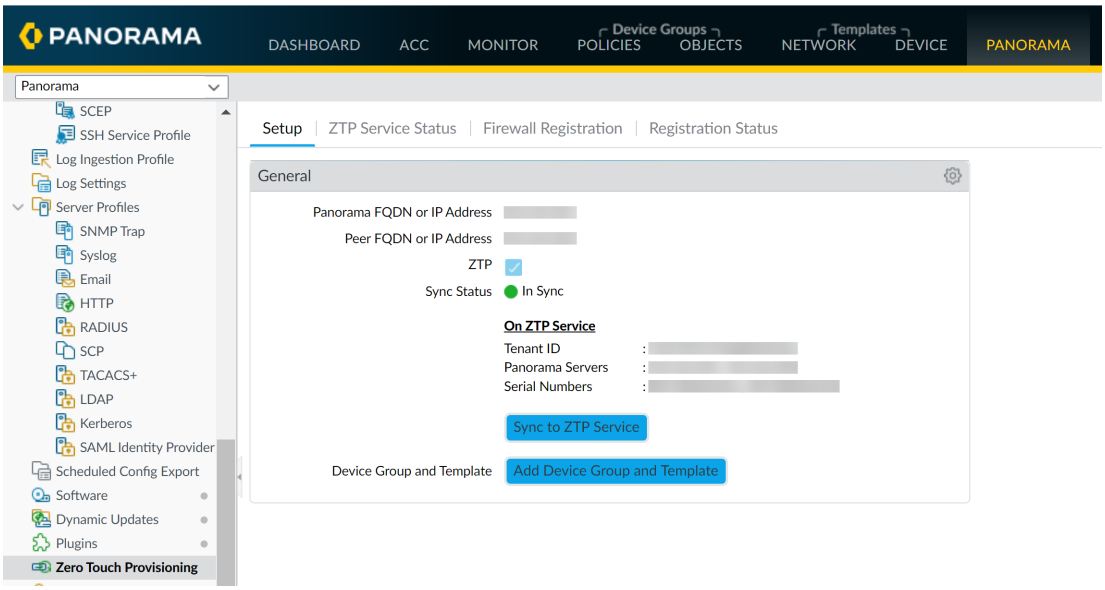
© 2020 Palo Alto Networks, Inc.

4. Cliquez sur **OK** pour enregistrer votre configuration.

3. Créez la règle de politique de sécurité pour permettre au pare-feux ZTP et à Panorama de communiquer.
   1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** > **Pre Rules (Règles avant)**, sélectionnez le **Device Group (Groupe d'appareils)** contenant vos règles de politique ZTP, et **ajoutez** une nouvelle règle.
   2. Saisissez un **Name (Nom)** descriptif pour la règle de politique.
   3. Sélectionnez **Source** > **Source Zone (Zone source)** et **ajoutez** la zone**Trust (Approuvée)**.
   4. Sélectionnez **Destination** > **Destination Zone (Zone de Destination)** et **ajoutez** la zone **Untrust (Non approuvée)**.
   5. Sélectionnez **Action** > **Action Settings (Paramètres des actions)** > **Action** puis sélectionnez **Allow (Autoriser)**.
4. Créez la règle de politique NAT pour permettre au pare-feu ZTP et à Panorama de communiquer.
   1. Sélectionnez **Policies (Politiques)** > **NAT** > **Pre Rules (Règles avant)**, sélectionnez le **Device Group (Groupe d'appareils)** contenant vos règles de politique ZTP, et **ajoutez** une nouvelle règle.
   2. Saisissez un **Name (Nom)** descriptif pour la règle de politique.
   3. Sélectionnez **Original Packet (Paquet d'origine)** et configurez ce qui suit :
      1. Pour la **Source Zone (Zone source)**, **ajoutez** la zone **Trust (Approuvée)**.
      2. Pour la **Destination Zone (Zone de destination)**, sélectionnez la zone **Untrust (Non approuvée)**.
      3. Pour **Destination Interface (Interface de destination)**, sélectionnez l'interface **ethernet1/1**.
   4. Cliquez sur **OK** pour enregistrer les modifications de votre configuration.

STEP 9 | Sélectionnez **Commit (Valider)** et **Commit to Panorama (Validez sur Panorama)**.

STEP 10 | **Synchronisez avec le service ZTP** et vérifiez que l'état de la synchronisation de Panorama s'affiche comme **`In Sync`**.



Configuration du compte administrateur de l'installateur ZTP

L'utilisateur admin de l'installateur ZTP est un compte d'administrateur créé pour le personnel non informatique ou le fournisseur d'installation pour intégrer les nouveaux pare-feux ZTP. L'admin de l'installateur utilise un rôle admin `installeradmin` créé automatiquement pour limiter la visibilité dans

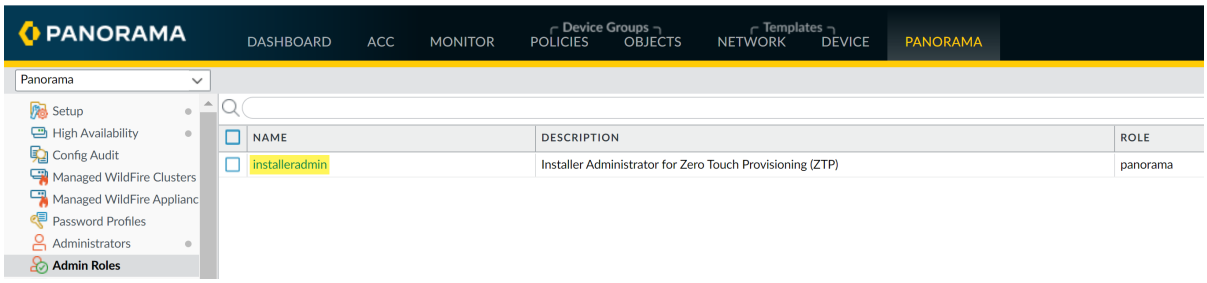
© 2020 Palo Alto Networks, Inc.

l'interface web de Panorama et ne permettre à l'installateur que la possibilité d'entrer la clé de réclamation du pare-feu ZTP et le numéro de série sur Panorama.

STEP 1 | Se connecter à l'interface Web Panorama.

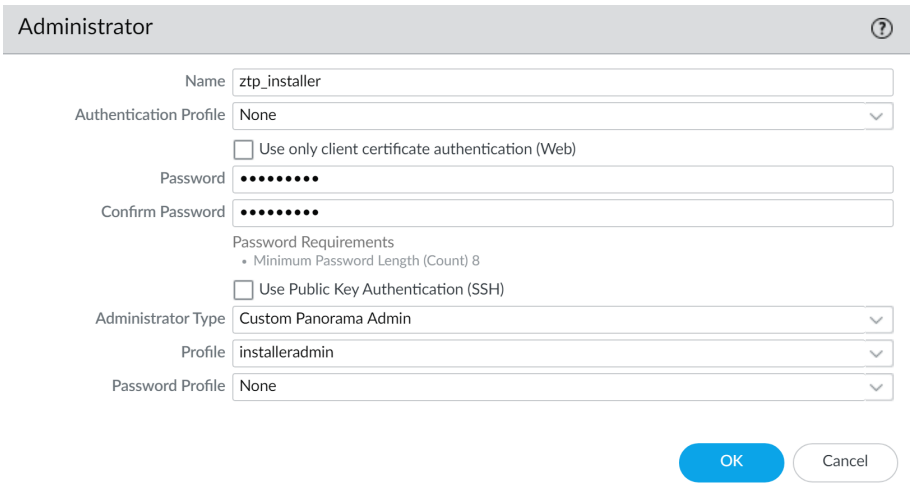
STEP 2 | Sélectionnez **Panorama** > **Admin Roles (Rôle admin)**et vérifiez que le rôle admin **`installeradmin`** est créé.

`installeradmin` est automatiquement créé après que vous ayez installé avec succès le plug-in ZTP sur Panorama.



STEP 3 | Configuration de l'utilisateur administrateur de l'installateur ZTP.

1. Sélectionnez **Panorama** > **Administrators (Administrateurs)** et **Add (Ajoutez)** un nouvel utilisateur admin.
2. Saisissez un **Name (Nom)** descriptif pour l'utilisateur admin de l'installateur ZTP.
3. Saisissez un **Password (Mot de passe)** sécurisé et **Confirm Password (Confirmez le mot de passe)**.
4. Pour le **Administrator Type (Type d'administrateur)**, sélectionnez **Custom Panorama Admin (Admin Panorama personnalisé)**.
5. Pour le **Profile (Profil)**, sélectionnez **installeradmin**
6. Cliquez sur **OK** pour enregistrer votre configuration.



STEP 4 | Sélectionnez **Commit (Valider)** et **Commit to Panorama (Validez sur Panorama)**.

Importation de pare-feu ZTP sur Panorama

Vous pouvez ajouter un seul pare-feu ZTP ou importer plusieurs pare-feux ZTP sur le serveur de gestion Panorama™.

- Ajoutez pare-feu ZTP à Panorama

© 2020 Palo Alto Networks, Inc.

- Importation de plusieurs pare-feu ZTP à Panorama

Ajoutez pare-feu ZTP à Panorama

Connectez-vous à l'interface web du serveur de gestion Panorama™ en tant que super-utilisateur, administrateur de Panorama ou administrateur de l'installateur ZTP pour ajouter un pare-feu ZTP à Panorama. Pour ajouter un pare-feu ZTP, vous devez saisir le numéro de série du pare-feu ZTP et la clé de réclamation fournis par Palo Alto Networks, puis enregistrer les pare-feux auprès du service ZTP. L'enregistrement du pare-feu revendique les pare-feux en tant que ressource dans votre compte dans le portail de support client et permet au service ZTP d'associer le pare-feu avec Panorama.

Lorsque vous ajoutez des pare-feux ZTP à Panorama, n'effectuez aucune validation sur le pare-feu ZTP avant d'avoir vérifié que le pare-feu est correctement ajouté à Panorama lors de l'Étape 4. Procéder à une validation locale sur le pare-feu ZTP désactive la fonctionnalité ZTP et a pour conséquence l'échec de l'ajout du pare-feu à Panorama.

STEP 1 | Se connecter à l'interface Web Panorama.

STEP 2 | Ajouter un pare-feu ZTP à Panorama.

Vous devez connecter l'interface Eth1/1 sur les pare-feux ZTP afin de correctement enregistrer les pare-feux ZTP dans le CSP et d'appliquer la politique et les configurations de réseau.

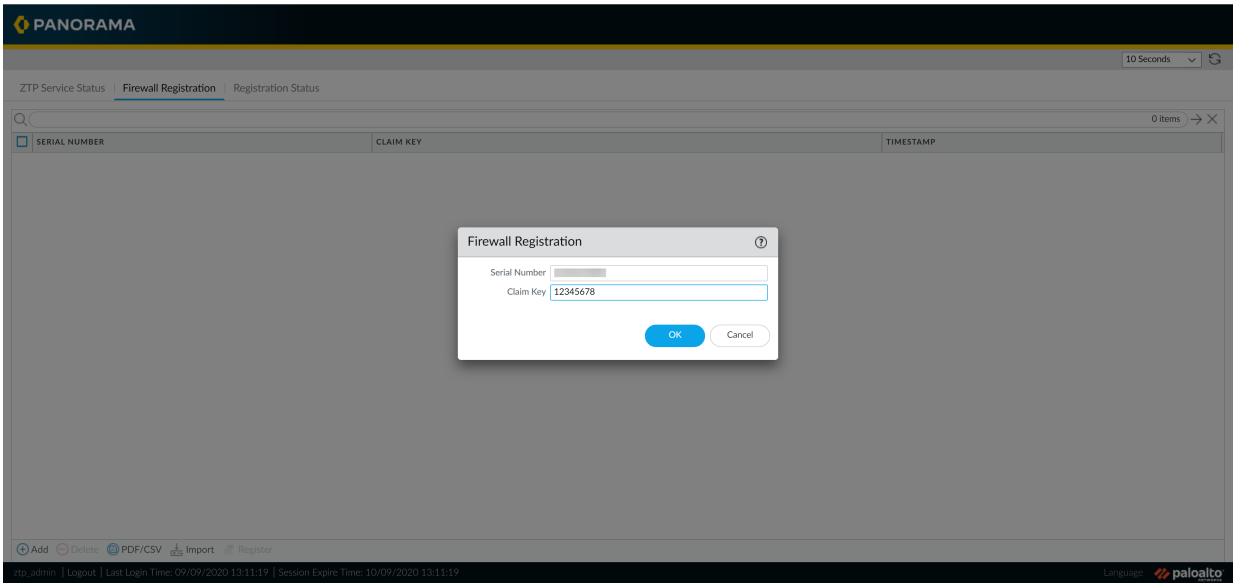
1. Sélectionnez **Firewall Registration (Enregistrement du pare-feu)** et **Add (Ajoutez)** un nouveau pare-feu ZTP.
2. Saisissez le **Serial Number (Numéro de série)** du pare-feu ZTP.
3. Saisissez la **Claim Key (Clé de réclamation)** pour le pare-feu ZTP fournie par Palo Alto Networks.

   La clé de réclamation numérique à huit chiffres est imprimée sur une étiquette physique fixée au dos du pare-feu ZTP que vous avez reçu de Palo Alto Networks.



4. Cliquez sur **OK** pour enregistrer votre configuration.

© 2020 Palo Alto Networks, Inc.



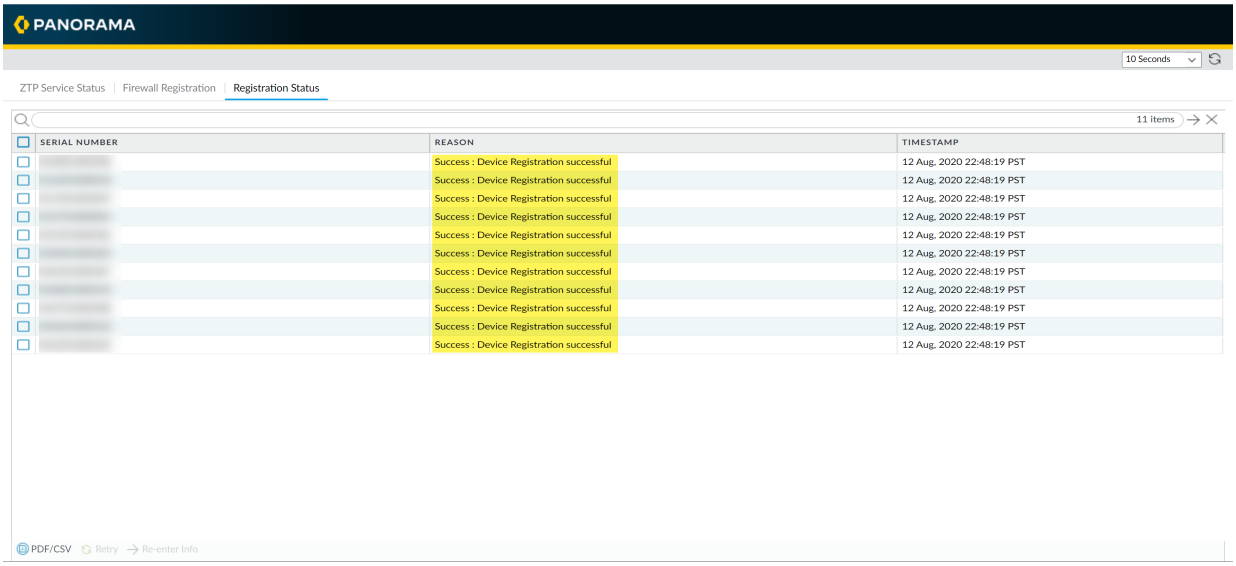
STEP 3 | Enregistrez le pare-feu ZTP.

1. Sélectionnez le pare-feu ZTP nouvellement ajouté et **Register (Enregistrez)** le pare-feu.
2. Lorsque vous y êtes invité, cliquez sur **Yes (Oui)** pour confirmer l'enregistrement du pare-feu ZTP.

STEP 4 | Vérifiez que le pare-feu est bien enregistré auprès du CSP.

Le pare-feu doit être bien enregistré auprès du CSP afin d'obtenir un certificat de périphérique.

1. Sélectionnez **Registration Status (Statut d'enregistrement)** et vérifiez que le pare-feu ZTP s'est enregistré avec succès auprès du CSP.



2. Se connecter à l'interface Web Panorama utilisant les identifiants admin.
3. Sélectionnez **Panorama** > **Managed Devices (Appareils gérés)** > **Summary (Résumés)** et vérifiez que le pare-feu ZTP est ajouté avec succès en tant que pare-feu géré.

© 2020 Palo Alto Networks, Inc.

Assurez-vous que la colonne To SW Version est configurée pour la bonne version de PAN-OS afin que le pare-feu ne se mette pas à niveau ou ne se downgrade pas involontairement. La fonctionnalité ZTP n'est prise en charge que pour PAN-OS 10.0.1 et les versions ultérieures. Par ailleurs, la version PAN-OS doit être la même ou une version antérieure de la version PAN-OS fonctionnant sur Panorama.

Pour plus d'informations, reportez-vous à la section Mettre à niveau un pare-feu ZTP*.*

STEP 5 | Ajoutez le pare-feu ZTP à un groupe de périphériques et à une pile de modèles.

Vous devez ajouter le pare-feu ZTP à un groupe de périphériques et à une pile de modèles pour que vos pare-feux apparaissent avec l'indication `Connected (Connecté)` pour appliquer les politiques et les configurations réseau.

1. Se connecter à l'interface Web Panorama utilisant les identifiants admin.
2. Sélectionnez **Panorama** > **Device Groups (Groupes de périphériques)**, add a device group (ajouter un groupe de périphériques), et le pare-feu ZTP vers le groupe de périphériques.

   Add a device group (Ajoutez un groupe de périphériques) pour créer et configurer un nouveau groupe de périphériques contenant les objets et les règles de politique pour vos pare-feux ZTP.
3. Sélectionnez**Panorama** > **Templates (Modèles)**, configure a template stack (configurez une pile de modèles), et le pare-feu ZTP vers la pile de modèles.

   Configure a template stack (Configurez une pile de modèles) pour créer et configurer une nouvelle pile de modèles contenant la configuration réseau pour vos pare-feux ZTP.

Importation de plusieurs pare-feu ZTP à Panorama

Connectez-vous à l'interface web du serveur de gestion Panorama™ en tant que super-utilisateur, administrateur de Panorama ou administrateur de l'installateur ZTP pour importer plusieurs pare-feux ZTP dans Panorama. Pour importer plusieurs pare-feux ZTP, vous devez importer un fichier CSV du numéro de série du pare-feu ZTP et la clé de réclamation correspondante fournis par Palo Alto Networks, puis enregistrer les pare-feux auprès du service ZTP. L'enregistrement du pare-feu revendique les pare-feux en tant qu'actifs dans votre compte dans le portail de support client et permet au service ZTP d'associer les pare-feux avec Panorama.

Lorsque vous ajoutez des pare-feux ZTP à Panorama, n'effectuez aucune validation (commit) sur le pare-feu ZTP avant d'avoir vérifié que le pare-feu est correctement ajouté à Panorama lors de l'étape 5. Procéder à une validation locale sur le pare-feu ZTP désactive la fonctionnalité ZTP et a pour conséquence l'échec de l'ajout du pare-feu à Panorama.

STEP 1 | Rassemblez les numéros de série et les clés de réclamation pour vos pare-feux ZTP.

La clé de réclamation numérique à huit chiffres est imprimée sur une étiquette physique fixée au dos du pare-feu ZTP que vous avez reçu de Palo Alto Networks.



STEP 2 | Créez un fichier CSV contenant les numéros de série et les clés de réclamation du pare-feu ZTP. La première colonne doit contenir les numéros de série et la deuxième colonne doit

© 2020 Palo Alto Networks, Inc.

contenir la clé de réclamation correspondante pour ce pare-feu. Reportez-vous à l'exemple ci-dessous pour référence.

	A	B
1	Serial Number	Claim Key
2	abcd1234	123456789
3	xyz7890	987654321

STEP 3 | Importez les pare-feux ZTP dans Panorama.

Vous devez connecter l'interface Eth1/1 sur les pare-feux ZTP afin de correctement enregistrer les pare-feux ZTP dans le CSP (compte support) et d'appliquer la politique et les configurations de réseau.

1. Se connecter à l'interface Web Panorama en utilisant les identifiants admin de l'installateur ZTP.
2. Sélectionnez **Panorama** > **Zero Touch Provisioning** > **Firewall Registration (Enregistrement du pare-feu)** et **Import (Importez)** les pare-feu ZTP.
3. **Browse (Parcourez)** et sélectionnez le fichier CSV contenant les informations sur le pare-feu ZTP puis cliquez sur **OK**.

STEP 4 | Enregistrez les pare-feux ZTP.

1. Sélectionnez les pare-feu ZTP nouvellement ajoutés et **Register (Enregistrez)** les pare-feux.
2. Lorsque vous y êtes invité, cliquez sur **Yes (Oui)** pour confirmer l'enregistrement des pare-feux ZTP.

STEP 5 | Vérifiez que le pare-feu est bien enregistré auprès du service ZTP.

1. Sélectionnez **Registration Status (Statut d'enregistrement)** et vérifiez que les pare-feux ZTP se sont enregistrés avec succès auprès du service ZTP.
2. Se connecter à l'interface Web Panorama utilisant les identifiants admin.
3. Sélectionnez **Panorama** > **Managed Devices (Appareils gérés)** > **Summary (Résumés)** et vérifiez que les pare-feux ZTP sont ajoutés avec succès en tant que pare-feu géré.

Assurez-vous que la colonne To SW Version est configurée pour la bonne version de PAN-OS afin que le pare-feu ne se mette pas à niveau ou ne se downgrade pas involontairement. La fonctionnalité ZTP n'est prise en charge que pour PAN-OS 10.0.1 et les versions ultérieures. Par ailleurs, la version PAN-OS doit être la même ou une version antérieure de la version PAN-OS fonctionnant sur Panorama.

Pour plus d'informations, reportez-vous à la section Mettre à niveau un pare-feu ZTP*.*

STEP 6 | Ajoutez les pare-feu ZTP à un groupe de périphériques et à une pile de modèles.

Vous devez ajouter le pare-feu ZTP à un groupe de périphériques et à une pile de modèles pour que vos pare-feux apparaissent avec l'indication `Connected (Connecté)` pour appliquer les politiques et les configurations réseau.

1. Se connecter à l'interface Web Panorama utilisant les identifiants admin.
2. Sélectionnez **Panorama** > **Device Groups (Groupes d'appareils)** et affectez les pare-feux au groupe de périphériques approprié.

   Add a device group (Ajoutez un groupe de périphériques) pour créer et configurer un nouveau groupe de périphériques contenant les objets et les règles de politique pour vos pare-feux ZTP.
3. Sélectionnez **Panorama** > **Templates (Modèles)** et affectez les pare-feux à la pile de modèles appropriée.

© 2020 Palo Alto Networks, Inc.

Configure a template stack (Configurez une pile de modèles) pour créer et configurer une nouvelle pile de modèles contenant la configuration réseau pour vos pare-feux ZTP.

Utiliser le CLI pour les tâches ZTP

Utilisez les commandes CLI suivantes pour effectuer des tâches ZTP (Zero Touch Provisioning) et consulter l'état du service ZTP.

Si vous souhaitez...	Utilisez ...
Administrer le pare-feu depuis le CLI du pare-feu	
Afficher le statut de connexion au service ZTP.	`> show system ZTP status`
Afficher le statut de connexion au serveur de gestion Panorama.	`> show panorama status`
Afficher le numéro du modèle ZTP et les informations du système de pare-feu.	`> show system info`
Désactiver la machine de statut ZTP sur le pare-feu. Lancer cette commande ne supprime aucune configuration ZTP existante. *Vous ne pouvez pas réactiver la machine de statut ZTP sur le pare-feu après l'avoir désactivée sur le CLI.* *Pour la réactiver, vous devez alors rétablir les paramètres d'usine du pare-feu.*	`> request disable ztp`
Enregistrer, configurer et gérer vos pare-feux ZTP depuis Panorama	
Créer un groupe de périphériques ou un modèle contenant les configurations nécessaires pour connecter les pare-feux gérés avec Panorama en utilisant le service ZTP sur l'interface Eth1/1.	`> request plugins ztp create dgroup-template device-group <device group name>` `> request plugins ztp create dgroup-template template <template name>`

© 2020 Palo Alto Networks, Inc.

Si vous souhaitez...	Utilisez ...
Ajouter un pare-feu ZTP à la liste des pare-feux en vue d'un enregistrement futur auprès du service ZTP.	`> request plugins ztp firewall-add <serial number> claim-key <claim key>`
Modifier le numéro de série d'un pare-feu ZTP qui a déjà été ajouté à la liste des pare-feux pour un enregistrement futur avec le service ZTP.	`> request plugins ztp firewall-add-modify firewall <old serial number> claim-key <claim key> new-serial <new serial number>`
Supprimer un pare-feu ZTP de la liste des pare-feux en vue d'un enregistrement futur auprès du service ZTP.	`> request plugins ztp firewall-delete firewall <serial number>`
Ajouter un pare-feu ZTP à la liste des pare-feux en vue d'un nouvel enregistrement auprès du service ZTP. Utiliser cette commande lorsqu'un pare-feu ZTP échoue initialement l'enregistrement avec le service ZTP et le nécessite.	`> request plugins ztp firewall-re-enter-info firewall <serial number> claim-key <claim key>`
Enregistrer votre serveur de gestion Panorama™ avec le service ZTP.	`> request plugins ztp panorama-registration`
Enregistrer un pare-feu ZTP auprès du service ZTP.	`> request plugins ztp firewall-registration firewall <serial number> claim-key <claim key>`
Enregistrer à nouveau des pare-feux ZTP auprès du service ZTP. Utiliser cette commande pour lancer le processus de réenregistrement pour un pare-feu ZTP qui a échoué lors de l'enregistrement initial avec le service ZTP.	`> request plugins ztp firewall-register-retry firewall <serial number> claim-key <claim key>`
Importer le numéro de série du pare-feu ZTP et réclamer les informations sur la clé. Le fichier spécifié doit être au format CSV.	`> request plugins ztp ztp-add-import import-path <file path>`
Consulter les informations sur le pare-feu ZTP et l'état du service ZTP depuis Panorama	
Retrouvez la liste des pare-feux ZTP enregistrés dans Panorama à partir du service ZTP.	`> request plugins ztp ztp-service-info`

© 2020 Palo Alto Networks, Inc.

Si vous souhaitez...	Utilisez ...
	Les détails suivants s'affichent : • `first-firewall-connect-time` : Horodatage de la date à laquelle le pare-feu ZTP s'est connecté pour la première fois au service ZTP. • `last-firewall-connect-time` : Horodatage de la date de la dernière connexion du pare-feu ZTP au service ZTP. • `registration-time` : Horodatage du moment où le pare-feu ZTP s'est enregistré auprès du service ZTP. • `isZTPFirewall` : Si le pare-feu est un pare-feu ZTP. • `created_by` : Utilisateur administratif qui a ajouté le pare-feu ZTP. • `Adresse IP` : L'adresse IP du pare-feu ZTP.
Consulter la liste des pare-feux ZTP dans la liste des pare-feux à enregistrer auprès du service ZTP.	`> show plugins ztp device-add-list`
Consulter l'état d'enregistrement de vos pare-feux ZTP.	`> show plugins ztp device-reg-status`
Consulter l'état de synchronisation du service ZTP pour les pare-feux ZTP.	`> request plugins ztp ztp-sync-status`
Afficher la totalité du plan de gestion de l'historique de connectivité ZTP. Cela sert à régler les problèmes de connectivité au service ZTP.	`> tail follow yes mp-log ms.log`

Désinstaller le plug-in ZTP

Suivez la procédure pour supprimer la configuration ZTp de votre serveur de gestion Panorama™ et désinstallez le plug-in ZTP. Si votre Panorama est en configuration High Availability (haute disponibilité - HA), répétez ces étapes sur les deux homologues HA de Panorama.

STEP 1 | Se connecter à l'interface Web Panorama.

STEP 2 | Supprimer le compte administrateur de l'installateur ZTP

1. Sélectionnez **Panorama** > **Administrators Administrateurs de Panorama)** et sélectionnez le compte administrateur de l'installateur ZTP que vous avez précédemment configuré.
2. **Supprimez** le compte administrateur de l'installateur ZTP.
3. Sélectionnez **Panorama** > **Administrators (Administrateurs)** et sélectionnez le rôle admin `installeradmin`.
4. **Supprimez** le rôle admin `installeradmin`.
5. Sélectionnez **Commit (Valider)** et **Commit to Panorama (Validez sur Panorama)**.

© 2020 Palo Alto Networks, Inc.

STEP 3 | Désinstallez le plug-in ZTP

1. Sélectionnez **Panorama** > **Plugins** et naviguez jusqu'au plug-in ZTP installé sur Panorama.
2. Dans la colonne Actions, **Remove Config (Supprimer la configuration)** pour supprimer les configurations en lien avec ZTP de Panorama
3. Cliquez sur **OK** lorsque l'on vous demande de confirmer la suppression de la configuration ZTP de Panorama.
4. Sélectionnez **Commit (Valider)** et **Commit to Panorama (Validez sur Panorama)**.
5. **Désinstallez** le plug-in ZTP.
6. Cliquez sur **OK** lorsqu'on vous y invite afin de désinstaller le plug-in ZTP de Panorama.

© 2020 Palo Alto Networks, Inc.

Gérer des groupes de périphériques

- Ajouter un groupe de périphériques
- Créer une hiérarchie de groupe de périphériques
- Créer des objets à utiliser dans la stratégie partagée de groupe ou de périphérique
- Revenir aux valeurs héritées de l'objet
- Gérer les objets partagés non utilisés
- Gérer la priorité des objets hérités
- Déplacer ou cloner une règle de stratégie ou un objet vers un autre groupe de dispositifs
- Sélectionner un fournisseur de filtrage des URL sur Panorama
- Pousser une règle de stratégie à un sous-ensemble des pare-feux
- Gérer la hiérarchie des règles

Ajouter un groupe de périphériques

Après avoir ajouté les pare-feu (voir Ajouter un pare-feu en tant que périphérique géré), vous pouvez les grouper en Groupes de périphériques (jusqu'à 1 024), comme suit. N'oubliez pas d'attribuer les deux pare-feux dans une configuration active / passive haute disponibilité (HD) pour le même groupe de périphériques de sorte que Panorama insère les mêmes règles de politique et les objets dans ces pare-feux. PAN-OS ne synchronise pas les règles insérées entre les paires HD. Pour gérer les règles et les objets aux différents niveaux administrateurs de votre organisation, Créer une hiérarchie de groupe de périphériques.

STEP 1 | Sélectionnez **Panorama** > **Device Groups (Groupes d'appareils)**, puis cliquez sur **Add (Ajouter)**.

STEP 2 | Entrez un **Name (Nom)** unique et une **Description** pour identifier le groupe de périphériques.

STEP 3 | Dans la section Périphériques, cochez les cases pour affecter les pare-feux au groupe. Pour rechercher une longue liste de pare-feux, utilisez les Filtres.



Vous ne pouvez assigner n'importe quel pare-feu qu'à un seul groupe de périphériques. Vous pouvez attribuer chaque système virtuel sur un pare-feu à un groupe de périphériques différents.

STEP 4 | Dans la section Reference Template (Modèle de référence), **Add (Ajoutez)** les modèles ou les piles de modèles contenant des objets auxquels la configuration du groupe de périphériques fait référence.

Vous devez affecter les références du modèle ou de la pile de modèles appropriées au groupe de périphériques afin d'associer avec succès le modèle ou la pile de modèles au groupe de périphériques. Cela vous permet de référencer les objets configurés dans un modèle ou une pile de modèles sans ajouter un périphérique sans rapport à une pile de modèles.

Ignorez cette étape si la configuration du groupe de périphériques ne fait référence à aucun objet configuré dans un modèle ou une pile de modèles.

STEP 5 | (Facultatif) Sélectionnez **Group HA Peers (Regrouper les homologues HD)** pour les pare-feu qui sont des homologues HD.

Vous ne pouvez regrouper des homologues HA de pare-feu gérés que s'ils font partie du même groupe de périphériques.

© 2020 Palo Alto Networks, Inc.

Le nom de pare-feu de la paire passive ou active-secondaire est entre parenthèses. Le regroupement d'homologues HA consiste en un changement visuel et aucune modification concernant la configuration en résulte.

STEP 6 | Sélectionnez le **Parent Device Group (Groupe de périphériques Parent)** (la valeur par défaut est **Shared (partagé)**) qui sera juste au-dessus de l'ensemble d'appareils que vous créez dans la hiérarchie de groupes de périphériques.

STEP 7 | Si vos règles de stratégie feront référence aux utilisateurs et groupes, assignez un pare-feu **Master (Maître)**.

Ce sera le seul pare-feu dans le groupe de périphériques d'où Panorama recueillera le nom d'utilisateur et les informations du groupe d'utilisateurs.

STEP 8 | Cliquez sur **OK** pour enregistrer vos modifications.

STEP 9 | Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)**, puis **Commit and Push (Valider et appliquer)** vos modifications à la configuration Panorama et au groupe de périphériques que vous avez ajouté.

Créer une hiérarchie de groupe de périphériques

STEP 1 | Planifiez la hiérarchie des groupes de périphériques.

1. Décider les niveaux de regroupement du dispositif, et les pare-feux et les systèmes virtuels que vous voulez assigner à chaque groupe de périphériques et à l'emplacement partagé. Vous ne pouvez assigner n'importe quel un pare-feu ou un système virtuel (vsys) qu'à un seul groupe de périphériques. Si un groupe de périphériques sera juste un conteneur organisationnel pour les groupes de périphériques de niveau inférieur, il n'est pas nécessaire de lui attribuer des pare-feu.
2. Supprimez les affectations de pare-feu ou de vsys à des groupes de périphériques existants si ces affectations ne s'adaptent pas à votre hiérarchie planifiée.
    1. Sélectionner **Panorama** > **Device Groups (Groupes de Périphériques)** et sélectionnez le groupe de périphérique.
    2. Dans la section périphériques, désactivez les cases à cocher des pare-feux et des systèmes virtuels que vous souhaitez supprimer et cliquez sur **OK**.
3. Si nécessaire, ajoutez plus de pare-feux que vous assignez aux groupes de périphériques : voir ajouter un pare-feu comme périphérique géré.
4. Si vous utilisez de multiples plug-ins sur Panorama pour effectuer une surveillance de points de terminaison, un groupe de périphériques contenant les pare-feux déployés sur un hyperviseur donné ne peut être dépendant ou parent d'un groupe de périphériques contenant des pare-feux déployés sur un hyperviseur différent. Pour plus d'informations, reportez-vous à la section Hiérarchie de groupe de périphériques.

STEP 2 | Pour chaque groupe de périphériques de niveau supérieur, ajoutez un groupe de périphériques.

1. Dans la page **Panorama** > **Device Groups (Groupes de périphériques)** ,cliquez sur **Add (Ajouter)** et entrez un **Name (Nom)** pour identifier le groupe de périphériques.
2. Dans la section Périphériques, cochez les cases pour attribuer des pare-feux et des systèmes virtuels au groupe de périphériques.
3. Laissez l'option **Parent Device Group (Groupe de périphériques parent)** sur **Shared (Partagé)** (la valeur par défaut) et cliquez sur **OK**.

STEP 3 | Pour chaque groupe de périphériques de niveau inférieur, ajoutez un groupe de périphériques.

© 2020 Palo Alto Networks, Inc.

- Pour les nouveaux groupes de périphériques à chaque niveau inférieur, répétez l'étape précédente, mais définissez le **Parent Device Group (groupe de périphériques parent)** dans un groupe de périphériques au prochain niveau au-dessus.
- Pour chaque groupe de périphériques existant, dans la page **Device Groups (Groupes de périphériques)**, sélectionnez le groupe de périphériques à modifier, sélectionnez **Parent Device Group (Groupe de périphériques parent)**, et cliquez sur **OK**.



Si vous déplacez un groupe de périphériques à un parent différent, tous ses groupes de périphériques descendants se déplacent avec lui, ainsi que tous les dispositifs, les règles de politique et objets associés à l'ensemble de périphériques et à ses descendants. Si le nouveau parent est dans un autre domaine d'accès, le groupe de périphériques déplacé n'aura plus l'appartenance dans le domaine d'accès initial. Si le nouveau domaine d'accès a accès en lecture-écriture au groupe de périphériques parent, il aura également accès en lecture-écriture au groupe de périphériques déplacé. Si le nouveau domaine d'accès a accès en lecture seule au parent, il n'aura aucun accès au groupe de périphériques déplacé. Pour configurer l'accès aux groupes de périphériques, consultez Configurer un domaine d'accès*.*

STEP 4 | Configurez, déplacez et clonez les objets et les règles de la politique au besoin pour tenir compte de l'héritage dans la hiérarchie de groupes de périphériques.

- Créez des objets à utiliser dans une stratégie de groupe partagée ou de périphériques ou modifiez des objets existants.

Vous ne pouvez modifier les objets qu'à leur *emplacement* : le groupe de périphériques qui lui seront confiés. Les groupes de périphériques descendants héritent des instances des objets de cet emplacement. Toutefois, vous pouvez éventuellement remplacer les valeurs d'objet héritées.

- Créer ou modifier des stratégies.
- Déplacer ou cloner une règle de stratégie ou un objet vers un autre groupe de périphériques.

STEP 5 | Remplacez les valeurs d'objet héritées.

Applicable uniquement si les valeurs de l'objet dans un groupe particulier d'appareil doivent être différentes des valeurs héritées d'un groupe de périphériques ancêtre.

Après le remplacement d'un objet, vous pouvez le remplacer à nouveau dans les groupes de périphériques descendants. Toutefois, vous ne pouvez jamais remplacer des objets partagés ou prédéfinis (par défaut).

Dans l'onglet **Objects (Objets)**, les objets hérités ont une icône verte dans la colonne nom, et la colonne emplacement affiche le groupe de périphériques ancêtre.

1. Dans l'onglet **Objects (objets)**, sélectionnez le type d'objet (par exemple, **objects (objets)** > **addresses (adresses)**).
2. Sélectionnez le **Device Group (Groupe de périphériques)** disposant de l'instance de substitution.
3. Sélectionnez l'objet et cliquez sur **Override (Remplacer)**.
4. Modifiez les valeurs. Vous ne pouvez pas modifier les paramètres de **Name (Nom)** ou les réglages **Shared (Partagé)**.
5. Cliquez sur **OK**. La colonne nom affiche une icône jaune vert qui se chevauchent pour l'objet pour indiquer qu'il est remplacé.



Si nécessaire, vous pouvez ultérieurement revenir aux valeurs d'objet héritées*.*

STEP 6 | Enregistrez et validez vos modifications.

© 2020 Palo Alto Networks, Inc.

Validez les modifications sur Panorama et appliquez-les aux groupes de périphériques après tout changement dans la hiérarchie.

Vous devez également appliquer les modifications aux modèles si un modèle référence des objets dans un groupe de périphériques (par exemple, les interfaces qui référencent les adresses) et qu'un pare-feu assigné au modèle n'est plus assigné à ce groupe de périphériques en raison d'un changement de hiérarchie.

Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)**, puis **Commit and Push (Valider et appliquer)** vos modifications à la configuration Panorama et aux groupes de périphériques que vous avez ajoutés ou modifiés.

Créer des objets à utiliser dans la stratégie partagée de groupe ou de périphérique

Vous pouvez utiliser un objet dans une règle de politique qui est à l'emplacement partagé, ou du même groupe que l'objet ou dans les descendants de ce groupe de périphériques (pour plus de détails, voir Objets de groupe de périphériques).

Reportez-vous à la section Utiliser les groupes d'adresses dynamiques dans la politique pour vérifier le nombre d'adresses IP enregistrées prises en charge sur Panorama si vous aviez l'intention d'exploiter les groupes d'adresses dynamiques afin de créer des politiques qui s'adaptent automatiquement aux changements qui surviennent dans votre réseau.

- Créer un objet partagé.

  Dans cet exemple, nous ajoutons un objet partagé pour les catégories de filtrage d'URL pour lesquelles nous voulons déclencher des alertes.

  1. Sélectionnez l'onglet **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **URL Filtering (Filtrage d'URL)** et cliquez sur **Add (Ajouter)**.

     L'onglet **Objects (Objet)s** n'apparaît qu'après que vous Ajouter un groupe de périphériques (au moins un).
  2. Entrez un **Name (Nom)** et une **Description**.
  3. Sélectionnez **Shared (Partagé)**.
  4. L'option **Disable Override (Désactiver la substitution)** est désactivée par défaut, ce qui signifie que vous pouvez substituer des instances héritées de l'objet dans tous les groupes de volumes. Pour désactiver les remplacements pour l'objet, sélectionnez la case à cocher.
  5. Dans l'onglet **Categories (Catégories)**, sélectionnez chaque catégorie pour laquelle vous souhaitez une notification.
  6. Dans la colonne **Action**, sélectionnez **Alert (Alerte)**.
  7. Cliquez sur **OK** pour enregistrer vos modifications de l'objet.
  8. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

- Créer un objet de groupe de périphériques.

  Dans cet exemple, nous ajoutons un objet adresse pour les serveurs web spécifiques sur votre réseau.

  1. Sélectionnez **Objects (Objets)** > **addresses (adresses)** et sélectionnez le **Device Group (groupe de périphériques)** dans lequel vous utiliserez l'objet.
  2. Cliquez sur **Add (Ajouter)**, puis entrez un **Name (Nom)** pour identifier l'objet.
  3. N'oubliez pas de laisser l'option **Shared (Partagé)** désactivée.

© 2020 Palo Alto Networks, Inc.

4. L'option **Disable Override (Désactiver la substitution)** est désactivée par défaut, ce qui signifie que vous pouvez substituer des instances héritées de l'objet dans tous les **Device Group (Groupes de périphériques)** sélectionnés. Pour désactiver la substitution pour l'objet, sélectionnez l'option **Disable Override (Désactiver la substitution)**.
5. Sélectionnez le **Type** d'objet de l'adresse et la valeur associée. Par exemple, sélectionnez **IP Range (Plage IP)** et saisissez la plage d'adresses IP pour les serveurs Web.
6. Cliquez sur **OK** pour enregistrer vos modifications de l'objet.
7. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)**, puis **Commit and Push (Valider et appliquer)** vos modifications à la configuration Panorama et au groupe de périphériques où vous avez ajouté l'objet.

- Afficher les objets partagés et les objets de groupe de périphériques dans Panorama.

  Dans les pages de l'onglet **Objects (Objets)**, la colonne emplacement indique si un objet est partagé ou est spécifique à un groupe de périphériques.

  1. Dans l'onglet **Objects (objets)**, sélectionnez le type d'objet (**Objects (objets)** > **Addresses (adresses)**, dans cet exemple).
  2. Sélectionnez le **Device Group (Groupe de périphériques)** auquel vous avez ajouté l'objet.

     L'onglet Objects (Objets) affiche uniquement les objets qui sont sélectionnés dans le Device Group (Groupe de périphériques) ou qui sont hérités d'un groupe de périphériques ancêtre ou de l'emplacement partagé.
  3. Vérifiez que l'objet de groupe de périphérique s'affiche. Notez que le nom de groupe de périphériques dans la colonne emplacement correspond à la sélection dans la liste déroulante **Device Group (Groupe de périphériques)**.

Revenir aux valeurs héritées de l'objet

Après la substitution des valeurs qu'un objet de groupe de périphériques hérite d'un groupe de périphériques ancêtre, vous pouvez ramener l'objet à ses valeurs d'ancêtre à tout moment. Dans l'onglet **Objects (Objets)** les objets substituées ont une icône jaune vert ( )qui se chevauchent dans la colonne Nom.

Si vous voulez imposer les valeurs de l'ancêtre à tous les objets substitués au lieu de ramener un objet spécifique, voir Gérer la priorité des objets hérités.

Pour les étapes permettant de remplacer des valeurs, consultez l'étape 5.

Pour plus d'informations sur l'héritage d'objets ainsi que les remplacements, voir Objets de groupe de périphériques.

STEP 1 | Dans l'onglet **objects (objets)**, sélectionnez le type d'objet (par exemple, les **objects (objets)** > **addresses (adresses)**) et sélectionnez le **Device Group (groupe de périphériques)** qui contient une instance de substitution de l'objet.

STEP 2 | Sélectionnez l'objet, cliquez sur **Revert (rétablir)**, puis sur **Yes (Oui)**. La colonne nom affiche une icône verte pour l'objet, indiquant qu'elle hérite désormais de toutes les valeurs d'un groupe de périphériques ancêtre.

STEP 3 | Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)**, puis **Commit and Push (Valider et appliquer)** vos modifications à la configuration de Panorama et au groupe de périphériques où vous avez rétabli l'objet.

© 2020 Palo Alto Networks, Inc.

Gérer les objets partagés non utilisés

Lorsque vous appliquez les modifications de configuration des Groupes de périphériques, Panorama applique par défaut tous les objets partagés aux pare-feu, que des règles de stratégie de groupe de périphériques ou partagées fassent référence aux objets ou non. Toutefois, vous pouvez configurer Panorama pour appliquer seulement les objets partagés faisant référence à des règles dans les groupes de périphériques. L'option **Share Unused Address and Service Objects with Devices (Partager les objets de service et d'adresse inutilisés avec les périphériques)** permet de limiter les objets que Panorama applique vers les pare-feu gérés.



Lorsque l'option Share Unused Address and Service Objects with Devices (Partager les objets de service et d'adresse inutilisés avec les périphériques) est désactivée, Panorama ignore les pare-feu Target (cible) lorsque vous Pousser une règle de stratégie à un sous-ensemble des pare-feux*. Cela signifie que tous les objets auxquels une règle fait référence sont transmis à tous les pare-feu du groupe de périphériques.*

Pour restreindre le nombre d'objets transmis à un ensemble de pare-feu feu gérés, ajoutez les règles de politique à un groupe de périphériques enfant et ajoutez une référence aux objets partagés, au besoin. Consultez Créer une hiérarchie de groupe de périphériques *pour obtenir plus d'informations sur la création d'un groupe de périphériques enfant.*

Sur les modèles d'entrée de gamme, tels que le PA-220, envisagez d'appliquer uniquement les objets partagés pertinents aux pare-feu gérés. En effet, le nombre d'objets pouvant être stockés sur les modèles d'entrée de gamme est considérablement inférieur à celui des modèles de milieu ou de haut de gamme. En outre, si vous avez beaucoup d'objets d'adresse et de service qui ne sont pas utilisés, la désactivation de l'option **Share Unused Address and Service Objects with Devices (Partager les objets de service et d'adresse inutilisés avec les périphériques)** réduit considérablement les temps de validation sur les pare-feu, car la configuration envoyée à chaque pare-feu est plus petite. Toutefois, la désactivation de cette option peut augmenter le temps de validation sur Panorama, car Panorama doit vérifier de manière dynamique si les règles de stratégie font référence à un objet particulier.

STEP 1 | Sélectionnez **Panorama** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les paramètres de Panorama.

STEP 2 | Désactivez l'option **Share Unused Address and Service Objects with Devices (Partager les objets de service et d'adresse inutilisés avec les périphériques)** pour appliquer uniquement les objets partagés référencés par des règles, ou activez-la pour réactiver l'application de tous les objets partagés.

STEP 3 | Cliquez sur **OK** pour enregistrer vos modifications.

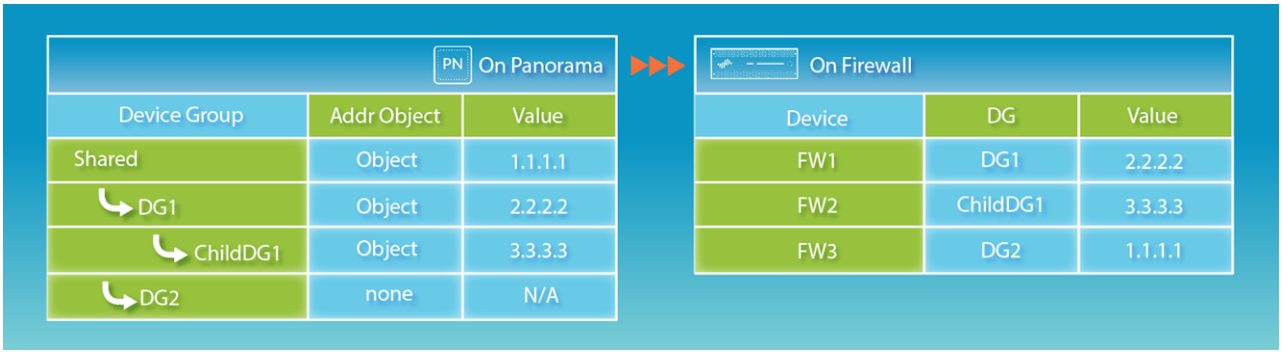
STEP 4 | Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

Gérer la priorité des objets hérités

Par défaut, lorsque le dispositif de groupes à différents niveaux dans la Hiérarchie de groupe de périphériques comporte un objet portant le même nom mais des valeurs différentes (à cause de remplacements, par exemple), des règles de stratégie dans un groupe de périphériques descendants utilisent les valeurs de l'objet en que descendant au lieu d'utiliser les valeurs de l'objet hérités de groupes de périphériques ancêtre. En option, vous pouvez inverser l'ordre de priorité pour pousser les valeurs du plus haut ancêtre contenant l'objet à tous les groupes de périphériques descendants. Après avoir activé

© 2020 Palo Alto Networks, Inc.

cette option, la prochaine fois que vous appliquerez les modifications de configuration sur des groupes de périphériques, les valeurs des objets hérités remplaceront les valeurs de tous les objets remplacés dans les groupes de périphériques descendants. La figure ci-dessous démontre la priorité des objets hérités dans un groupe de périphériques :



Si un pare-feu a des objets définis localement avec le même nom que des objets de groupe partagés ou des périphériques que Panorama a introduit, une défaillance de validation arrive.

Si vous voulez ramener un objet spécifique substitué à ses valeurs d'ancêtre plutôt que d'insérer les valeurs de l'ancêtre de tous les objets substitués, voir Revenir aux valeurs héritées de l'objet.

STEP 1 | Sélectionnez **Panorama** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les paramètres de Panorama.

STEP 2 | Si vous voulez inverser la hiérarchie par défaut, sélectionnez **Objects defined in ancestors will take higher precedence (Les objets définis dans les ancêtres auront une priorité supérieure)**. La boîte de dialogue affiche alors le lien de **Find Overridden Objects (trouver des objets de substitution)**, qui offre la possibilité de voir le nombre d'objets (en ombragé) substitués qui auront des valeurs de l'ancêtre, après avoir validé ce changement. Vous pouvez survoler le message de la quantité à afficher les noms des objets.

Si vous voulez revenir à la hiérarchie par défaut, désélectionnez **Objects defined in ancestors will take higher precedence (Les objets définis dans les ancêtres auront une priorité supérieure)**.

Find Overridden Objects (Trouver des objets substitués) ne détecte que l'objet de groupe de périphériques partagé qui partage un nom avec un autre objet du groupe de périphériques.

STEP 3 | Cliquez sur **OK** pour enregistrer vos modifications.

STEP 4 | Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

STEP 5 | (Facultatif) Si vous avez sélectionné **Objects defined in ancestors will take higher precedence (Les objets définis dans les ancêtres auront une priorité supérieure)**, Panorama n'applique pas les objets ancêtres tant que vous n'appliquez pas les modifications de configuration aux groupes de périphériques : sélectionnez **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)** et **Push (Appliquez)** vos changements.

© 2020 Palo Alto Networks, Inc.

Déplacer ou cloner une règle de stratégie ou un objet vers un autre groupe de dispositifs

Sur Panorama, si une règle de stratégie ou l'objet que vous déplacerez ou clonerez d'un groupe de périphériques possède des références aux objets qui ne sont pas disponibles dans le groupe de périphériques cible (**Destination**), vous devez déplacer ou cloner les objets référencés et la règle de référencement ou l'objet dans la même opération. Dans une hiérarchie de groupe de périphériques, rappelez-vous que les objets référencés peuvent être disponibles via l'héritage. Par exemple, les objets partagés sont disponibles dans tous les groupes de volumes. Vous pouvez effectuer une recherche globale pour vérifier les références. Si vous déplacez ou clonez un objet substitué, veillez à ce que les remplacements soient activés pour cet objet dans le groupe de périphériques parent de la **Destination** (voircréer des objets à utiliser dans la stratégie de groupe de périphériques ou d'appareils partagés).

Lorsque vous clonez plusieurs règles de politiques, l'ordre dans lequel vous sélectionnez les règles détermine l'ordre dans lequel elles sont copiées dans le groupe de périphériques. Par exemple, si vous avez les règles 1 à 4 et que votre ordre de sélection est 2-1-4-3, le groupe de périphériques dans lequel ces règles seront clonées affichera les règles dans le même ordre que celui que vous avez sélectionné. Cependant, vous pouvez réorganiser les règles comme bon vous semble une fois qu'elles ont été copiées avec succès.

STEP 1 | Connectez-vous à Panorama et sélectionnez la règle de base (par exemple, **Policy (Stratégie)** > **Security (Sécurité)** > **Pre Rules (Pré-règles)**) ou type d'objet (par exemple, **Objects (Objets)** > **Addresses (Adresses)**).

STEP 2 | Sélectionnez le **Device Group (groupe de périphériques)** et sélectionnez une ou plusieurs règles ou objets.

STEP 3 | Effectuez l'une des étapes suivantes :

- (Règles uniquement) **Move (Déplacer)** > **Move to other device group (Déplacer vers un autre groupe de périphériques)**.
- (Pour les objets uniquement) **Move (Déplacer)**.
- (Règles ou objets) **Clone (Cloner)**.

STEP 4 | Dans la liste déroulante **Destination**, sélectionnez le nouveau groupe de périphériques ou **Shared (Partagé)**. La valeur par défaut sélectionné précédemment est **Device Groupe (Groupe de périphériques)**.

STEP 5 | (Règles uniquement) Sélectionnez **Rule order (Ordre des règles)** :

- **Move top (Déplacer vers le haut)** (par défaut) — la règle se mettra en avant de toutes les autres règles.
- **Move bottom (Déplacer vers le bas)** la règle viendra après toutes les autres règles.
- **Before rule (Avant la règle)** - Dans la liste déroulante adjacente, sélectionnez la règle qui vient après les règles sélectionnées.
- **After rule (Après la règle)** —Dans le déroulant adjacent, sélectionnez la règle qui précède les règles sélectionnées.

STEP 6 | L'**Error out on first detected error in validation (erreur sur la première erreur détectée lors de la validation)** de la case est cochée par défaut, ce qui signifie que Panorama affichera la première erreur qu'il trouve et arrêtera derechercher plus d'erreurs. Par exemple, une erreur se produit si le groupe de périphériques de **Destination** n'est pas un objet qui est référencé

© 2020 Palo Alto Networks, Inc.

dans la règle que vous déplacez. Lorsque vous déplacez ou clonez de nombreux éléments à la fois, sélectionner cette case à cocher peut simplifier le dépannage. Si vous désactivez la case à cocher, Panorama trouvera toutes les erreurs avant de les afficher. Indépendamment de ce paramètre, Panorama ne déplacera ou clonera quoi que ce soit jusqu'à ce que vous corrigiez toutes les erreurs pour tous les éléments sélectionnés.

STEP 7 | Cliquez sur **OK** pour démarrer la validation de l'erreur. Si Panorama détecte des erreurs, il les corrigera et retentera l'opération de déplacement ou de clonage. Si Panorama ne trouve pas d'erreurs, il effectue l'opération.

STEP 8 | Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)**, **Edit Selections (Modifier les sélections)** dans la portée d'application, sélectionnez **Device Groups (Groupes de périphériques)**, sélectionnez les groupes de périphériques d'origine et de destination, cliquez sur **OK**, puis **Commit and Push (Valider et appliquer)** vos modifications à la configuration Panorama et aux groupes de périphériques.

Sélectionner un fournisseur de filtrage des URL sur Panorama

Le filtrage des URL vous permet de configurer les pare-feux pour surveiller et contrôler l'accès à Internet pour vos utilisateurs. Les règles de stratégie que vous configurez pour contrôler l'accès Web (sécurité, QoS, portail captif, et règles de décryptage) des catégories d'URL de référence. Le vendeur de filtrage URL que vous sélectionnez sur Panorama détermine quelles catégories d'URL sont référencées dans les règles que vous ajoutez aux groupes de volumes et insérez aux pare-feux.

Par défaut, panorama utilise Pan-DB, une base de données de filtrage d'URL qui est étroitement intégrée dans PAN-OS et les réseaux Palo Alto Threat Intelligence Cloud. PAN-DB fournit la mise en cache locale de haute performance pour maximiser les performances en ligne pour les recherches d'URL. L'autre option de fournisseur est BrightCloud, une base tierce de données d'URL .

Contrairement aux pare-feux, panorama ne télécharge pas la base de données URL et ne requiert pas de licence de filtrage d'URL.

Les rubriques suivantes décrivent comment modifier le fournisseur de filtrage d'URL sur Panorama ou et sur Panorama et sur les pare-feu gérés. Vous pouvez également modifier le fournisseur de filtrage d'URL juste sur les pare-feux.

- Panorama et les Firewalls doivent-ils avoir des fournisseurs de filtrage d'URL correspondants ?
- Modifiez le fournisseur de filtrage d'URL sur Panorama HD
- Modifiez le fournisseur de filtrage d'URL sur Panorama non-HD
- Migrer Panorama et les pare-feu HD de BrightCloud à PAN-DB
- Migrer Panorama et les pare-feux non-HD de BrightCloud à PAN-DB

Panorama et les Firewalls doivent-ils avoir des fournisseurs de filtrage d'URL correspondants ?

Sur n'importe quel serveur unique de gestion de panorama ou pare-feu, un seul fournisseur de filtrage d'URL peut être actif : PAN-DB ou BrightCloud. Lors de la sélection d'un fournisseur pour Panorama, vous devez prendre en compte le fournisseur et la version PAN-OS des pare-feux gérés :

- PAN-OS 5.0.x et les versions antérieures de - Panorama ainsi que les pare-feux exigent des fournisseurs de filtrage des URL correspondants.
- PAN-OS 6.0.x et les versions ultérieures - Panorama ainsi que les pare-feux ne nécessitent pas de fournisseurs de filtrage des URL correspondants. Si une incompatibilité de fournisseur est détectée, le

© 2020 Palo Alto Networks, Inc.

pare-feu répertorie les catégories d'URL dans les profils de filtrage d'URL et les règles qu'il a reçues de Panorama sur les catégories d'URL qui s'harmonisent avec celles du fournisseur activé sur le pare-feu.

Par conséquent, pour un déploiement dans lequel certains pare-feux s'exécutent sous PAN-OS 6.0 ou version ultérieure et certains pare-feux qui s'exécutent sur des versions antérieures de PAN-OS, Panorama doit utiliser le même fournisseur de filtrage d'URL que les pare-feux qui exécutent des versions antérieures de PAN-OS. Par exemple, si les pare-feux qui exécutent Pan-OS 5.0 utilisent Pan-DB et les pare-feux qui exécutent Pan-OS 7.0 utilisent BrightCloud, panorama doit utiliser Pan-DB.

Modifiez le fournisseur de filtrage d'URL sur Panorama HD

Dans un déploiement de haute disponibilité (HD), chaque homologue Panorama doit être dans un état non fonctionnel lorsque vous modifiez le filtrage d'URL fournisseur. Par conséquent, pour éviter de perturber les opérations de Panorama, modifiez le filtrage d'URL fournisseur sur le Panorama passif (Panorama2 dans cet exemple), puis déclenchez le basculement avant de modifier le fournisseur sur le Panorama actif (Panorama1 dans cet exemple).

STEP 1 | Modifiez le filtrage d'URL fournisseur sur chaque paire HD Panorama.

Terminez cette tâche sur Panorama2 (paire passive) avant Panorama1 (paire active).

1. Connectez-vous à l'interface Web Panorama.
2. Sélectionnez **Panorama (Panorama)** > **High Availability (Haute Disponibilité)** et **Suspend local Panorama (suspendez le Panorama local)**.

   Lorsque vous effectuez cette étape sur Panorama1, le basculement se produit et Panorama2 devient actif.
3. Sélectionnez **Panorama (Panorama)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les Paramètres Généraux.
4. Sélectionnez le fournisseur de la **URL Filtering Database (base de données de filtrage d'URL)** : **paloaltonetworks** (PAN-DB) or **brightcloud**.
5. Sélectionnez **Panorama** > **High Availability (Haute Disponibilité)** et **Make local Panorama functional (rendez le Panorama local fonctionnel)**.

   Lorsque vous effectuez cette étape sur Panorama1 avec la préemption activée sur les deux homologues HD, Panorama1 retourne automatiquement au statut actif et Panorama2 retourne au statut passif.

STEP 2 | Vérifiez que les catégories d'URL sont disponibles pour le référencement dans les politiques.

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **URL Filtering (Filtrage des URL)**.
2. Cliquez sur **Add (Ajouter)** et vérifiez que l'onglet **Categories (Catégories)** de la boîte de dialogue de filtrage du profil affiche les catégories d'URL associées au fournisseur sélectionné.

Modifiez le fournisseur de filtrage d'URL sur Panorama non-HD

Effectuez cette procédure pour modifier le filtrage d'URL fournisseur sur un serveur de gestion Panorama qui n'est pas déployé dans une configuration haute disponibilité (HD).

STEP 1 | Modifier le fournisseur de filtrage d'URL.

1. Sélectionnez **Panorama (Panorama)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les Paramètres Généraux.
2. Sélectionnez le fournisseur de la **URL Filtering Database (base de données de filtrage d'URL)** : **paloaltonetworks** (PAN-DB) or **brightcloud**.

© 2020 Palo Alto Networks, Inc.

STEP 2 | Vérifiez que les catégories d'URL sont disponibles pour le référencement dans les politiques.

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **URL Filtering (Filtrage des URL)**.
2. Cliquez sur **Add (Ajouter)** et vérifiez que l'onglet **Categories (Catégories)** de la boîte de dialogue de filtrage du profil affiche les catégories d'URL associées au fournisseur sélectionné.

Migrer Panorama et les pare-feu HD de BrightCloud à PAN-DB

Effectuez cette procédure pour migrer le fournisseur de filtrage d'URL de BrightCloud à Pan-dB sur panorama et aux pare-feu lorsque les pare-feu sont déployés dans une configuration haute disponibilité (HD). Dans cet exemple, le pare-feu actif (ou actif-primaire) est nommé FW1 etc. et le pare-feu passif (ou actif-secondaire) est nommé FW2. La migration mappe automatiquement les catégories d'URL BrightCloud aux catégories d'URL Pan-DB.

STEP 1 | Déterminez quels pare-feu nécessitent de nouvelles licences de filtrage d'URL Pan-DB.

1. Connectez-vous à Panorama et sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Licenses (Licences)**.
2. Vérifiez la colonne URL pour déterminer quels pare-feu possèdent des licences Pan-DB et si les licences sont valides ou expirées.

   Un pare-feu peut avoir des licences valides pour BrightCloud et PAN-DB, mais une seule licence peut être active.

   Si vous ne savez pas si une licence de filtrage d'URL PAN-DB est active, accédez à l'interface Web du pare-feu, sélectionnez Device (Périphérique) > Licenses (Licences) et vérifiez que le champ Active (Actif) affiche Yes (Oui) dans la section Filtrage d'URL PAN-DB.
3. Achetez une nouvelle licence pour chaque pare-feu qui n'a pas de licence Pan-DB valide.

   Dans les déploiements HD, chaque homologue de pare-feu a besoin d'une licence Pan-DB et d'un code d'autorisation distincts. Palo Alto Networks envoie un email contenant des codes d'activation pour les licences que vous achetez. Si vous ne trouvez pas ce courriel, contactez le support client avant de procéder.

STEP 2 | Modifiez le fournisseur de filtrage d'URL dans Pan-DB sur Panorama.

Accédez à l'interface panorama Web et effectuez l'une des tâches suivantes :

- Modifiez le fournisseur de filtrage d'URL sur Panorama HD
- Modifiez le fournisseur de filtrage d'URL sur Panorama non-HD

STEP 3 | Configurez les paramètres de session TCP sur les deux homologues du pare-feu HD pour garantir que les sessions qui ne sont pas encore synchronisées échouent lorsque vous suspendez un homologue.

Connectez-vous à l'ILC de chaque pare-feu et exécutez la commande suivante :

```
> set session tcp-reject-non-syn no
```

STEP 4 | Migrez le fournisseur de filtrage d'URL vers Pan-dB sur chaque homologue de pare-feu HD.

Terminez cette tâche sur FW2 (homologue passif ou actif-secondaire) avant FW1 (homologue actif ou actif-primaire).

© 2020 Palo Alto Networks, Inc.

1. Accédez à l'interface Web du pare-feu, sélectionnez **Device (Périphérique)** > **High Availability (Haute Disponibilité)** > **Operational Commands (Commandes opérationnelles)**, et **Suspend local device (Suspendez le périphérique local)**.

   L'exécution de cette étape sur FW1 et déclenchez le basculement vers FW2.
2. Sélectionnez **Device (Périphérique)** > **Licenses (Licences)**.
3. Dans la section License Management (Gestion des licences), sélectionnez **Activate feature using authorization code (Activer la fonction à l'aide du code d'autorisation)**, saisissez l'**Authorization Code (Code d'autorisation)** et cliquez sur **OK**.

   L'activation de la licence Pan-DB désactive automatiquement la licence BrightCloud.
4. Dans la section filtrage des URL PAN-DB, **Download (Téléchargez)** le fichier Seed, sélectionnez votre région, puis cliquez sur **OK (OK)**.
5. Validez et appliquez vos modifications de configuration :
   1. Accédez à l'interface Web de Panorama.
   2. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** et **Edit Selections (Modifier les sélections)** dans la portée d'application.
   3. Sélectionnez **Device Groups (Groupes de périphériques)**, sélectionnez le pare-feu et cliquez sur **OK**.
   4. **Commit and Push (Validez et appliquez)** vos modifications à la configuration Panorama et aux groupes de périphériques.
6. Accédez à l'interface Web du pare-feu, sélectionnez **Device (Dispositif)** > **High Availability (Haute Disponibilité)** > **Operational Commands (Commandes opérationnelles)**, et **Make local device functional (Activez le périphérique local)**.

   Lorsque vous effectuez cette étape sur FW1 etc. avec la préemption activée sur les deux pare-feu, FW1 revient automatiquement à l'état actif (ou actif-primaire) et FW2 retourne au statut passif (ou actif-secondaire).

STEP 5 | Rétablir les deux homologues HD de pare-feu aux paramètres de session TCP d'origine.

Exécutez la commande suivante à l'ILC de chaque pare-feu :

```
> set session tcp-reject-non-syn yes
```

Migrer Panorama et les pare-feux non-HD de BrightCloud à PAN-DB

Effectuez cette procédure pour migrer le fournisseur de filtrage d'URL de BrightCloud à Pan-dB sur panorama et aux pare-feux lorsque les pare-feux sont déployés dans une configuration haute disponibilité (HD). La migration mappe automatiquement les catégories d'URL BrightCloud aux catégories d'URL Pan-DB.

STEP 1 | Déterminez quels pare-feu nécessitent de nouvelles licences de filtrage d'URL Pan-DB.

1. Connectez-vous à Panorama et sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Licenses (Licences)**.
2. Vérifiez la colonne URL pour déterminer quels pare-feu possèdent des licences Pan-DB et si les licences sont valides ou expirées.

   Un pare-feu peut avoir des licences valides pour BrightCloud et PAN-DB, mais une seule licence peut être active.

   Si vous ne savez pas si une licence de filtrage d'URL PAN-DB est active, accédez à l'interface Web du pare-feu, sélectionnez Device (Périphérique) > Licenses (Licences) et vérifiez que le champ Active (Actif) affiche Yes (Oui) dans la section Filtrage d'URL PAN-DB.

© 2020 Palo Alto Networks, Inc.

3. Achetez de nouvelles licences pour les pare-feux qui n'ont pas de licences Pan-DB valides.

   Palo Alto Networks envoie un email contenant des codes d'activation pour les licences que vous achetez. Si vous ne trouvez pas ce courriel, contactez le support client avant de procéder.

STEP 2 | Modifiez le fournisseur de filtrage d'URL dans Pan-DB sur Panorama.

Accédez à l'interface panorama Web et effectuez l'une des tâches suivantes :

- Modifiez le fournisseur de filtrage d'URL sur Panorama HD
- Modifiez le fournisseur de filtrage d'URL sur Panorama non-HD

STEP 3 | Migrez le fournisseur de filtrage d'URL vers Pan-BB sur chaque pare-feu.

1. Accédez à l'interface Web de pare-feu et sélectionnez **Device (Périphérique)** > **Licenses (Licences)**.
2. Dans la section gestion des licences, sélectionnez **Activate feature using authorization code (Activer la fonction à l'aide du code d'autorisation)**, saisissez le **Authorization Code (Code D'autorisation)** et cliquez sur **OK (OK)**.

   L'activation de la licence Pan-DB désactive automatiquement la licence BrightCloud.
3. Dans la section filtrage des URL PAN-DB, **Download (Téléchargez)** le fichier Seed, sélectionnez votre région, puis cliquez sur **OK (OK)**.
4. Validez et appliquez vos modifications de configuration :
   1. Accédez à l'interface Web de Panorama.
   2. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** et **Edit Selections (Modifier les sélections)** dans la portée d'application.
   3. Sélectionnez **Device Groups (Groupes de périphériques)**, sélectionnez le pare-feu et cliquez sur **OK**.
   4. **Commit and Push (Validez et appliquez)** vos modifications à la configuration Panorama et aux groupes de périphériques.

Pousser une règle de stratégie à un sous-ensemble des pare-feux

Une stratégie *cible* permet de spécifier les pare-feux dans un groupe de périphériques dans lesquels insérer les règles de la politique. Cela vous permet d'exclure un ou plusieurs pare-feux ou des systèmes virtuels, ou d'appliquer une règle uniquement à des pare-feux spécifiques ou à des systèmes virtuels dans un groupe de périphériques.

Au fur et à mesure de l'évolution de votre base de règles et de la transmission de règles nouvelles ou modifiées aux pare-feu, les informations sur les modifications et les audits sont perdues au fil du temps, sauf si vous les archivez lors de la création ou de la modification de la règle. Utilisez l'archive des commentaires d'audit pour afficher le commentaire d'audit et l'historique des journaux de configuration d'une règle sélectionnée ainsi que pour comparer deux versions de règle de politique pour voir les modifications que la règle a subies. L'historique des commentaires d'audit d'une règle transmise de Panorama peut uniquement être consulté à partir du serveur de gestion Panorama. Cependant, vous pouvez afficher les commentaires d'audit dans les journaux de configuration qui sont transmis à Panorama à partir des pare-feu gérés. Cependant, l'archive des commentaires d'audit ne peut être consulté pour les règles créées ou modifiées localement sur le pare-feu. Pour vous assurer que les commentaires d'audit sont capturés lors de la création ou de la modification d'une règle, Appliquez la règle de politique, la description, l'étiquette et le commentaire d'audit.

La possibilité de cibler une règle vous permet de conserver les stratégies centralisées sur Panorama. Les règles ciblées vous permettent de définir les règles (en tant que règles partagées ou de règles avant ou après du groupes de périphériques) sur Panorama et d'améliorer la visibilité et l'efficacité lors de la gestion des règles (voir Politique de groupe de périphériques).Les règles ciblées vous permettent de définir les

© 2020 Palo Alto Networks, Inc.

règles (en tant que pré ou post-règles de groupe partagé ou de périphérique) sur Panorama (pour plus de détails, voir Stratégies de groupe de périphériques) et d'améliorer la visibilité et l'efficacité de la gestion des règles. L'archive des commentaires d'audit procure une visibilité accrue en vous permettant de suivre les modifications apportées à vos règles de politique au fil du temps, et les raisons de ces modifications, ce qui vous permet d'effectuer l'audit de l'évolution des règles tout au long de leur cycle de vie.

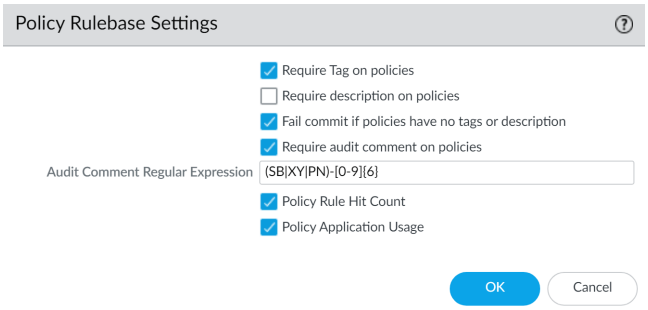
STEP 1 | (Pratique exemplaire) Appliquez les commentaires d'audit pour les règles de politique.

Bien que cette étape soit facultative, il est recommandé d'appliquer les commentaires d'audit pour les règles de politique pour vous assurer de saisir la raison pour laquelle la règle est créée ou modifiée. Cela vous aide également à préserver l'exactitude de l'historique des règles à des fins d'audit.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les Policy Rulebase Settings (Paramètres de la base de règles de politique).
2. Activez l'option **Require audit comment on policies (Exiger un commentaire d'audit à l'égard des politiques)**.
3. Configurez l'expression régulière des commentaires d'audit pour spécifer le format des commentaires d'audit.

   Lors de la création ou de la modification d'une règle, exigez que les commentaires d'audit respectent un format donnée en fonction de vos besoin d'affaires et d'audit en spécifiant des expressions en nombre et en lettres. Par exemple, vous pouvez utiliser ce paramètre pour spécifier des expressions régulières qui correspondent à vos formats d'attribution du numéros de billets :

   - **`[0-9]{<Nombre de chiffres>}`** : exige que le commentaire d'audit contienne un nombre minimum de chiffres allant de 0 à 9. Par exemple, **`[0-9]{6}`** exige la présence de six chiffres dans une expression numérique composée de chiffres entre 0 et 9 Configurez le nombre minimum de chiffres, selon vos besoins.
   - **`<Expression en lettres>`** : exige que le commentaire d'audit contienne une expression en lettres. Par exemple, **`Reason for Change-`** exige que l'administrateur commence son commentaire d'audit avec cette expression.
   - **`<Expression en lettres>-[0-9]{<Nombre de chiffres>}`** : exige que le commentaire d'audit contienne un préfixe défini suivi d'un nombre minimum de chiffres allant de 0 à 9. Par exemple, **`SB-[0-9]{6}`** exige que le commentaire d'audit commence par **`SB-`**, suivi d'au moins six chiffres présentés sous une expression numérique comportant des chiffres de 0 à 9, comme **`SB-012345`**.
   - **`(<Expression en lettres>)|(<Expression en lettres>)|(<Expression en lettres>)|-[0-9]{<Nombre de chiffres>}`** : exige que le commentaire d'audit contienne un préfixe se servant de l'une des expressions en lettres prédéfinie et un nombre minimum de chiffres allant de 0 à 9. Par exemple, **`(SB|XY|PN)-[0-9]{6}`** exige que le format du commentaire d'audit commence par **`SB-`**, **`XY-`** ou **`PN-`** , suivi d'une expression numérique contenant au moins six chiffres de 6 à 0, comme **`SB-012345`**, **`XY-654321`** ou **`PN-012543`**.
4. Cliquez sur **OK** pour appliquer les nouveaux paramètres de la base de règles de politique.



5. Sélectionnez **Commit (Valider)** et **Commit to Panorama (Validez sur Panorama)**.

© 2020 Palo Alto Networks, Inc.

STEP 2 | Créer une règle.

Dans cet exemple, nous définissons une règle préalable dans les modules de sécurité qui permet aux utilisateurs du réseau interne d'accéder à des serveurs dans la zone démilitarisée.

1. Sous l'onglet **Policies (stratégies)**, sélectionnez le **Device Group (groupe de périphériques)** pour lequel vous souhaitez définir une règle.
2. Sélectionnez les modules. Pour cet exemple, sélectionnez **Policies (Stratégies)** > **Security (Sécurité)** > **Pre-Rules (Pré-règles)** et **Add (Ajoutez)** une règle.
3. Dans l'onglet **General (Général)**, donnez un **Name (Nom)** description à la règle et saisissez un **Audit Comment (Commentaire d'audit)**.
4. Dans l'onglet **Source**, réglez la **Source Zone (Zone Source)** sur **Trust (Approuvée)**.
5. Dans l'onglet **Destination**, réglez la **Destination Zone (Zone de destination)** sur **DMZ**.
6. Dans l'onglet **Service/ URL Category (Catégorie de service/d'URL)**, définissez le **Service** sur **application-default (par défaut de l'application)**.
7. Dans l'onglet **Actions**, définissez la valeur **Action** sur **Allow (Autoriser)**.
8. Laissez toutes les autres valeurs à leurs valeurs par défaut.

STEP 3 | Cibler la règle pour inclure ou exclure un sous-ensemble de pare-feux.

Pour appliquer la règle à un ensemble sélectionné de pare-feux :

1. Sélectionnez l'onglet **Target (Cible)** dans la boîte de dialogue Policy Rule (Règle de politique).
2. Sélectionnez les pare-feu auxquels vous souhaitez appliquer la règle.

   Si vous ne sélectionnez pas de pare-feux à cibler, la règle est ajoutée à tous les pare-feux (non cochés) dans le groupe de périphériques.

   Bien que la case des systèmes virtuels dans le groupe de périphériques soit décochée, tous les systèmes virtuels hériteront pas défaut de la règle lors de la validation, sauf si vous sélectionnez un ou plusieurs systèmes virtuels auxquels vous souhaitez appliquer la règle.
3. (Facultatif) Pour exclure un sous-ensemble de pare-feu de l'héritage de la règle, **Install on all but specified devices (Installez sur tous les périphériques sauf ceux qui sont spécifiés)** et sélectionnez les pare-feu que vous souhaitez exclure.

   Si vous sélectionnez Install on all but specified devices (installer sur tous les appareils sauf spécifiés) et ne sélectionnez pas de périphérique, la règle n'est ajoutée à aucun des pare-feux dans le groupe de périphériques.
4. Cliquer sur **OK**pour enregistrer la règle.

STEP 4 | Validez et appliquez les modifications de configuration.

1. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** et **Edit Selections (Modifier les sélections)** dans la portée d'application.
2. Sélectionnez **Device Groups (Groupes de périphériques)**, sélectionnez le groupe de périphériques dans lequel vous avez ajouté la règle, puis cliquez sur **OK**.
3. **Commit and Push (Validez et appliquez)** vos modifications à la configuration Panorama et aux groupes de périphériques.

STEP 5 | Résoudre les problèmes de correspondances du trafic à la règle de politique pour vérifier que les règles autorisent et refusent le trafic comme prévu.

© 2020 Palo Alto Networks, Inc.

Gérer la hiérarchie des règles

L'ordre des règles de stratégie est essentiel pour la sécurité de votre réseau. Au sein de toute couche de politique (partagé, ensemble d'instruments, ou règles définies localement) et les modules (par exemple, pré-règles de sécurité partagées), le pare-feu évalue les règles du haut vers le bas dans l'ordre où elles apparaissent dans les pages de l'onglet **Policies (stratégies)**. Le pare-feu correspond à un paquet contre la première règle qui répond aux critères définis et ne tient pas compte des règles suivantes. Donc, pour appliquer une correspondance plus spécifique, déplacer les règles plus spécifiques au-dessus des règles plus génériques.

Pour comprendre l'ordre dans lequel le pare-feu évalue les règles par couche et par type (pré-règles, règles post et règles par défaut) dans la hiérarchie des groupes de périphériques*, voir* Stratégies de groupe de périphériques*.*

STEP 1 | Affichez la hiérarchie de chaque règle de base.

1. Sélectionnez l'onglet **Policies (stratégies)**, puis cliquez sur **Preview Rules (règles de prévisualisation)**.
2. Filtrer l'aperçu par **Rulebase (modules)** (par exemple, la **Security (sécurité)** ou **QoS**).
3. L'Aperçu pour afficher les règles d'un **Device Group (groupe de périphériques)** spécifique et des règles qu'elle hérite de groupes de périphériques partagés et de l'emplacement ancêtre du filtre. Vous devez sélectionner un groupe de périphériques disposant de pare-feux qui lui sont assignés.
4. Filtrer la prévisualisation de **Device (périphérique)** pour afficher ses règles définies localement.
5. Cliquez sur l'icône de la flèche verte pour appliquer vos sélections de filtre à la prévisualisation (voir Politique de groupe de périphériques
6. Fermez la boîte de dialogue Aperçu de règles combinées lorsque vous avez terminé la prévisualisation des règles.

STEP 2 | Supprimer ou désactiver des règles, si nécessaire.

Pour déterminer quelles règles un pare-feu n'utilise pas actuellement, sélectionnez ce pare-feu dans le Context (Contexte) du menu déroulant sur Panorama, sélectionnez les modules (par exemple, les Policies (politiques) > Security (sécurité)), puis sélectionnez la case à cocher Highlight Unused Rules (mettre en évidence les règles non utilisées). Un fond orange en pointillés indique les règles que le pare-feu n'utilise pas.

1. Sélectionnez la règle de base (par exemple, **Policies (Politiques)** > **Security (Sécurité)** > **Pre Rules (Pré Règles)**) qui contient la règle que vous allez supprimer ou désactiver.
2. Sélectionnez le **Device Group (groupe de périphériques)** qui contient la règle.
3. Sélectionnez la règle, puis cliquez sur **Delete (supprimer)** ou **Disable (désactiver)** comme vous le souhaitez. Les règles désactivées apparaissent dans une police en italique.

STEP 3 | Repositionner les règles au sein d'un module, si nécessaire.

Pour repositionner les règles locales sur un pare-feu, accéder à son interface web en sélectionnant ce pare-feu dans le Context (cadre) du menu déroulant avant d'effectuer cette étape.

1. Sélectionnez la règle de base (par exemple, **Policies (Politiques)** > **Security (Sécurité)** > **Pre Rules (Pré Règles)**) qui contient la règle que vous allez déplacer.
2. Sélectionnez le **Device Group (groupe de périphériques)** qui contient la règle.
3. Sélectionnez la règle, sélectionnez **Move (déplacer)** et sélectionnez :

© 2020 Palo Alto Networks, Inc.

- **Move Top (Déplacer vers le haut)** déplace la règle au-dessus de toutes les autres règles dans le groupe de périphériques (mais pas au-dessus des règles héritées des groupes de périphériques partagés ou ancêtres).
- **Move Up (Déplacer vers le haut)** déplace la règle au-dessus de toutes les autres règles dans le groupe de périphériques (mais pas au-dessus des règles héritées des groupes de périphériques partagés ou ancêtres).
- **Move Down (Déplacer vers le bas)** déplace la règle sous celle qui la suit.
- **Move Bottom (Déplacer vers le bas)** déplace la règle sous toutes les autres règles.
- **Move to other device group (Déplacer à un autre groupe de périphériques)** — voir déplacer ou cloner une règle de stratégie ou un objet à un autre groupe de périphériques.

STEP 4 | Si vous avez modifié les règles, validez et appliquez les modifications.

1. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** et **Edit Selections (Modifier les sélections)** dans la portée d'application.
2. Sélectionnez **Device Groups (Groupes de périphériques)**, sélectionnez le groupe de périphériques contenant les règles que vous avez modifiées ou supprimées, puis cliquez sur **OK**.
3. **Commit and Push (Validez et appliquez)** vos modifications à la configuration Panorama et aux groupes de périphériques.

© 2020 Palo Alto Networks, Inc.

Gérer les modèles et les piles de modèle

Utiliser des modèles et des piles de modèle pour définir les configurations de base communes permettant aux pare-feux l'exploitation de votre réseau. Voir Modèles et piles de modèles pour un aperçu des questions que vous devriez prendre en considération au moment de décider quels pare-feux ajouter à quels modèles, commander des modèles dans une pile pour gérer des couches de paramètres spécifiques à et pare-feux et des groupes communs, et les paramètres prépondérants du modèle avec des valeurs spécifiques du pare-feu.



Pour supprimer un modèle, vous devez d'abord désactiver/supprimer localement les paramètres de modèle sur le pare-feu. Seuls les administrateurs avec le rôle de super-utilisateur peuvent désactiver un modèle.

- Fonctionnalités des modèles et exceptions
- Ajouter un modèle
- Configuration d'une pile de modèles
- Configurer une variable de modèle ou de pile de modèles
- Importer et écraser les variables de la pile de modèles existante
- Remplacer un paramètre de modèle
- Désactiver/supprimer les paramètres de modèle

Fonctionnalités des modèles et exceptions

Vous pouvez utiliser des modèles et des piles de modèles pour définir un large éventail de paramètres mais vous ne pouvez effectuer les tâches suivantes que localement sur chaque pare-feu géré :

- Configurez une liste de blocs de périphériques.
- Effacer les journaux.
- Activez les modes opérationnels tels que le mode normal, le mode multi-vsys ou le mode FIPS-CC.
- Configurez les adresses IP des pare-feu dans une paire haute disponibilité.
- Configurer une clé principale et les diagnostics.
- Comparer les fichiers de configuration (Audit de configuration).



Pour Gérer les licences et les mises a jour (logiciel et contenu) pour les pare-feu, utilisez les options de l'onglet Panorama > Device Management (Gestion de périphériques); n'utilisez pas de modèles.

- Renommer un vsys sur un pare-feu multi-vsys.

Ajouter un modèle

Vous devez ajouter au moins un modèle avant que Panorama n'affiche les onglets **Device (Périphérique)** et **Network (Réseau)** requis pour définir le réseau mis en place et les éléments de configuration de périphérique pour les pare-feu. Panorama prend en charge jusqu'à 1 024 modèles. Chaque pare-feu géré doit appartenir à une pile de modèles. Bien que les modèles contiennent des configurations de périphériques gérés, les piles de modèles vous permettent de gérer et de transmettre les configurations de modèles à tous les pare-feu gérés qui sont affectés à la pile de modèles.



Combinez les modèles dans une pile de modèles pour éviter de dupliquer de nombreuses configurations parmi les modèles (voir modèles et piles de modèles et configurer une pile de modèles).

© 2020 Palo Alto Networks, Inc.

STEP 1 | Ajoutez un modèle.

1. Sélectionnez **Panorama** > **Templates (Modèles)**.
2. Cliquer sur **Add (Ajouter)** et entrez un **Name (Nom)** unique pour identifier le modèle.
3. (Facultatif) Saisissez une **Description** de l'interface.
4. Cliquez sur **OK** pour sauvegarder le modèle.
5. Si le modèle possède un système virtuel (vsys) avec des configurations (par exemple, des interfaces) que vous souhaitez que Panorama envoie aux pare-feu qui ne disposent pas de système virtuel, sélectionnez le modèle que vous avez créé, sélectionnez le système virtuel dans la liste déroulante **Default VSYS (VSYS par défaut)** et cliquez sur **OK**.
6. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)**, puis **Commit and Push (Validez et appliquez)** vos modifications à la configuration Panorama et au modèle.

STEP 2 | Vérifiez que le modèle est disponible.

Après avoir ajouté le premier modèle, Panorama affiche les onglets du **Device (Appareil)** et du **Network (Réseau)**. Ces onglets affichent un menu déroulant **Template (Modèle)**. Vérifiez que le menu déroulant affiche le modèle que vous venez d'ajouter.

STEP 3 | Configurez une pile de modèles et ajoutez le modèle à la pile de modèle.

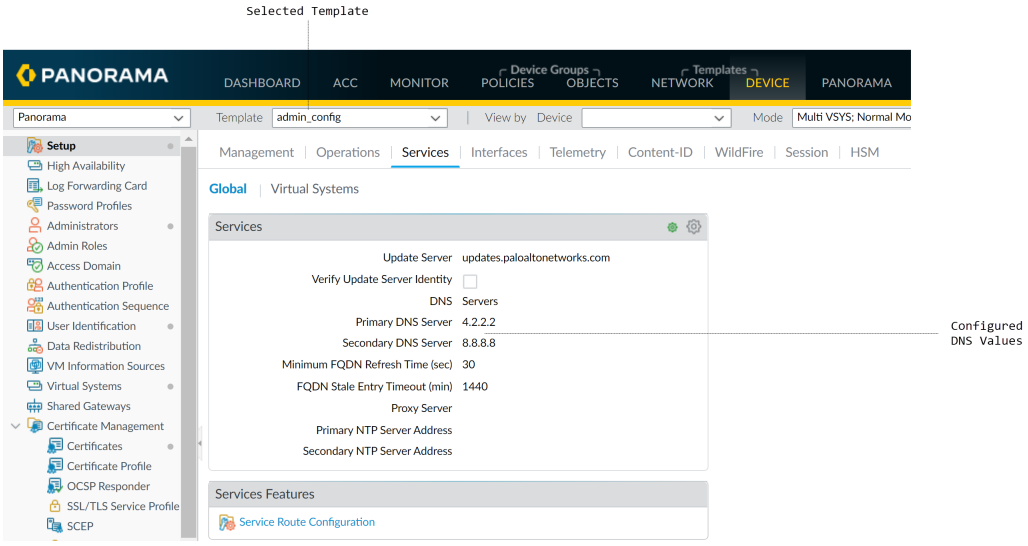
STEP 4 | Utilisez le modèle pour appliquer une modification de la configuration de pare-feu.

Renommer un vsys est autorisé uniquement sur le pare-feu local, pas sur Panorama. Sinon, on obtient un tout nouveau système virtuel ou le mappage du nouveau nom du système virtuel au mauvais système virtuel sur le pare-feu.

Par exemple, définissez un serveur DNS (Domain Name System) principal pour les pare-feu du modèle.

Vous pouvez également Configurer un modèle ou une variable de pile de modèles pour envoyer des valeurs spécifiques au périphérique aux périphériques gérés.

1. Dans l'onglet **Device (Périphérique)**, sélectionnez le **Template (Modèle)** dans la liste déroulante.
2. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Services (Services)** > **Global (Global)** et modifiez la section Services.
3. Saisissez une adresse IP pour le **Primary DNS Server (serveur DNS principal)**.

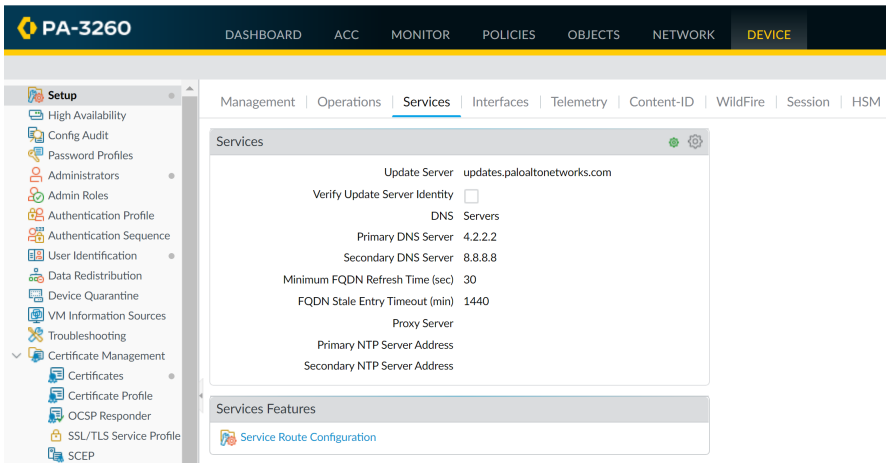


© 2020 Palo Alto Networks, Inc.

4. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)**, puis **Commit and Push (Validez et appliquez)** vos modifications à la configuration Panorama et au modèle.

STEP 5 | Vérifiez que le pare-feu est configuré avec les paramètres de modèle que vous avez appliqués depuis Panorama.

1. Dans la liste déroulante **Context (Contexte)**, sélectionnez un des pare-feu auquel vous avez appliqué le paramètre de modèle.
2. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Services** > **Global**. L'adresse IP que vous avez transmise à partir du modèle s'affiche. L'en-tête de section Services affiche une icône ( ) de modèle pour indiquer que les paramètres de la section possèdent les valeurs transmises à partir d'un modèle.



STEP 6 | Résoudre les problèmes de connectivité aux ressources réseaux pour vérifier que vos pare-feu peuvent accéder à vos ressources réseau.

Configuration d'une pile de modèles

On peut configurer une pile de modèles. Celle-ci vous permet de combiner plusieurs modèles pour transmettre des configurations complètes à vos pare-feu gérés. Bien que les modèles soient des parties modulaires de la configuration de votre pare-feu que vous pouvez réutiliser sur différentes piles, vous pouvez également configurer la pile de modèles pour se substituer aux configurations restantes que vous devez appliquer sur tous les pare-feu affectés à la pile. Panorama prend en charge jusqu'à 1 024 piles de modèles et chaque pile peut contenir jusqu'à 8 modèles. Vous pouvez référencer des objets configurés dans une pile de modèles à partir d'un modèle appartenant à la pile des modèles. Dans le cas où la pile de modèles et un modèle de la pile possèdent des valeurs conflictuelles, c'est la valeur configurée dans la pile de modèles qui sera transmise. Pour plus de détails et de planification, consultez modèles et piles de modèles.

Ajouter un modèle *pour configurer les interfaces, les VLAN, les câbles virtuels, les tunnels IPSec, les proxy DNS et les systèmes virtuels. Ces objets doivent être configurés et transmis à partir d'un modèle, et non d'une pile de modèles. Une fois transmis à partir d'un modèle, vous pouvez remplacer ces objets, à l'exception des systèmes virtuels, dans la pile de modèles.*

STEP 1 | Planifiez des modèles et leur ordre dans la pile.

Ajoutez un modèle que vous prévoyez d'affecter à la pile de modèles.

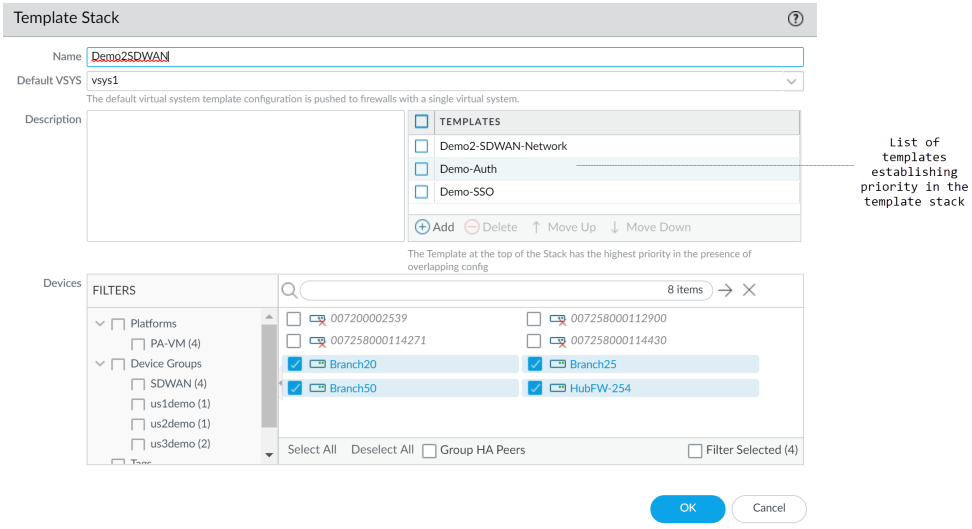
© 2020 Palo Alto Networks, Inc.

Lors de la planification de l'ordre de priorité des modèles dans la pile (pour les paramètres qui se chevauchent), vous devez vérifier l'ordre pour éviter des erreurs de configuration. Par exemple, considérez une pile dans laquelle l'interface ethernet 1/1 est du type couche 3 dans le modèle A, mais une couche de type 2 avec un VLAN dans le modèle B. Si le modèle A a une priorité plus élevée, Panorama va forcer ethernet 1/1 comme un type de couche 3 mais affecté à un VLAN.

À noter également qu'un modèle de configuration ne peut faire référence à une configuration dans un autre modèle, même si les deux modèles sont dans la même pile. Par exemple, une configuration de la zone dans le modèle A ne peut faire référence à un profil de protection en zone de modèle B.

STEP 2 | Créez une pile de modèle.

1. Sélectionnez **Panorama** > **Templates (Modèles)** et cliquez sur **Add Stack (Ajouter une pile)**.
2. Entrez un **Name (Nom)** unique pour identifier la pile.
3. Pour chacun des modèles, la pile va combiner (jusqu'à 8), cliquez sur **Add (Ajouter)** et sélectionnez le modèle. La boîte de dialogue répertorie les modèles ajoutés par ordre de priorité en ce qui concerne les paramètres en double, où les valeurs dans les modèles supérieurs remplacent celles qui sont plus bas dans la liste. Pour modifier l'ordre, vous devez sélectionner un modèle et **Déplacer en haut** ou **Déplacer en bas**.



4. Dans la section périphériques, activez les cases à cocher pour affecter les pare-feux au modèle. Pour les pare-feu avec plusieurs systèmes virtuels, vous ne pouvez pas affecter des systèmes virtuels individuels, seulement un pare-feu entier. Vous pouvez affecter n'importe quel pare-feu à une seule pile de modèles.

   Chaque fois que vous ajoutez un nouveau pare-feu géré à Panorama, vous devez l'affecter à la pile de modèles appropriée. Panorama n'assigne pas automatiquement de nouveaux pare-feu à un modèle ou à une pile de modèles. Lorsque vous appliquez les modifications de configuration à un modèle, Panorama transmet la configuration à chacun des pare-feu affectés au modèle.
5. (Facultatif) Sélectionnez **Group HA Peers (Regrouper les homologues HD)** pour afficher une seule case à cocher pour les pare-feu qui se trouvent dans une configuration de haute disponibilité (HD). Les icônes indiquent l'état HD : vert pour actif et jaune pour passif. Le nom du pare-feu de la paire secondaire est entre parenthèses.

   Pour une paire HD active/passive, ajoutez les deux homologues au même modèle afin que les deux reçoivent les configurations. Pour une paire HD active/active, l'ajout des deux homologues au même

© 2020 Palo Alto Networks, Inc.

modèle dépend de savoir si chaque paire exige les mêmes configurations. Pour obtenir la liste des configurations que PAN-OS synchronise entre paires HD, consultez Synchronisation de Disponibilité Elevée.

6. Cliquez sur **OK** pour sauvegarder la pile de modèle.

STEP 3 | (Optionnel) Configurez un modèle ou une variable de pile de modèles.

STEP 4 | Modifiez les paramètres **Network (Réseau)** et **Device (Périphérique)**, si nécessaire.

Vous n'êtes autorisé à renommer un système virtuel que sur le pare-feu local. Si vous renommez un système virtuel sur Panorama, il en résulte un tout nouveau système virtuel, ou le nom du système virtuel est associé au mauvais système virtuel sur le pare-feu.

Dans un contexte de pare-feu individuel, vous pouvez substituer les paramètres que Panorama applique depuis une pile de la même manière que vous substituez les réglages appliqués depuis d'un modèle : voir Remplacer un modèle ou une variable de pile de modèles.

1. Filtrer les onglets pour afficher uniquement les paramètres spécifiques au mode à modifier :

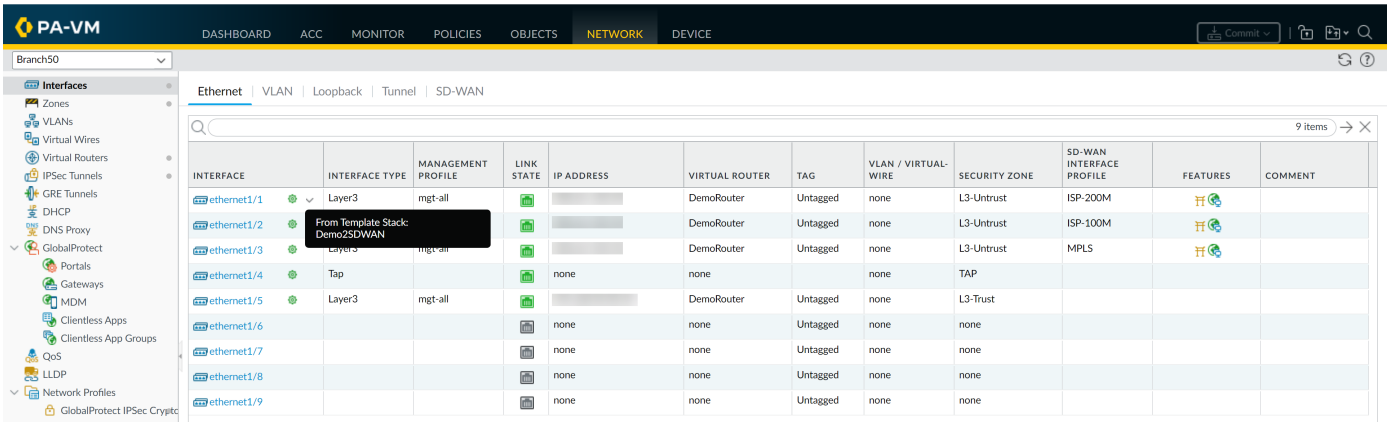
   Tandis que Panorama force des paramètres spécifiques seulement aux pare-feux qui prennent en charge ces modes, cette pression sélective n'ajustera pas les valeurs propres à chaque mode. Par exemple, si un modèle a un pare-feu en mode Federal Information Processing Standards (FIPS) et un profil de IKE Crypto qui utilise des algorithmes non-FIPS, l'application du modèle échouera. Pour éviter ces erreurs, utilisez le menu déroulant Mode dans les onglets Network (Réseau) et Device (Périphérique) pour filtrer les options de valeur et les caractéristiques spécifiques au mode.

   - Dans la liste déroulante **Mode**, activez ou désactivez les options de filtre **Multi VSYS (Multi VSYS)**, **Operational Mode (Mode opérationnel)** et **VPN Mode (Mode VPN)**.
   - Définissez toutes les options de **Mode** afin de tenir compte de la configuration d'un pare-feu en particulier en le sélectionnant dans la liste déroulante **Device (Périphérique)**.
2. Configurez vos interfaces et la connectivité réseau. Par exemple, Configurez les zones et les interfaces pour segmenter votre réseau pour gérer et contrôler le trafic qui traverse votre pare-feu.
3. Modifiez les paramètres si nécessaire.
4. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)**, **Edit Selections (Modifier les sélections)** dans la portée d'application, sélectionnez **Templates (Modèles)**, sélectionnez les pare-feu affectés à la pile de modèles, puis **Commit and Push (Valider et appliquer)** vos modifications à la configuration Panorama et à la pile de modèles.

STEP 5 | Vérifiez que la pile de modèle fonctionne comme prévu.

1. Sélectionnez le modèle ou la pile de modèles dans le menu déroulant **Context (Contexte)**.
2. Sélectionnez un onglet auquel vous avez transmis les modifications de configuration à l'aide de la pile de modèles.
3. Les valeurs extraites de la pile de modèles affichent une icône de modèle ( ) pour indiquer que les paramètres de la section ont des valeurs extraites d'une pile de modèles. Passez votre souris sur la pile pour quelle est la pile de modèles à partir de laquelle la valeur a été poussée.

© 2020 Palo Alto Networks, Inc.



STEP 6 | Résoudre les problèmes de connectivité aux ressources réseaux pour vérifier que vos pare-feu peuvent accéder à vos ressources réseau.

Configurer une variable de modèle ou de pile de modèles

Pour vous permettre de réutiliser plus facilement des modèles ou des piles de modèles, vous pouvez utiliser des variables de pile de modèles et de modèles pour remplacer les adresses IP, les ID de groupe et les interfaces dans vos configurations. Les variables de modèle sont définies au niveau du modèle ou de la pile de modèles, et vous pouvez les utiliser pour remplacer les adresses IP, les plages IP, le FQDN, les interfaces dans les configurations IKE, VPN et HA et les ID de groupe. Les variables définies dans le modèle remplacent les variables définies dans la pile de modèles car les configurations de modèle ont une priorité plus élevée que les configurations de pile de modèles. Les variables vous permettent de réduire le nombre total de modèles et de piles de modèles que vous devez gérer, tout en vous permettant de conserver les valeurs spécifiques au pare-feu ou à l'appareil. Par exemple, si vous disposez d'une pile de modèles avec une configuration de base, vous pouvez utiliser des variables pour créer des valeurs qui ne s'appliquent pas à tous les pare-feu du modèle ou de la pile de modèles. Cela vous permet de gérer et de pousser les configurations à partir de moins de gabarits et de piles de gabarit tout en tenant compte des valeurs spécifiques au pare-feu ou à l'appareil dont vous auriez besoin avant de pouvoir créer un nouveau gabarit ou pile de modèle.

Comment créer un modèle ou une pile de modèles :

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Ajouter un modèle et piles de modèles

1. Ajouter un modèle
2. Configurer une pile de modèle.

STEP 3 | Sélectionner **Panorama** > **Templates (Modèles)** et **Manage (Gérez)** (la colonne des variables) la pile de modèles ou les modèles pour lesquels vous voulez créer une variable.

STEP 4 | **Add (Ajoutez)** la nouvelle variable.

Un nom de variable doit commencer par le symbole de dollar ($).

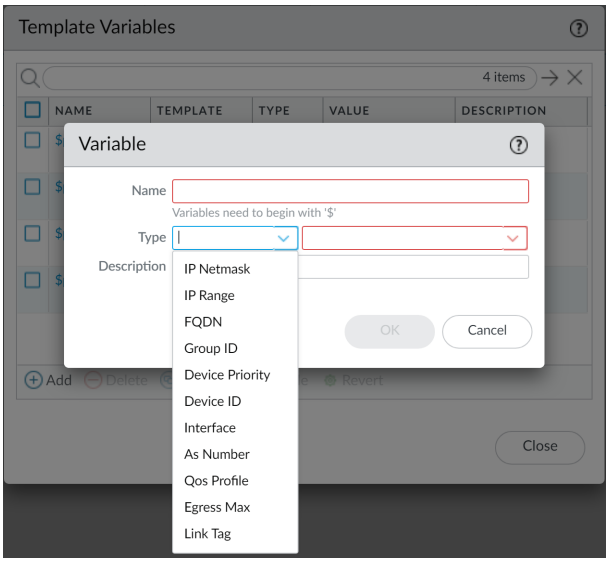
1. Nommez la nouvelle variable. Par exemple, les variables s'appellent `$DNS-primary` et `$DNS-secondary`.
2. Sélectionnez le **Type** de variable et saisissez la valeur correspondante pour le type de variable sélectionné.

© 2020 Palo Alto Networks, Inc.

Pour cet exemple, sélectionnez **IP Netmask**.

3. (Facultatif) Saisissez une Description de la variable.
4. Cliquez sur **OK** et **Close (Fermez)**.

Des variables peuvent également être créées en ligne lorsque les variables sont prises en charge.



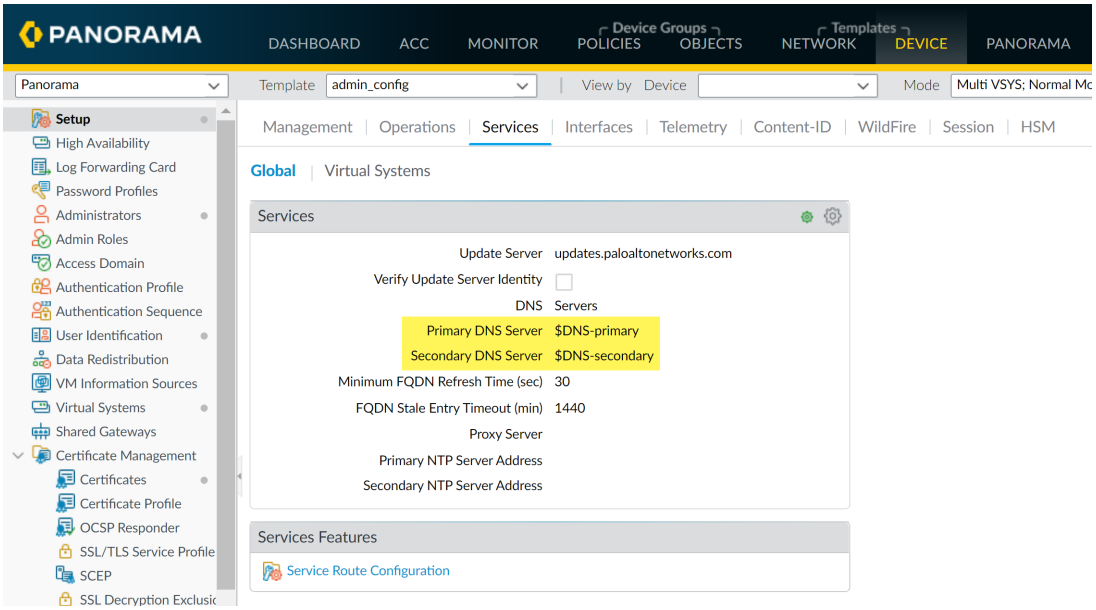
STEP 5 | A partir de la liste déroulante **Template (Modèle)**, sélectionnez le modèle ou la pile de modèles auquel appartient la variable.

STEP 6 | Entrez la variable à l'endroit approprié.

Dans cet exemple, référez-vous à l'ancienne valeur DNS.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Services** et modifiez les services.
2. Saisissez **`$DNS-primary`** ou sélectionnez **Primary DNS Server (Serveur DNS principal)** dans le menu déroulant.
3. Saisissez **$DNS-secondary** ou sélectionnez **Secondary DNS Server (Serveur DNS secondaire)** dans le menu déroulant.
4. Cliquez sur **OK**.

© 2020 Palo Alto Networks, Inc.

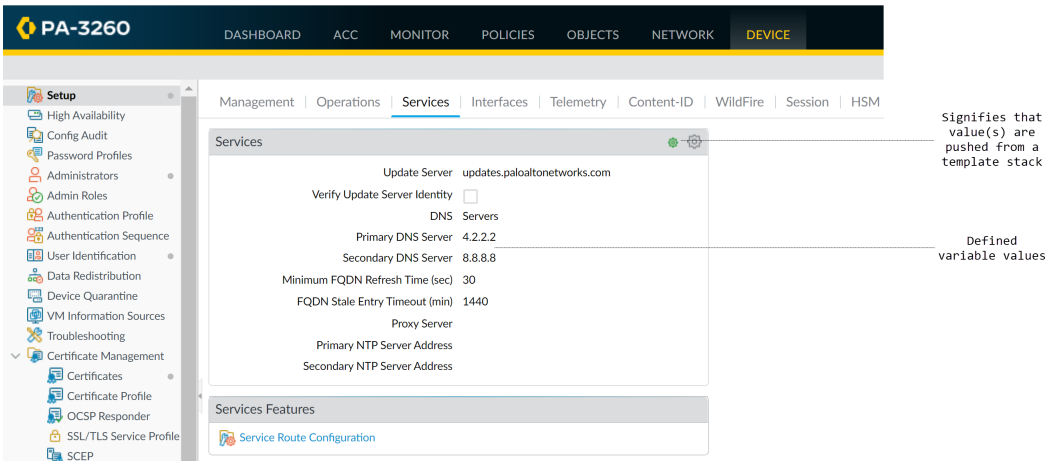


STEP 7 | Cliquez sur **Commit (Valider)** et **Commit and Push (Validez et appliquez)** vos modifications aux pare-feu que vous gérez.

Lorsque vous transmettez une configuration de groupe de périphériques qui contient des références à des variables d'un modèle ou d'une piles de modèles, vous devez Edit Selections (Modifier les sélections) et Include Device and Network Templates (Inclure les modèles de périphériques et de réseaux).

STEP 8 | Vérifiez que les valeurs de toutes les variables ont été transmises aux périphériques gérés.

1. Dans la liste déroulante **Context (Contexte)**, sélectionnez un pare-feu appartenant à la pile de modèles pour laquelle la variable a été créée.
2. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Services**.
3. Les paramètres qui possèdent des valeurs définies par un modèle ou une pile de modèles sont indiqués par le symbole ( ). Passez la souris sur l'indicateur pour afficher le modèle ou la pile de modèles auquel appartient la définition de variable. Lors de l'affichage à partir du contexte du pare-feu, les variables s'affichent en tant qu'adresse IP que vous avez configurée pour la variable.



STEP 9 | Résoudre les problèmes de connectivité aux ressources réseaux pour vérifier que vos pare-feu peuvent accéder à vos ressources réseau.

© 2020 Palo Alto Networks, Inc.

Importer et écraser les variables de la pile de modèles existante

Utilisez les variables des piles de modèles pour remplacer les adresses IP, les plages d'adresses IP, le FQDN, les interfaces ou les ID de groupe de vos configurations de pare-feux. Les variables vous permettent de réduire le nombre total de modèles et de piles de modèles que vous devez gérer, tout en vous permettant de conserver les valeurs spécifiques au pare-feu.

L'importation des variables des piles de modèles vous permet de remplacer les valeurs de plusieurs variables existantes, et vous ne pouvez créer de nouvelles variables de piles de modèles lors de l'importation. Pour obtenir de plus amples renseignements sur la création d'une nouvelle variable de modèle ou de pile de modèles, consultez la section Configurer une variable de modèle ou de pile de modèles.

STEP 1 | Se connecter à l'interface Web Panorama.

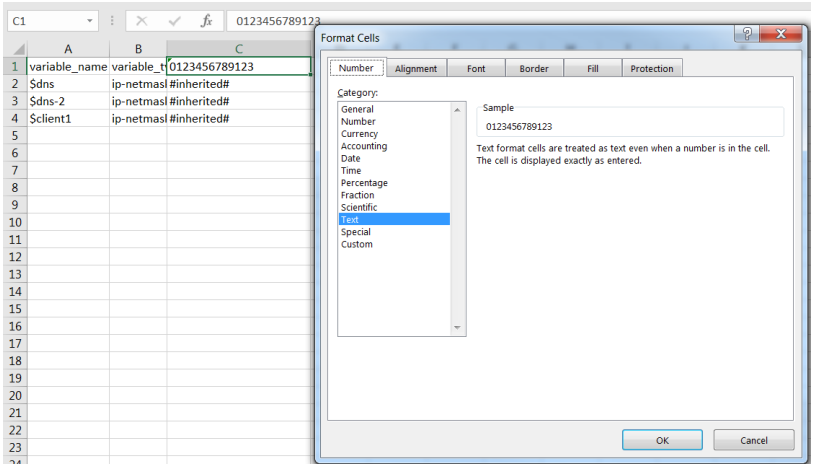
STEP 2 | Exportez les variables existantes d'une pile de modèles.

1. Sélectionnez **Panorama** > **Templates (Modèles)** et sélectionnez un modèle ou une pile de modèles.
2. Sélectionnez **Variable CSV** > **Export (Exporter)**. Les variables de la pile de modèles configurées sont téléchargées localement sous forme de fichier CSV.
3. Ouvrez le CSV exporté.

STEP 3 | Modifiez le fichier CSV contenant les variables de la pile de modèles à importer vers Panorama au format suivant :

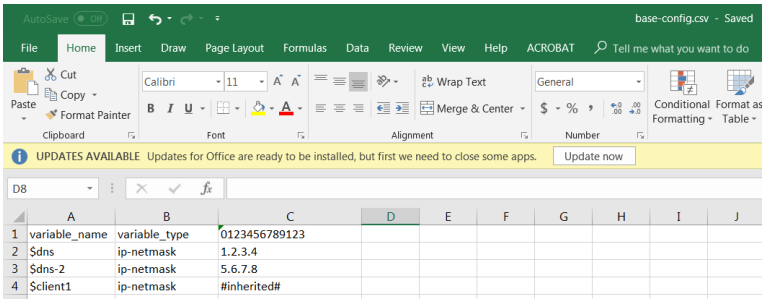
Les valeurs qui s'affichent en tant que `#inherited#` sont des valeurs qui sont définies dans la pile de modèles.

1. Corrigez le nombre de cellules contenant le numéro de série du pare-feu. Répétez cette étape pour tous les pare-feu du fichier CSV.
   1. Double-cliquez sur la cellule contenant le numéro de série du pare-feu, puis sélectionnez **Format Cells (Mettre en forme les cellules)**.
   2. Sélectionnez **Number (Numéro)** > **Text (Texte)**, puis cliquez sur **OK**.
   3. Ajoutez un **0** au début du numéro de série.



2. Saisissez une nouvelle valeur pour la variable du modèle souhaitée.
3. Sélectionnez **File (Fichier)** > **Save As (Enregistrer sous)**, puis enregistrez le fichier au format **CSV UTF-8**.

© 2020 Palo Alto Networks, Inc.



STEP 4 | Importez le fichier CSV vers la pile de modèles.

1. Se connecter à l'interface Web Panorama.
2. Sélectionnez **Panorama** > **Templates (Modèles)** et sélectionnez la pile de modèles pour laquelle vous avez exporté les variables lors de l'étape 2.
3. Sélectionnez **Variable CSV** > **Import (Importer)** et **Browse (Recherchez)** le fichier CSV modifié lors de l'étape 3.
4. Cliquez sur **OK** pour importer les variables de la pile de modèles.

STEP 5 | Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

STEP 6 | Saisissez les variables à l'endroit approprié.

STEP 7 | Cliquez sur **Commit (Valider)** et **Commit and Push (Validez et appliquez)** vos modifications aux pare-feu que vous gérez.

Lorsque vous transmettez une configuration de groupe de périphériques qui contient des références à des variables d'un modèle ou d'une piles de modèles, vous devez Edit Selections (Modifier les sélections) et Include Device and Network Templates (Inclure les modèles de périphériques et de réseaux).

Remplacer un modèle ou une valeur de pile de modèles

Bien que les modèles et les blocs de modèles vous permettent d'appliquer une configuration de base à plusieurs pare-feux, vous pouvez configurer des paramètres spécifiques au pare-feu qui ne s'appliquent pas à tous les pare-feu dans un modèle ou une pile de modèles. Inversement, vous pouvez remplacer les paramètres du modèle pour créer une configuration de pile de modèles que vous pouvez appliquer comme configuration de base à tous vos pare-feu gérés. Le remplacement vous permet de faire des exceptions ou d'apporter des modifications à vos paramètres. Par exemple, si vous utilisez un modèle pour créer une configuration de base mais que quelques pare-feu dans un environnement de laboratoire de test nécessitent des paramètres différents pour l'adresse IP du serveur DNS ou le serveur NTP (Network Time Protocol), vous pouvez remplacer le modèle et la pile de modèles dans les paramètres.

Si vous souhaitez désactiver ou supprimer tous les paramètres de modèle ou de la pile sur un pare-feu au lieu de substituer un paramètre unique, voir Désactiver / supprimer les paramètres du modèle.

Vous pouvez remplacer un modèle ou une piles de modèles de l'"une des façons suivantes :

- Remplacer une valeur de modèle sur un pare-feu ou remplacer un modèle ou une pile de modèles en utilisant des variables : Il existe deux façons de remplacer des valeurs transférées au serveur à partir d'un modèle ou d'une pile de modèles. La première façon est de définir la valeur localement sur le pare-feu pour remplacer la valeur transférée au serveur à partir d'un modèle ou d'une pile de modèles. La

© 2020 Palo Alto Networks, Inc.

seconde façon est de définir une variable spécifique au pare-feu pour remplacer les variables qui ont été envoyées à partir d'un modèle ou d'une pile de modèles.

- Remplacer une valeur de modèle en utilisant une pile de modèles : Définir les valeurs ou les variables sur la pile de modèles et remplacer les valeurs qui ont été envoyées à partir d'un modèle.

Remplacer une valeur de modèle sur le pare-feu

Remplacer un paramètre sur le pare-feu local qui a été transmis à partir d'un modèle ou d'une pile de modèles pour créer des configurations spécifiques au pare-feu. Cela vous permet de gérer la configuration du modèle de base ou de la pile de modèles à partir de Panorama™, tout en conservant les configurations spécifiques au pare-feu qui ne s'appliquent pas aux autres pare-feu.

STEP 1 | Accédez à l'interface Web du pare-feu.

Accédez directement au pare-feu en entrant son adresse IP dans le champ URL de votre navigateur ou utilisez la liste déroulante **Context (contexte)** dans Panorama pour basculer vers le contexte de pare-feu.

STEP 2 | Remplacez une valeur transmise par un modèle ou une pile de modèles.

Dans cet exemple, vous remplacerez l'adresse IP du serveur DNS que vous avez attribuée en utilisant un modèle dans Ajouter un modèle.

1. Sélectionnez **Device (Périphérique)** > **Setup (Paramètres)** > **Services** et modifiez la section Services.
2. Cliquez sur l'îcone du modèle( ) pour que le **Primary DNS Server (serveur DNS principal)** active les remplacements pour ce champ.
3. Saisissez une nouvelle adresse IP pour le **Primary DNS Server (serveur DNS principal)**. Un symbole de remplacement du modèle ( ) indique que la valeur du modèle a été remplacée.
4. Cliquez sur **OK (OK)** et sur **Commit (Valider)** pour enregistrer vos modifications.

Remplacer une valeur d'un modèle à l'aide d'une pile de modèles

Vous pouvez utiliser les valeurs d'une pile de modèles pour remplacer les configurations envoyées au pare-feu à partir d'un modèle, pour créer une configuration d'une pile de modèles que vous pouvez utiliser pour gérer la configuration de base de vos pare-feu gérés depuis Panorama ™. Cela vous permet de tirer parti des capacités de gestion de Panorama pour transmettre les modifications de configuration à plusieurs périphériques à partir d'un seul emplacement. Dans cet exemple, vous utiliserez une pile de modèles pour remplacer la variable d'adresse IP du serveur DNS principal appelée `$DNS` qui a été extraite d'un modèle.

Panorama peut utiliser une pile de modèles pour remplacer les interfaces configurées dans un modèle sauf pour les sous-interfaces Layer2 d'une interface agrégée.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | A partir de la liste déroulante **Template (Modèle)** sélectionnez la pile de modèles qui remplacera la configuration du modèle.

STEP 3 | Remplacez la configuration du modèle transmise.

1. Sélectionnez **Device (Périphérique)** > **Setup (Paramètres)** > **Services** et modifiez la section Services.
2. Configurez le **Primary DNS (DNS principal)** avec l'adresse IP pour remplacer la configuration de modèle transmis et cliquez sur **OK**.

STEP 4 | **Commit and Push (Validez et appliquez)** les modifications de configuration.

© 2020 Palo Alto Networks, Inc.

Remplacer une valeur de modèle à l'aide d'une variable de pile de modèles

Vous pouvez utiliser les valeurs et les variables d'une pile de modèles pour remplacer les configurations envoyées au pare-feu à partir d'un modèle, pour créer une configuration d'une pile de modèles que vous pouvez utiliser pour gérer la configuration de base de vos pare-feu gérés depuis Panorama ™. Cela vous permet de tirer parti des capacités de gestion de Panorama pour transmettre les modifications de configuration à plusieurs pare-feu à partir d'un seul emplacement. Dans cet exemple, vous créez une pile de modèles pour remplacer la variable d'adresse IP du serveur DNS principal appelée `$DNS` qui a été extraite d'un modèle.

Panorama peut utiliser une pile de modèles pour remplacer les interfaces configurées dans un modèle sauf pour les sous-interfaces Layer2 d'une interface agrégée*.*

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Remplacer la variable de modèle.

1. Sélectionnez **Panorama** > **Templates (Modèles)**.
2. **Manage (Gérez)** (colonne Variables) la pile de modèles contenant la variable du modèle que vous devez remplacer.
3. Trouvez et sélectionnez la variable **$DNS**.
4. Sélectionnez **Override (Remplacer)**.
5. Saisissez une nouvelle valeur de variable, puis cliquez sur **OK**.

STEP 3 | **Commit and Push (Validez et appliquez)** vos modifications.

Remplacer une valeur d'un modèle ou d'une pile de modèles à l'aide de variables

Vous pouvez utiliser des variables spécifiques au pare-feu pour remplacer les variables transmises au pare-feu géré à partir d'un modèle ou d'une pile de modèles pour créer des configurations spécifiques au pare-feu. Cela vous permet de gérer la configuration de base du modèle ou de la pile de modèles tout en conservant les configurations spécifiques au pare-feu qui ne s'appliquent pas aux autres pare-feu. Vous pouvez faire tout cela depuis Panorama™. Cela vous permet de tirer parti des capacités de gestion de Panorama tout en tenant compte des configurations spécifiques requises pour les pare-feu individuels. Dans cet exemple, la variable de l'adresse IP du serveur DNS principal appelée `$DNS` qui a été extraite d'un modèle sera remplacée pour créer une variable spécifique au pare-feu.

Vous pouvez remplacer les variables de modèle ou de piles de modèles qui n'ont pas été remplacées. Si une variable d'un modèle ou d'une pile de modèles à déjà été substituée, Revert (Rétablissez) cette substitution pour créer une variable spécifique au pare-feu.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Remplacez la variable du modèle ou de la pile de modèles.

1. Sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)** > **Summary (Récapitulatif)**.
2. **Edit (Modifiez)** (colonne Variables) le pare-feu contenant la variable que vous devez remplacer.
3. Trouvez et sélectionnez la variable **$DNS**.
4. Sélectionnez **Override (Remplacer)**.
5. Entrez la nouvelle adresse IP propre au pare-feu et cliquez sur **OK**.

STEP 3 | **Commit and Push (Validez et appliquez)** vos modifications.

© 2020 Palo Alto Networks, Inc.

Désactiver/supprimer les paramètres de modèle

Si vous souhaitez cesser d'utiliser un modèle ou une pile de modèle pour la gestion de la configuration sur un pare-feu géré, vous pouvez désactiver le modèle ou la pile. Pour désactiver, vous pouvez copier les valeurs de modèle/pile à la configuration locale du pare-feu ou supprimer les valeurs.



Si vous voulez substituer un paramètre unique au lieu de désactiver ou supprimer chaque paramètre de modèle ou de la pile, consultez substituer un paramètre de modèle*.*

Consultez les modèles et les piles de modèles *pour plus de détails sur la façon de les utiliser pour gérer les pare-feu.*

STEP 1 | Accéder à l'interface web du pare-feu géré en tant qu'administrateur avec le rôle de super-utilisateur. Vous pouvez accéder directement au pare-feu en entrant son adresse IP dans le champ d'adresse URL du navigateur ou, dans Panorama, sélectionnez le pare-feu dans la liste déroulante **Context (Context)**.

STEP 2 | Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les paramètres de Panorama.

STEP 3 | Cliquez sur **Disable Device and Network Template** (désactiver le périphérique et le modèle de réseau).

STEP 4 | (Facultatif) Sélectionnez **Import Device and Network Template before disabling (Importer le modèle de réseau et de périphériques avant la désactivation)** pour enregistrer les paramètres de configuration en local sur le pare-feu. Si vous ne sélectionnez pas cette option, PAN-OS supprimera tous les paramètres transmis à Panorama à partir du pare-feu.

STEP 5 | Cliquez deux fois sur **OK**, puis **Commit (validez)** les modifications.

© 2020 Palo Alto Networks, Inc.

Gérer la clé principale de Panorama

Panorama, les pare-feu, les collecteurs de journaux et les appareils WF-500 utilisent une clé principale pour chiffrer les éléments de nature délicate de la configuration. Ils disposent d'une clé principale par défaut qu'ils utilisent pour chiffrer les mots de passe et les éléments de configuration.

Dans le cadre d'une pratique de sécurité standard, vous devriez remplacer la clé principale par défaut et changer la clé sur chaque pare-feu, collecteur de journaux, appareil WildFire et Panorama avant son expiration. Vous devez déployer la même clé principale sur tous vos périphériques gérés et vous devez configurer la clé principale sur Panorama pour transmettre avec succès la configuration de Panorama à vos périphériques gérés. Pour garantir le déploiement uniforme des clés, déployez une nouvelle clé principale ou renouvelez une clé principale venant à expiration sur plusieurs pare-feu, collecteurs de journaux et appareils WF-500 directement à partir de Panorama. Reportez-vous à la rubrique Configuration de la clé principale pour obtenir de plus amples informations sur la configuration d'une clé principale.

STEP 1 | Se connecter à l'interface Web Panorama.

STEP 2 | (Pratique exemplaire) Sélectionnez **Commit (Valider)** et **Commit and Push (Validez et appliquez)** les modifications apportées à la configuration qui sont en attente.

Panorama doit chiffrer de nouveau les données à l'aide de la nouvelle clé principale. Pour veiller à ce que tous les éléments de configuration soient chiffrés avec la nouvelle clé principale, vous devriez valider toutes les modifications en attente avant de déployer la nouvelle clé principale.

STEP 3 | Configurez la clé principale du pare-feu, du collecteur de journaux et de l'appareil WildFire pour qu'elle se renouvelle automatiquement à son expiration.

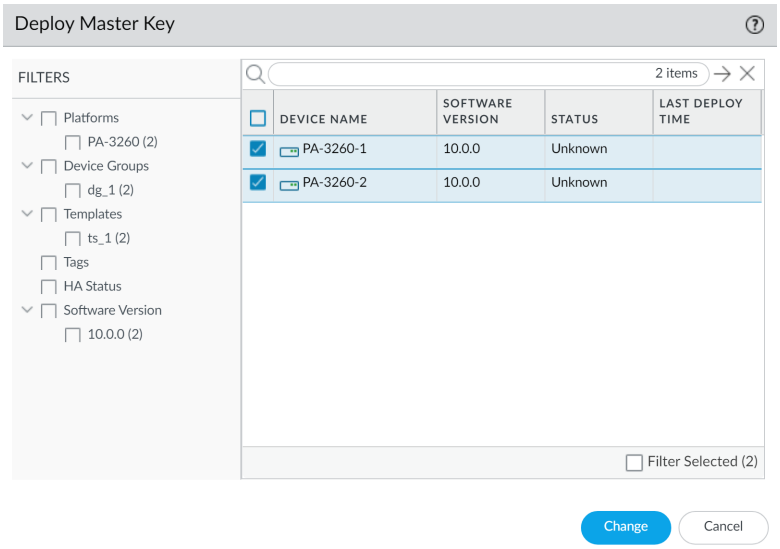
Le renouvellement automatique de la clé principale vous permet de préserver le chiffrement de votre configuration en cas d'expiration de la clé avant une période de maintenance. Il ne s'agit toutefois pas d'un remplacement au déploiement d'une nouvelle clé principale à l'expiration de la clé. Tenez compte du nombre de jours avant votre prochaine fenêtre de maintenance disponible lors de la configuration du renouvellement automatique de la clé principale après l'expiration de la durée de vie de la clé.

1. Sélectionnez **Device (Périphérique)** > **Master Key and Diagnostics (Clé principale et diagnostics)**, puis modifiez la section Master Key (Clé principale).
2. Configurez Panorama pour qu'il procède au **Auto Renew with Same Master Key (renouvellement automatique avec la même clé principale)** pendant un nombre de jours ou d'heures indiqués.

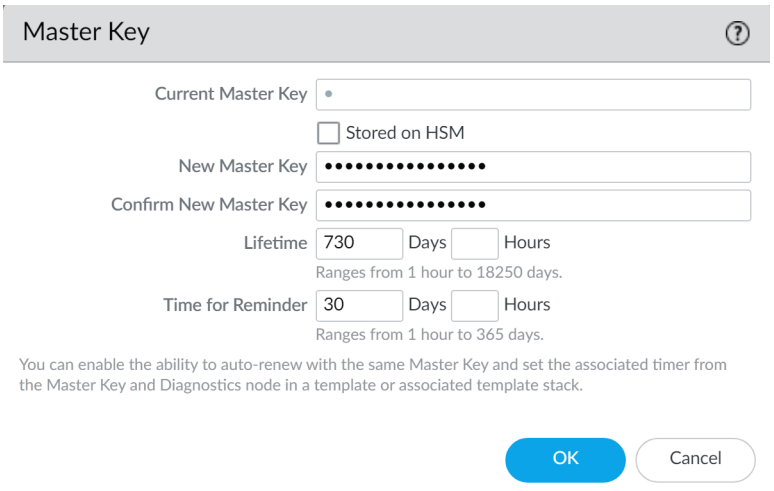
STEP 4 | Déployez la clé principale aux pare-feu gérés.

1. Sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)** > **Summary (Récapitulatif)**, puis **Deploy Master Key (Déployez la clé principale)**.
2. Sélectionnez tous les périphériques, puis **Change (Modifiez)** la clé principale.

© 2020 Palo Alto Networks, Inc.



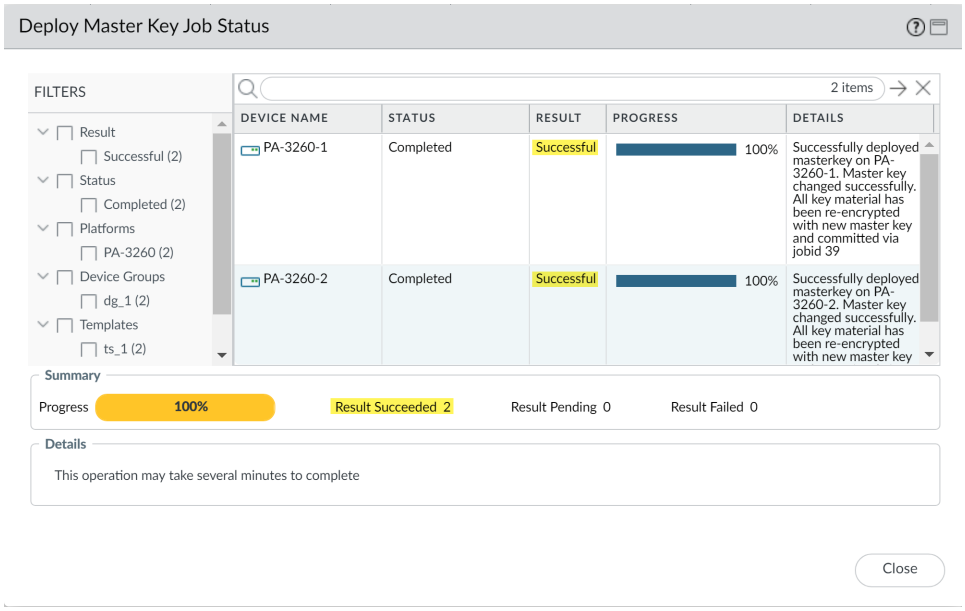
3. Configurez la clé principale :
    1. Si vous renouvelez une clé principale, saisissez la **Current Master Key (Clé principale actuelle)**. Si vous remplacez la clé principale par défaut par une nouvelle clé principale, n'indiquez pas de **Current Master Key (Clé principale actuelle)**.
    2. Précisez la **New Master Key (Nouvelle clé principale)** et **Confirm Master Key (Confirmez la clé principale)**.
    3. Configurez la **Lifetime (Durée de vie)** de la clé principale et la **Time for Reminder (Durée du rappel)**.
    4. Cliquez sur **OK**.



4. Vérifiez que la clé principale a été déployée avec succès à tous les périphériques sélectionnés.

    Un journal système est généré lorsque vous déployez une nouvelle clé principale à partir de Panorama.

© 2020 Palo Alto Networks, Inc.



STEP 5 | Déployez la clé principale aux collecteurs de journaux. La clé principale doit être identique à la clé déployée à l'étape 3.

1. Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)**, puis **Deploy Master Key (Déployer la clé principale)**.
2. Sélectionnez tous les périphériques, puis **Change (Modifiez)** la clé principale.
3. Configurez la clé principale :
    1. Si vous renouvelez une clé principale, saisissez la **Current Master Key (Clé principale actuelle)**. Si vous remplacez la clé principale par défaut par une nouvelle clé principale, n'indiquez pas de **Current Master Key (Clé principale actuelle)**.
    2. Précisez la **New Master Key (Nouvelle clé principale)** et **Confirm Master Key (Confirmez la clé principale)**.
    3. Configurez la **Lifetime (Durée de vie)** de la clé principale et la **Time for Reminder (Durée du rappel)**.
    4. Cliquez sur **OK**.
4. Vérifiez que la clé principale a été déployée avec succès à tous les périphériques sélectionnés.

    Un journal système est généré lorsque vous déployez une nouvelle clé principale à partir de Panorama.

STEP 6 | Déployez la clé principale aux appareils WildFire gérés. La clé principale doit être identique à la clé déployée à l'étape 3.

1. Sélectionnez **Panorama** > **Managed WildFire appliances (appareils WildFire gérés)**, puis **Deploy Master Key (Déployer la clé principale)**.
2. Sélectionnez tous les périphériques, puis **Change (Modifiez)** la clé principale.
3. Configurez la clé principale :
    1. Si vous renouvelez une clé principale, saisissez la **Current Master Key (Clé principale actuelle)**. Si vous remplacez la clé principale par défaut par une nouvelle clé principale, n'indiquez pas de **Current Master Key (Clé principale actuelle)**.
    2. Précisez la **New Master Key (Nouvelle clé principale)** et **Confirm Master Key (Confirmez la clé principale)**.
    3. Configurez la **Lifetime (Durée de vie)** de la clé principale et la **Time for Reminder (Durée du rappel)**.

© 2020 Palo Alto Networks, Inc.

4. Cliquez sur **OK**.

4. Vérifiez que la clé principale a été déployée avec succès à tous les périphériques sélectionnés.

   Un journal système est généré lorsque vous déployez une nouvelle clé principale à partir de Panorama.

STEP 7 | Configurez la clé principale sur Panorama. La clé principale doit être identique à la clé déployée sur les pare-feu, les collecteurs de journaux et les appareils WildFire aux étapes 3 à 5.

1. Sélectionnez **Panorama** > **Master Key and Diagnostics (Clé principale et diagnostics)**, puis configurez la clé principale.
   1. Si vous renouvelez une clé principale, saisissez la **Current Master Key (Clé principale actuelle)**. Si vous remplacez la clé principale pas défaut par une nouvelle clé principale, n'indiquez pas de **Current Master Key (Clé principale actuelle)**.
   2. Configurez la **New Master Key (Nouvelle clé principale)** et **Confirm Master Key (Confirmez la clé principale)**.
   3. Configurez la **Lifetime (Durée de vie)** de la clé principale et la **Time for Reminder (Durée du rappel)**.
   4. Cliquez sur **OK**.
2. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

© 2020 Palo Alto Networks, Inc.

Configurer Entreprise Data Loss Prevention (prévention des pertes de données - DLP)

Appliquez les normes de sécurité des données de votre organisation afin d'éviter une mauvaise utilisation accidentelle des données ou un vol avec Entreprise Data Loss Prevention (prévention des pertes de données - DLP).

- Aperçu d'Entreprise Data Loss Prevention (prévention des pertes de données - DLP)
- Avec quoi Data Loss Prevention (prévention des pertes de données - DLP) Enterprise est-il compatible ?
- Profils prédéfinis de filtrage des données
- Installer le plug-in Entreprise Data Loss Prevention (prévention des pertes de données - DLP)
- Créer un modèle de données.
- Création d'un profil de filtrage des données
- Activez Enterprise Data Loss Prevention (prévention des pertes de données - DLP)
- Affichez les détails des journaux Enterprise Data Loss Prevention (Prévention des pertes de données - DLP)
- Modifier les paramètres de Enterprise Data Loss Prevention (prévention des pertes de données - DLP)
- Activer les Modèles de données et les Profils de filtrage existants
- Désinstaller le plug-in Entreprise Data Loss Prevention (prévention des pertes de données - DLP)

Aperçu d'Entreprise Data Loss Prevention (prévention des pertes de données - DLP)

Data Loss Prevention (prévention des pertes de données - DLP) est un ensemble d'outils et de processus qui vous permettent de protéger les informations sensibles de tout accès, mauvaise utilisation, extraction ou partage non autorisés. Le plug-in DLP est installé sur le serveur de gestion Panorama où vous pouvez gérer de façon centralisée les modèles de données et les profils de filtrage des données qui appliquent les normes de sécurité des données de votre entreprise et éviter la perte de données sensibles venant des utilisateurs mobiles et des réseaux à distance pour vos pare-feux gérés. Les modèles de données et les profils de filtrage des données sont conçus pour fonctionner sur tous les modèles de Panorama et de pare-feux utilisant PAN-OS 10.0.2 et les versions ultérieures afin de fournir une sécurité des données homogène sur tous les sites et emplacements. Afin d'exploiter Enterprise DLP, Panorama et les pare-feux gérés doivent être connectés à internet.

Enterprise DLP est un service basé sur le cloud qui utilise des algorithmes d'apprentissage machine supervisés afin de classer les documents en Financier, Juridique, Soins de santé et autres catégories de classification de documents afin de les protéger des expositions, pertes de données et exfiltration de données. Ces modèles peuvent identifier les informations dans le trafic passant sur votre réseau et les protéger de toute exposition.

Enterprise DLP vous permet de protéger les données sensibles avec les méthodes suivantes :

- **Empêche les téléchargements de fichiers de fuiter vers une application web non approuvée** : découvrez et mettez un arrêt conditionnel à la fuite de données sensibles vers des applications web non approuvées.
- **Surveille les téléchargements vers les applications web approuvées** : découvrez et surveillez les données sensibles lorsqu'elles sont téléchargées sur des applications d'entreprise approuvées.

Pour vous aider à inspecter le contenu et à analyser les données dans le contexte approprié afin d'identifier avec précision les données sensibles et de les sécuriser pour éviter les incidents, Enterprise DLP est activé via un service cloud. Enterprise DLP est compatible avec plus de 380 modèles de données et de nombreux profils de filtrage des données prédéfinis. Enterprise DLP est conçu pour mettre à votre disposition

© 2020 Palo Alto Networks, Inc.

automatiquement les nouveaux modèles et profils afin de les utiliser dans les règles de politique de sécurité dès qu'ils sont ajoutés au service cloud. Utilisez les outils suivants pour configurer Enterprise DLP :

- Data Patterns (Modèles de données) : vous aident à détecter le contenu sensible et la façon dont ce contenu est partagé ou consulté sur votre réseau.

  Les modèles de données prédéfinis et les paramètres intégrés vous permettent de protéger facilement les fichiers qui contiennent certaines propriétés de fichier (comme le titre du document ou son auteur), les numéros de carte de crédit, les informations réglementées de différents pays (comme les numéros de permis de conduire) et les étiquettes DLP d'outils tiers. Afin d'améliorer les taux de détection des données sensibles dans votre entreprise, vous pouvez ajouter des modèles de données prédéfinis en créant des modèles de données personnalisés qui sont spécifiques à votre inspection du contenu et à vos exigences en matière de protection des données. Dans un modèle de données personnalisé, vous pouvez aussi définir des expressions régulières et des propriétés de fichier afin de rechercher des métadonnées ou des attributs dans les propriétés personnalisées ou étendus du fichier et les utiliser dans un profil de filtrage de données.
- Data Filtering Profiles (Profils de filtrage de données) : Améliorent la classification des données et surveillent les capacités disponibles sur vos pare-feux gérés afin d'empêcher la perte de données et réduire le risque métier.

  Les profils de filtrage des données sont une collection de modèles de données qui sont regroupés afin de rechercher un objet ou un type de contenu spécifique. Afin d'effectuer l'analyse de contenu, les predefined data filtering profiles (profils de filtrage des données prédéfinis) ont des modèles de données incluant des identifiants de données, des mots clés standards dans le secteur d'activité et une logique intégrée sous forme d'apprentissage machine, des expressions régulières et des sommes de contrôle pour les modèles de données financiers et juridiques. Lorsque vous utilisez le profil de filtrage des données dans une règle de politique de sécurité, le pare-feu peut inspecter le trafic à la recherche d'une correspondance et effectuer une action.

  Après avoir utilisé les modèles de données (prédéfinis ou personnalisés), vous gérez les profils de filtrage des données depuis Panorama. Vous pouvez utiliser un profil de filtrage des données prédéfini ou créer un nouveau profil et lui ajouter des modèles de données. Vous pouvez ensuite créer des security policies (politiques de sécurité) et appliquer les profils que vous avez ajoutés aux politiques que vous créez. Si un utilisateur télécharge un fichier et que les données du fichier correspondent aux critères des politiques, le pare-feu géré crée une notification d'avertissement ou bloque le téléchargement de fichier.

Lorsque vous appliquez un profil de filtrage des données à une règle de politique de sécurité, le pare-feu géré génère un data filtering log (journal de filtrage des données) contenant les informations détaillées au sujet du trafic qui correspond à un ou plusieurs modèles de données dans le profil de filtrage des données. Les détails du journal active Forensics (Investigation numérique) en vous permettant de vérifier pourquoi un fichier téléchargé a généré une notification d'avertissement ou a été bloqué.

Vous consultez les fragments de données dans les journaux de filtrage des données. Par défaut, les pare-feux gérés utilisent un masquage des données afin de masquer partiellement les fragments pour éviter que les données sensibles soient exposées. Vous pouvez configurer vos pare-feux gérés afin de complètement masquer les informations sensibles, ne pas masquer les fragments ou désactiver l'extraction et l'affichage de fragments de données.

Afin d'améliorer la précision de la détection et de réduire les faux positifs, vous pouvez également spécifier :

- **Proximity keywords (Mots clé de proximité)** : un actif se voit assigner une probabilité de précision supérieure lorsqu'un mot clé se trouve à une distance inférieure à 200 caractères de l'expression. Si un document a un numéro à 16 chiffres immédiatement suivi par `Visa`, il est plus que probable qu'il s'agisse d'un numéro de carte de crédit. Mais si Visa est le titre du texte et que le numéro à 16 chiffres se trouve sur la dernière page d'un document de 22 pages, il est peu probable que ce soit un numéro de carte de crédit.

© 2020 Palo Alto Networks, Inc.

Vous pouvez aussi utiliser plus d'un mot clé dans un groupe de mots clés et inclure ou exclure des mots clés afin de trouver quand les occurrences de mots spécifiques apparaissent ou n'apparaissent pas dans les 200 caractères d'une expression.

- **Confidence levels (Niveaux de confiance)** : En plus des mots clés de proximité, les niveaux de confiance vous permettent de préciser la probabilité de l'occurrence des mots clés de proximité dans une correspondance de modèle. Lorsque le niveau de confiance est **Low (Faible)** le pare-feu géré n'utilise pas les mots clés de proximité pour identifier une correspondance ; avec un niveau de confiance **High (Elevé)** le pare-feu géré recherche les mots clés de proximité dans les 200 caractères des expressions régulières dans le modèle avant d'envisager que le modèle de données dans un fichier ne soit une correspondance.
- **Basic and weighted regular expressions (expressions régulières de base et pondérées)** : une expression régulière (abrégée en regex) décrit la façon de rechercher un modèle de texte spécifique puis d'afficher les occurrences de correspondance lorsqu'une correspondance de modèle est localisée. Il existe deux types d'expressions régulières :*basic (de base)* et *weighted (pondérées)*.
  - Une **basic regular expression (expression régulière de base)** recherche un modèle de texte spécifique. Lorsqu'un modèle est localisé, le service affiche les occurrences de correspondance.
  - Une **weighted regular expression (expression régulière pondérée)** attribue un score à une saisie de texte. Lorsque le seuil du score est dépassé, le service renvoie une correspondance pour le modèle.

    Pour réduire les faux positifs et rentabiliser la performance de recherche de vos expressions régulières, vous pouvez attribuer des scores à l'aide de la fonction de construction d'une expression régulière pondérée lorsque vous create data patterns (Créez des modèles de données) afin de localiser et calculer les scores pour les informations qui sont importantes pour vous. L'attribution de score applique un seuil de correspondance et lorsqu'un seuil de score est dépassé, comme lorsque suffisamment d'expressions d'un modèle correspondent à un actif, cet actif sera indiqué comme étant une correspondance pour le modèle.

    Pour plus d'informations, y compris un cas d'utilisation et les bonnes pratiques, consultez Configure Regular Expressions (Configurer les expressions régulières) dans le Guide de l'administrateur de Prisma SaaS.

Avec quoi Data Loss Prevention (prévention des pertes de données - DLP) Enterprise est-il compatible ?

Enterprise Data Loss Prevention (DLP) est compatible avec tous les pare-feux basés sur du matériel et les pare-feux virtuels VM-Series sauf les pare-feux de la CN-Series fonctionnant sur PAN-OS 10.0.2 ou des versions ultérieures utilisant la version de contenu des Applications et Menaces minimum 8334-6362.

Voici les applications compatibles et les paramètres opérationnels que vous pouvez utiliser avec Data Loss Prevention (prévention des pertes de données - DLP) Entreprise.

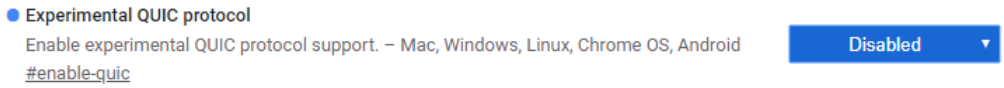
Application Web	PDF	doc/docx	ppt/pptx	xls/xlsx	rtf	Csv	Télécharge multiples	Taille du fichier
Navigation web	Oui	Oui	Oui	Oui	Oui	Oui	Oui	20MB
Application web Onedrive	Oui	Oui	Oui	Oui	Oui	Oui	Oui	20MB
Application web Sharepoint	Oui	Oui	Oui	Oui	Oui	Oui	Oui	20MB

© 2020 Palo Alto Networks, Inc.

Application Web	PDF	doc/docx	ppt/pptx	xls/xlsx	rtf	Csv	Télécharge multiples	Taille du fichier
Application web Gmail	Oui	Oui	Oui	Oui	Oui	Oui	Oui	20MB
Application web Box	Oui	Oui	Oui	Oui	Oui	Oui	Oui	20MB
Application web Slack	Oui	Oui	Oui	Oui	Oui	Oui	Oui	20MB

- **Applications** : vous pouvez appliquer DLP aux téléchargements basés sur le web (basés sur HTTP ou HTTPS) pour les applications suivantes :
  - Box (l'ID de l'application est boxnet-uploading)
  - Gmail (l'ID de l'application est gmail-uploading)

    Pour utiliser Gmail, vous devez désactiver le protocole QUIC. Palo Alto Networks conseille de désactiver QUIC dans Chrome. Pour faire cela, tapez `chrome://flags/` dans la barre d'URL de Chrome, localisez Experimental QUIC Protocol, et sélectionnez Disabled (désactivé).

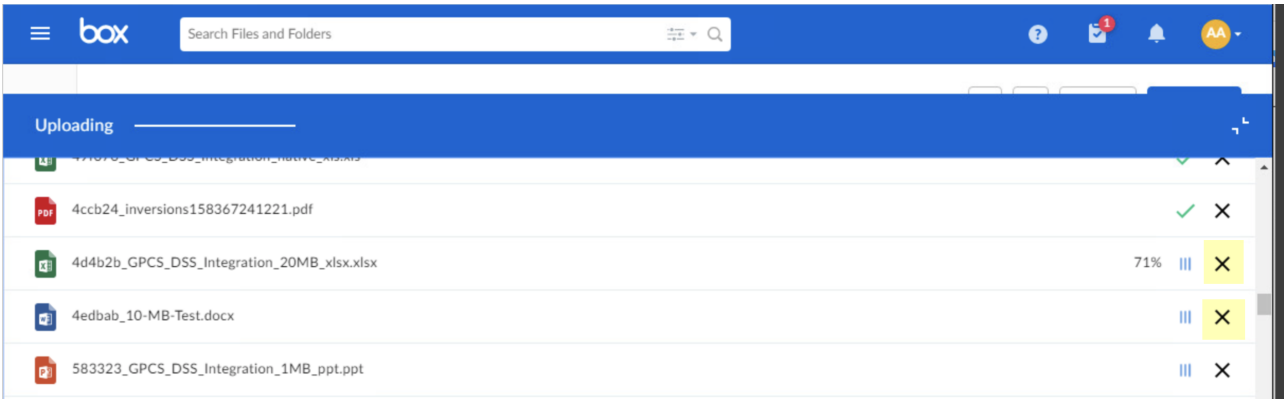
    

  - Microsoft OneDrive (l'ID de l'application est sharepoint-online-uploading)
  - Microsoft SharePoint (l'ID de l'application est sharepoint-online-uploading)
  - Slack (l'ID de l'application est slack-uploading)
  - Navigation Web (l'ID de l'application est web-browsing)
- **Opérations sur fichiers** : vous pouvez télécharger des fichiers via HTTP et HTTPS (mais pas FTP ni SMTP) en utilisant HTTP/1.1.

  Certaines applications, comme SharePoint et OneDrive, utilisent HTTP/2 par défaut. Pour utiliser des fichiers HTTP/2 avec HTTP/1.1, vous devez créer un profil de déchiffrement et une politique de sécurité pour supprimer les en-têtes ALPN. Pour plus d'informations, reportez-vous à la section Activez Enterprise Data Loss Prevention (prévention des pertes de données - DLP) *.*
- **Data flow (flux de données)** : les mises en téléchargement de fichiers sont possibles (les téléchargements ne sont pas possibles).
- **Concurrent file uploads (téléchargements simultanés de fichiers)** : il est possible de mettre en téléchargement simultané jusqu'à 25 fichiers.
- **File size (taille des fichiers)** : jusqu'à 20 MB de fichiers.

  Si vous utilisez Box pour mettre en téléchargement plusieurs fichiers simultanément et qu'un ou plusieurs fichiers fait plus de 20 MB, le téléchargement de tous les fichiers ne se fera pas. Pour continuer, localisez les fichiers dans Box qui font plus de 20 MB et cliquez sur **X** pour arrêter la mise en téléchargement de ces fichiers.

© 2020 Palo Alto Networks, Inc.



- **File types (types de fichiers)** : Microsoft Office (.doc, .docx, .ppt, .pptx, .xls, .xlsx) .csv, .pdf, et .rtf.
- **Response (Réponse)** : Les actions de blocage et d'alerte sont compatibles avec les fichiers HTTP et HTTPS. La page de Blocage n'affiche pas le nom du fichier que le pare-feu a bloqué.
- **Data Patterns and Data Filtering Profiles (Modèles de données et Profils de filtrage des données)**— Utilisez des modèles de données et des profils de filtrage des données prédéfinis ou créez vos propres modèles de données et profils de filtrage de données. Le clonage de modèles de données n'est actuellement pas possible ; cependant, vous pouvez cloner des profils de filtrage des données prédéfinis si vous souhaitez ajouter, supprimer ou modifier des identifiants de données dans le profil existant.

  Pour chaque profil de filtrage des données, Entreprise DLP autorise un maximum de 10 modèles de données pour une règle de blocage et 50 modèles de données pour une règle d'alerte.

  Les modèles de données prédéfinis utilisent l'apprentissage machine ou une détection basée sur regex (expressions régulières) pour les fichiers scannés. Enterprise DLP renvoie des verdicts pour les modèles de données basés sur l'apprentissage machine prédéfinis pour les fichiers scannés jusqu'à 1MB :

  - `Bank - Bankruptcy Filings (Banque - Dossiers de faillite)`
  - `Bank - Statements (Banque - Relevés)`
  - `Financial - Financial Accounting (Finances - Comptabilité)`
  - `Financial - Generic (Finances - Généralités)`
  - `Financial - Invoice (Finances - Factures)`
  - `Financial - Personal Finance (Finances - Finances personnelles)`
  - `Health - Generic (Santé - Généralités)`
  - `Legal - Generic (Juridique - Généralités)`
  - `Legal - Lawsuits (Juridique -Procès)`
  - `Legal - Merger and acquisition (Juridique - Fusions et acquisitions)`
  - `Legal - Patent Filings (Juridique - Dossiers de brevets)`
  - `Legal - Standard Business Agreements (Juridique - Accords commerciaux standards)`
  - `Source Code- Cfamily (Code source - Cfamily)`
  - `Source Code- Generic (Code source - Généralités)`
  - `Source Code- java (Code source - java)`
  - `Source Code- java (Code source - java)`
  - `Source Code- perl (Code source - perl)`
  - `Source Code- powershell (Code source -powershell)`
  - `Source Code- python (Code source - python)`
  - `Source Code- r (Code source - r)`
  - `Source Code- ruby (Code source - ruby)`
  - `Source Code- vbs (Code source - vbs)`
  - `Source Code- verilog (Code source - verilog)`

© 2020 Palo Alto Networks, Inc.

- Source Code- vhd1 (Code source - vhd1)
- Source Code- x86_assembly (Code source - x86_assembly)

Profils prédéfinis de filtrage des données

Le tableau suivant décrit les profils prédéfinis de filtrage des données fournis avec Entreprise Data Loss Prevention (prévention des pertes de données - DLP) :

Profil prédéfini de filtrage des données	Filtre les
Bulk CCN (divers numéros de cartes de crédit)	Les numéros de cartes de crédit ou de cartes de crédit Voyager (plus de 100).
CCPA	Respect de la California Consumer Privacy Act (Loi relative à la vie privée des consommateurs de Californie)
Documents financiers d'entreprise	Comptabilité financière et informations financières générales.
Informations financières	Relevés bancaires, numéros de routage bancaire, numéros de carte de crédit (vérification stricte), dossiers de faillite.
RGPD	Numéros de permis de conduire, identifiants fiscaux, documents d'identification nationaux, numéros de passeports.
la loi Gramm-Leach-Bliley Act (GLBA)	Numéros de cartes de crédit, numéros de cartes de crédit Voyager, informations sur bande magnétique, Identifiant fiscal américain (TIN), document d'identification national américain, numéro de sécurité sociale (NSS).
Soins de santé	Numéros de Clinical Laboratory Improvement Amendments (CLIA - amendements relatifs à l'amélioration des laboratoires cliniques), Numéros de la Drug Enforcement Administration (DEA) et autres documents des services de soins de santé.
Propriété intellectuelle	Code sources, clés sécurisées AWS, clés sécurisées, confidentialité d'entreprise. Il existe deux types de propriété intellectuelle. Le profil de filtrage des données de **Propriété intellectuelle - Basique** contient un sous-groupe des modèles de données qui sont incluses dans le profil de filtrage des données de **Propriété intellectuelle**.
Juridique	Documents juridiques incluant les procès, les fusions et acquisitions, les contrats commerciaux standards, les brevets, les dossiers de faillite.
Logiciel malveillant	Tous les documents de Microsoft Office, PDF et fichiers exécutables portables ainsi les menaces connues issues de la base WildFire. Le verdict se base sur un hachage, qui est l'empreinte digitale unique d'un fichier.

© 2020 Palo Alto Networks, Inc.

Profil prédéfini de filtrage des données	Filtre les
Informations d'identification personnelle (IIP)	Identifiants fiscaux, identifiants nationaux, numéros de passeports et numéros de permis de conduire.
Propos vulgaires	Censurés, personnels, incluant/excluant, homophobes, à caractère sexuel.
Auto-destruction	Tendances suicidaires.
Contenu sensible	Document d'identité national, informations bancaires, clés sécurisées AWS ou clés d'accès, documents confidentiels d'entreprise, CCN.
Information Online Code of Practice (Code de pratique en ligne des informations) PIOCP du Royaume-Uni	Identifiants fiscaux ou Documents d'identité nationaux.

Installer le plug-in Entreprise Data Loss Prevention (prévention des pertes de données - DLP)

Pour installer le plug-in Entreprise Data Loss Prevention (prévention des pertes de données - DLP) sur votre serveur de gestion Panorama™ et vos pare-feux gérés, vous devez télécharger le plug-in depuis le portail Support de Palo Alto Networks, récupérer le plug-in dans Panorama puis l'installer. Vous devez installer le plug-in sur Panorama et vos pare-feux gérés afin d'exploiter le Entreprise DLP.

Vos modèles de données existants (Objects (Objets) > Custom Objects (Personnaliser les objets) > Data Patterns (Modèles de données) et les profils de filtrage de données (Objects (Objets) > Security Profiles (Profils de sécurité) > Data Filtering (filtrage des données)) sont automatiquement masqués après que vous ayez installé le plug-in Entreprise DLP sur Panorama. Pour afficher vos modèles de données et profils de filtrage existants, consultez Activer les Modèles de données et les Profils de filtrage existants.

STEP 1 | Enregistrez votre Panorama et vos managed firewalls (pare-feux gérés) sur le portail Support (CSP) de Palo Alto Networks.

STEP 2 | Installez le certificat du périphérique sur Panorama

STEP 3 | Installez le certificat de périphérique pour les pare-feux gérés.

Vous devez installer le certificat du périphérique sur tous vos pare-feux gérés exploitant Entreprise DLP.

STEP 4 | Installer le plug-in sur Panorama

1. Connectez-vous à l'interface Web Panorama.
2. Sélectionnez **Panorama** > **Plugins (Plug-ins)**, puis cherchez la dernière version du plug-in DLP.
3. **Download (Téléchargez)**et **Install (Installez)** le plug-in Enterprise DLP sur Panorama.

STEP 5 | Installez le plug-in sur vos pare-feux gérés.

1. Sélectionnez **Panorama** > **Device Deployment (déploiement des périphériques)** > **Plugins** et recherchez la dernière version du plug-in Enterprise DLP.

© 2020 Palo Alto Networks, Inc.

2. **Download (Téléchargez)** et **Install (Installer)** le plug-in Enterprise DLP sur vos pare-feux gérés.
3. Sélectionnez les **Devices (Périphériques)** sur lesquels vous voulez installer le plug-in.
4. Cliquez sur **OK** pour installer le plug-in.

STEP 6 | Validez et appliquez à vos pare-feux gérés afin de terminer l'installation du plug-in Entreprise DLP.

Cette étape est nécessaire afin que les noms des profils de filtrage des données de Entreprise DLP apparaissent dans les journaux de filtrage des données.

Alors que l'on peut Valider et Appliquer, cela n'est pas conseillé pour les modifications de la configuration d'Enterprise DLP et exige que vous sélectionniez manuellement les modèles impactés et les pare-feux gérés dans la sélection d'Étendue de la transmission.

1. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements de configuration.
2. Sélectionnez **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)** et **Edit Selections (Modifier les sélections)**.
3. Sélectionnez **Device Groups (Groupe de périphériques)** et **Inclure les modèles de périphérique et de réseau**.
4. Cliquez sur **OK**.
5. **Push (Appliquez)** les modifications de votre configuration à vos pare-feux gérés.

STEP 7 | Activez votre licence Enterprise DLP sur le portail Support (CSP) de Palo Alto Networks.

Répétez l'étape pour tous les pare-feux exploitant Entreprise DLP.

1. Connectez-vous au Customer Support Portal (Portail assistance clientèle) de Palo Alto Networks.
2. Sélectionnez **Assets (Actifs)** > **Devices (Périphériques)** puis cliquez sur le bouton de modification ( ) dans la colonne Actions.
3. Dans la fenêtre des Licences de périphériques, sélectionnez **Activate Auth-Code (Activez le code d'autorisation)** et saisissez le **Authorization Code (Code d'autorisation)**.

   Le code d'autorisation (auth code) vous est automatiquement fourni par Palo Alto Networks dans un e-mail lors de l'achat de la licence du plug-in Entreprise DLP.
4. Cliquez sur **Agree and Submit (Accepter et envoyer)**.

STEP 8 | Créez un Palo Alto Networks Support ticket (Ticket d'assistance Palo Alto Networks) afin de permettre le transfert de la licence Enterprise DLP entre les pare-feux.

Demandez que la licence Entreprise DLP soit transférable vous permet de transférer votre licence DLP vers d'autres pare-feux gérés.

Dans le ticket d'assistance, incluez les informations:

- Demandez un transfert de pare-feu pour la licence Entreprise DLP.
- L'ID de votre compte CSP et l'e-mail associé à votre compte CSP.
- Numéro de série des pare-feux gérés. Si vous activez la licence Entreprise DLP sur plusieurs pare-feux gérés, incluez tous les numéros de série des pare-feux gérés dans un seul ticket d'assistance.
- Codes d'autorisation utilisés pour activer la licence Entreprise DLP sur les pare-feux gérés.
- (En option) Si vous avez des pare-feux gérés qui appartiennent à un compte CSP différent, indiquez l'ID du compte CSP auquel ces pare-feux gérés sont associés.

STEP 9 | Vérifiez que Panorama et les pare-feux gérés appartiennent au même compte CSP.

Il est nécessaire que Panorama et les pare-feux gérés appartiennent au même compte CSP car elle vous permet de partager les profils de données pour appliquer la politique de sécurité de façon cohérente.

© 2020 Palo Alto Networks, Inc.

1. Connectez-vous au Customer Support Portal (Portail assistance clientèle) de Palo Alto Networks.
2. Sélectionnez **Assets (Actifs)** > **Devices (Périphériques)** et attribuez votre Panorama et vos pare-feux gérés.

STEP 10 | Activez le plug-in Entreprise DLP sur vos pare-feux gérés.

1. Sélectionnez **Panorama** > **Device Deployment** > **License (Licence de déploiement de périphérique Panorama)** et **Activez** le plug-in Enterprise DLP.
2. Saisissez le **Auth Code (Code d'autorisation)** des pare-feux gérés ciblés.

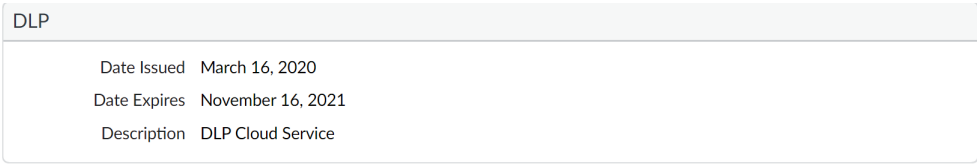
   Le code d'autorisation vous est automatiquement fourni par Palo Alto Networks par e-mail lors de l'achat de la licence du plug-in Entreprise DPL.
3. **Activez** la licence plug-in Entreprise DLP sur vos pare-feux gérés.

STEP 11 | Sélectionnez **Objects (Objets)** > **DLP** > **DLP Data Filtering (Filtrage des données DLP)** et vérifiez que les profils de filtrage des données prédéfinis s'affichent.

Panorama est automatiquement rempli avec les profils de filtrage de données prédéfinis lorsque Panorama se connecte au service cloud DLP.

STEP 12 | Vérifiez que la licence Entreprise DLP est bien activée sur vos pare-feux gérés.

1. Lancez l'interface Web du pare-feu.
2. Sélectionnez **Device (Périphérique)** > **Licenses (Licences)** et vérifiez que la licence a été activée avec succès.



Créer un modèle de données.

Les modèles de données vous permettent d'indiquer les critères de correspondance et d'identifier les modèles en utilisant des expressions régulières, les propriétés du fichier ou des mots clés qui représentent les informations sensibles sur votre réseau. Tous les modèles de données créés sont partagés dans tous les groupes de périphériques.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Sélectionnez **Objects (Objets)** > **DLP** > **Modèles de données DLP** et précisez le **Device Group (Groupe de périphériques).**

STEP 3 | **Add (Ajoutez)** un nouveau modèle de données.

STEP 4 | Indiquez un **Type** et des critères pour le modèle de données et donnez-lui un **Name (Nom)**.

Utilisez le type de modèle de données suivant :

- **Regular Expression (Expression régulière)** : Crée des expressions régulières qui seront utilisées dans le modèle de données.

  Vous pouvez choisir des modèles de données **Basic (de base)** ou **Advanced (Avancés)**. Utilisez le modèle de données **Advanced (Avancé)** pour créer une expression régulière de base ou pondérée. Les expressions régulières pondérées permettent d'attribuer un score à chaque saisie de texte, et lorsque suffisamment d'expressions d'un modèle correspondent à un actif, cet actif sera indiqué comme étant une correspondance pour le modèle.

© 2020 Palo Alto Networks, Inc.

Vous utilisez ensuite le générateur de requêtes dans la zone **Regular Expressions (Expressions régulières)** pour ajouter des expressions régulières (**Basic (de base)**) ou pondérées (**Advanced (Avancées)**).

Vous pouvez saisir un ou plusieurs **Mots clés de proximité** à utiliser dans le modèle de filtrage des données. Utilisez les mots clés de proximité dans un profil de filtrage des données avec une Confiance élevée. Lorsque vous téléchargez un fichier, le pare-feu géré recherche les mots clés de proximité que vous avez indiqués dans les 200 caractères des expressions régulières avant de tenir compte du modèle des données indiqué comme étant une correspondance du fichier.

- **File Property (Propriété du fichier)** : Ajoutez un modèle de propriétés du fichier pour la correspondance.

  Pour la gouvernance des données et la protection des informations, si vous utilisez des étiquettes de classification ou des balises intégrées dans MS Office et des documents PDF pour inclure plus d'informations pour des besoins d'audit et de suivi, vous pouvez créer un modèles de donnés de propriétés de fichier pour correspondre aux métadonnées ou attributs qui font partie des propriétés personnalisées ou étendues du fichier. Que vous utilisiez ou non un mécanisme de classification automatisé comme Titus ou nécessitiez que les utilisateurs ajoutent une étiquette, vous pouvez indiquer une paire nom-valeur pour correspondre avec une propriété personnalisée ou étendue intégrée dans le fichier.

  Enterprise DLP est compatible avec les modèles de données de propriétés de fichier de MS Office et des documents PDF. Les formats OLE (.doc/.ppt) ou XML (.docx/.pptx) de MS Office sont compatibles.

  Vous ajoutez ensuite un **Tag Name (Nom d'étiquette)**et une **Tag Value (Valeur d'étiquette)**.

  Un **Tag Name (Nom d'étiquette)** et une **Tag Value (Valeur d'étiquette)** sont une paire associée qui précise la propriété que vous souhaitez rechercher (par exemple, vous pouvez préciser un **Tag Name (Nom d'étiquette)** en **Etiquette** et une **Tag Value (Valeur d'étiquette)** sur **Confidential (Confidentiel)**). Vous pouvez ajouter autant de propriétés de fichier que vous le souhaitez. Lorsque vous référencez ensuite le modèle de données de propriétés dans le profil de filtrage des données, une correspondance booléenne OU est utilisée dans les critères de correspondance.

STEP 5 | Cliquez sur **OK** pour enregistrer le modèle de données.

STEP 6 | Validez et appliquez les modifications de votre configuration à vos pare-feux gérés en vous appuyant sur Entreprise DLP.



Alors que l'on peutValider et Appliquer, cela n'est pas conseillé pour les modifications de la configuration d'Enterprise DLP et exige que vous sélectionniez manuellement les modèles impactés et les pare-feux gérés dans la sélection d'Étendue de la transmission.

1. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements de configuration.
2. Sélectionnez **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)** et **Edit Selections (Modifier les sélections)**.
3. Sélectionnez **Device Groups (Groupe de périphériques)** et **Inclure les modèles de périphérique et de réseau**.
4. Cliquez sur **OK**.
5. **Push (Appliquez)** les modifications de votre configuration à vos pare-feux gérés.

STEP 7 | Création d'un profil de filtrage des données en utilisant un ou plusieurs modèles de données.

© 2020 Palo Alto Networks, Inc.

Création d'un profil de filtrage des données

Créez un profil de filtrage des données pour ajouter des modèles de données et indiquez les niveaux de correspondance et de confiance. Tous les profils de filtrage des données prédéfinis et personnalisés sont disponibles sur tous les groupes de périphériques.

Lors de la création d'un profil de filtrage des données utilisant des modèles de données prédéfinis, tenez compte du type de détection utilisé par les modèles de données prédéfinis car cela détermine la façon dont Enterprise DLP donne un verdict pour les fichiers analysés. Par exemple, lorsque vous créez un profil de filtrage des données qui inclue trois modèles de données basés sur l'apprentissage machine et 7 modèles de données basés sur une regex, Enterprise DLP renvoie un verdict basé sur les modèles basés sur les 7 regex si le fichier analysé fait plus de 1 Mo.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | (En option) Créez un ou plusieurs data patterns (modèles de données).

STEP 3 | Sélectionnez **Objects (Objets)** > **DLP** > **DLP Data Filters (Filtres de données DLP)** et précisez le **Device Group (Groupe de périphériques).**

STEP 4 | **Add (Ajoutez)** un nouveau profil de filtrage des données

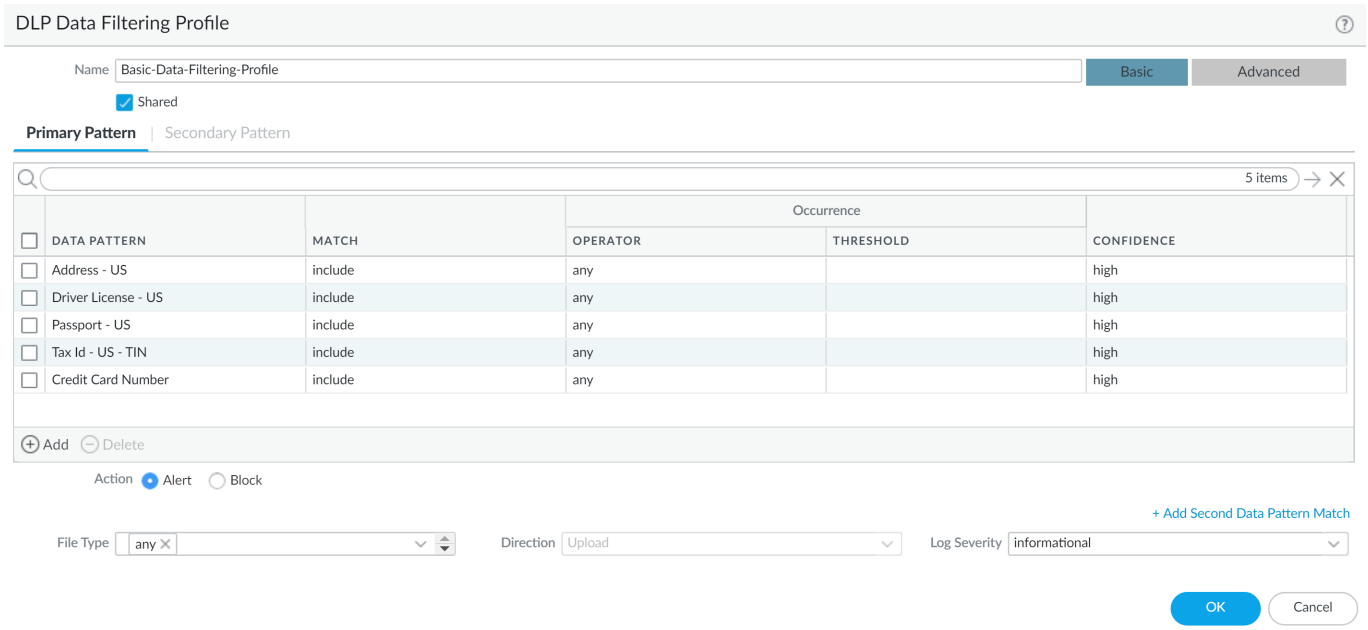
STEP 5 | Configurez le modèle principal du profil de filtrage des données.

- Si vous sélectionnez l'option **Basic (de base)**, configurez les options suivantes :
  - **Primary Pattern (Modèle principal)** : **Add (Ajoutez)** un ou plusieurs modèles de données à préciser en tant que critères de correspondance.

    Si vous précisez plus d'un modèle de données, le pare-feu géré utilise une recherche booléenne OU une correspondance avec les critères de correspondance.
  - **Match (Correspondance)** : sélectionnez si le modèle que vous précisez doit correspondre (**include (inclure)**) ou non (**exclude (eclure)**) les critères indiqués.
  - **Operator (Opérateur)** : Sélectionnez un opérateur pour utiliser avec le paramètre **Threshold (Seuil)**. Indiquez **Any (Indifférent)** pour ignorer le seuil.
  - **Threshold (Seuil)** : Indiquez une valeur à utiliser avec le**Operator (Opérateur)** indiqué.

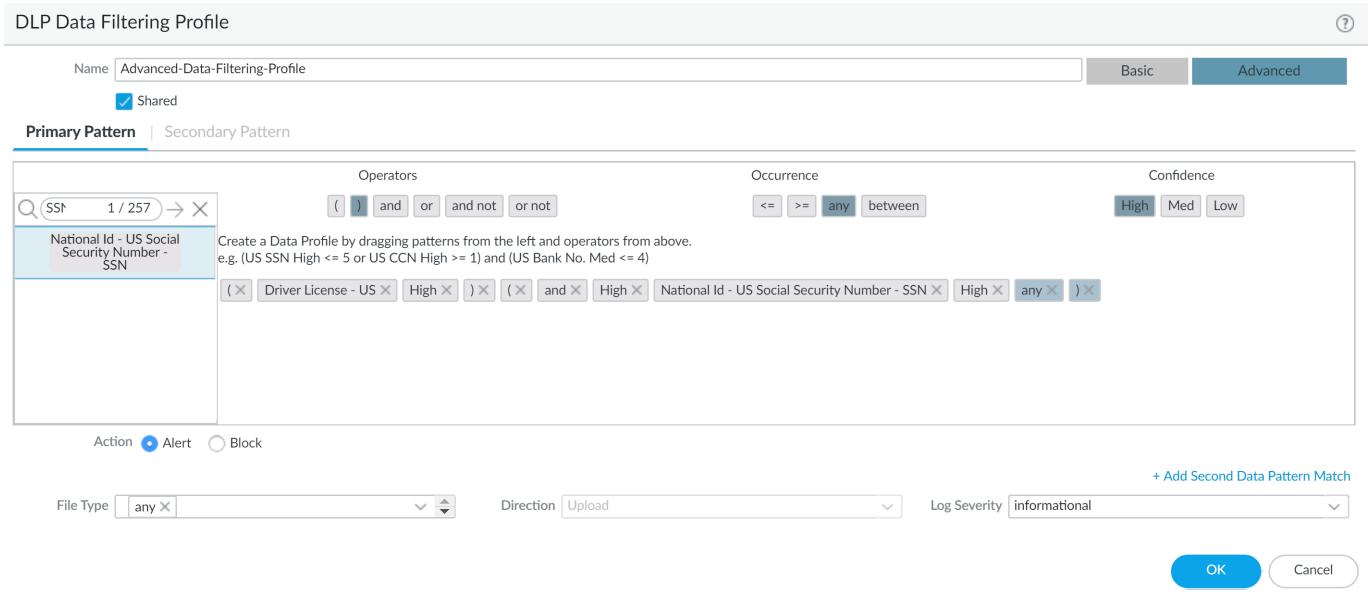
    Par exemple, pour correspondre à un modèle qui apparait 3 fois ou plus dans un fichier, sélectionnez **Operator (Opérateur)** de **more_than_or_equal_to (supérieur ou égal à)** et un **Threshold (Seuil)** de **3**.
  - **Confidence (Confiance)** : Utilisez cela avec les mots clés de proximité que vous avez indiqué dans le data pattern (modèle de données) que vous avez créé. Indiquer un niveau de confiance **Low (Faible)**signifie que le pare-feu géré n'utilise pas de mots clés de proximité. Indiquer un niveau de confiance **High (élevé)** signifie que le pare-feu géré recherche les mots clés de proximité du modèle dans les 200 caractères des expressions régulières dans le modèle avant de tenir compte du modèle de données dans un fichier qui peut correspondre.

© 2020 Palo Alto Networks, Inc.



- Si vous sélectionnez l'option **Advanced (Avancée)**, créez des expressions et faisant glisser des modèles de données, des niveaux de **Confidence (Confiance)**, des **Operators (Opérateurs)**, et des valeurs d'**Occurrence** dans le champ au centre de la page.

  Précisez les valeurs dans l'ordre où elles apparaissent dans la copie d'écran suivante (data pattern, **Confidence (confiance)**, et **Operator (Opérateur)** ou valeurs d'**Occurrence**).



STEP 6 | Sélectionnez une **Action** (**Alert (Alerte)** ou **Block (Bloquer)**) à effectuer sur le fichier.

STEP 7 | Indiquez un **File Type (Type de fichier)**.

Laissez le type de fichier sur **any (indifférent)** pour correspondre à n'importe quel supported file type (type de fichier compatible).

STEP 8 | Sélectionnez une **Direction** de **upload (téléchargement)**.

© 2020 Palo Alto Networks, Inc.

Les téléchargements ne sont pas pris en charge.

STEP 9 | (En option) Réglez la **Log Severity (Sévérité des Journaux)** enregistrée pour des fichiers correspondant à cette règle.

La sévérité par défaut est **Informational (informations)**.

STEP 10 | Cliquez sur **OK** pour enregistrer votre configuration.

STEP 11 | Associez le profil de filtrage des données à une règle de politique de sécurité.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et précisez le **Device Group (Groupe de périphériques)**.
2. Sélectionnez la règle de politique de sécurité à laquelle vous souhaitez ajouter le profil de filtrage des données.
3. Sélectionnez **Actions** et définissez le **Profile Type (Type de profil)** sur **Profiles (Profils)**.
4. Sélectionnez le Profil de**Data Filtering (filtrage de données)** que vous avez créé auparavant.
5. Cliquez sur **OK** pour enregistrer votre configuration.

STEP 12 | Validez et appliquez les modifications de votre configuration à vos pare-feux gérés en vous appuyant sur Entreprise DLP.

Alors que l'on peutValider et Appliquer, cela n'est pas conseillé pour les modifications de la configuration d'Enterprise DLP et exige que vous sélectionniez manuellement les modèles impactés et les pare-feux gérés dans la sélection d'Étendue de la transmission.

1. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements de configuration.
2. Sélectionnez **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)** et **Edit Selections (Modifier les sélections)**.
3. Sélectionnez **Device Groups (Groupe de périphériques)** et **Inclure les modèles de périphérique et de réseau**.
4. Cliquez sur **OK**.
5. **Push (Appliquez)** les modifications de votre configuration à vos pare-feux gérés.

Activez Enterprise Data Loss Prevention (prévention des pertes de données - DLP)

Suivez ces étapes pour configurer vos pare-feux gérés pour exploiter Enterprise Data Loss Prevention (prévention des pertes de données - DLP) avec succès.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | (Pare-feux matériels uniquement) Créez un service route (itinéraire de service) afin de permettre aux pare-feux de se connecter à internet.

Un itinéraire de service doit être configuré pour exploiter correctement Enterprise DLP sur ces plateformes de pare-feu.

Créez un itinéraire de service pour tous les modèles de firewall (pare-feu) exploitant PAN-OS 10.0 et des versions ultérieures.

© 2020 Palo Alto Networks, Inc.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Services** puis sélectionnez le modèle qui contient la configuration Enterprise DLP.
2. Cliquez sur **Service Route Configuration (Configuration d'itinéraire de service)** dans **Service Features (Fonctionnalités du service)** et sélectionnez **Customize (Personnaliser)**.
3. Cliquez sur **Dataplane (Plan de données)** et configurez **Source Interface (Interface de la source)** et **Source Address (Adresse de la source)**.

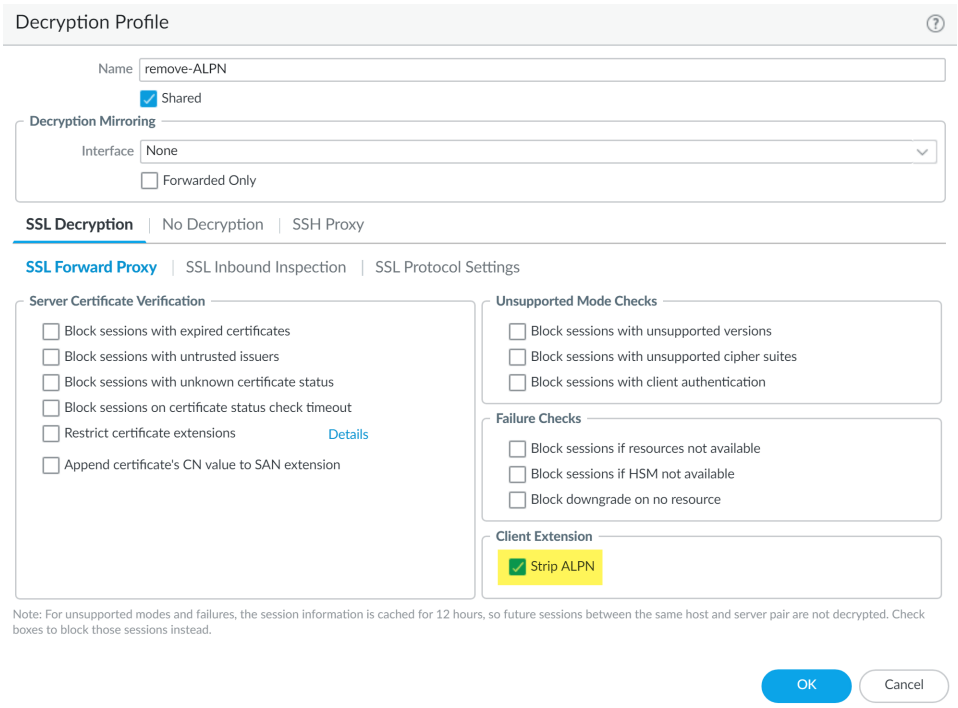
   L'interface de la source doit avoir une connectivité internet. ConsultezConfigure Interfaces (Configurer les interfaces) et Create an Address Object (Créer un objet d'adresse) pour plus d'informations sur la création de l'interface et de l'adresse de la source.
4. Sélectionnez (cochez) **Dataplane (Plan de données)** et cliquez sur **OK** pour enregistrer les modifications de votre configuration.
5. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Content-ID (ID de contenu)** et copiez le FDQN du **Public Cloud Server (Serveur cloud public)** dans la partie **Service URL Setting (Paramètre de l'URL du service)**.
6. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et **Add (Ajouter)** une security policy rule (règle de politique de sécurité) autorisant le trafic depuis l'interface de la source vers le FQDN du serveur cloud public.

STEP 3 | Créez un profil de déchiffrement pour supprimer les en-têtes Application-Layer Protocol Negotiation (ALPN) des fichiers téléchargés.

Enterprise DLP est compatible avec HTTP/1.1. Certaines applications, comme SharePoint et OneDrive sont compatibles avec HTTP/2 par défaut pour les téléchargements. Afin que les fichiers téléchargés depuis des applications qui utilisent HTTP/2 soient compatibles avec Enterprise DLP, respectez les étapes suivantes :

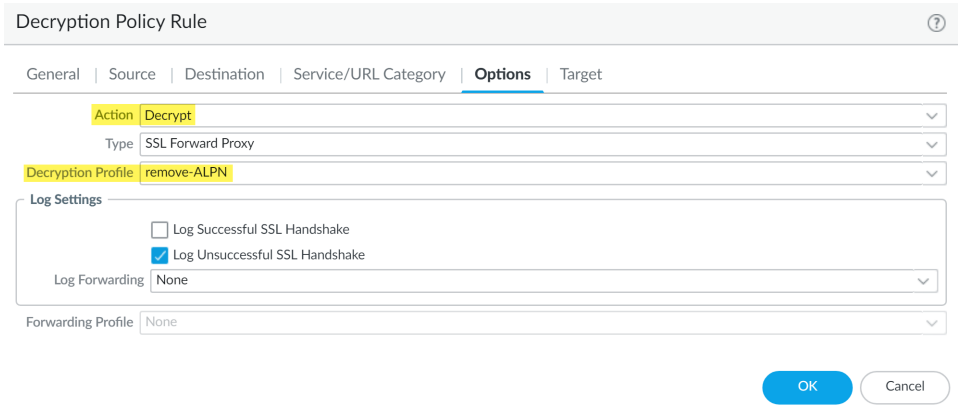
1. Sélectionnez **Objects (Objets)** > **Decryption (Déchiffrement)** > **Decryption Profile (Profil de déchiffrement)** et précisez le **Device Group (Groupe de périphériques)**.
2. **Add (Ajouter)** un nouveau profil de déchiffrement.
3. Saisissez un **Name (Nom)** descriptif.
4. (En option) Activez (cochez) **Shared (Partagé)** pour que ce profil de déchiffrement soit disponible sur tous les groupes de périphériques.
5. Sélectionnez **SSL Decryption (Déchiffrement SSL)** > **SSL Forward Proxy (Proxy de transfert SSL)** et activez (cochez) **Strip ALPN (Enlever l'ALPN)** dans **Client Extension (Extension client)**
6. Cliquez sur **OK** pour enregistrer votre configuration.

© 2020 Palo Alto Networks, Inc.



STEP 4 | Créez la règle de politique pour supprimer les en-têtes ALPN des fichiers téléchargés.

1. Sélectionnez **Policies (Politiques)** > **Decryption (Déchiffrement)** et précisez le **Device Group (Groupe de périphériques)**.
2. **Add (Ajoutez)** une nouvelle règle de politique de déchiffrement et configurez-la comme vous le souhaitez.
3. Sélectionnez **Options (Options)**.
4. Dans **Action**, sélectionnez **Decrypt (Déchiffrer)**.
5. Sélectionnez le **Decryption Profile (Profil de déchiffrement)** que vous avez créé.
6. Cliquez sur **OK** pour enregistrer votre configuration.



STEP 5 | Désactivez le protocole QUIC afin d'interdire ce trafic sur les ports 80 et 443.

De nombreuses applications web compatibles, comme Gmail, nécessitent que vous désactiviez le protocole QUIC pour que Enterprise DLP fonctionne correctement.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et précisez le **Device Group (Groupe de périphériques)**.

© 2020 Palo Alto Networks, Inc.

2. **Add (Ajoutez)** une règle de politique de sécurité qui interdit le trafic à l'aide de l'application **quic**.
3. Sélectionnez **Objects (Objets)** > **Services (Services)** et précisez le **Device Group (Groupe de périphériques)**.
4. **Add (Ajoutez)** deux services : un pour UDP sur le port 80 et un pour UDP sur le port 443.

   Les versions les plus récentes de QUIC peuvent être mal identifiées**unknown-udp (udp inconnu)**. Pour cette raison, Palo Alto Networks conseille d'ajouter des services pour le port UDP 80 et le port UDP 443 et de créer une politique de sécurité supplémentaire pour refuser le trafic UDP sur ces ports.
5. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et précisez le **Device Group (Groupe de périphériques)**.
6. **Add (Ajoutez)** une règle de politique de sécurité incluant les services que vous avez créés afin de refuser le trafic vers les ports UDP 80 et 443.

   Une fois terminé, vous aurez deux politiques de sécurité : une qui bloque le protocole QUIC et une qui bloque le trafic sur les ports UDP 80 et 443.

STEP 6 | Créer un modèle de données..

STEP 7 | Création d'un profil de filtrage des données.

STEP 8 | Associez le profil de filtrage des données à une règle de politique de sécurité.

Consultez Create a Security Policy Rule (Créez une règle de politique de sécurité) pour plus d'informations sur la création d'une nouvelle règle de politique de sécurité.



Pour rétrograder votre serveur de gestion Panorama à une version PAN-OS antérieure, vous devez retirer tous les modèles de données Enterprise DLP et les profils de filtrage de données référencés dans vos règles de politique de sécurité. Tenez compte de cela lorsque vous créez et organisez vos règles de politique qui référencent les modèles de donnés et les profiles de filtrage de Enterprise DLP.

Par exemple, créez un groupe de périphériques contenant toutes vos règles de politique de sécurité contenant des références aux modèles de données et profils de filtrage de Enterprise DLP. Cela vous permet de rapidement modifier les règles de politique concernées si vous avez besoin de rétrograder la version de Panorama PAN-OS.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** > **Pre Rules (Règles préalables)** et précisez le **Device Group (Groupe de périphériques)**.
2. Sélectionnez la règle de politique de sécurité à laquelle vous souhaitez ajouter le profil de filtrage des données.
3. Sélectionnez **Actions** et définissez le **Profile Type (Type de profil)** sur **Profiles (Profils)**.
4. Sélectionnez le Profil de**Data Filtering (filtrage de données)** que vous avez créé.
5. Cliquez sur **OK** pour enregistrer votre configuration.

STEP 9 | Validez et appliquez les modifications de votre configuration à vos pare-feux gérés en vous appuyant sur Entreprise DLP.



Alors que l'on peutValider et Appliquer, cela n'est pas conseillé pour les modifications de la configuration d'Enterprise DLP et exige que vous sélectionniez manuellement les modèles impactés et les pare-feux gérés dans la sélection d'Étendue de la transmission.

1. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements de configuration.

© 2020 Palo Alto Networks, Inc.

2. Sélectionnez **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)** et **Edit Selections (Modifier les sélections)**.
3. Sélectionnez **Device Groups (Groupe de périphériques)** et **Inclure les modèles de périphérique et de réseau**.
4. Cliquez sur **OK**.
5. **Push (Appliquez)** les modifications de votre configuration à vos pare-feux gérés.

Affichez les détails des journaux Enterprise Data Loss Prevention (Prévention des pertes de données - DLP)

Lorsque les pare-feux gérés détectent un contenu sensible au cours de la mise en téléchargement d'un fichier et que vous avez créé une Alerte ou une action de Blocage, un journal de filtrage des données est généré. Vous pouvez filtrer et afficher les données détaillées du journal du trafic détecté comme les informations de la règle de politique, la source et la destination du trafic et le profil de données auquel le modèle de données est associé. De plus, le journal détaillé affiche le modèle de données spécifique correspondant au trafic et affiche le nombre total d'occurrences uniques et totales de correspondances de modèle de données. L'affichage des journaux détaillés n'est disponible que dans Panorama.

Lorsque les pare-feux gérés détectent un contenu sensible au cours de la mise en téléchargement d'un fichier et que vous avez créé une Alerte ou une action de Blocage, un journal est généré. Vous pouvez afficher le contenu sensible, appelé un *snippet*, à partir des journaux de filtrage des données. Un snippet est la preuve ou les informations identifiables associées à une correspondance de modèle. Par exemple, si vous avez précisé un modèle de données de Numéro de carte de crédit, le pare-feu géré renvoie le numéro de sécurité sociale de l'utilisateur en tant que snippet de correspondance. Par défaut, le pare-feu géré renvoie des snippets.

Le pare-feu géré utilise le *data masking (masquage de données)* pour masquer les données dans les snippets. Par défaut, le journal de filtrage des données affiche les quatre derniers chiffres en clair (masquage partiel). Par exemple, le journal de filtrage des données affiche un snippet de numéro de carte de crédit de la façon suivante`XXXX-XXXX-XXXX-1234`. Vous pouvez aussi indiquer les données qui doivent entièrement s'afficher en clair ou masquer entièrement les données afin de cacher toutes les valeurs.

Pour afficher les journaux spécifiques DLP, y compris les snippets de fichier, suivez les étapes suivantes.

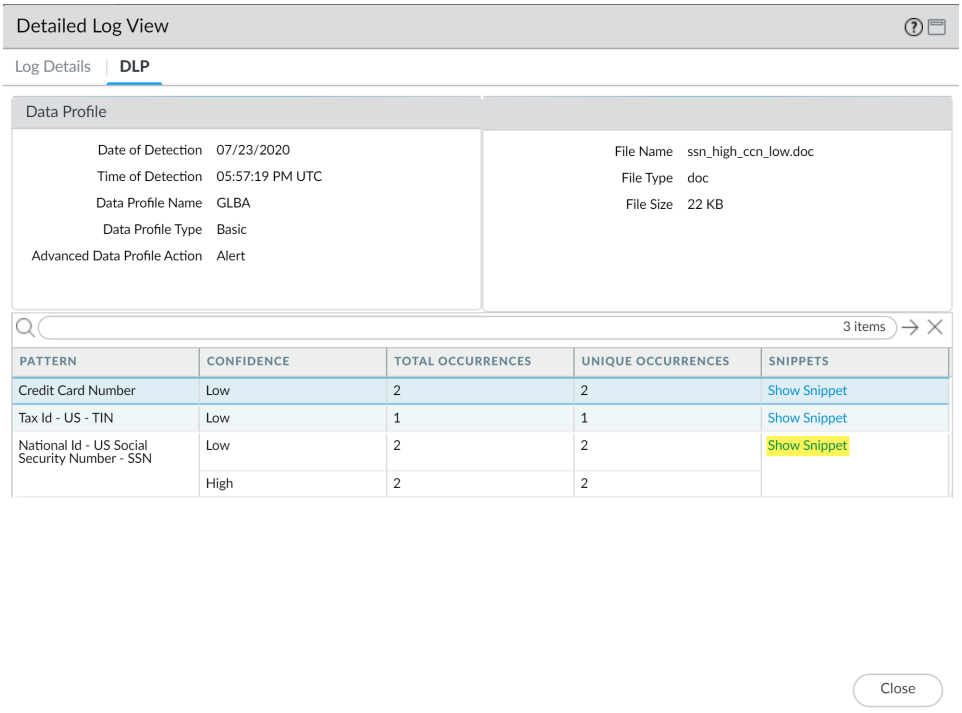
STEP 1 | Activez Enterprise Data Loss Prevention (prévention des pertes de données - DLP) .

STEP 2 | Sélectionnez **Monitor** > **Logs** > **Data Filtering (Surveiller le filtrage des données)** et**Filter (Filtrer)**les journaux de filtrage des données en saisissant **`( subtype eq dlp )`**.

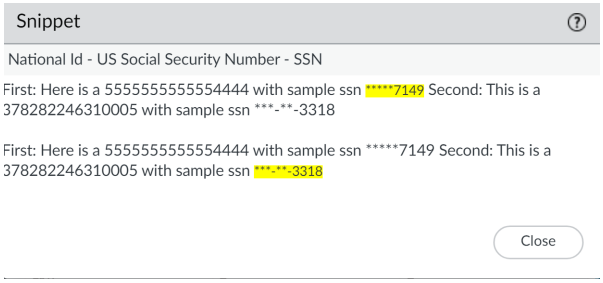
STEP 3 | Affichez plus de détails sur le fichier, y compris les snippets du fichier.

1. Cliquez sur la loupe ( ) sur la gauche du nom du journal spécifique dont vous souhaitez afficher plus de détails.
2. Sélectionnez **DLP** pour afficher les détails du modèle.
3. Sélectionnez**Show Snippet (Afficher le snippet)** pour afficher un snippet des données qui correspondent au modèle de données spécifique.

© 2020 Palo Alto Networks, Inc.



4. Examinez le snippet masqué afin de comprendre quelles données ont été détectées.



Activer les Modèles de données et les Profils de filtrage existants

Après avoir installé le plug-in Enterprise Data Loss Prevention (prévention des pertes de données - DLP), les modèles de données et les profils de filtrage existants ne s'affichent plus mais vous pouvez toujours y faire référence dans les règles de politique de sécurité. Si vous avez des modèles et profils de data filtering (filtrage de données) configurés que vous souhaitez modifier après avoir installé le plug-in Enterprise DLP, vous pouvez à nouveau les afficher dans l'interface web de Panorama.

STEP 1 | Connectez-vous à l'CLI de Panorama.

STEP 2 | Activer les Modèles de données et les Profils de filtrage existants

```
admin> request plugins dlp hide-old-config no
```

Panorama renvoie`pass (réussi)` pour confirmer que les modèles de données et les profils de filtrage s'affichent maintenant.

© 2020 Palo Alto Networks, Inc.

Saisissez la commande suivante pour ne plus afficher les modèles de données et les profils de filtrage existants.

```
admin> request plugins dlp hide-old-config yes
```

STEP 3 | Connectez-vous à l'interface Web Panorama.

STEP 4 | Modifiez vos Modèles de données et Profils de filtrage existants

1. Sélectionnez **Objects (Objets)** > **Custom Objects (Objets personnalisés)** > **Data Patterns (Modèles de données)** et modifiez vos modèles de données.
2. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de Sécurité)** > **Data Filtering (Filtrage des données)** et modifiez vos profils de filtrage de données.

STEP 5 | Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** puis sélectionnez le **Device Group (Groupe de périphériques)** afin de modifier vos règles de politique de sécurité comme vous le souhaitez.

STEP 6 | Validez et appliquez les modifications de votre configuration à vos pare-feux gérés en vous appuyant sur Entreprise DLP.

Alors que l'on peutValider et Appliquer, cela n'est pas conseillé pour les modifications de la configuration d'Enterprise DLP et exige que vous sélectionniez manuellement les modèles impactés et les pare-feux gérés dans la sélection d'Étendue de la transmission.

1. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.
2. Sélectionnez **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)** et **Edit Selections (Modifier les sélections)**.
3. Sélectionnez **Device Groups (Groupe de périphériques)** et **Inclure les modèles de périphérique et de réseau**.
4. Cliquez sur **OK**.
5. **Push (Appliquez)** les modifications de votre configuration à vos pare-feux gérés.

Modifier les paramètres de Enterprise Data Loss Prevention (prévention des pertes de données - DLP)

Modifiez les paramètres de Enterprise Data Loss Prevention (prévention des pertes de données - DLP) afin de modifier les paramètres de Contenu Cloud pour la recherche de fichiers, configurez les paramètres de filtrage de données et configurez combien de données sensibles sont masquées dans les fragments de données DLP.

- Modifier les paramètres de contenu Cloud
- Modifier les paramètres de filtrage des données de Enterprise Data Loss Prevention (prévention des pertes de données - DLP)
- Modifier les paramètres de fragment de Enterprise Data Loss Prevention (prévention des pertes de données - DLP)

Modifier les paramètres de contenu Cloud

Par défaut, Enterprise Data Loss Prevention (prévention des pertes de données - DLP) est configuré avec un Contenu Cloud Fully Qualified Domain Name (nom de domaine complet - FQDN) qui renvoie

© 2020 Palo Alto Networks, Inc.

automatiquement vers le serveur des services Cloud pour analyser vos fichiers Enterprise DLP. Si vous avez des exigences particulières de localisaton des données, vous pouvez indiquer un serveur de Services Cloud régional en modifiant le FQDN du Contenu Cloud pour qu'il envoie vos fichiers Enterprise Data Loss Prevention (prévention des pertes de données - DLP) pour analyse.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Content-ID (ID du Contenu)** et sélectionnez le **Template (Modèle)** associé aux pare-feux gérés exploitant Enterprise DLP.

STEP 3 | Modifier le FQDN de contenu Cloud

1. Modifier les **Cloud Content Settings (paramètres de contenu Cloud)**.
2. Modifiez le**Public Cloud Server (Serveur Cloud public)** sur la base des exigences de résidence de vos données.
   - **APAC**—**`apac.hawkeye.services-edge.paloaltonetworks.com`**
   - **Europe**—**`eu.hawkeye.services-edge.paloaltonetworks.com`**
   - **United States**—**`us.hawkeye.services-edge.paloaltonetworks.com`**
3. Cliquez sur **OK** pour enregistrer votre configuration.

STEP 4 | Validez et appliquez les modifications de votre configuration à vos pare-feux gérés en vous appuyant sur Entreprise DLP.

Alors que l'on peutValider et Appliquer, cela n'est pas conseillé pour les modifications de la configuration d'Enterprise DLP et exige que vous sélectionniez manuellement les modèles impactés et les pare-feux gérés dans la sélection d'Étendue de la transmission.

1. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements de configuration.
2. Sélectionnez **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)** et **Edit Selections (Modifier les sélections)**.
3. Sélectionnez **Device Groups (Groupe de périphériques)** et **Inclure les modèles de périphérique et de réseau**.
4. Cliquez sur **OK**.
5. **Push (Appliquez)** les modifications de votre configuration à vos pare-feux gérés.

Modifier les paramètres de filtrage des données de Enterprise Data Loss Prevention (prévention des pertes de données - DLP)

Configurez les paramètres du réseau pour les fichiers analysés vers le service cloud Enterprise Data Loss Prevention (prévention des pertes de données - DLP) et spécifiez les actions que le pare-feu exploitant Enterprise DLP prendra.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **DLP** et sélectionnez le **Template (Modèle)** associé aux pare-feux gérés exploitant Enterprise DLP.

STEP 3 | Modifiez les paramètres de filtrage des données.

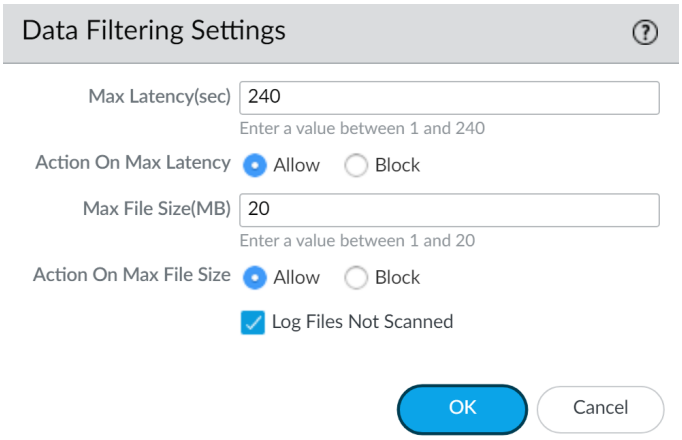
1. Indiquez la **Max Latency (sec) (latence max en sec.)** de téléchargement d'un fichier pour qu'une action soit prise par le pare-feu.

© 2020 Palo Alto Networks, Inc.

2. Indiquez **Action on Max Latency (action sur latence max.)** (**Block (bloquer)** ou **Allow (Autoriser)**) que le pare-feu prendra lorsqu'un fichier analysé devant être stocké dans le service cloud DLP atteint la **Max Latency (latence max.)** configurée.

   Sélectionner Block (Bloquer) s'applique uniquement aux Enterprise DLP data filtering profiles (profils de filtrage de données Enterprise DLP) configurés pour bloquer les fichiers. Ce paramètre n'a pas d'impact sur les profils de filtrage de Enterprise DLP configurés pour alerter lorsque le trafic contenant des données sensibles est analysé.
3. Indiquez la **Max File Size (MB) (taille de fichier max. en Mo)** afin d'appliquer une taille de fichier maximale aux fichiers stockés dans le service cloud DLP.
4. Indiquez **Action on Max File Size (action sur taille de fichier max.)** (**Block (bloquer)** ou **Allow (Autoriser)**) que le pare-feu prendra lorsqu'un fichier analysé devant être stocké dans le service cloud DLP atteint la **Max File Size (taille de fichier max.)** configurée.

   Sélectionner Block (Bloquer) s'applique uniquement aux Enterprise DLP data filtering profiles (profils de filtrage de données Enterprise DLP) configurés pour bloquer les fichiers. Ce paramètre n'a pas d'impact sur les profils de filtrage de Enterprise DLP configurés pour alerter lorsque le trafic contenant des données sensibles est analysé.
5. Cochez (activez) **Log Files Not Scanned (Fichiers journaux non analysés)** pour générer une alerte dans le journal d filtrage des données lorsqu'un fichier ne peut pas être analysé vers le service cloud DLP.
6. Cliquez sur **OK** pour enregistrer votre configuration.



STEP 4 | Validez et appliquez les modifications de votre configuration à vos pare-feux gérés en vous appuyant sur Entreprise DLP.

Alors que l'on peutValider et Appliquer, cela n'est pas conseillé pour les modifications de la configuration d'Enterprise DLP et exige que vous sélectionniez manuellement les modèles impactés et les pare-feux gérés dans la sélection d'Étendue de la transmission.

1. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements de configuration.
2. Sélectionnez **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)** et **Edit Selections (Modifier les sélections)**.
3. Sélectionnez **Device Groups (Groupe de périphériques)** et **Inclure les modèles de périphérique et de réseau**.
4. Cliquez sur **OK**.
5. **Push (Appliquez)** les modifications de votre configuration à vos pare-feux gérés.

© 2020 Palo Alto Networks, Inc.

Modifier les paramètres de fragment de Enterprise Data Loss Prevention (prévention des pertes de données - DLP)

Configurez les pare-feux pour conserver les fragments de données sensibles qui correspondent à vos Enterprise DLP data patterns (modèles de données de Enterprise DLP) dans le service cloud DLP et configurez la façon de masquer les données sensibles si elles sont conservées.

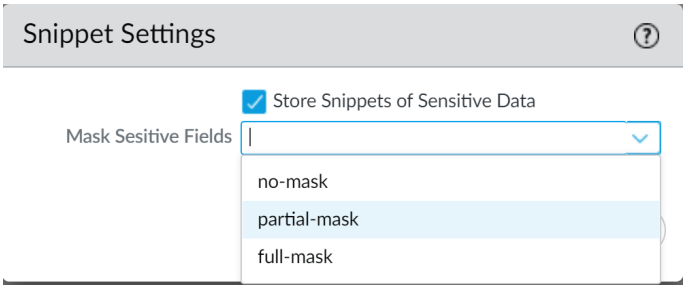
STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Sélectionnez **Panorama** > **DLP** > **Configuration** et modifiez les paramètres des fragments.

STEP 3 | Cochez (activez) **Store Snippets of Sensitive Data (Conserver les fragments de données sensibles)** pour conserver les fragments de données sensibles qui correspondent à vos Enterprise DLP data patterns (modèles de données Enterprise DLP) dans le service cloud DLP.

STEP 4 | Configurez comment **Mask Sensitive Field (masquer le champ sensible)** pour un stockage dans le service cloud DLP.

- **no-mask (pas de masque)** : le fragment de données sensibles correspondant n'est pas masqué et est entièrement visible lorsqu'il est stocké dans le service cloud DLP.
- **partial-mask (masquage partiel)**: le fragment de données sensibles correspondant est partiellement masqué et affiche quatre caractères lorsqu'il est stocké dans le service cloud DLP.
- **full-mask (masquage complet)** : le fragment de données sensibles correspondant est entièrement masqué lorsqu'il est stocké dans le service cloud DLP.



STEP 5 | Cliquez sur **OK** pour enregistrer votre configuration.

STEP 6 | Validez et appliquez les modifications de votre configuration à vos pare-feux gérés en vous appuyant sur Entreprise DLP.

Alors que l'on peutValider et Appliquer, cela n'est pas conseillé pour les modifications de la configuration d'Enterprise DLP et exige que vous sélectionniez manuellement les modèles impactés et les pare-feux gérés dans la sélection d'Étendue de la transmission.

1. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements de configuration.
2. Sélectionnez **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)** et **Edit Selections (Modifier les sélections)**.
3. Sélectionnez **Device Groups (Groupe de périphériques)** et **Inclure les modèles de périphérique et de réseau**.
4. Cliquez sur **OK**.
5. **Push (Appliquez)** les modifications de votre configuration à vos pare-feux gérés.

© 2020 Palo Alto Networks, Inc.

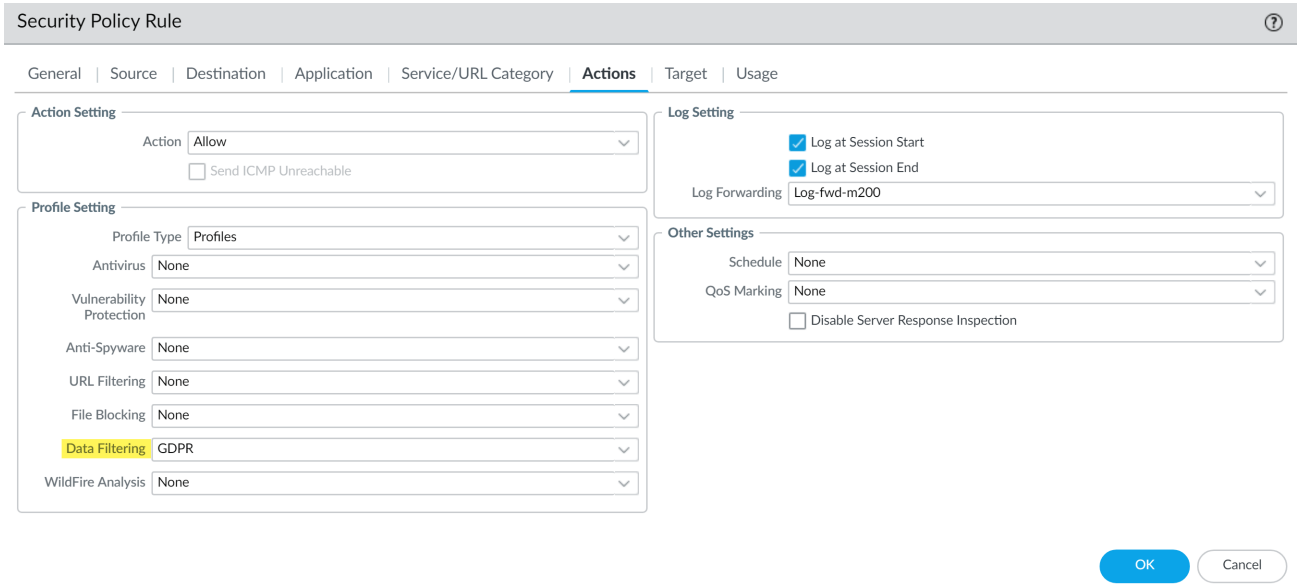
Désinstaller le plug-in Entreprise Data Loss Prevention (prévention des pertes de données - DLP)

Pour désinstaller le plug-in Entreprise data Loss Prevention (prévention des pertes de données - DLP), vous devez supprimer toutes les références à des profils de filtrage des données d'Entreprise Data Loss Prevention (prévention des pertes de données - DLP) de toutes vos règles de politique de sécurité avant de pouvoir désinstaller le plug-in sur votre serveur de gestion Panorama™ et les pare-feux gérés Après avoir réussi à désinstaller le plug-in, vous pouvez continuer à déclasser votre Panorama et vos pare-feux gérés.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Sélectionnez **Policies** > **Security (Sécurité des politiques)** et supprimez tous les profiles de filtrage de données d'Enterprise DLP de vos règles de politique de sécurité.

Cette étape est nécessaire pour désinstaller correctement le plug-in Entreprise DLP.



STEP 3 | Validez et appliquez les modifications de votre configuration à vos pare-feux gérés en vous appuyant sur Entreprise DLP.

Alors que l'on peutValider et Appliquer, cela n'est pas conseillé pour les modifications de la configuration d'Enterprise DLP et exige que vous sélectionniez manuellement les modèles impactés et les pare-feux gérés dans la sélection d'Étendue de la transmission.

1. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** pour valider vos changements de configuration.
2. Sélectionnez **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)** et **Edit Selections (Modifier les sélections)**.
3. Sélectionnez **Device Groups (Groupe de périphériques)** et **Inclure les modèles de périphérique et de réseau**.
4. Cliquez sur **OK**.
5. **Push (Appliquez)** les modifications de votre configuration à vos pare-feux gérés.

STEP 4 | Désinstallez le plug-in Entreprise DLP de vos pare-feux gérés.

1. Accédez au CLI du pare-feu géré.

© 2020 Palo Alto Networks, Inc.

2. Désinstallez le plug-in Entreprise DLP à l'aide de la commande suivante :

```
admin> request plugins uninstall dlp
```

   Saisissez **y** lorsque l'on vous invitera à confirmer la désinstallation du plug-in Entreprise DLP.

STEP 5 | Désinstallez le plug-in Entreprise DLP de Panorama.

1. Connectez-vous à l'interface Web Panorama.
2. Sélectionnez **Panorama** > **Plugins (Plug-ins de Panorama)** et **Désinstallez** le plug-in Enterprise DLP.

STEP 6 | Validez et appliquez les modifications de votre configuration à vos pare-feux gérés en vous appuyant sur Entreprise DLP.



Alors que l'on peutValider et Appliquer, cela n'est pas conseillé pour les modifications de la configuration d'Enterprise DLP et exige que vous sélectionniez manuellement les modèles impactés et les pare-feux gérés dans la sélection d'Étendue de la transmission.

1. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** pour valider vos changements de configuration.
2. Sélectionnez **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)** et **Edit Selections (Modifier les sélections)**.
3. Sélectionnez **Device Groups (Groupe de périphériques)** et **Inclure les modèles de périphérique et de réseau**.
4. Cliquez sur **OK**.
5. **Push (Appliquez)** les modifications de votre configuration à vos pare-feux gérés.

© 2020 Palo Alto Networks, Inc.

Redistribuer les données vers les pare-feux gérés.

Pour vous assurer que tous les pare-feux qui appliquent des politiques et génèrent des rapports possèdent les données et les horodatages d'authentification nécessaires pour l'ensemble de vos règles de politique, vous pouvez tirer parti de votre infrastructure Panorama pour redistribuer les mappages et les horodatages.

- Configurez le serveur de gestion Panorama pour qu'il redistribue les données.
  1. Ajoutez des pare-feux, des systèmes virtuels ou des agents User-ID Windows en tant qu'agents de redistribution vers Panorama.
     1. Sélectionnez **Panorama** > **Data Redistribution (Redistribution des données)** et **Add (Ajoutez)** chaque agent de redistribution.
     2. Entrez un **Name (Nom)** pour identifier l'agent de redistribution.
     3. Confirmez que l'agent est **Enabled (Activé)**.
     4. Entrez le nom de l'**Host (Hôte)** ou l'adresse IP de l'interface MGT sur le pare-feu.
     5. Entrer le numéro de **Port** sur lequel le pare-feu écoutera les requêtes de redistribution de données (la valeur par défaut est 5007).
     6. Si l'agent de redistribution est un pare-feu ou un système virtuel, entrez le **Collector Name (Nom du collecteur)** et la **Collector Pre-Shared Key (Clé pré-partagée du collecteur)**.
     7. Sélectionnez le **Data type (type de données)** que vous souhaitez redistribuer. Vous pouvez sélectionnez tous les types de données mais vous devez sélectionner au moins un des types de données suivants :
        - **Mappages des Utilisateurs IP**
        - **Étiquettes IP**
        - **Étiquettes d'utilisateurs**
        - **HIP**
        - **Quarantine List (liste de quarantaine)**
     8. Cliquez sur **OK** pour enregistrer la configuration.
  2. Activez l'interface MGT de Panorama pour répondre aux requêtes de redistribution des données provenant des pare-feux :

     Si le serveur de gestion Panorama dispose d'une configuration de haute disponibilité (HD), effectuez cette étape sur chaque homologue HD afin que la redistribution se poursuive si Panorama est interrompu.

     1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Interfaces** et **Management (Gestion)**.
     2. Sélectionnez **User-ID** dans la section Network Services (Services de réseau) et cliquez sur **OK**.
  3. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** pour activer vos modifications sur Panorama.

- Configurez les pare-feux pour recevoir les données que Panorama redistribue.
  1. Sélectionnez **Device** > **Data Redistribution** > **Agents (Agents de redistribution des données des périphériques)** puis sélectionnez le **Template (Modèle)** auquel les pare-feux sont assignés.
  2. **Add (ajoutez)** un agent et saisissez un **Name (Nom)**.
  3. Sélectionnez comment vous voulez ajouter l'agent :
     - **Serial Number (Numéro de série)** : Sélectionnez le **Serial Number (Numéro de série)** du Panorama que vous voulez utiliser dans la liste :

© 2020 Palo Alto Networks, Inc.

- **panorama** : La Panorama actif ou solitaire.
- **panorama2** : (HA uniquement) Le Panorama passif

- **Host and Port (Hôte et port)** : indiquez les informations suivantes :
  - Sélectionnez le nom de l'**Host (Hôte)** ou l'adresse IP de l'interface MGT sur le pare-feu.
  - Indiquez si l'hôte est un **LDAP Proxy**.
  - Entrer le numéro de **Port** sur lequel le pare-feu écoutera les requêtes de redistribution de données (la valeur par défaut est 5007).
  - Si l'agent de redistribution est un pare-feu ou un système virtuel, entrez le **Collector Name (Nom du collecteur)** et la **Collector Pre-Shared Key (Clé pré-partagée du collecteur)**.
  - Sélectionnez le **Data type (type de données)** que vous souhaitez redistribuer.

4. Confirmez que l'agent est **Enabled (Activé)** et cliquez sur **OK** pour enregistrer configuration.
5. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** pour activer vos modifications sur Panorama et appliquer les modifications aux pare-feux.

- Vérifiez que Panorama et les pare-feux reçoivent des données redistribués.
  1. Affichez les statistiques de l'agent**Panorama** > **Data Redistribution** > **Agents (Agents de redistribution des données de Panorama)** et sélectionnez **Status (Statut)** pour afficher un résumé de l'activité de l'agent de redistribution, comme le nombre de mappages que le pare-feu client a reçu.
  2. Confirmez que le **Source Name (Nom de la source)** dans les journaux User-ID (**Monitor** > **Logs** > **User-ID** Surveiller les journaux User-ID) pour vérifier que le pare-feu reçoit les mappages des agents de redistribution.
  3. Affichez le journal d'indicateur d'adresse IP (**Monitor** > **Logs** > **IP-Tag** Surveiller les journaux d'indicateur d'adresse IP) pour confirmer que le pare-feu client reçoit des données.
  4. Accédez à la CLI d'un pare-feu ou d'un serveur de gestion Panorama qui redistribue les données.
  5. Affichez tous les mappages d'utilisateur en exécutant la commande suivante :

```
> show user ip-user-mapping all
```

  6. Consignez l'adresse IP associée à un nom d'utilisateur.
  7. Accédez à la CLI d'un pare-feu ou du serveur de gestion Panorama qui reçoit les données redistribuées.
  8. Affichez les informations de mappage et l'horodatage d'authentification de *<adresse-IP>* que vous avez consignées :

```
> show user ip-user-mapping ip <IP-address>
IP address:    192.0.2.0 (vsys1)
User:          corpdomain\username1
From:          UIA
Idle Timeout:  10229s
Max. TTL:      10229s
MFA Timestamp: first(1) - 2016/12/09 08:35:04
Group(s):      corpdomain\groupname(621)
```

L'exemple suivant indique l'horodatage d'une réponse à une demande d'authentification (facteur). Pour les règles d'authentification qui utilisent l'authentification multifacteur (MFA), le résultat présente plusieurs horodatages.

© 2020 Palo Alto Networks, Inc.

Transition d'un pare-feu à une gestion Panorama

Si vous avez déjà déployé des pare-feux Palo Alto Networks et les avez configuré localement mais que, maintenant, voulez utiliser Panorama pour leur gestion centralisée, vous devez effectuer la planification de pré-migration. La migration consiste à importer les configurations de pare-feu à Panorama et vérifier que les pare-feux fonctionnent comme prévu après la transition. Si certains paramètres sont propres à chaque pare-feu, vous pouvez continuer à accéder aux pare-feux pour gérer les paramètres uniques. Vous pouvez gérer n'importe quel paramètre de pare-feu donné en insérant sa valeur depuis Panorama ou en le configurant localement sur le pare-feu, mais vous ne pouvez pas gérer le réglage grâce, et à Panorama et au pare-feu. Si vous souhaitez exclure certains paramètres du pare-feu de gestion Panorama, vous pouvez :

- Migrer la configuration entière du pare-feu et puis, sur Panorama, supprimez les paramètres que vous souhaitez gérer localement sur les pare-feux. Vous pouvez également remplacer un paramètre de modèle que Panorama lance sur un pare-feu au lieu de supprimer le paramètre sur Panorama.
- Charger une configuration partielle de pare-feu, incluant les seuls paramètres pour lesquels vous utiliserez Panorama pour gérer.



Les pare-feux ne perdront pas les journaux pendant la transition vers la gestion Panorama.

- Planifiez la Transition vers la gestion de Panorama
- Migrer un pare-feu vers la gestion Panorama
- Migrer une paire HD de pare-feu vers la gestion Panorama
- Charger une Configuration partielle de pare-feu dans Panorama

Planifiez la Transition vers la gestion de Panorama

Les tâches suivantes sont une présentation générale de la planification nécessaire pour migrer des pare-feux à la gestion de Panorama :

- ❑ Décidez quels pare-feux vont migrer.
- ❑ Planifiez une fenêtre de maintenance et assurez-vous qu'il n'y a pas de modifications de configuration en attente dans Panorama ou les pare-feux.
- ❑ Conservez vos configurations de Panorama et pare-feu qui fonctionnent avant la migration.
  - Exportez l'état du périphérique vers vos pare-feux.
  - Exportez une sauvegarde nommée de configuration Panorama de la configuration Panorama en cours.
- ❑ Déterminez les versions de Panorama et du logiciel de pare-feu et les versions de leur contenu, et comment vous ferezGestion des licences et des mises à jour. Pour plus d'informations, reportez-vous à la section Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire.
- ❑ Planification de votre déploiement Panorama en ce qui concerne l'URL de filtrage de base de données (BrightCloud ou PAN-DB), les journaux collectés et les rôles d'administrateur.
- ❑ Planifier la façon de gérer les paramètres partagés.

  Planifier Hiérarchie de groupe de périphériques, Modèles et piles de modèle d'une manière qui permettra de réduire la redondance et de rationaliser la gestion des paramètres partagés parmi tous les pare-feux ou dans les paramètres du pare-feu. Pendant la migration, vous pouvez choisir d'importer des objets de l'emplacement partagé sur le pare-feu dans partagé sur Panorama, avec les exceptions suivantes :

© 2020 Palo Alto Networks, Inc.

- Si un objet de pare-feu partagé a le même nom et la même valeur qu'un objet Panorama partagé existant, l'importation exclut cet objet pare-feu.
- Si le nom ou la valeur de l'objet pare-feu partagé diffère d'un objet Panorama partagé existant, Panorama importe l'objet pare-feu dans chaque groupe de périphériques créé pour l'importation.
- Si une configuration importée dans un modèle fait référence à un objet de pare-feu partagé, ou si un objet de pare-feu partagé fait référence à une configuration importée dans un modèle, Panorama importe l'objet en tant qu'objet partagé, que vous cochiez la case **Import devices' shared objects into Panorama's shared context (Importer les objets partagés des périphériques vers le contexte partagé de Panorama)** ou non.

- Déterminer si le pare-feu comporte des éléments de configuration (stratégies, objets, et autres paramètres) que vous ne souhaitez pas importer, soit parce que Panorama contient déjà des éléments similaires ou parce que ces éléments sont spécifiques au pare-feu (par exemple, les paramètres de fuseau horaire) et vous ne voulez pas utiliser Panorama pour les gérer. Vous pouvez effectuer une recherche globale afin de déterminer si des éléments similaires existent sur Panorama.
- Décider des zones communes pour chaque groupe de périphériques. Cela inclut une stratégie de nommage de zone pour les pare-feux et les systèmes virtuels dans chaque groupe de périphériques. Par exemple, si vous avez des zones nommées Branch LAN et WAN, Panorama peut appliquer des règles de stratégie qui référencent ces zones sans se rendre compte des variations dans le type de port ou de médias, modèle ou schéma d'adressage logique.
- Créer un plan de test après la migration.

  Vous allez utiliser le plan de test pour vérifier que les pare-feux fonctionnent aussi efficacement après la migration qu'ils le faisaient avant. Le plan pourrait inclure des tâches telles que :

  - Surveillez les pare-feux pendant au moins 24 heures après la migration.
  - Surveillez les journaux de pare-feu et de Panorama pour des anomalies.
  - Vérifiez les connexions d'accès administrateur sur Panorama.
  - Tester divers types de trafic provenant de sources multiples. Par exemple, contrôle de graphiques de bande passante , comptes de session et entrées de journal de trafic de déni de la règle (voirUtiliser Panorama pour la visibilité). Les études doivent porter un échantillon représentatif des configurations de stratégie.
  - Vérifiez auprès de votre centre d'opérations réseau (COR) et le centre d'opérations de sécurité (COS) tous les problèmes signalés par les utilisateurs.
  - Inclure d'autres critères de test permettant de vérifier les fonctionnalités du pare-feu.

Migrer un pare-feu vers la gestion Panorama

Lorsque vous importez une configuration de pare-feu, Panorama crée automatiquement un modèle pour contenir le réseau importé et les paramètres du périphérique. Pour contenir les objets et les stratégies importées, Panorama crée automatiquement un groupe de périphériques pour chaque pare-feu ou un ensemble de périphériques pour chaque système virtuel (vsys) dans un pare-feu multi-vsys.

Lorsque vous effectuez les étapes suivantes, Panorama importe la configuration complète du pare-feu . Vous pouvez également charger une configuration partielle de pare-feu dans Panorama.



Panorama peut importer des configurations à partir de pare-feux qui exécutent Pan-OS 5.0 ou versions ultérieures et peut insérer les configurations à ces pare-feux. L'exception est que Panorama 6.1 et les versions ultérieures ne peuvent pas insérer les configurations aux pare-feux exécutant PAN-OS 6.0.0 à 6.0.3.

Vous pouvez importer les configurations depuis des pare-feux qui sont déjà des périphériques gérés, mais seulement s'ils ne sont pas encore attribués à des groupes de périphériques ou des modèles.

© 2020 Palo Alto Networks, Inc.

STEP 1 | Planifier la migration.

Consultez la liste de contrôle dans Planifier la Transition vers la Gestion Panorama.

STEP 2 | Ajouter le pare-feu en tant que périphérique géré.

Ajouter un pare-feu en tant que périphérique géré :

1. Connectez-vous à Panorama, sélectionnez **Panorama** > **Managed Devices (Périphériques Gérés** > **Summary (Récapitulatif)** et cliquez sur **Add (Ajouter)**.
2. Entrez le numéro de série du pare-feu, puis cliquez sur **OK**.

   Si vous allez importer plusieurs configurations de pare-feux, entrez le numéro de série de chacun d'eux sur une ligne distincte. Facultativement, vous pouvez copier et coller les numéros de série depuis un tableau Microsoft Excel.
3. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

STEP 3 | Établir une connexion du pare-feu à Panorama.

1. Connectez-vous au pare-feu, sélectionnez **Device (Périphérique)** > **Setup (Configuration)** et modifiez les Paramètres de Panorama.
2. Dans les champs de **Panorama Servers (serveurs Panorama)**, entrez les adresses IP du serveur d'administration Panorama.
3. Cliquez sur **OK**, puis sur **Commit (Valider)**.

STEP 4 | Importer la configuration du pare-feu dans Panorama.

Si vous décidez ultérieurement de ré-importer une configuration de pare-feu, commencez par retirer les groupes de périphériques et le modèle du pare-feu auxquels elle appartient. Si les noms du groupe de périphériques et du modèle sont identique au nom d'hôte du pare-feu, vous pouvez alors supprimer le groupe de périphériques et le modèle avant de réimporter la configuration du pare-feu ou utiliser les champs Device Group Name Prefix (Préfixe de nom de groupe de périphériques) pour définir de nouveaux noms à donner au groupe de périphériques et au modèle créés lors de la réimportation. De plus, les pare-feu ne perdent pas de journaux lorsque vous les retirez des groupes de périphériques ou des modèles.

1. Depuis Panorama, sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)**, cliquez sur **Import device configuration to Panorama (Importer la configuration du périphérique vers Panorama)** et sélectionnez le **Device (périphérique)**.

   Panorama ne peut pas importer une configuration depuis un pare-feu qui est attribué à un groupe de périphériques ou à un modèle existant.
2. (Facultatif) Modifiez le **Template Name (Nom du modèle)**. La valeur par défaut est le nom du pare-feu. Vous ne pouvez pas utiliser un modèle ou une pile de modèles existants.
3. (Facultatif) Modifier les noms de **Device Group (Groupe de périphériques)**. Pour un pare-feu multi-vsys (multi-systèmes virtuels), chaque groupe de périphériques a un nom de vsys par défaut ; ajoutez alors une chaîne de caractères en tant que préfixe de nom de groupe de périphériques pour chacun. Sinon, la valeur par défaut est le nom du pare-feu. Vous ne pouvez pas utiliser le nom d'un modèle existant.

   La case Import devices' shared objects into Panorama's shared context (Importer les objets partagés des périphériques vers le contexte partagé de Panorama) est cochée par défaut, ce qui signifie que Panorama importe des objets appartenant à Partagé sur le pare-feu dans Partagé sur Panorama. Si un objet importé n'est pas dans le

© 2020 Palo Alto Networks, Inc.

contexte partagé du pare-feu, il est appliqué à chaque groupe de périphériques importé. Si vous décochez la case, les copies de Panorama ne compareront pas les objets importés et appliqueront tous les objets de pare-feu partagés aux groupes de périphériques importés au lieu de Partagés. Cela pourrait créer des objets dupliqués, alors cocher la case est recommandé dans la plupart des cas. Pour comprendre les conséquences d'importer des objets partagés ou dupliqués dans Panorama, consultez planifier comment gérer les paramètres partagés*.*

4. Sélectionnez un **Rule Import Location (emplacement d'importation de règle)** pour les règles de stratégie importées : **Pre Rulebase (Pré Modules)** ou **Post Rulebase (Post Modules)**. Quel que soit votre choix, Panorama importe les règles de sécurité par défaut (défaut intrazone et interzone) dans la post-règle de base.

   Si Panorama comporte une règle portant le même nom qu'une règle de pare-feu que vous importez, Panorama affiche les deux règles. Supprimez une des règles avant d'effectuer une validation de Panorama pour éviter une erreur de validation.

5. Cliquez sur **OK**. Panorama affiche l'état de l'importation, le résultat, les détails sur vos sélections, les détails sur ce qui a été importé et tous les avertissements. Cliquez sur **Close (Fermer)**.
6. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

STEP 5 | Transmettez la configuration de Panorama au périphérique nouvellement ajouté.

Pour empêcher de dupliquer la règle ou des noms d'objets, transmettez la configuration du groupe de périphériques de Panorama au pare-feu afin d'éviter de commettre des erreurs.

Cette étape est nécessaire pour réussir la migration de la gestion des pare-feu au serveur de gestion Panorama. L'incapacité à effectuer cette étape entraîne des erreurs de configuration et des échecs de validation.

1. Se connecter à l'interface Web Panorama et sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)** et cliquez sur **Export or push device config bundle (Exporter ou appliquer la solution de configuration des périphériques)**.
2. Cliquez sur **Export or push device config bundle (Exporter ou transmettre la solution de configuration des périphériques)**, sélectionnez le **Device (Périphérique)** dans le menu déroulant, puis cliquez sur **OK**.
3. Sélectionnez l'**Device (appareil)** duquel vous avez importé la configuration, cliquez sur **OK**, et cliquez sur **Push & Commit (Pousser & Valider)**. Panorama insère le module et initie une validation sur le pare-feu.
4. Cliquez sur **Close (Fermer)** une fois la transmission validée avec succès.
5. Lancez l'interface Web du pare-feu et assurez-vous que la configuration a été validée avec succès. Autrement, **Commit (validez)** les modifications localement sur le pare-feu.
6. Sur l'interface Web de Panorama, sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)** > **Summary (Récapitulatif)** et vérifiez que le groupe de périphériques et la pile de modèles sont synchronisés pour le pare-feu passif. Vérifiez que les règles de politiques, les objets et les paramètres réseau du pare-feu passif correspondent au pare-feu actif. Sur l'interface Web du pare-feu, vérifiez que les objets de configuration affichent un engrenage vert (.), qui indique que l'objet de configuration est transmis depuis Panorama.
7. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

STEP 6 | Affiner la configuration importée.

1. Dans Panorama, sélectionnez **Panorama** > **Config Audit (Vérification de configuration)** , sélectionnez la **Running config (configuration courante)** et la **Candidate config (configuration candidate)** pour comparaison, cliquez sur **Go (aller)** et analysez le résultat.

© 2020 Palo Alto Networks, Inc.

2. Mettre à jour le groupe de périphériques et les configurations de modèles au besoin en fonction de l'audit de configuration et des avertissements que Panorama affiche après l'importation. Par exemple :
   - Supprimer des objets superflus et les règles de stratégie.
   - Déplacer ou cloner une règle de stratégie ou un objet vers un autre groupe de périphériques.
   - Déplacer des pare-feux à différents groupes de périphériques ou modèles.
   - Déplacez un groupe de périphériques créé par Panorama lors de l'importation dans un groupe de périphériques parent différent : Sélectionnez **Panorama** > **Device Groups (Groupes de périphériques)**, sélectionnez le groupe de périphériques que vous voulez déplacer, sélectionnez un nouveau **Parent Device Group (groupe de périphériques Parent)**, et cliquez sur **OK**.

STEP 7 | Insérez le module de configuration du pare-feu dans le pare-feu pour supprimer toutes les règles et objets de la configuration locale.

Cette étape est nécessaire pour empêcher de dupliquer la règle ou des noms d'objets, ce qui provoque des erreurs de validation lorsque vous appuyez sur la configuration du groupe périphérique du Panorama du pare-feu à l'étape suivante.

1. Dans Panorama, sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.
2. Sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)** et cliquez sur **Export or push device config bundle (Exporter ou appliquer la solution de configuration des périphériques)**.
3. Sélectionnez l'**Device (appareil)** duquel vous avez importé la configuration, cliquez sur **OK**, et cliquez sur **Push & Commit (Pousser & Valider)**. Panorama insère le module et initie une validation sur le pare-feu.

STEP 8 | Appliquez les configurations de groupe et modèle de périphérique pour terminer la transition vers une gestion centralisée.

Si vous migrez plusieurs pare-feux, effectuez toutes les étapes précédentes — dont celle-ci — pour chaque pare-feu avant de continuer.

1. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** et **Edit Selections (Modifier les sélections)** dans la portée d'application.
2. Sélectionnez **Device Groups (Groupes de périphériques)** et sélectionnez les groupes de périphériques contenant les configurations de pare-feu importées.
3. Sélectionnez **Merge with Device Candidate Config (Fusionner avec la configuration candidate du périphérique)**, **Include Device and Network Templates (Inclure les modèles de périphérique et de réseau)** et **Force Template Values (Forcer les valeurs de modèle)**.
4. Cliquez sur **OK** pour enregistrer les modifications dans la portée d'application.
5. **Commit and Push (Validez et appliquez)** vos modifications.

STEP 9 | Consolider toutes les configurations de pare-feu importées.

Cette étape est requise si vous migrez plusieurs pare-feu.

1. Après avoir importé toutes les configurations de pare-feu, mettez à jour les groupes de périphériques et les modèles si nécessaire pour éliminer la redondance et simplifier la gestion de la configuration : reportez-vous à la section Affiner la configuration importée. (vous n'avez pas besoin de pousser à nouveau les faisceaux de configuration du pare-feu.)
2. (Vous n'avez pas besoin de reforcer les modules de configuration du pare-feu).

   Si les pare-feux auront des zones locales, vous devez les créer avant d'effectuer une validation de groupe ou de modèle de périphérique ; Panorama ne peut pas interroger les pare-feux pour le nom de zone ou de la configuration de la zone. Si vous allez utiliser les règles de pare-feu local, s'assurer que

© 2020 Palo Alto Networks, Inc.

leurs noms sont uniques (ne pas dupliquer dans Panorama). Si nécessaire, vous pouvez Remplacer un modèle ou une valeur de pile de modèles avec une valeur spécifique au pare-feu.

3. Validez et appliquez vos modifications :
    1. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** et **Edit Selections (Modifier les sélections)** dans la portée d'application.
    2. Sélectionnez **Device Groups (Groupes de périphériques)**, sélectionnez les groupes de périphériques que vous avez modifiés, et **Include Device and Network Templates (Inclure les modèles de périphérique et de réseau)**.
    3. Cliquez sur **OK** pour enregistrer les modifications dans la portée d'application.
    4. **Commit and Push (Validez et appliquez)** vos modifications.

STEP 10 | Exécutez votre plan de test post-migration.

Effectuez les tâches de vérification que vous avez conçues lors de la planification de la migration afin de confirmer que les pare-feu fonctionnent aussi efficacement avec la configuration affichée par Panorama qu'avec leur configuration locale d'origine : voir Créer un plan de test post-migration.

Migrer une paire HD de pare-feu vers la gestion Panorama

Si vous possédez une paire de pare-feu dans une configuration haute disponibilité que vous souhaitez gérer à l'aide de Panorama, vous avez la possibilité d'importer la configuration locale vers votre paire haute disponibilité de pare-feu vers Panorama sans avoir à recréer de configurations ou de politiques. Vous devez d'abord importer les configurations de pare-feu dans Panorama, qui sont utilisées pour créer un nouveau groupe de périphériques et un nouveau modèle. Vous effectuerez une application spéciale de la configuration du groupe de périphériques et du modèle aux pare-feu pour remplacer les configurations de pare-feu locales et synchroniser les pare-feu avec Panorama.

STEP 1 | Planifier la migration.

Consultez la liste de contrôle dans Planifier la Transition vers la Gestion Panorama.

STEP 2 | Désactivez la synchronisation de la configuration entre les homologues HD.

Répétez ces étapes pour les deux pare-feu de la paire HD.

1. Connectez-vous à l'interface Web de chaque pare-feu, sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)** et modifiez la section Setup (Configuration).
2. Désactivez **Enable Config Sync (Activer la synchronisation de la configuration)** et cliquez sur **OK**.
3. Cliquez sur **Commit (Valider)** pour valider les modifications apportées à la configuration de chaque pare-feu.

STEP 3 | Connectez chaque pare-feu à Panorama.

Si Panorama reçoit déjà des journaux de ces pare-feu, vous n'avez pas besoin d'effectuer cette étape. Passez à l'étape 5.

Répétez ces étapes pour les deux pare-feu de la paire HD.

1. Connectez-vous à l'interface Web de chaque pare-feu, sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les paramètres de Panorama.
2. Dans les champs **Panorama Servers (Serveurs Panorama)** , entrez les adresses IP des serveurs de gestion Panorama, confirmez que **Panorama Policy and Objects (Politiques et objets Panorama)** et **Device and Network Template (Modèle de périphérique et de réseau)** sont activés et sélectionnez **OK**.

© 2020 Palo Alto Networks, Inc.

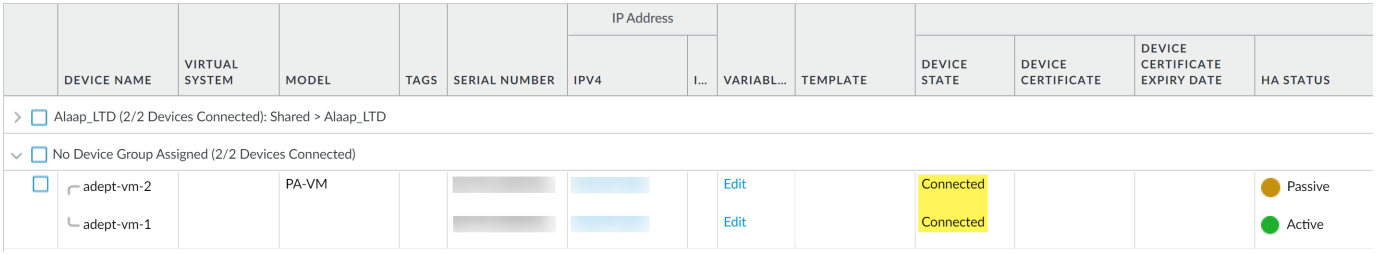
3. Cliquez sur **Commit (Valider)** pour valider les modifications apportées à la configuration de chaque pare-feu.

STEP 4 | Ajouter chaque pare-feu en tant que périphérique géré.

Si Panorama reçoit déjà des journaux de ces pare-feu, vous n'avez pas besoin d'effectuer cette étape. Passez à l'étape 5.

Ajouter un pare-feu en tant que périphérique géré.

1. Se connecter à l'interface Web Panorama, sélectionnez Panorama (Panorama) > Managed Devices (Périphériques gérés), puis cliquez sur **Add (Ajouter)**.
2. Entrez le numéro de série de chaque pare-feu, puis cliquez sur **OK**.
3. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.
4. Vérifiez que l'état du périphérique de chaque pare-feu est Connected (Connecté).



STEP 5 | Importez la configuration de chaque pare-feu dans Panorama.

N'envoyez aucune configuration de groupe de périphériques ou de pile de modèles vers vos pare-feux gérés lors de cette étape. Envoyer la configuration de groupe de périphériques et de pile de modèles au cours de cette étape efface la configuration HA du pare-feu local selon les étapes suivantes.

Si vous décidez ultérieurement de ré-importer une configuration de pare-feu, commencez par retirer les groupes de périphériques et le modèle du pare-feu auxquels elle appartient. Si les noms du groupe de périphériques et du modèle sont identique au nom d'hôte du pare-feu, vous pouvez alors supprimer le groupe de périphériques et le modèle avant de réimporter la configuration du pare-feu ou utiliser les champs Device Group Name Prefix (Préfixe de nom de groupe de périphériques) pour saisir un nouveau nom à donner au groupe de périphériques et au modèle créés lors de la réimportation. De plus, les pare-feu ne perdent pas de journaux lorsque vous les retirez des groupes de périphériques ou des modèles.

1. Depuis Panorama, sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)**, cliquez sur **Import device configuration to Panorama (Importer la configuration du périphérique vers Panorama)** et sélectionnez le **Device (périphérique)**.

   Panorama ne peut pas importer une configuration depuis un pare-feu qui est attribué à un groupe de périphériques ou à une pile de modèles existants.
2. (Facultatif) Modifiez le **Template Name (Nom du modèle)**. La valeur par défaut est le nom du pare-feu. Vous ne pouvez pas utiliser un modèle ou une pile de modèles existants.
3. (Facultatif) Modifier les noms de **Device Group (Groupe de périphériques)**. Pour un pare-feu multi-vsys (multi-systèmes virtuels), chaque groupe de périphériques a un nom de vsys par défaut ; ajoutez alors une chaîne de caractères en tant que préfixe de nom de groupe de périphériques pour chacun.

© 2020 Palo Alto Networks, Inc.

Sinon, la valeur par défaut est le nom du pare-feu. Vous ne pouvez pas utiliser le nom d'un modèle existant.

La case Import devices' shared objects into Panorama's shared context (Importer les objets partagés des périphériques vers le contexte partagé de Panorama) est cochée par défaut, ce qui signifie que Panorama importe des objets appartenant à Partagé sur le pare-feu dans Partagé sur Panorama. Si un objet importé n'est pas dans le contexte partagé du pare-feu, il est appliqué à chaque groupe de périphériques importé. Si vous décochez la case, les copies de Panorama ne compareront pas les objets importés et appliqueront tous les objets de pare-feu partagés aux groupes de périphériques importés au lieu de Partagés. Cela pourrait créer des objets dupliqués, alors cocher la case est recommandé dans la plupart des cas. Pour comprendre les conséquences d'importer des objets partagés ou dupliqués dans Panorama, consultez planifier comment gérer les paramètres partagés*.*

4. **Commit to Panorama (Validez sur Panorama)**.
5. Sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)**, puis **Export or push device config bundle (Exporter ou appliquer la solution de configuration des périphériques)**. Sélectionnez le **Device (Périphérique)**, sélectionnez **OK**, puis **Push & Commit (Transmettez et appliquez)** la configuration.

   Le paramètre Enable Config Sync (Activation de la synchronisation de la configuration) à l'étape 2 doit être désactivé sur les deux pare-feu avant d'appliquer le groupe de périphériques et la pile de modèles.
6. Lancez l'interface Web de l'homologue HA du pare-feu et assurez-vous que la configuration envoyée lors de l'étape antérieure a été validée avec succès. Autrement, **Commit (validez)** les modifications localement sur le pare-feu.
7. Répétez les étapes 1 à 6 ci-dessus sur le deuxième pare-feu. Le processus créera un groupe de périphériques et une pile de modèles pour chaque pare-feu.

STEP 6 | Ajoutez la paire de pare-feu HA dans le même groupe de périphériques et la même pile de modèles.

Sautez cette étape si la paire HA est dans une configuration active / active.

1. Sélectionnez **Panorama** > **Device Group (Groupe de périphériques)**, sélectionnez le groupe de périphériques du deuxième pare-feu et cliquez sur **Delete (Effacer)** pour la supprimer.
2. Sélectionnez le groupe de périphériques pour le premier pare-feu, sélectionnez le deuxième pare-feu, cliquez sur **OK** et **Commit to Panorama (Valider sur Panorama)** pour l'ajouter au même groupe de périphériques que l'homologue HD.
3. Sélectionnez **Panorama** > **Templates (Modèles)**, sélectionnez la pile de modèles pour le deuxième pare-feu et cliquez sur **Delete (Effacer)** pour la supprimer.
4. Sélectionnez la pile de modèles pour le premier pare-feu, ajoutez le deuxième pare-feu, sélectionnez **OK** et **Commit to Panorama (Valider sur Panorama)** pour l'ajouter au même modèle que l'homologue HD.
5. Supprimez les paramètres HA dans le modèle associé aux pare-feux qui ont récemment migré.
   1. Sélectionnez **Device** > **Setup** > **High Availability (haute disponibilité de la configuration du périphérique)**
   2. Sélectionnez **Remove All (Supprimer tous)**.
   3. **Commit to Panorama (Validez sur Panorama)**.
6. Envoyez les configurations du groupe de périphériques et de la pile de modèles vers vos pare-feux gérés.

© 2020 Palo Alto Networks, Inc.

Tout d'abord, envoyez la configuration du groupe de périphériques et de la pile de modèles vers votre homologue HA passif puis vers l'homologue HA actif.

1. Sélectionnez **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)** et **Edit Selections (Modifier les sélections)**.
2. Activez (sélectionnez) **Merge Device Candidate Config (Fusionner la configuration candidate du périphérique)**, **Include Device and Network Templates (Inclure les modèles de périphérique et de réseau)** et **Force Template Values (Forcer les valeurs de modèle)**.
3. Cliquez sur **OK**.
4. **Push (Appliquez)** à vos pare-feux gérés.
5. Lancez l'interface web de l'homologue HA actif et sélectionnez **Device** > **High Availability** > **Operational Commands (Commandes opérationnelles haute disponibilité du périphérique)**pour **Suspend local device (suspendre le périphérique local)**.

   Basculez sur l'homologue HA passif avant de modifier l'homologue HA actif pour conserver vos conditions de sécurité tout en terminant la migration de la configuration.
6. Répétez les étapes 1à 4 pour l'homologue HA maintenant passif.
7. Lancez l'interface web de l'homologue HA maintenant actif et sélectionnez **Device** > **High Availability** > **Operational Commands (Commandes opérationnelles haute disponibilité du périphérique)**pour **Suspend local device (suspendre le périphérique local)**.

   Cela restaure les rôles homologue HA actif/passif.
7. Sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)** > **Summary (Récapitulatif)** et vérifiez que le groupe de périphériques et le modèle sont synchronisés pour le pare-feu passif. Vérifiez que les règles de politiques, les objets et les paramètres réseau du pare-feu passif correspondent au pare-feu actif.

STEP 7 | Activez la synchronisation de la configuration entre les homologues HD.

Répétez ces étapes pour les deux pare-feu de la paire HD si vous envisagez de conserver une configuration locale qui doit être synchronisée.

1. Connectez-vous à l'interface Web de chaque pare-feu, sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)** et modifiez la section Setup (Configuration).
2. Sélectionnez **Enable Config Sync (Activer la synchronisation de la configuration)**, puis cliquez sur **OK**.
3. Cliquez sur **Commit (Valider)** pour valider les modifications apportées à la configuration de chaque pare-feu.

Charger une Configuration partielle de pare-feu dans Panorama

Si certains paramètres de configuration d'un pare-feu sont communs aux autres pare-feu, vous pouvez charger ces paramètres spécifiques dans Panorama et les forcer ensuite dans tous les autres pare-feu ou les pare-feu dans des groupes de périphériques particuliers et les modèles.

Le chargement d'une configuration d'un serveur de gestion Panorama nécessite une validation complète et doit être effectuée par un super utilisateur. Des validations complètes sont nécessaires pour effectuer certaines opérations de Panorama, telles que le rétablissement et le chargement d'un instantané de configuration, et ne sont pas prises en charge pour les profils de rôle d'administrateur personnalisés.

STEP 1 | Planifiez la transition vers Panorama

Consultez la liste de contrôle dans Planifier la Transition vers la Gestion Panorama.

STEP 2 | Résoudre la gestion des paramètres dupliqués, c'est-à-dire ceux qui ont les mêmes noms dans Panorama et dans un pare-feu.

© 2020 Palo Alto Networks, Inc.

Avant de charger une configuration de pare-feu partielle, Panorama et ce pare-feu ont peut-être déjà dans des paramètres dupliqués. Charger une configuration de pare-feu peut aussi ajouter des paramètres au Panorama s'il y a des doublons de paramètres dans les autres pare-feu gérés.

Si Panorama a des règles de stratégie ou d'objets avec les mêmes noms que ceux d'un pare-feu, un échec de validation se produit lorsque vous essayez de pousser les paramètres de groupe de périphériques dans ce pare-feu. Si Panorama possède des paramètres de modèle avec les mêmes noms que ceux d'un pare-feu, les valeurs du modèle remplacent les valeurs de pare-feu lorsque vous appuyez sur le modèle.

1. Sur Panorama, effectuez une recherche globale afin de déterminer si les paramètres dupliqués existent.
2. Supprimez ou renommez les paramètres en double sur le pare-feu si vous utiliserez Panorama pour les gérer, ou supprimez ou renommez les paramètres dupliqués sur Panorama si vous utilisez le pare-feu pour les gérer. Si vous utilisez le pare-feu pour gérer les paramètres du périphérique ou du réseau, au lieu de supprimer ou de renommer les doublons sur Panorama, vous pouvez également appliquez les paramètres depuis Panorama (étape 6) et Remplacer un modèle ou une valeur de pile de modèles sur le pare-feu par des valeurs spécifiques au pare-feu.

STEP 3 | Exporter la configuration entière de pare-feu sur votre ordinateur local.

1. Sur le pare-feu, sélectionnez **Device (Périphérique)** > **Setup (configuration)** > **Operations (Opérations)**.
2. Cliquer **Save named configuration snapshot (enregistrer la configuration nommée snapshot)**, entrer un **Name (Nom)** pour identifier la configuration et cliquez sur **OK**.
3. Cliquez sur **Export named configuration snapshot (Exporter nommé instantané de la configuration)**, sélectionnez le **Name (Nom)** de la configuration que vous venez d'enregistrer et cliquez sur **OK**. Le pare-feu exporte la configuration dans un fichier XML.

STEP 4 | Importer la configuration du pare-feu dans Panorama.

1. Sur Panorama, sélectionnez **Panorama** > **Setup (configuration)** > **Operations (Opérations)**.
2. Cliquez sur **Import named Panorama configuration snapshot (Importer un snapshot de configuration nommé Panorama)**, **Browse (Naviguer)** le fichier de configuration de pare-feu que vous avez exporté vers votre ordinateur, puis cliquez **OK**.

Après avoir utilisé cette option pour importer un fichier de configuration de pare-feu, vous ne pouvez pas utiliser l'interface web de Panorama pour le charger. Vous devez utiliser l'API XML ou l'ILC, tel que décrit à l'étape suivante.

STEP 5 | Charger la partie désirée de la configuration du pare-feu dans Panorama.

Pour spécifier une partie de la configuration (par exemple, tous les objets d'application), vous devez identifier le :

- La Source Xpath - Le nœud XML dans le fichier de configuration du pare-feu d'où vous le chargez.
- La Destination Xpath - Le nœud XML dans la configuration Panorama où vous le chargez.

Utiliser l'API XML ou l'ILC pour identifier et charger la configuration partielle :

1. Utilisez le pare-feu XML API ou l'ILC pour identifier le xpath source.

   Par exemple, le xpath pour les objets d'application dans vsys1 du pare-feu est :

```
/config/devices/entry[@name='localhost.localdomain']/vsys/
entry[@name='vsys1']/application
```

2. Utilisez le Panorama XML API ou l'ILC pour identifier le xpath de la destination.

© 2020 Palo Alto Networks, Inc.

Par exemple, pour charger les objets d'application dans un groupe de périphériques nommé Ouest des États-Unis, l'expression xpath est :

```
/config/devices/entry[@name='localhost.localdomain']/device-group/
entry[@name='US-West']/application
```

3. L'ILC de Panorama permet de charger la configuration et de valider la modification :

```
# load config partial mode [append|merge|replace] from-xpath <source-
xpath> to-xpath <destination-xpath> depuis <filename>
# commit
```

Par exemple, entrez la commande suivante pour charger les objets de l'application de vsys1 sur une configuration de pare-feu importée appelée fw1-config.xml dans un groupe de périphériques nommé US-West sur Panorama :

```
# load config partial mode merge from-xpath devices/
entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/application
 to-xpath /config/devices/entry[@name='localhost.localdomain']/device-
group/entry[@name='US-West']/application from fw1-config.xml
# commit
```

STEP 6 | Insérer les configurations de groupe et modèle de périphérique dans le pare-feu pour terminer la transition vers une gestion centralisée.

1. Sur le pare-feu, supprimez les règles ou les objets qui ont les mêmes noms que ceux de Panorama. Si le groupe de périphériques pour ce pare-feu dispose d'autres pare-feu avec des règles ou des objets qui sont dupliqués dans Panorama, effectuez cette étape également sur les pare-feu. Pour plus d'informations, reportez-vous à l'étape 2.
2. Sur Panorama, appliquez la configuration partielle vers le pare-feu.
    1. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** et **Edit Selections (Modifier les sélections)** dans la portée d'application.
    2. Sélectionnez **Device Groups (Groupes de périphériques)** et sélectionnez les groupes de périphériques contenant les configurations de pare-feu importées.
    3. Sélectionnez **Merge with Device Candidate Config (Fusionner avec la configuration candidate du périphérique)**, **Include Device and Network Templates (Inclure les modèles de périphérique et de réseau)** et **Force Template Values (Forcer les valeurs de modèle)**.
    4. Cliquez sur **OK** pour enregistrer les modifications dans la portée d'application.
    5. **Commit and Push (Validez et appliquez)** vos modifications.
3. Si le pare-feu dispose d'un périphérique ou d'un paramètre de réseau pour lequel vous n'utiliserez pas Panorama pour gérer, Remplacer un modèle ou une valeur de pile de modèles sur le pare-feu.

STEP 7 | Exécutez votre plan de test post-migration.

Effectuez les tâches de vérification que vous avez conçues lors de la planification de la migration afin de confirmer que le pare-feu fonctionne aussi efficacement avec la configuration affichée par Panorama qu'avec sa configuration locale d'origine: voir Créer un plan de test post-migration.

© 2020 Palo Alto Networks, Inc.

Surveillance de périphériques sur Panorama

Après avoir ajouté vos pare-feu et configuré les règles de stratégie, vous pouvez surveiller l'état d'intégrité pour vous assurer que vos pare-feu fonctionnent dans des paramètres adéquats. Pour les règles de stratégie, surveillez les correspondances de trafic de règles afin d'identifier les règles correspondant à votre trafic.

- Surveiller l'état de santé du dispositif
- Surveiller la règle de Politique d'utilisation

Surveiller l'état de santé du dispositif

Surveillez les informations d'intégrité de vos pare-feu gérés pour identifier et résoudre les problèmes matériels avant qu'ils n'affectent la sécurité de votre réseau. Panorama ™ et les pare-feu gérés doivent exécuter PAN-OS® 8.1, ou une version ultérieure, mais les pare-feu n'ont pas besoin de faire partie d'un groupe de périphériques ou d'une pile de modèles pour surveiller leurs performances de session, de journalisation, de ressources et d'environnement. Panorama stocke les 90 derniers jours de statistiques de surveillance de l'état de vos pare-feu gérés. Lorsque vous sélectionnez un pare-feu, vous pouvez afficher les graphiques et les tableaux temporels pour les sessions, les environnements, les interfaces, la journalisation, les ressources et les performances haute disponibilité. Panorama calcule la performance de base de chaque mesure en utilisant des moyennes sur sept jours et l'écart-type pour déterminer une plage de fonctionnement normale pour le pare-feu spécifique. Outre le suivi de la référence et la comparaison des performances temporelles, vous pouvez afficher les pare-feu qui ont des statistiques divergentes et isoler les problèmes liés aux performances avant qu'ils n'affectent votre réseau. Lorsque Panorama identifie qu'une mesure se trouve en dehors de la plage de fonctionnement normale, elle marque la mesure et remplit l'onglet Périphériques déviants avec le pare-feu déviant.

Les données de surveillance de l'intégrité sont stockées dans Panorama et sont conservées dans le cas où un pare-feu soit supprimé. Lorsqu'un pare-feu est supprimé de la gestion Panorama, les données de surveillance de l'intégrité ne s'affichent plus mais sont conservées pendant 90 jours. Après 90 jours, toutes les données de surveillance d'intégrité du pare-feu supprimé sont supprimées de Panorama. Si un pare-feu est ajouté à la gestion Panorama, les dernières données de surveillance de l'état de santé à partir de la suppression du pare-feu s'affichent.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)** > **Health (Santé)** pour surveiller l'intégrité des pare-feu gérés.

Afficher **All Devices (Tous les périphériques)** pour afficher la liste de tous les pare-feu gérés et les statistiques d'intégrité surveillées. Sélectionnez un pare-feu individuel pour afficher la vue détaillée des périphériques avec des graphiques à tendance temporelle et des tableaux de métriques surveillées.

© 2020 Palo Alto Networks, Inc.

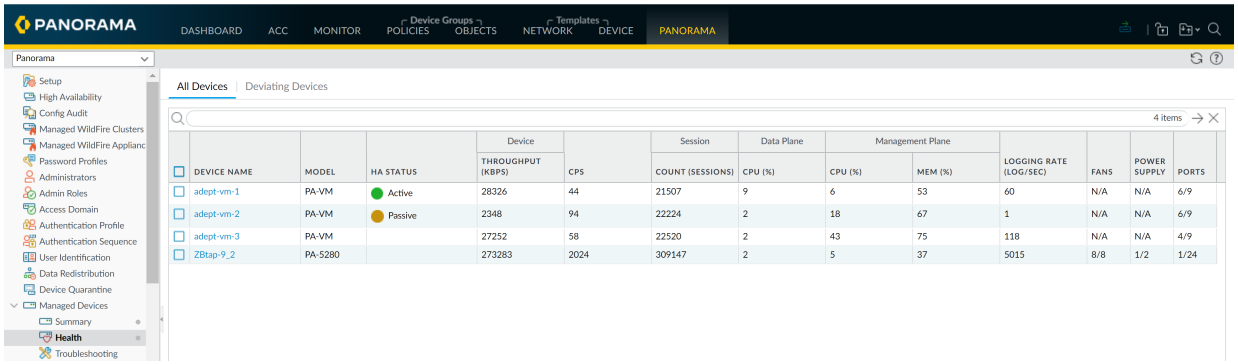


Figure 12: Surveillance de l'intégrité du pare-feu géré

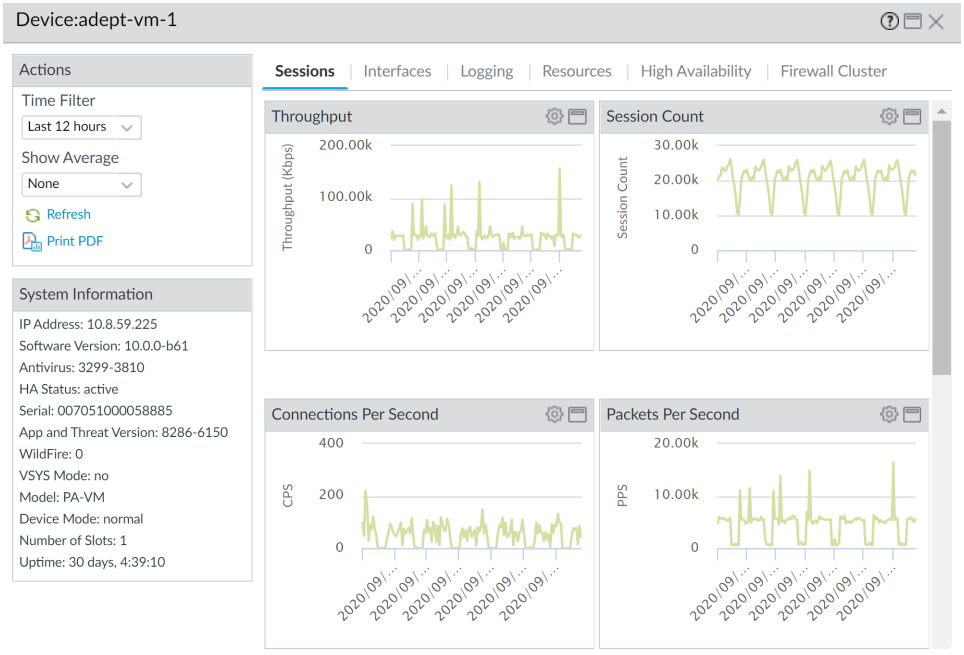
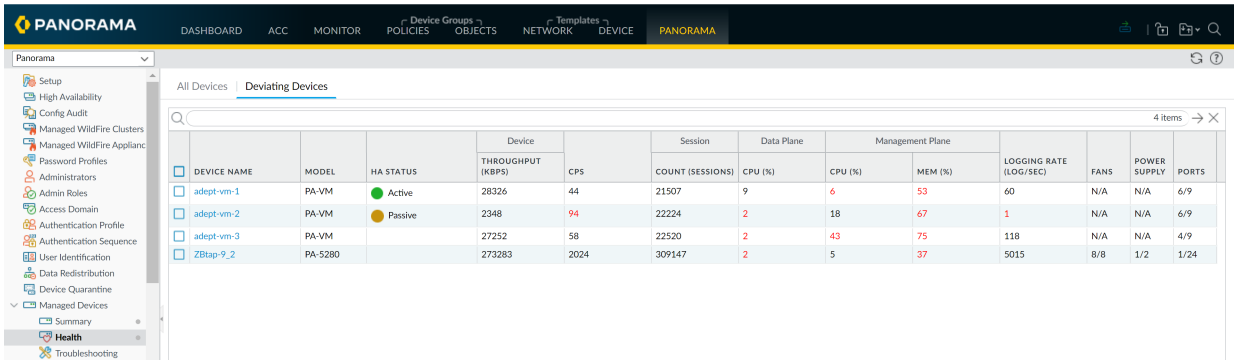


Figure 13: Vue détaillée de l'appareil

STEP 3 | Sélectionnez **Deviating Devices (Déviations de périphériques)** pour afficher les pare-feu dont les indicateurs de santé ont varié en dehors de la référence calculée

Panorama répertorie tous les pare-feu qui envoient des mesures qui s'écartent de la référence calculée et affiche les mesures divergentes en rouge.



© 2020 Palo Alto Networks, Inc.

Surveiller la règle de Politique d'utilisation

Au fur et à mesure que vos politiques d'utilisation changent, faire le suivi de l'utilisation de la règle Panorama vous permet d'évaluer si votre mise en œuvre de la politique continue de répondre à vos besoins de sécurité. Cette visibilité vous aide à identifier et à supprimer les règles inutilisées afin de réduire les risques de sécurité et à organiser votre base de règles de politique. En outre, le suivi de l'utilisation des règles vous permet de valider rapidement les ajouts de nouvelles règles et les modifications de règles, ainsi que de surveiller l'utilisation des règles pour les opérations et les tâches de dépannage. Sur Panorama, vous pouvez afficher l'utilisation de la règle des pare-feux dans un groupe de périphériques - auquel vous avez transmis les politiques - afin de déterminer si l'ensemble, si certains ou si aucun des pare-feux sont associés au trafic, au lieu de ne contrôler que le nombre total de visites par l'intermédiaire de tous les pare-feux d'un groupe de périphériques.. Vous pouvez rapidement filtrer les règles à l'aide des données d'utilisation des règles, comme les dates de création et de modification, au cours d'une période de temps pouvant être personnalisée. Les informations d'utilisation des règles qui s'affichent demeurent inchangées au redémarrage de l'équipement, au redémarrage du plan de données et lors des mises à niveau.

Sur Panorama, vous pouvez afficher les détails de l'utilisation des règles pour les pare-feux gérés qui exécutent PAN-OS 8.1 ou toute version ultérieure, sur lesquels le nombre de correspondances d'utilisation des règles de politique est activé (par défaut) et sur lesquels vous avez défini des règles de politique et auxquels vous les avez transmis à l'aide de groupes de périphériques. Panorama ne peut récupérer les détails sur l'utilisation des règles pour les règles de politique configurées localement sur le pare-feu. Vous devez donc vous connecter au pare-feu pour afficher les informations sur l'utilisation des règles pour les règles configurées localement.

Après avoir filtré votre base de règles de politique, les administrateurs peuvent prendre une mesure pour supprimer, désactiver, activer et étiqueter les règles de politique directement depuis l'optimiseur de politiques. Par exemple, vous pouvez filtrer les règles non utilisées puis les étiqueter afin de les examiner et déterminer si elles peuvent être supprimées ou conservée en toute sécurité dans la base de règles. En permettant aux administrateurs de prendre une mesure directement depuis l'optimiseur de politiques, vous pouvez réduire les coûts et temps de gestion nécessaires en simplifiant la gestion du cycle de vie de vos règles et vous assurer que vos pare-feux ne sont pas configurés avec un excès anormal de règles.

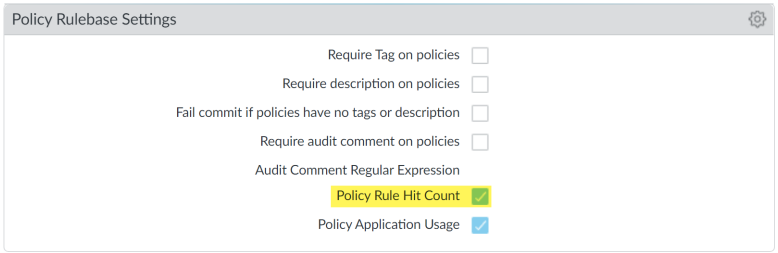
Les données sur l'utilisation des règles de politique peuvent également s'avérer utiles lors de l'utilisation de l'optimiseur de politique afin d'établir la priorité des règles à migrer ou nettoyer en premier.

Pour afficher l'utilisation d'une règle partagée ou d'un groupe de périphériques spécifique :

STEP 1 | Se connecter à l'interface Web Panorama.

STEP 2 | Vérifiez que le **nombre de correspondance à la règle de politique** est activé.

1. Naviguer vers les paramètres de la base de règles de politique (**Panorama** > **Setup (Configuration)** > **Management (Gestion)**.
2. Vérifiez que le **Policy Rule Hit Count (Nombre de correspondance à la règle de politique)** est activé.



© 2020 Palo Alto Networks, Inc.

STEP 3 | Sélectionnez **Policies (Politiques)** > *<policy rule> (<règle de politique>)* pour afficher une règle.

STEP 4 | Faites passer le contexte du groupe de périphériques à **Shared (partagé)** ou au groupe de périphériques spécifique que vous souhaitez afficher.

STEP 5 | Déterminez si la règle est utilisée (Utilisation des règles). La politique de la règle d'utilisation contient l'un des éléments suivants :

Les pare-feu doivent utiliser PAN-OS 8.1 ou une version ultérieure et le Nombre de correspondances à la règle de politique doit être activé pour Panorama pour en déterminer l'utilisation.

- **Utilisée** : lorsque tous les pare-feu du groupe de périphériques - auquel vous avez transmis la règle de politique - trouvent du trafic qui correspond à règle de politique.
- **Utilisée partiellement** : lorsque certains pare-feu du groupe de périphériques - auquel vous avez transmis la règle de politique - trouvent du trafic qui correspond à règle de politique.
- **Non-utilisé** : lorsqu'aucun pare-feu du groupe de périphériques - auquel vous avez transmis la règle de politique - ne trouve de trafic qui correspond à règle de politique.
- **Em-dash (—)** : lorsqu'aucun pare-feu du groupe de périphériques - auquel vous avez transmis la règle de politique - n'a activé le Nombre de correspondances à la règle de politique ou que celui-ci n'est pas disponible pour Panorama afin de déterminer l'utilisation de la règle.
- **Modified (Modification)** : Date et heure de la dernière modification de la règle de politique.
- **Created (Création)** : Date et heure de création de la règle de politique.

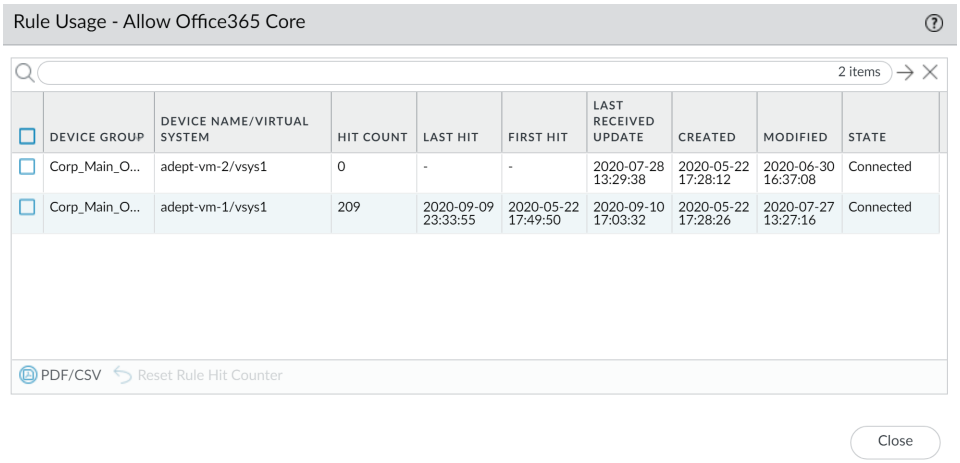


Si la règle a été créée lorsque Panorama exécutait PAN-OS 8.1 et que le paramètre du Nombre de correspondances à la règle de politique est activé, la date et l'heure de la première correspondance sont utilisées en tant que date et heure de création lors de la mise à niveau vers PAN-OS 9.0 ou des versions ultérieures. Si la règle a été créée dans PAN-OS 8.1 lorsque le paramètre du Nombre de correspondances à la règle de politique est désactivé, ou si la règle a été créée lorsque Panorama exécutait PAN-OS 8.0 ou toute version antérieure, la date de création de la règle sera égale à celle de la mise à niveau de Panorama vers PAN-OS 9.0 ou une version ultérieure.

Rule Usage		DAYS WITH NO NEW APPS	MODIFIED	CREATED
RULE USAGE	APPS SEEN			
Used	6	150	2020-06-24 10:34:...	2020-04-09 11:34:03
Unused	0	-	2020-06-24 10:34:...	2020-04-16 11:42:46
Used	11	57	2020-06-24 10:34:...	2020-04-16 11:42:46
Partially Used	3	111	2020-06-24 10:34:...	2020-05-22 17:26:44
Unused	0	-	2020-06-24 10:34:...	2020-05-22 22:45:53

STEP 6 | Cliquez sur l'état de l'utilisation des règles pour afficher la liste des pare-feux utilisant la règle et les données relatives au Nombre de correspondances pour le trafic correspondant à cette règle sur chaque pare-feu.

© 2020 Palo Alto Networks, Inc.



STEP 7 | (Facultatif) Affichez les données relatives au nombre de correspondances d'utilisation des règles de politique pour les pare-feux individuels qui composent le groupe de périphériques.

1. Cliquez sur **Preview Rules (Aperçu des règles)**.
2. À partir du contexte Périphérique, sélectionnez le pare-feu pour lequel vous souhaitez afficher les données d'utilisation de la règle de politique.

STEP 8 | Sélectionnez **Policies (Politiques)**, et dans la boîte de dialogue de l'Optimiseur de politique, cliquez sur le filtre **Rule Usage (Utilisation des règles)**.

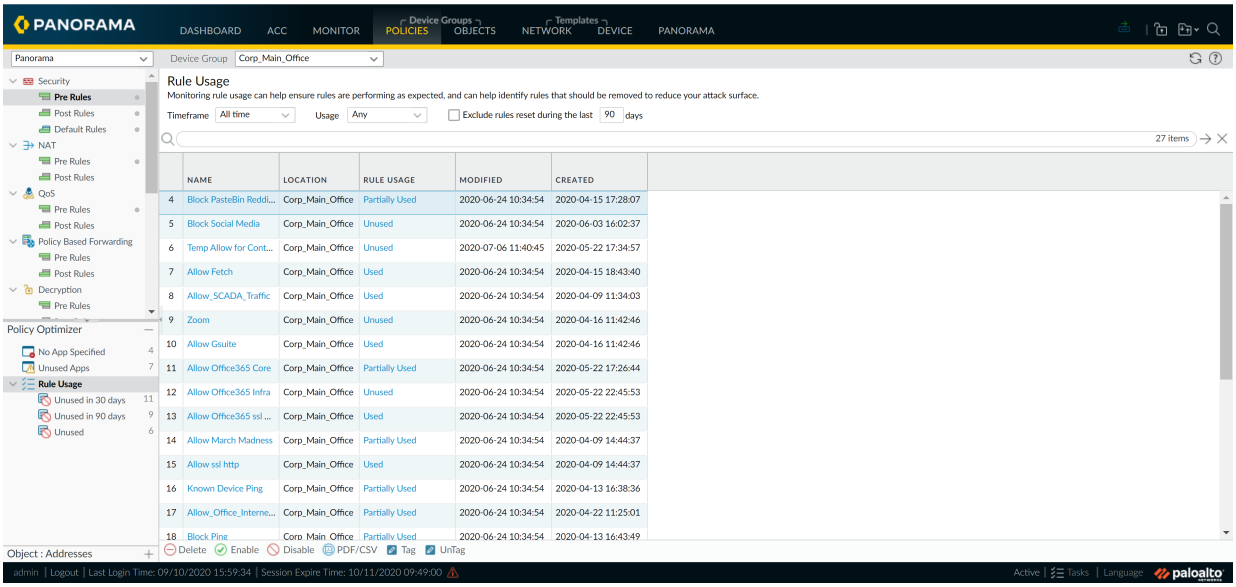
STEP 9 | Filtrez les règles de la base de règles sélectionnée.

Vous pouvez filtrer l'utilisation des règles pour les règles transmises aux pare-feu à partir de Panorama. Panorama ne peut filtrer l'utilisation des règles pour les règles configurées localement sur le pare-feu.

Utilisez le filtre d'utilisation des règles pour évaluer l'utilisation des règles sur une période de temps donnée. Par exemple, filtrez la base de règles sélectionnée pour connaître les règles non utilisées au cours des 30 derniers jours. Vous pouvez également évaluer l'utilisation des règles en utilisant d'autres attributs, comme les dates de création et de modification, ce qui vous permet de filtrer le bon ensemble de règles à passer en revue. Vous pouvez utiliser ces données pour vous aider à gérer le cycle de vie de vos règles pour déterminer si une règle doit être supprimée afin de réduire la surface d'attaque de votre réseau.

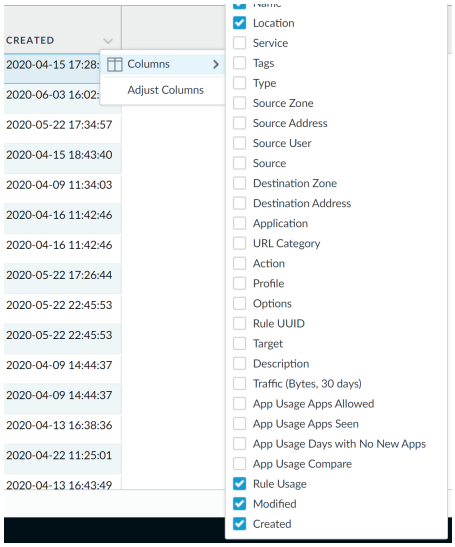
1. Sélectionnez la **Timeframe (Période)** à laquelle vous souhaitez appliquer le filtre, ou spécifiez une période **Custom (Personnalisée)**.
2. Sélectionnez la règle **Usage** pour laquelle vous souhaitez appliquer le filtre.
3. (Facultatif) Si vous avez réinitialisé les données d'utilisation d'une règle, cochez la case **Exclure les règles réinitialisées au cours des derniers** *<nombre de jours>* **jours** et déterminez quand exclure une règle en fonction du nombre de jours que vous avez indiqué depuis la réinitialisation de la règle. Seules les règles qui ont été réinitialisées avant le nombre de jours indiqués sont incluses dans les résultats du filtrage.

© 2020 Palo Alto Networks, Inc.



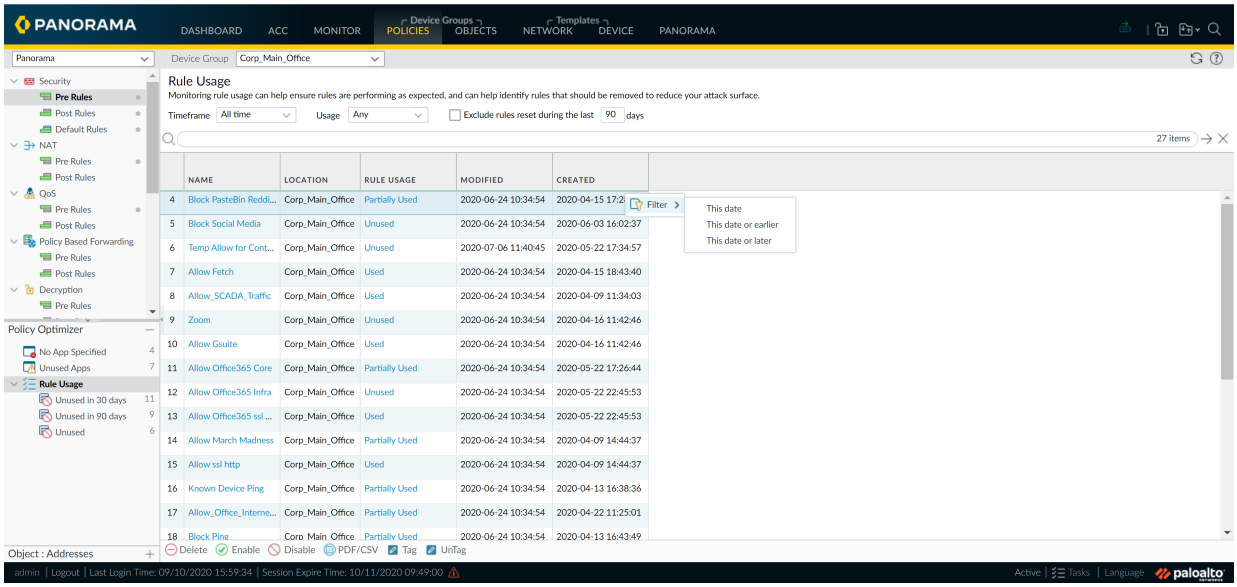
4. (Facultatif) Spécifiez des filtres de recherche qui reposent sur des données sur les règles supplémentaires, autres que l'utilisation des règles.

   1. Faites glisser votre souris sur l'en-tête de colonne et, dans le menu déroulant, sélectionnez **Columns (Colonnes)**.
   2. Ajoutez des colonnes supplémentaires à utiliser pour le filtrage ou à afficher.



   3. Faites glisser votre souris sur les données des colonnes à utiliser pour le filtrage et sélectionnez **Filter (Filtrer)** dans le menu déroulant. Pour les données comprenant des dates, sélectionnez l'option de filtrage souhaitée : **This date (Cette date)**, **This date or earlier (Cette date ou avant cette date)** ou **This date or later (Cette date ou après cette date)**.
   4. Cliquez sur **Apply Filter (Appliquer le filtre)** (→).

© 2020 Palo Alto Networks, Inc.



STEP 10 | Prenez une mesure pour une ou plusieurs politiques non utilisées.

1. Sélectionnez une ou plusieurs règles de politique non utilisées.
2. Effectuez l'une des actions suivantes :
   - **Delete (Supprimer)** : supprimez une ou plusieurs règles de politique sélectionnées.
   - **Enable (Activer)** : activez une ou plusieurs règles de politique sélectionnées.
   - **Disable (Désactiver)** : désactivez une ou plusieurs règles de politique sélectionnées.
   - **Tag (Etiqueter)** : appliquez une ou plusieurs étiquettes de groupe à une ou plusieurs règles de politique. L'étiquette de groupe doit déjà exister afin d'étiqueter la règle de politique.
   - **Untag (Supprimer l'étiquette)** : retirez une ou plusieurs étiquettes de groupe d'une ou plusieurs règles de politique.
3. Sélectionnez**Commit** (Validez) et **Commit and Push** (Validez et appliquez) vos modifications.

© 2020 Palo Alto Networks, Inc.

Cas d’utilisation : Configurer des pare-feux en utilisant Panorama

Disons que vous voulez utiliser Panorama dans une configuration de haute disponibilité pour gérer une douzaine de pare-feux sur votre réseau : vous avez six pare-feux déployés à travers six succursales, une paire de pare-feux dans une configuration de haute disponibilité à chacun des deux centres de données et un pare-feu dans chacun des deux bureaux régionaux de direction.

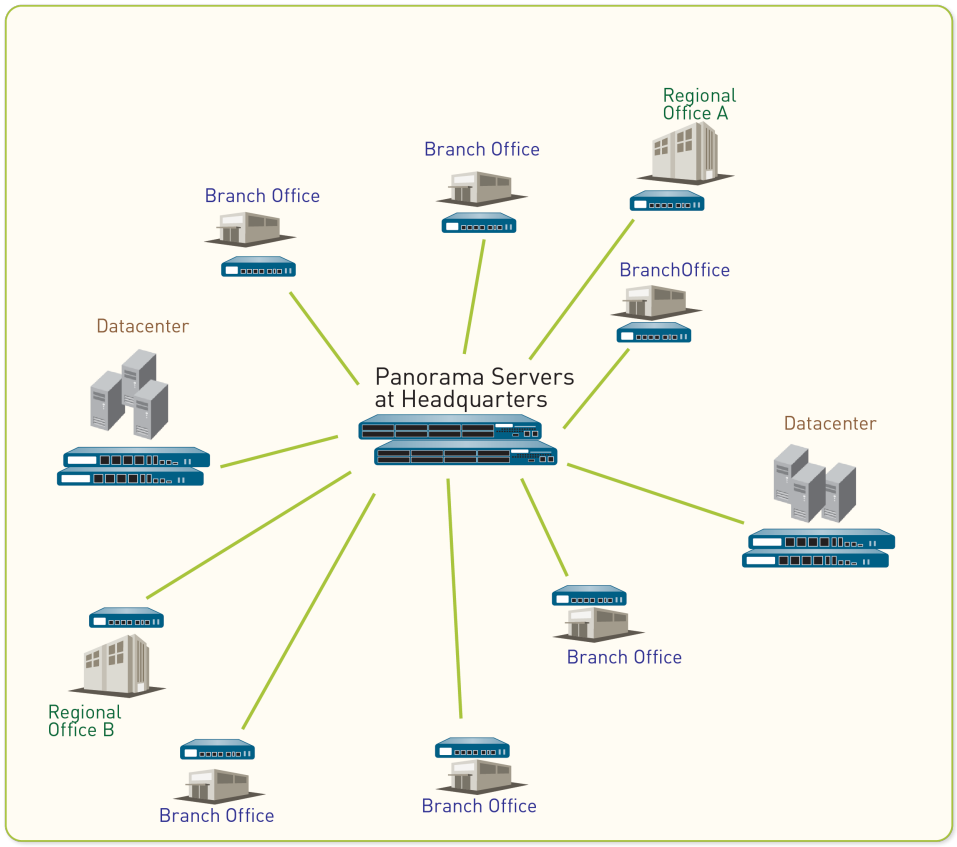


Figure 14: Exemple de distribution de pare-feu

La première étape de la création de votre stratégie de gestion centralisée consiste à déterminer comment regrouper les pare-feux en groupes de périphériques et modèles, pour transmettre les configurations efficacement à partir de Panorama. Vous pouvez fonder le regroupement sur les fonctions de l'entreprise, les lieux géographiques ou les domaines administratifs des pare-feux. Dans cet exemple, vous créez deux groupes de périphériques et trois modèles pour administrer les périphériques à l'aide de Panorama.

- Groupes de périphériques dans ce cas d'utilisation
- Modèles dans ce cas d'utilisation
- Paramétrer la configuration et les stratégies centralisées

Groupes de périphériques dans ce cas d'utilisation

Dans Cas d’utilisation : Configurer des pare-feux en utilisant Panorama, nous devons définir deux groupes de périphériques basés sur les fonctions, que les pare-feu produiront :

© 2020 Palo Alto Networks, Inc.

- "DG_BranchAndRegional" pour regrouper les périphériques servant de portails de sécurité dans les succursales et les sièges régionaux. Nous avons placé les pare-feu de la succursale et les pare-feu des bureaux régionaux dans le même groupe de périphériques, car les pare-feu dotés de fonctions similaires nécessiteront des règles de bases de politique similaires.
- "DG_DataCenter" pour regrouper les dispositifs qui sécurisent les serveurs aux centres de données.

Nous pouvons alors administrer les règles de stratégie partagée entre les deux groupes de périphériques comme administrer les règles de groupe d'appareils distincts pour les groupes du siège régional et les succursales régionales. Puis, pour plus de flexibilité, l'administrateur local d'un siège régional ou d'une succursale peut créer des règles locales qui correspondent à des sources, des destinations et des flux de services spécifiques pour accéder à des applications et des services nécessaires à ce bureau. Dans cet exemple, nous créons la hiérarchie suivante pour les règles de sécurité. Vous pouvez utiliser une approche similaire pour tous les autres modules.

Device Groups	DG_BranchAndRegional		DG_DataCenter
Rules	**Regional**	**Branch**	**Datacenter**
Shared pre-rule	Allow DNS and SNMP services.		
	Acceptable use policy that denies access to specified URL categories and peer-to-peer traffic that is of risk level 3, 4, and 5.		
Device Group pre-rule	Allow Facebook to all users in the marketing group in the regional offices only.		Allow access to the Amazon cloud application for the specified hosts/servers in the datacenter.
Local rules on a device	None		
Device Group post-rule	None		
Shared post-rule	To enable logging for all Internet-bound traffic on your network, create a rule that allows or denies all traffic from the trust zone to the untrust zone.		

Figure 15: Hiérarchie des règles de sécurité

Modèles dans ce cas d'utilisation

Lorsque nous regroupons des pare-feux pour les modèles, nous devons tenir compte des différences dans la configuration du réseau. Par exemple, si la configuration de l'interface n'est pas la même, les interfaces sont à la différence des caractères, les interfaces utilisées ne se ressemblent pas dans la capacité de régime et lien numérotation ou la zone aux mappages d'interface sont différentes — les pare-feux doivent être dans des modèles distincts. En outre, la façon dont les pare-feux sont configurés pour accéder aux ressources réseau peut être différente car les pare-feux sont répartis géographiquement ; par exemple, le serveur DNS, serveurs syslog et passerelles qui ils accèdent aux peuvent être différents. Ainsi, pour permettre une configuration optimale de base dans Cas d'utilisation : Configurer des pare-feux en utilisant Panorama, vous devez placer les pare-feu dans des modèles distincts comme suit :

- T_Branch pour les pare-feux du Bureau de direction
- T_Regional pour les pare-feux de bureau régional
- T_DataCenter pour les pare-feux du centre de données

© 2020 Palo Alto Networks, Inc.

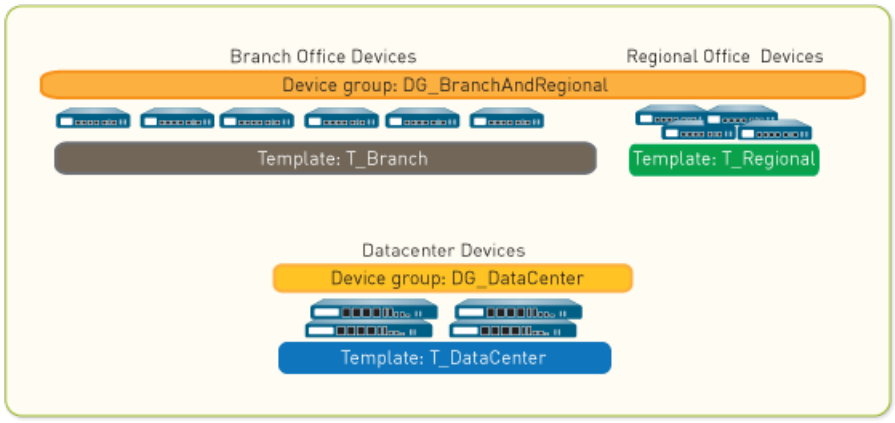


Figure 16: Exemple de groupe de périphériques

Si vous prévoyez de déployer vos pare-feux dans une configuration active/active HD, assignez chaque pare-feu dans la paire HD à un modèle distinct. Cette opération vous offre la souplesse nécessaire à l'installation des configurations réseau sur chaque homologue. Par exemple, vous pouvez gérer la configuration réseau dans un modèle séparé pour chaque homologue, de sorte que chacun puisse se connecter à des routeurs en amont ou en aval, et ils peuvent présenter des configurations d'homologues OSPF ou BGP différentes.

Paramétrer la configuration et les stratégies centralisées

Dans Cas d'utilisation : Configurer des pare-feux en utilisant Panorama, il nous faudrait effectuer les tâches suivantes pour déployer et administrer les pare-feu de manière centralisée :

- Ajouter des pare-feu gérés et déployer les mises à jour
- Utilisez des modèles pour gérer une configuration de base.
- Utiliser des groupes de périphériques pour insérer les règles de stratégie
- Prévisualiser les règles et valider les modifications

Ajouter des pare-feu gérés et déployer les mises à jour

La première tâche dans Cas d'utilisation : Configurer des pare-feux en utilisant Panorama consiste à ajouter les pare-feu en tant que périphériques gérés et à déployer des mises à jour de contenu et des mises à jour logicielles PAN-OS sur ces pare-feu.

STEP 1 | Pour chaque pare-feu que Panorama va gérer, Ajouter un pare-feu en tant que périphérique géré.

Dans cet exemple, ajoutez 12 pare-feux.

STEP 2 | Déployez les mises à jour de contenu sur les pare-feux. Si vous avez acheté un abonnement de prévention de menaces, vous avez accès aux bases de données de contenu et d'antivirus. Tout d'abord installer les **Applications** ou les **Applications and Threats (Applications et les bases de données de menaces)**, puis l'**Antivirus**.

Pour consulter l'état ou la progression de toutes les tâches effectuées sur Panorama, reportez-vous à la section Utilisez le Gestionnaire de Tâches Panorama.

© 2020 Palo Alto Networks, Inc.

1. Sélectionnez **Panorama (Panorama)** > **Device Deployment (Déploiement du périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**.
2. Cliquez sur **Check Now (Vérifier maintenant)** pour rechercher les dernières mises à jour. Si la valeur figurant dans la colonne Action est **Download (Télécharger)**, cela indique qu'une mise à jour est disponible.
3. Cliquez sur **Download (Télécharger)**. Une fois le téléchargement terminé, la valeur se trouvant dans la colonne Action passe à **Install (Installer)**.
4. Dans la colonne **Action**, cliquez sur **Install (Installer)**. Utilisez des filtres ou les balises définies par l'utilisateur pour sélectionner les pare-feux gérés sur lesquels vous souhaitez installer la mise à jour.
5. Cliquez sur **OK**, puis surveillez l'état, la progression et le résultat de la mise à jour de contenu pour chaque pare-feu. La**Result (Résultat)** colonne indique le succès ou l'échec de l'installation.

STEP 3 | Déployez les mises à jour logicielles sur les pare-feux.

1. Sélectionnez **Panorama** > **Device Deployment (Déploiement de périphérique)** > **Software (Logiciel)**.
2. Cliquez sur **Check Now (Vérifier maintenant)** pour rechercher les dernières mises à jour. Si la valeur figurant dans la colonne Action est **Download (Télécharger)**, cela indique qu'une mise à jour est disponible.
3. Localisez la version dont vous avez besoin pour chaque modèle de matériel, puis cliquez sur **Download (Télécharger)**. Une fois le téléchargement terminé, la valeur se trouvant dans la colonne Action passe à **Install (Installer)**.
4. Dans la colonne Action, cliquez sur le lien **Install (Installer)**. Utilisez des filtres ou des balises définies par l'utilisateur pour sélectionner les pare-feux gérés sur lesquels vous souhaitez installer cette version.
5. Activez la case à cocher **Reboot device after install (Redémarrer le périphérique après l'installation)** ou **Upload only to device (do not install) (Charger sur le périphérique seulement (ne pas installer))** puis cliquez sur **OK**. La colonne **Results (Résultats)** affiche le succès ou l'échec de l'installation.

Utilisez des modèles pour gérer une configuration de base.

La seconde tâche du cas d'utilisation : Configurez les pare-feux à l'aide de Panorama consiste à créer les modèles dont vous aurez besoin pour insérer la configuration de base sur les pare-feux.

STEP 1 | Pour chaque modèle que vous allez utiliser, Ajouter un modèle et attribuer les pare-feux appropriés à chacun d'eux.

Dans cet exemple, créer des modèles nommés T_Branch, T_Regional et T_DataCenter.

STEP 2 | Définir un serveur DNS, un serveur NTP , un serveur syslog et bannière de connexion. Répétez cette étape pour chaque modèle.

1. Dans l'onglet **Device (Périphérique)**, sélectionnez le **Template (Modèle)** dans la liste déroulante.
2. Définir les serveurs DNS et NTP :
    1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Services (Services)** > **Global (Global)** et modifiez la section Services.
    2. Dans l'onglet **Services (Services)**, entrez une adresse IP pour le **Primary DNS Server (serveur DNS principal)**.

        Pour n'importe quel pare-feu qui a plus qu'un système virtuel (vsys), pour chaque vsys, ajoutez un profil de serveur DNS au modèle (Device (dispositif) > Server Profiles (profils de serveur) > DNS (DNS)).
    3. Dans l'**NTP** (NTP) onglet, entrez une adresse IP pour le **Primary NTP Server (serveur NTP primaire)**.
    4. Cliquez sur **OK** pour enregistrer vos modifications.

© 2020 Palo Alto Networks, Inc.

3. Ajoutez une bannière de connexion : sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** , modifiez les paramètres généraux, saisissez le texte de la **Login Banner (bannière de connexion)** et cliquez sur **OK**.
4. Configurez un profil de serveur Syslog (**Device (Périphérique)** > **Server Profiles (Profils Serveur)** > **Syslog**).

STEP 3 | Activez l'accès à HTTPS, SSH et SNMP pour gérer l'interface de gestion des pare-feux gérés. Répétez cette étape pour chaque modèle.

1. Dans l'onglet **Device (Périphérique)**, sélectionnez le **Template (Modèle)** dans la liste déroulante.
2. Sélectionnez **Setup (Configuration)** > **Management (Gestion)**, puis modifiez les paramètres d'interface de gestion.
3. Sous Services, sélectionnez les cases à cocher **HTTPS**, **SSH** et **SNMP** cases à cocher et cliquez sur **OK**.

STEP 4 | Créer un profil de Protection de Zone pour les pare-feux dans le modèle du centre de données (T_DataCenter).

1. Sélectionnez l'onglet **Network (Réseau)** et, dans le menu déroulant **Template (Modèle)**, sélectionnez T_DataCenter.
2. Sélectionnez **Network Profiles (Profils réseau)** > **Zone Protection (Zone de protection)** et cliquez sur **Add (Ajouter)**.
3. Dans cet exemple, nous allons activer la protection contre une Saturation SYN : dans l'onglet **Flood Protection (Protection contre la saturation)**, cochez la case **SYN**, définissez la valeur **Action** sur **SYN Cookies (Cookies SYN)** et définissez le nombre de paquets/seconde de la valeur **Alert (Alerte)** sur `100`, définissez le nombre de paquets/seconde de la valeur **Activate (Activer)** sur `1000`, puis définissez le nombre de paquets/seconde **Maximum** sur `10000`.
4. Dans cet exemple, nous allons activer les alertes : dans l'onglet **Reconnaissance Protection (Protection contre la reconnaissance)**, cochez les cases **Enable (Activer)** cases à cocher pour le **TCP Port Scan (scan d'hôte de port TCP)**, le **Host Sweep (scan d'hôte)**, et le **UDP Port Scan (scan de port UDP)**. Assurez-vous que les valeurs Action sont définies sur **alert (alerte)** (valeur par défaut).
5. Cliquez sur **OK** pour enregistrer le profil de Protection de Zone.

STEP 5 | Configurer les paramètres de l'interface et de la zone dans le modèle de centre de données (T_DataCenter) et joignez ensuite le profil de Protection de Zone, que vous venez de créer.



Avant d'effectuer cette étape, vous devez avoir configuré les interfaces localement sur les pare-feux. Au minimum, pour chaque interface, vous devez avoir défini le type d'interface, l'attribuer à un routeur virtuel (si nécessaire) et l'attacher à une zone de sécurité.

1. Sélectionnez l'onglet **Network (Réseau)** et, dans le menu déroulant **Template (Modèle)**, sélectionnez T_DataCenter.
2. Sélectionnez **Network (Réseau)** > **Interface** et, dans la colonne interface, cliquez sur le nom de l'interface.
3. Sélectionnez le **Interface Type (Type d'interface)** dans le menu déroulant.
4. Dans la liste déroulante **Virtual Router (Routeur virtuel)**, cliquez sur **New Virtual Router (Nouveau routeur virtuel)**. Lorsque vous définissez le routeur, assurez-vous que le **Name (nom)** correspond à la définition présente sur le pare-feu.
5. Dans la liste déroulante **Security Zone (Zone de sécurité)**, cliquez sur **New Zone (Nouvelle zone)**. Lorsque vous définissez la zone, assurez-vous que le **Name (nom)** correspond à la définition présente sur le pare-feu.
6. Cliquez sur **OK** pour enregistrer vos modifications d'interface.
7. Sélectionnez **Network (Réseau)** > **Zones**, puis sélectionnez la zone que vous venez de créer. Vérifiez que l'interface correcte est associée à la zone.

© 2020 Palo Alto Networks, Inc.

8. Dans la liste déroulante **Zone Protection Profile (Profil de Protection de Zone)**, sélectionnez le profil que vous avez créé et cliquez sur **OK**.

STEP 6 | Appliquez vos modifications de modèle.

1. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** et **Edit Selections (Modifier les sélections)** dans la portée d'application.
2. Sélectionnez **Templates (Modèles)** et sélectionnez les pare-feu affectés aux modèles dans lesquels vous avez effectué des modifications.
3. **Commit and Push (Validez et appliquez)** vos modifications à la configuration Panorama et au modèle.

Utiliser des groupes de périphériques pour insérer les règles de stratégie

La première tâche du cas d'utilisation : Configurer les pare-feu à l'aide de Panorama consiste à créer les groupes de périphériques pour gérer les règles de politiques sur les pare-feu.

STEP 1 | Créer des groupes de périphériques et attribuer les pare-feux appropriés à chaque groupe de périphériques : voir ajouter un groupe de périphériques.

Dans cet exemple, créez des groupes de périphériques nommés DG_BranchAndRegional et DG_DataCenter.

Lorsque vous configurez le groupe DG_BranchAndRegional de périphériques, vous devez affecter un **Master (maître)** pare-feu. C'est le seul pare-feu dans le groupe qui rassemble les utilisateurs et les informations de mappage de groupe pour l'évaluation des politiques.

STEP 2 | Créez une pré-règle partagée, pour activer les services DNS et SNMP.

1. Créez un groupe d'applications partagées, pour les services DNS et SNMP.
    1. Sélectionnez **Objects (Objets)** > **Application Group (Groupe d'applications)** et cliquez sur **Add (Ajouter)**.
    2. Entrez un **Name (nom)** et sélectionnez la case à cocher pour créer un objet de groupe d'applications partagées **Shared (Partagées)**.
    3. Cliquez sur **Add (Ajouter)**, saisissez **DNS**, et sélectionnez **dns**dans la liste. Répéter pour SNMP et sélectionnez **snmp**, **snmp-trap**.
    4. Cliquez sur **OK** pour créer le groupe d'applications.
2. Création de la règle partagée.
    1. Sélectionnez l'onglet **Policies (Politiques)** et, dans le menu déroulant **Device Group (Groupe de périphériques)**, sélectionnez **Shared (Partagé)**.
    2. Sélectionnez la règle de base **Security (Sécurité)** > **Pre-Rules (Pré-règles)**.
    3. Cliquez sur **Add (Ajouter)** et entrez un **Name (Nom)** pour la règle de sécurité.
    4. Dans les onglets **Source** et **Destination** de la règle, cliquez sur **Add (Ajouter)** et entrez une **Source Zone (Zone source)** et une **Destination Zone (Zone de destination)** pour le trafic.
    5. Dans l'onglet **Applications**, cliquez sur **Add (Ajouter)**, saisissez le nom d'objet de groupe d'applications que vous avez créé au préalable, puis sélectionnez-le dans le menu déroulant.
    6. Dans l'**Actions** onglet, mettre **Action** sur **Allow (permettre)**, et cliquer **OK**.

STEP 3 | Définissez la politique d'utilisation acceptable de l'entreprise pour tous les bureaux. Dans cet exemple, créez une règle commune qui restreint l'accès à certaines catégories d'URL et refuse l'accès au trafic poste-à-poste qui est du niveau de risque 3, 4 ou 5.

1. Sélectionnez l'onglet **Policies (Politiques)** et, dans le menu déroulant **Device Group (Groupe de périphériques)**, sélectionnez **Shared (Partagé)**.
2. Sélectionnez **Security (Sécurité)** > **Pre-Rules (Pré-Règles)** et cliquez sur **Add (Ajouter)**.
3. Dans l'onglet **General (général)**, entrez un **Name (Nom)** pour la règle de sécurité.

© 2020 Palo Alto Networks, Inc.

4. Dans les onglets **Source** et **Destination**, cliquez sur **Add (Ajouter)** et sélectionnez **any (tout)** pour les **Source Zone (Zone source)** et **Destination Zone (Zone de destination)** du trafic.
5. Dans l'onglet **Application**, définissez le filtre d'application :
    1. Cliquez sur **Add (Ajouter)**, puis cliquez sur **New Application Filter (Nouveau filtre d'application)** dans le bas de la liste déroulante.
    2. Saisissez un **Name (Nom)**, et cochez la case **Shared (Partagé)**.
    3. Dans la colonne Risques, sélectionnez les niveaux **3**, **4**, et **5**.
    4. Dans la colonne Technologie, sélectionnez **peer-to-peer (poste-à-poste)**.
    5. Cliquez sur **OK** pour enregistrer le nouveau filtre.
6. Dans l'**Service/URL Category (Catégorie de service/d'URL)** section Catégorie d'URL , cliquez sur **Add (Ajouter)** et sélectionnez les catégories d'URL que vous souhaitez bloquer, (par exemple, **streaming-media (les supports de diffusion)**, **dating (rencontres)**, et **online-personal-storage (le stockage personnel en ligne)**).
7. Vous pouvez également joindre le profil de filtrage d'URL par défaut —dans l'**Actions (Actions)** onglet, section de paramètre de profil, sélectionnez les **Profile Type (Type de profil)** option **Profiles (Profils)**, et sélectionnez l'**URL Filtering (filtrage d'URL)** option **default (défaut)**.
8. Cliquez sur **OK** pour enregistrer la pré-règle de sécurité.

STEP 4 | Autoriser Facebook à tous les utilisateurs dans le groupe de Marketing dans les bureaux régionaux uniquement.

L'activation d'une règle de sécurité basée sur l'utilisateur et le groupe a les tâches préalables requises suivantes :

- Mettre en place l'ID utilisateur sur les pare-feux.
- Activez l'ID utilisateur pour chaque zone qui contient les utilisateurs que vous souhaitez identifier.
- Définissez un pare-feu principal pour le groupe de périphériques DG_BranchAndRegional (voir l'étape 1).

1. Sélectionnez l'onglet **Policies (stratégies)** et, dans le menu déroulant **Device Group (Groupe de périphériques)**, sélectionnez DG_BranchAndRegional.
2. Sélectionnez la règle de base **Security (Sécurité)** > **Pre-Rules (Pré-règles)**.
3. Cliquez sur **Add (Ajouter)** et entrez un **Name (Nom)** pour la règle de sécurité.
4. Dans l'onglet **Source**, **Add (Ajoutez)** la zone source qui contient les utilisateurs du groupe Marketing.
5. Dans l'onglet **Destination**, **Add (Ajouter)** la zone de destination.
6. Dans l'onglet **User (utilisateur)**, **Add (ajoutez)** le groupe d'utilisateurs de Marketing à la liste des utilisateurs de la Source.
7. Dans l'onglet **Application (Application)**, cliquez sur **Add (Ajouter)**, saisissez `Facebook`, puis sélectionnez cette option dans le menu déroulant.
8. Dans l'onglet **Action**, définissez la valeur **Action** sur **Allow (Autoriser)**.
9. Dans l'onglet **Target (Cible)**, sélectionnez les pare-feux du bureau régional, et cliquez sur **OK**.

STEP 5 | Autoriser l'accès à l'application cloud d'Amazon pour les hôtes/serveurs spécifiés dans le centre de données.

1. Créez un objet adresse pour les serveurs/hôtes dans le centre de données qui ont besoin d'accéder à l'application de cloud d'Amazon.
    1. Sélectionnez**Objects (Objets)** > **Addresses (Adresses)** et, dans le menu déroulant **Device Group (groupe de périphériques)**, sélectionnez DG_DataCenter.
    2. Cliquez sur**Add (Ajouter)** et entrez un **Name (Nom)** pour l'adresse objet.
    3. Sélectionnez le **Type** et spécifiez une adresse IP et le masque de réseau (**IP Netmask (Masque de réseau IP)**, une plage d'adresses IP (**IP Range (Plage d'adresses IP)**), ou un **FQDN (Nom de domaine complet)**.

© 2020 Palo Alto Networks, Inc.

4. Cliquez sur**OK** pour enregistrer la règle.

2. Créer une règle de sécurité qui permet d'accéder à l'application cloud d'Amazon.
    1. Sélectionnez **Policies (Stratégies)** > **Security (Sécurité)** > **Pre-Rules (Pré-règles)** et, dans la liste déroulante **Device Group (Groupe de périphériques)**, sélectionnez DG_DataCenter.
    2. Cliquez sur **Add (Ajouter)** et entrez un **Name (Nom)** pour la règle de sécurité.
    3. Sélectionnez l'onglet **Source**, **Add (Ajoutez)** la zone source pour le centre de données et **Add (Ajoutez)** l'objet d'adresse (adresse source) que vous venez de définir.
    4. Sélectionnez l'onglet **Destination** et **Add (Ajoutez)** la zone de destination.
    5. Sélectionnez l'onglet **Application (Application)**, cliquez sur **Add (Ajouter)**, taper**`amazon`** et sélectionnez les applications Amazon dans la liste.
    6. Sélectionnez l'onglet **Action** et définissez **Action** sur **Allow (Autoriser)**.
    7. Cliquez sur **OK** pour enregistrer la règle.

STEP 6 | Pour activer la connexion pour la journalisation du trafic Internet de votre réseau, créez une règle qui fait correspondre la zone de confiance à une zone non approuvée.

1. Sélectionnez l'onglet **Policies (Politiques)** et, dans le menu déroulant **Device Group (Groupe de périphériques)**, sélectionnez **Shared (Partagé)**.
2. Sélectionnez la règle de base **Security (Sécurité)** > **Pre-Rules (Pré-règles)**.
3. Cliquez sur **Add (Ajouter)** et entrez un **Name (Nom)** pour la règle de sécurité.
4. Dans les onglets **Source (Source)** et **Destination (Destination)** pour la règle, **Add (ajoutez)** **`zone de confiance`** dans la Zone Source et **`zone de méfiance`** comme zone de Destination.
5. Dans l'onglet **Action**, définissez la valeur **Action** sur **Deny (Refuser)**, définissez le **Log Setting (Paramètre de journaux)** sur **Log at Session end (Se connecter en fin de session)**, et cliquez sur **OK**.

Prévisualiser les règles et valider les modifications

La dernière tâche de Cas d'utilisation : Configurer des pare-feux en utilisant Panorama consiste à réviser les règles et à valider les modifications que vous avez apportées à Panorama, aux groupes de périphériques et aux modèles.

STEP 1 | Prévisualisez les règles.

Cette prévisualisation vous permet d'évaluer en un seul coup d'œil la façon dont vos règles sont organisées dans une règle de base particulière.

1. Sélectionnez **Policies (Politiques)** et **Preview Rules (Prévisualiser les règles)**.
2. Sélectionnez une **Rulebase (Base de règle)**, **Device Group (Groupe de périphériques)**, et **Device (Périphérique)**.
3. Fermez la boîte de dialogue de la prévisualisation lorsque vous avez terminé.

STEP 2 | Validez et appliquez vos modifications de configuration.

1. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** et **Edit Selections (Modifier les sélections)** dans la portée d'application.
2. Sélectionnez **Device Groups (Groupes de périphériques)**, sélectionnez les groupes de périphériques que vous avez ajoutés et **Include Device and Network Templates (Inclure les modèles de périphérique et de réseau)**.
3. Cliquez sur **OK** pour enregistrer les modifications dans la portée d'application.
4. **Commit and Push (Validez et appliquez)** vos modifications.

STEP 3 | Vérifiez que Panorama a appliqué les configurations de politique et de modèle.

1. Dans l'en-tête de Panorama, définissez le **Context (Contexte)** au pare-feu pour accéder à son interface Web.

© 2020 Palo Alto Networks, Inc.

2. Passez en revue les configurations de politique et de modèle pour vous assurer que vos modifications sont présentes.

Gérer les déploiements de pare-feu à grande échelle

Panorama™ fournit plusieurs options de gestion d'un déploiement à grande échelle. Pour consolider toutes les fonctions de gestion, Panorama prend en charge la gestion d'un maximum de 5 000 pare-feux au moyen d'un appareil M-600 en mode Gestion uniquement ou jusqu'à 2 500 pare-feux avec un appareil virtuel Panorama en mode Gestion uniquement. Pour simplifier le déploiement et la gestion opérationnelle d'un déploiement de pare-feu à grande échelle comptant plus de 5 000 pare-feu, le plug-in Panorama Interconnect vous permet de gérer plusieurs nœuds de serveur de gestion Panorama à partir d'un seul contrôleur Panorama.

- Déterminer la solution optimale de déploiement à grande échelle du pare-feu
- Capacité de gestion accrue des périphériques pour l'appareil virtuel Panorama et M-600
- Panorama Interconnect

© 2020 Palo Alto Networks, Inc.

Déterminer la solution optimale de déploiement à grande échelle du pare-feu

Pour alléger le fardeau opérationnel associé à la gestion de la configuration de votre déploiement de pare-feu à grande-échelle, Palo Alto Networks offre différentes options de gestion des pare-feux pour répondre le mieux à votre scénario de déploiement.

Si votre déploiement de pare-feux à grande échelle se compose d'un seul serveur de gestion Panorama, ou d'un nombre restreint de tels serveurs, vous pouvez déployer un appareil M-600 pour gérer jusqu'à 5 000 pare-feux, ou un appareil virtuel Panorama pour gérer jusqu'à 2 500 pare-feux, pour exploiter toutes les capacités de Panorama à partir d'un seul serveur de gestion Panorama. La Capacité de gestion accrue des périphériques pour l'appareil virtuel Panorama et M-600 convient parfaitement aux déploiements dimensionnés verticalement, dans lesquels vous gérez un grand nombre de pare-feux à partir d'un seul serveur de gestion Panorama plutôt qu'en déployant plusieurs serveurs de gestion Panorama pour gérer un nombre plus faible de pare-feux.

Si votre déploiement de pare-feu à grande échelle se compose de plusieurs serveurs de gestion Panorama ayant des configurations similaires, le plug-in Panorama Interconnect vous autorise à gérer plusieurs nœuds Panorama à partir d'un seul contrôleur Panorama. Ce plugiciel simplifie le déploiement et la gestion opérationnelle de déploiements de pare-feu à grande échelle, car il vous permet de gérer la politique et la configuration d'une manière centralisée à partir d'un contrôleur Panorama. À partir du contrôleur Panorama, les configurations du groupe de périphériques et de la pile de modèles sont synchronisées sur les nœuds Panorama et transmis aux périphériques gérés. Le plug-in Panorama Interconnect convient parfaitement aux déploiements de pare-feux dimensionnés horizontalement comptant plusieurs serveurs de gestion Panorama distribués.

© 2020 Palo Alto Networks, Inc.

Capacité de gestion accrue des périphériques pour l'appareil virtuel Panorama et M-600

L'appareil M-600 en mode Gestion uniquement peut gérer jusqu'à 5 000 pare-feux ou un appareil virtuel Panorama en mode Gestion uniquement peut gérer jusqu'à 2 500 pare-feux, ce qui vous permet de réduire l'empreinte de gestion de votre déploiement de pare-feu à grande échelle.

- Exigences de la capacité de gestion accrue des périphériques
- Déploiement de Panorama pour la gestion accrue des périphériques

Exigences de la capacité de gestion accrue des périphériques

Vous pouvez gérer jusqu'à 5 000 pare-feux en utilisant un seul appareil M-600 en mode Gestion uniquement ou gérer jusqu'à 2 500 pare-feux en utilisant un seul appareil virtuel Panorama en mode Gestion uniquement. La gestion de si grands déploiements à partir d'un seul serveur de gestion Panorama allège la complexité opérationnelle de la gestion de la configuration et réduit le risque de conformité et de sécurité lié à la gestion de plusieurs serveurs de gestion Panorama.

Pour la collecte des journaux, un seul serveur de gestion Panorama est idéal, car il offre un emplacement centralisé pour afficher et analyser les données des journaux des périphériques gérés et vous évite d'avoir à accéder à chaque serveur de gestion Panorama individuel. Pour assurer la redondance en cas de défaillance du système ou du réseau, Palo Alto Networks vous recommande de déployer deux serveurs de gestion Panorama dans une configuration haute disponibilité (HD).

Pour générer des rapports prédéfinis, vous devez activer l'utilisation des données Panorama pour les rapports prédéfinis. Des rapports prédéfinis sont alors générés à part des données des journaux qui ont déjà été collectées par Panorama ou le collecteur de journaux dédié, ce qui réduit ainsi l'utilisation des ressources lors de la génération des rapports. L'activation de ce paramètre est nécessaire ; autrement, le rendement de Panorama pourrait être affecté, et Panorama pourrait cesser de répondre.

Pour gérer un maximum de 5 000 pare-feu, le serveur de gestion Panorama doit respecter les exigences minimales suivantes :

Exigences	Appareil M-Series	Appareil virtuel Panorama
Modèle	M-600	Tous les hyperviseurs Panorama pris en charge. Pour plus d'informations, reportez-vous à la section Modèles Panorama.
Panorama Mode	Gestion uniquement	Gestion uniquement
Nombre de pare-feux gérés	5 000	2 500
Disque système	240 Go SSD : Utilisé pour stocker les fichiers du système d'exploitation et les journaux système.	• 81 Go : Utilisé pour stocker les fichiers du système d'exploitation et les journaux système • Disque supplémentaire offrant une capacité minimale de 90 Go.

© 2020 Palo Alto Networks, Inc.

Exigences	Appareil M-Series	Appareil virtuel Panorama
Cœurs	28 (avec Multithreads)	28 (avec Multithreads)
Mémoire	256 Go	250 Go
Collecte de journaux	La collecte des journaux locale n'est pas prise en charge. Voir Déployer Panorama avec des collecteurs de journaux dédiés pour définir la collecte de journaux.	La collecte des journaux locale n'est pas prise en charge. Voir Déployer Panorama avec des collecteurs de journaux dédiés pour définir la collecte de journaux.
Journalisation et génération de rapports	Activez le paramètre **Use Panorama Data for Pre-Defined Reports (Utiliser les données de Panorama pour les rapports prédéfinis)** (**Panorama** > **Setup (Configuration)** > **Management (Gestion)** > **Logging and Reporting Settings (Paramètres de journalisation et de génération de rapports)** > **Log Export and Reporting (Exportation de journaux et génération de rapports)**)	Activez le paramètre **Use Panorama Data for Pre-Defined Reports (Utiliser les données de Panorama pour les rapports prédéfinis)** (**Panorama** > **Setup (Configuration)** > **Management (Gestion)** > **Logging and Reporting Settings (Paramètres de journalisation et de génération de rapports)** > **Log Export and Reporting (Exportation de journaux et génération de rapports)**)

Déploiement de Panorama pour la gestion accrue des périphériques

Pour déployer Panorama en vue d'une gestion accrue des périphériques, déterminez votre scénario de déploiement et suivez la procédure :

- Installation de Panorama pour la capacité de gestion accrue des périphériques
- Mise à niveau de Panorama pour la capacité de gestion accrue des périphériques

Installation de Panorama pour la capacité de gestion accrue des périphériques

Activez la licence de gestion des périphériques pour gérer plus de 1 000 pare-feux à partir d'un seul serveur de gestion M-600 Panorama™ ou d'un seul appareil virtuel Panorama.

STEP 1 | Communiquez avec votre représentant des ventes de Palo Alto Networks pour obtenir la licence de gestion Panorama qui vous permet de gérer un maximum de 5 000 pare-feu.

- Si vous déployez un appareil M-600, obtenez la licence de gestion des périphériques `PAN-M-600-P-1K`.
- Si vous déployez un appareil virtuel Panorama, obtenez la licence de gestion des périphériques `PAN-PRA-1000`.

STEP 2 | Configurez le serveur de gestion Panorama.

- (appareils M-600 uniquement) Configuration de l'appareil de série M.

OU

© 2020 Palo Alto Networks, Inc.

- Configuration de l'appareil virtuel Panorama.

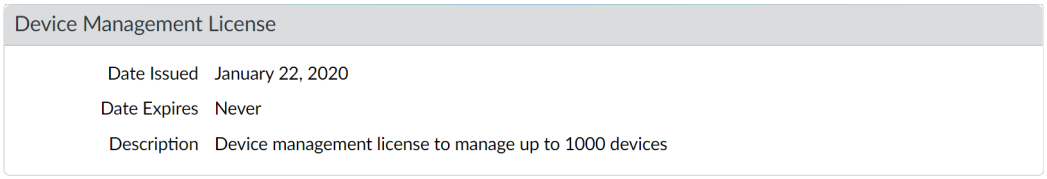
STEP 3 | Faites passer le serveur de gestion Panorama au mode Gestion uniquement si Panorama n'est pas encore défini sur ce mode.

- Commencer à l'étape 5 pour Configurer un appareil de série M en mode de Gestion seulement.
- Configurer un appareil virtuel Panorama en mode de Gestion seulement.

STEP 4 | Enregistrez votre serveur de gestion Panorama et installez les licences.

1. Enregistrer Panorama.
2. Activer une licence d'assistance Panorama.
3. Activez la licence de gestion des périphériques sur le serveur de gestion Panorama.
   - Activer / récupérer une licence de gestion de pare-feu sur l'appareil de la série M.
   - Activer / Récupérer une licence de gestion de pare-feu lorsque l'appareil virtuel Panorama n'est pas connecté à Internet.
   - Activer / Récupérer une licence de gestion de pare-feu lorsque l'appareil virtuel Panorama est connectée à Internet..

STEP 5 | Sélectionnez **Panorama** > **Licenses (Licences)** et vérifiez que la licence de gestion des périphériques est activée avec succès.



Si vous activez une nouvelle licence de gestion des périphériques sur Panorama, vous pouvez gérer un maximum de 5 000 pare-feux avec un appareil M-600, ou jusqu'à 2 500 pare-feux avec un appareil virtuel Panorama, mais la description suivante s'affiche `Device management license to manage up to 1000 devices or more (Licence de gestion des périphériques permettant de gérer jusqu'à 1 000 périphériques ou plus).`

Mise à niveau de Panorama pour la capacité de gestion accrue des périphériques

Procédez à la mise à niveau vers PAN-OS 9.1 ou une version ultérieure pour utiliser votre licence de gestion de périphériques existante sur votre appareil M-600 et gérer jusqu'à 5 000 pare-feux ou sur votre appareil virtuel Panorama™ pour gérer jusqu'à 2 500 pare-feux.

STEP 1 | Augmenter les processeurs et la mémoire sur l'appareil virtuel Panorama si l'appareil virtuel Panorama ne répond pas déjà aux exigences minimales en matière de ressources pour une gestion accrue des périphériques.

Examinez le Exigences de la capacité de gestion accrue des périphériques pour vérifier si votre appareil virtuel Panorama existant répond aux exigences minimales avant de le mettre à niveau.

STEP 2 | Connectez-vous à l'ILC Panorama.

STEP 3 | Faites passer le serveur de gestion Panorama au mode Gestion uniquement si Panorama n'est pas encore défini sur ce mode.

© 2020 Palo Alto Networks, Inc.

- (appareils M-600 uniquement) Commencer à l'étape 5 pour Configurer un appareil de série M en mode de Gestion seulement.

OU

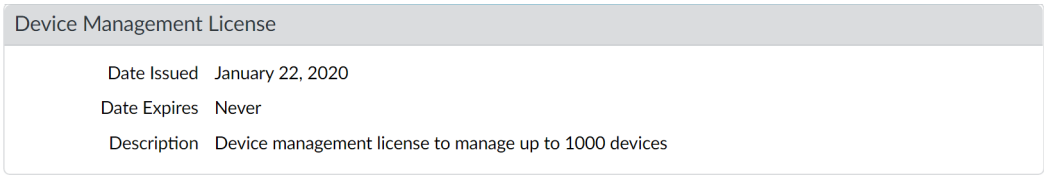
- Configurer un appareil virtuel Panorama en mode de Gestion seulement.

STEP 4 | Se connecter à l'interface Web Panorama.

STEP 5 | Mettez à niveau le serveur de gestion Panorama.

- Installer des mises à jour pour Panorama avec une connexion Internet.
- Installer des mises à jour pour Panorama lorsqu'il n'est pas connecté à Internet.
- Installer les mises à jour pour Panorama dans une configuration HD.

STEP 6 | Sélectionnez **Panorama** > **Licenses (Licences)** et vérifiez que la licence de gestion des périphériques est activée avec succès.



Si vous avez activé votre licence de gestion des périphériques, puis que vous avez procédé à la mise à niveau vers PAN-OS 9.1 ou une version ultérieure, vous pouvez gérer un maximum de 5 000 pare-feux avec un appareil M-600, ou jusqu'à 2 500 pare-feux avec un appareil virtuel Panorama, mais la description suivante s'affiche `Device management license to manage up to 1000 devices.`

© 2020 Palo Alto Networks, Inc.

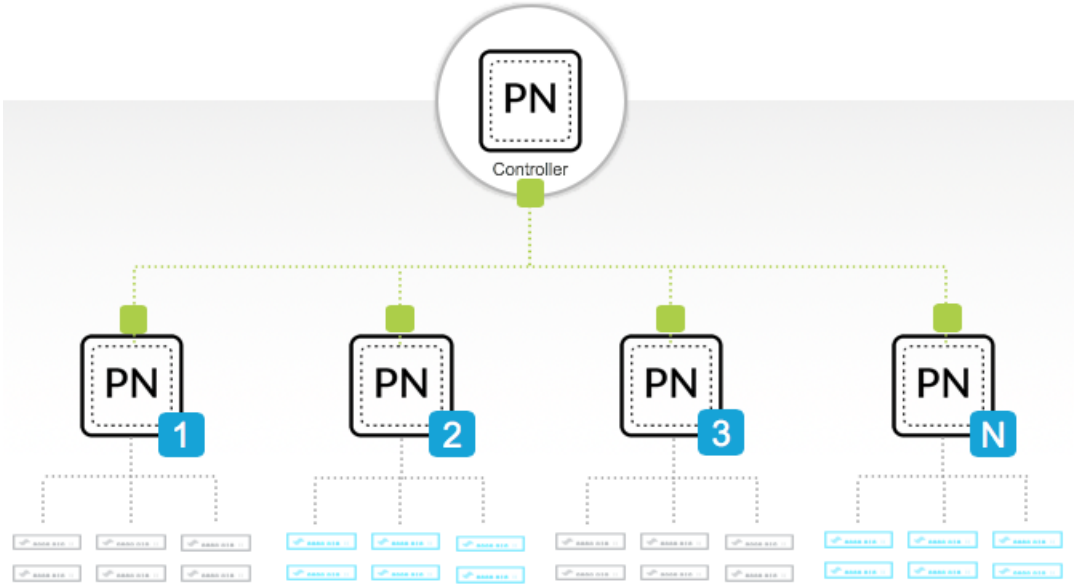
Panorama Interconnect

Utilisez Panorama™ Interconnect pour gérer la configuration de votre déploiement de pare-feu à grande échelle. Panorama Interconnect convient parfaitement lors de la gestion de la configuration de plusieurs serveurs de gestion Panorama possédant des configurations similaires.

- Présentation de Panorama Interconnect
- Exigences de Panorama Interconnect
- Activer l'authentification entre le contrôleur Panorama et les nœuds
- Configurer le plugiciel (plug-in) Panorama Interconnect
- Synchroniser Panorama Interconnect
- Gestion des pare-feu au moyen de Panorama Interconnect
- Mettre à niveau le plugiciel (plug-in) Panorama Interconnect

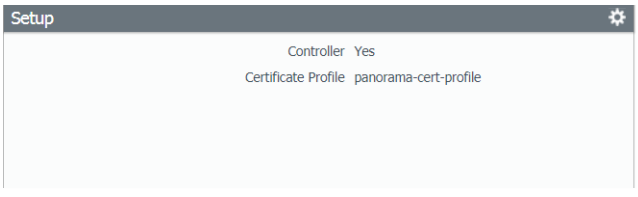
Présentation de Panorama Interconnect

Lorsque vous disposez de configurations homogènes sur un grand nombre de pare-feu qui dépasse la capacité de gestion d'une seule instance Panorama ou si vous avez déployé plusieurs serveurs de gestion Panorama™, vous pouvez utiliser le plugiciel Interconnect sur Panorama pour réduire la charge opérationnelle. Le plugiciel Interconnect vous permet de configurer un contrôleur Panorama qui gère un maximum de 64 nœuds Panorama, pour vous permettre de simplifier la configuration et les politiques courantes sur les appareils Panorama et les pare-feu gérés de votre réseau. Par exemple, vous pouvez configurer le contrôleur Panorama comme point central pour la gestion de la configuration propre à Panorama, comme les rôles administrateur sur les nœuds Panorama et les configurations courantes de tous les groupes de périphériques et de toutes les piles de modèles que vous appliquez aux nœuds Panorama pour la gestion de l'ensemble des pare-feu. La figure suivante illustre la hiérarchie de Panorama Interconnect, où le contrôleur Panorama gère plusieurs nœuds Panorama, qui, à leur tour, gèrent plusieurs périphériques.

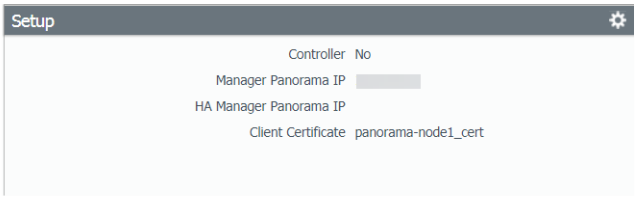


La figure suivante présente un exemple d'une page de **Setup (Configuration)** Panorama Interconnect pour un contrôleur Panorama et un nœud Panorama, lorsqu'ils ont été configurés avec succès.

© 2020 Palo Alto Networks, Inc.



Panorama Controller



Panorama Node

Les tâches suivantes doivent être effectuées pour configurer le plugiciel Panorama Interconnect :

Tâche	Détails
Passez en revue Exigences de Panorama Interconnect	les pare-feu et les serveurs de gestion Panorama doivent satisfaire aux exigences système et opérationnelles afin de déployer avec succès le plugiciel Panorama Interconnect. Cela comprend l'installation et l'activation des licences et l'enregistrement du serveur de gestion Panorama.
Activer l'authentification entre le contrôleur Panorama et les nœuds	Générez ou importez les certificats d'autorité de certification et d'émission pour les nœuds, et configurez un profil de certificat, pour sécuriser la communication entre le contrôleur Panorama et les nœuds Panorama.
Configurer le plugiciel (plug-in) Panorama Interconnect	Téléchargez, installez et configurez le plugiciel Panorama Interconnect sur le contrôleur Panorama et sur les nœuds Panorama.
Préparez le contrôleur Panorama pour appliquer la configuration aux pare-feu gérés.	Sur le contrôleur Panorama, Ajouter un groupe de périphériques et Configuration d'une pile de modèles pour configurer les règles de politique, objets et paramètres pour permettre aux pare-feu de fonctionner sur le pare-feu.
Synchroniser Panorama Interconnect	Appliquez la configuration propre à Panorama ainsi que les configurations de la pile de modèles et du groupe de périphériques, du contrôleur Panorama et des nœuds Panorama.
Gestion des pare-feu au moyen de Panorama Interconnect	Ajoutez un ou plusieurs pare-feu et appliquez la configuration synchronisée du nœud Panorama aux périphériques gérés.

Exigences de Panorama Interconnect

Planifiez et passez en revue les exigences du déploiement réussi du plugiciel Panorama™ Interconnect sur vos serveurs de gestion Panorama :

- Planification de votre déploiement de Panorama Interconnect
- Exigences système de Panorama Interconnect

© 2020 Palo Alto Networks, Inc.

- Exigences en matière de certificats pour Panorama Interconnect

Planification de votre déploiement de Panorama Interconnect

Pour un déploiement réussi du plugiciel Panorama™ Interconnect sur vos serveurs de gestion Panorama :

- ❑ Examinez les exigences système de Panorama Interconnect.

  Vérifiez que vos Panoramas et les pare-feux gérés répondent aux exigences de ressources minimales et que vos pare-feux sont des pare-feux à vsys unique.
- ❑ Planifiez votre configuration de device group (groupe de périphériques) et de template stack (pile de modèles) pour vos nœuds Panorama et vos pare-feux gérés.

  La gestion de la configuration est centralisée sur le contrôleur de Panorama et est reproduite sur tous les nœuds Panorama gérés par le Contrôleur Panorama. Assurez-vous que cette configuration est simple, compacte et largement identique pour tous les nœuds Panorama.

  Interconnect est compatible avec une configuration centralisée basée sur des groupe de périphériques et des modèles qui comprennent la configuration d'objets, politiques, pare-feux et réseaux. La fonction progressive (incremental) ajoutée par les plug-ins d'intégration Panorama comme NSX, SD-WAN et Prisma Access n'est pas compatible avec un déploiement Interconnect.

  *La configuration du nœud Panorama ne peut être gérée que depuis le contrôleur Panorama. Les modifications de configuration effectuées sur le nœud Panorama sont supprimées lorsque vous*synchronisez le Nœud Panorama avec le Contrôleur Panorama.
- ❑ Définissez le contrôleur Panorama et les nœuds Panorama sur le mode Gestion uniquement. Consultez la section Configurer un appareil de série M en mode de Gestion seulement ou Configurer un appareil virtuel Panorama en mode de Gestion seulement pour obtenir de plus amples renseignements sur la modification du mode du serveur de gestion Panorama.

  Le déploiement de Panorama Interconnect ou d'un contrôleur Panorama ou d'un nœud Panorama en mode Panorama avec collecte de journaux locale peut entraîner une réduction de la performance compte tenu de la plus forte demande en ressources provenant des processus de gestion et des processus de collecte des journaux.
- ❑ Enregistrer Panorama et Installer les licences pour le contrôleur Panorama et les nœuds Panorama.
- ❑ Déployez un ou plusieurs collecteurs de journaux dédiés pour la collecte des journaux. Reportez-vous à la section Configurer Panorama pour obtenir de plus amples renseignements sur les exigences en matière de stockage des journaux et les procédures de déploiement d'un serveur de gestion Panorama en mode Collecte de journaux.

  Les journaux et les rapports ne sont disponibles que depuis les Nœuds Panorama.
- ❑ Assurez-vous que le contrôleur Panorama et tous les Nœuds Panorama sont en mode Opérationnel avant d'installer le plugiciel. Le plugiciel Panorama Interconnect ne prend pas en charge les serveurs de gestion Panorama en mode FIPS et pourrait faire en sorte que le serveur de gestion Panorama ne réponde plus.
- ❑ Obtenez une Certificate Authority (autorité de certification ; CA) et générez des certificats de nœuds Panorama signés par la CA du contrôleur Panorama pour sécuriser la communication entre le contrôleur Panorama et les nœuds Panorama. Pour plus d'informations, reportez-vous à la section Activer l'authentification entre le contrôleur Panorama et les nœuds.
- ❑ Activez l'accès HTTPS sur le contrôleur Panorama, les nœuds Panorama et les périphériques gérés, afin de pouvoir Se connecter à l'interface Web Panorama et aux interfaces Web des pare-feu. Panorama Interconnect ne prend pas en charge l'accès à la CLI et à l'API.

© 2020 Palo Alto Networks, Inc.

Exigences système de Panorama Interconnect

Veillez à ce que les pare-feu et serveurs de gestion Panorama™ respectent les exigences système suivantes pour réussir l'installation du plugiciel Panorama Interconnect et la gestion de votre déploiement de pare-feu à grande échelle :

- Panorama Interconnect ne peut prendre en charge que les pare-feu d'un seul système virtuel

Exigences	Contrôleur et nœuds Panorama	Pare-feu
Mode	Gestion uniquement (recommandé)	S. O.
Processeurs et mémoire	16 processeurs et 32 Go de mémoire	S. O.
Disque système	81 Go	S. O.
Systèmes d'exploitation pris en charge	À partir de PAN-OS 8.1.3	À partir de PAN-OS 7.1
Modèles compatibles	• **Appareils M-Series** : M-600 • **Appareil virtuel Panorama** : Reportez-vous à la section Modèles Panorama pour connaître tous les modèles d'appareil virtuel Panorama pris en charge.	• **Pare-feu physiques** : Reportez-vous à Modèles de pare-feu pour connaître tous les modèles de pare-feu physiques pris en charge. • **Pare-feu VM** : Reportez-vous à Modèles VM-Series pour connaître tous les pare-feu VM-Series pris en charge.

Exigences en matière de certificats pour Panorama Interconnect

Pour sécuriser la communication entre le contrôleur Panorama™ et les nœuds Panorama, assurez-vous que les certificats que vous utilisez respectent les exigences suivantes :

- ❑ Une Certificate Authority (Autorité de certification ; CA) responsable de l'émission des certificats aux nœuds Panorama est requise sur le contrôleur Panorama. Vous devez soit procéder à la création d'un certificat CA racine auto-signé ou à l'Importation d'un certificat et d'une clé privée que vous signerez. Veuillez noter que vous devez configurer le certificat CA à l'onglet **Panorama** pour configurer le plugiciel Interconnect.
- ❑ Importez un certificat ou générez un certificat unique pour chaque nœud Panorama. Le certificat CA sur le contrôleur Panorama doit émettre les certificats que vous utilisez sur les nœuds.
  - Si vous importez un certificat vers le nœud Panorama, assurez-vous que le **Common Name (Nom commun)** du certificat correspond au numéro de série du nœud Panorama.
  - Le certificat doit être au format PKCS12 ou PEM et doivent inclure une clé privée pour que les nœuds Panorama puissent s'authentifier avec succès.

© 2020 Palo Alto Networks, Inc.

Activer l'authentification entre le contrôleur Panorama et les nœuds

Créez un profil de certificat pour sécuriser la communication entre le contrôleur Panorama™ et les nœuds Panorama.

- Obtenir le certificat CA du contrôleur Panorama
- Générer le certificat de nœud Panorama
- Créer un profil de certificat pour l'authentification des nœuds Panorama

Obtenir le certificat CA du contrôleur Panorama

Créez une Certificate Authority (Autorité de certification ; CA) de confiance responsable de l'émission des certificats aux nœuds Panorama™ pour sécuriser les connexions à Internet. Une CA de confiance est requise lorsque vous configurez Panorama dans des déploiements de pare-feu à large échelle.

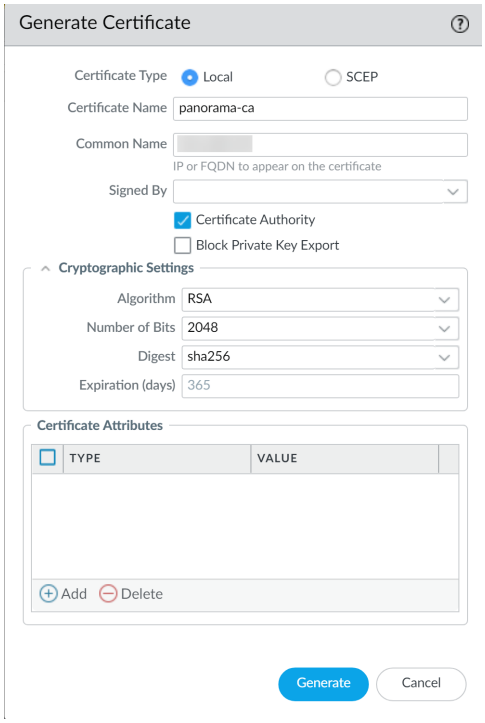
STEP 1 | Se connecter à l'interface Web Panorama du contrôleur Panorama.

STEP 2 | Créez le certificat d'autorité de certification.

- **Générez un nouveau certificat d'autorité de certification**

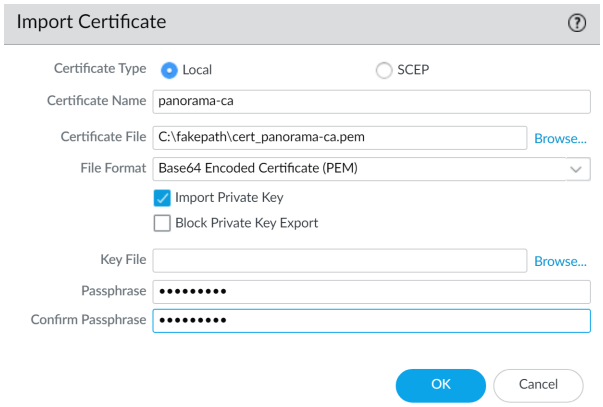
1. Sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)**, puis **Generate (Générez)** un nouveau certificat.
2. Comme **Certificate Type (Type de certificat)**, sélectionnez **Local**.
3. Saisissez un **Certificate Name (Nom de certificat)**, tel que **`panorama-CA`**. Le nom est sensible à la casse et peut contenir 31 caractères maximum. Il doit être unique et utiliser uniquement des lettres, des nombres, des traits d'union et des traits de soulignement.
4. Dans le champ **Common Name (Nom commun)**, saisissez l'adresse IP ou le nom de domaine complet du contrôleur Panorama.
5. Laissez le champ **Signed By (Signé par)** vide pour indiquer que le certificat est auto-signé.
6. Cochez la case **Certificate Authority (Autorité de certification)**.
7. **Generate (Générez)** le certificat de l'autorité de certification.

© 2020 Palo Alto Networks, Inc.



- **Importez un certificat d'autorité de certification.**

1. Sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)**, puis **Import (Importez)** le certificat de l'autorité de certification.
2. Saisissez un **Certificate Name (Nom de certificat)**, tel que **`panorama-CA`**. Le nom est sensible à la casse et peut contenir 31 caractères maximum. Il doit être unique et utiliser uniquement des lettres, des nombres, des traits d'union et des traits de soulignement.
3. **Browse (Recherchez** le **Certificate File (fichier de certificat)**.
4. Sélectionnez un **File Format (Format de fichier)** :
   - **Base64 Encoded Certificate (PEM) (Certificat codé en base-64 (PEM))** : vous devez importer la clé séparément du certificat. Cochez la case **Import Private Key (Importer clé privée)**, puis **Browse (Cherchez)** le **Key File (Fichier de la clé)**.
   - **Encrypted Private Key and Certificate (PKCS12)**—Format le plus courant, dans lequel la clé et le certificat sont enregistrés dans un conteneur unique (**Certificate File (Fichier du certificat)**).
5. Saisissez et confirmez la **Passphrase (Phrase secrète)** utilisée pour crypter la clé.
6. Cliquez sur **OK**. La page Certificates (Certificats) affiche alors le certificat d'autorité de certification importé.



© 2020 Palo Alto Networks, Inc.

STEP 3 | Cliquez sur **Commit (Valider)** et **Commit to Panorama (Validez sur Panorama)**.

Générer le certificat de nœud Panorama

Pour que le contrôleur Panorama™ puisse authentifier chaque nœud Panorama, créez un certificat unique que chaque nœud Panorama. Le contrôleur et le nœud Panorama utilisent l'authentification basée sur les certificats pour communiquer en toute sécurité. Avant de générer les certificat de nœud Panorama uniques, Obtenir le certificat CA du contrôleur Panorama.

Si votre nœud Panorama se situe dans une configuration High Availability (haute disponibilité - HA), vous devez créer et importer les certificats des deux nœuds Panorama pour chaque homologue dans la configuration HA.

STEP 1 | Se connecter à l'interface Web Panorama du contrôleur Panorama.

STEP 2 | Sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)**, puis **Generate (Générez)** un nouveau certificat.

1. Comme **Certificate Type (Type de certificat)**, sélectionnez **Local**.

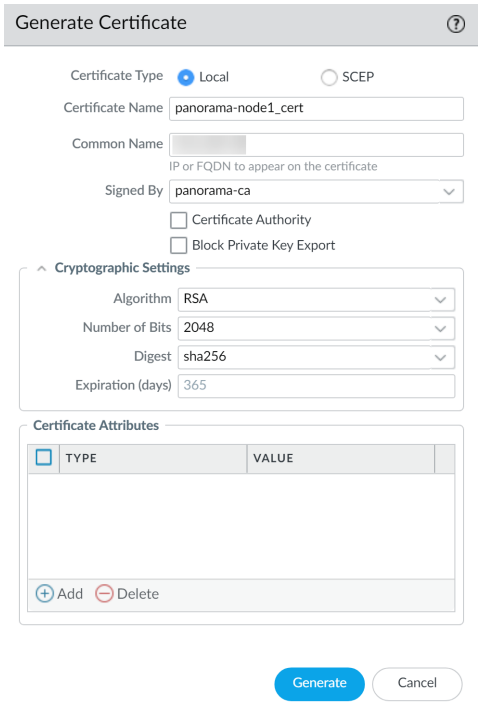
   Le protocole SCEP n'est pas pris en charge à l'heure actuelle.

2. Saisissez un **Certificate Name (Nom de certificat)**, tel que **`panorama-node1_cert`**. Le nom est sensible à la casse et peut contenir 31 caractères maximum. Il doit être unique et utiliser uniquement des lettres, des nombres, des traits d'union et des traits de soulignement.
3. Dans le champ **Common Name (Nom commun)**, saisissez le numéro de série du nœud Panorama.

   Le numéro de série doit être saisi dans le champ Common Name (Nom commun) pour authentifier la connexion entre le contrôleur Panorama et le nœud Panorama. Le nœud Panorama ne peut se connecter au contrôleur Panorama si le numéro de série n'est pas saisi dans ce champ.

4. Dans le champ **Signed By (Signé par)**, sélectionnez le certificat CA.
5. **Generate (Générez)** le certificat.

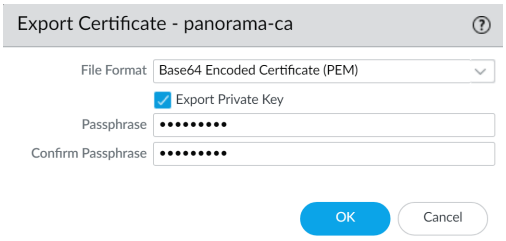
© 2020 Palo Alto Networks, Inc.



STEP 3 | Cliquez sur **Commit (Valider)** et **Commit to Panorama (Validez sur Panorama)**.

STEP 4 | Exportez les certificats de chacun des nœuds Panorama générés à l'étape 2.

1. Sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **Certificates (Certifcats)**, sélectionnez le certificat, puis **Export Certificate (Exportez le certificat)**.
2. Sélectionnez le **File Format (Format de fichier)** :
   - **Certificat codé Base64 (PEM)** : Vous permet d'exporter le certificat et la clé privée séparément. Si vous souhaitez que le fichier exporté puisse inclure la clé privée, cochez la case **Export Private Key (Exporter la clé privée)**.
   - **Clé privée cryptée et certificat (PKCS12)** : Exporter le certificat et la clé privée en un seul fichier.
3. Cochez la case **Export private key (Exporter la clé privée)**.
4. Saisissez une **Passphrase (Phrase secrète)** et **Confirm Passphrase (Confirmez la phrase secrète)** pour chiffrer la clé privée. Cette phrase secrète est utilisée lors de l'importation de la clé du certificat vers les nœuds Panorama.
5. Cliquez sur **OK (OK)** pour enregistrer le certificat/fichier de clé sur votre ordinateur.



6. Donnez un nom de fichier descriptif au certificat pour que vous puissiez facilement identifier le nœud Panorama auquel il doit être importé, puis **Save (Enregistrez)** le certificat.

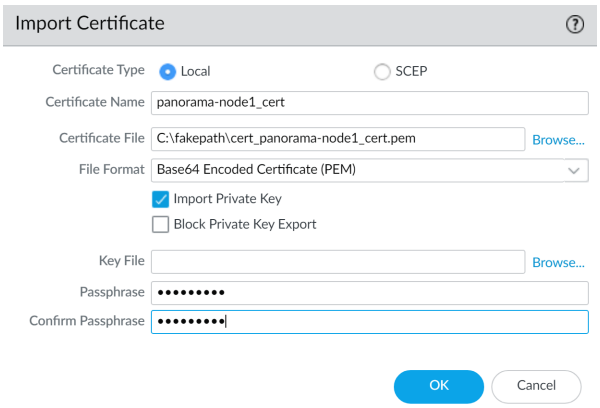
STEP 5 | Importez le certificat à chaque nœud Panorama.

1. Se connecter à l'interface Web Panorama du nœud Panorama.

© 2020 Palo Alto Networks, Inc.

2. Sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)**, puis **Import (Importez)** un certificat :
   1. Comme **Certificate Type (Type de certificat)**, sélectionnez **Local**.

      Le protocole SCEP n'est pas pris en charge à l'heure actuelle.
   2. Saisissez le même **Certificate Name (Nom de certificat)**. Le nom est sensible à la casse et peut contenir 31 caractères maximum. Il doit être unique et utiliser uniquement des lettres, des nombres, des traits d'union et des traits de soulignement.
   3. **Browse (Cherchez)** le certificat que vous avez exporté à l'étape 4.
   4. Cochez la case **Import private key (Importer la clé privée)**.
   5. Saisissez la **Passphrase (Phrase secrète)** et **Confirm Passphrase (Confirmez la phrase secrète)** utilisée pour chiffrer la clé privée.
   6. Cliquez sur **OK** pour importer le certificat.



3. Cliquez sur **Commit (Valider)** et **Commit to Panorama (Validez sur Panorama)**.

Créer un profil de certificat pour l'authentification des nœuds Panorama

Les profils de certificat définissent les Certificate Authority (autorité de certification - CA) à utiliser pour vérifier les certificats du nœud Panorama utilisés pour sécuriser la communication entre le contrôleur Panorama™ et les nœuds Panorama et pour vérifier le statut de révocation du nœud Panorama. Un profil de certificat est nécessaire pour configurer Panorama pour des déploiement de pare-feux à grande échelle.

STEP 1 | Se connecter à l'interface Web Panorama du contrôleur Panorama.

STEP 2 | Obtenir le certificat CA du contrôleur Panorama.

STEP 3 | Générer le certificat de nœud Panorama utilisé pour sécuriser la configuration entre le contrôleur Panorama et les nœuds Panorama. Répétez cette étape pour tous les nœuds Panorama.

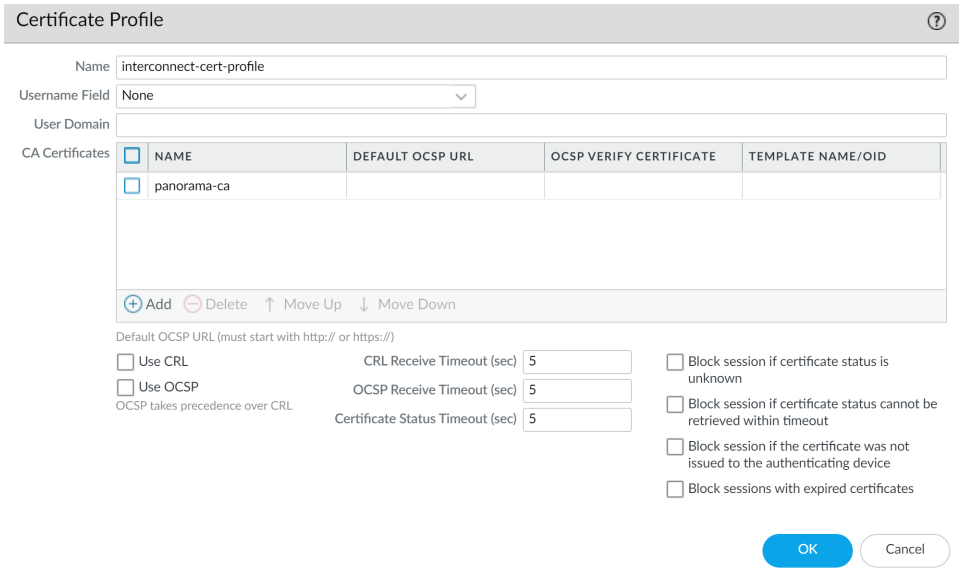
STEP 4 | Créez un profil de certificat.

CRL et OCSP ne sont pas pris en charge à l'heure actuelle.

1. Sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificat)**, puis **Add (Ajouter)** un nouveau profil de certificat.
2. Donnez un **Name (Nom)** au profil de certificat.

© 2020 Palo Alto Networks, Inc.

3. **Add (Ajoutez)** le certificat CA créé à l'étape 2.
4. Cliquez sur **OK** pour terminer l'ajout du profil de certificat.



STEP 5 | Cliquez sur **Commit (Valider)** et **Commit to Panorama (Validez sur Panorama)**.

Configurer le plugiciel (plug-in) Panorama Interconnect

Centralisez la pile de modèles et la gestion des groupes de périphériques des déploiement de pare-feu à grande échelle au moyen de Panorama™ Interconnect pour transmettre les configurations reproduites d'un contrôleur Panorama vers des nœuds Panorama pour garantir l'uniformité des configurations et des politiques de sécurité sur les pare-feu. Panorama Interconnect vous permet d'établir un contrôleur Panorama à partir duquel gérer les nœuds Panorama, lesquels gèrent les pare-feu et transmettent les configurations. Vous pouvez ainsi gérer la configuration des déploiements de pare-feu à grande échelle à partir d'un seul emplacement, ce qui vous permet de réduire le temps que vous devez consacrer à la configuration de plusieurs serveurs de gestion Panorama et de réduire vos failles de sécurité qui pourraient découler d'une mauvaise configuration. Avant de configurer le plugiciel Panorama Interconnect sur vos serveurs de gestion Panorama, passez en revue les Exigences de Panorama Interconnect.

Si votre nœud Panorama est dans une configuration High Availability (haute disponibilité - HA), vous devez configurer le plug-in Panorama Interconnect sur les deux homologue HA Panorama.

STEP 1 | Installez le plugiciel Panorama Interconnect. Vous devez installer le plugiciel Panorama™ Interconnect sur le contrôleur Panorama et sur tous les nœuds Panorama.

1. Se connecter à l'interface Web Panorama.
2. Sélectionnez **Panorama** > **Plugins (Plugiciels)**, puis cherchez `Interconnect`.
3. **Download (Téléchargez)**, puis **Install (Installez)** le plugiciel Panorama Interconnect.
4. Cliquez sur **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** pour terminer d'installer le plugiciel Panorama Interconnect

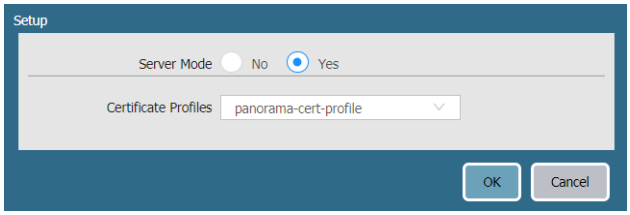
STEP 2 | Activer l'authentification entre le contrôleur Panorama et les nœuds afin de sécuriser l'authentification entre le contrôleur Panorama et les nœuds Panorama.

STEP 3 | Configurez le plugiciel sur le contrôleur Panorama. Répétez cette étape sur l'homologue haute disponibilité, si le contrôleur Panorama est dans une configuration HA.

© 2020 Palo Alto Networks, Inc.

Une fois Panorama configuré en tant que contrôleur Panorama, vous ne pouvez reconfigurer le contrôleur Panorama en tant que nœud Panorama. Vérifiez que vous configurez le bon serveur de gestion Panorama en tant que contrôleur Panorama avant de poursuivre.

1. Sélectionnez **Panorama** > **Interconnect** > **Setup (Configuration)**, puis modifiez la **Interconnect Plugin Setup (Configuration du plugiciel Interconnect)** :
2. Dans le champ **Server Mode (Mode du serveur)**, sélectionnez **Yes (Oui)**.
3. Sélectionnez le **Certificate Profile (Profil de certificat)** que vous avez créé à l'étape 2.
4. Cliquez sur **OK** pour enregistrer les paramètres.

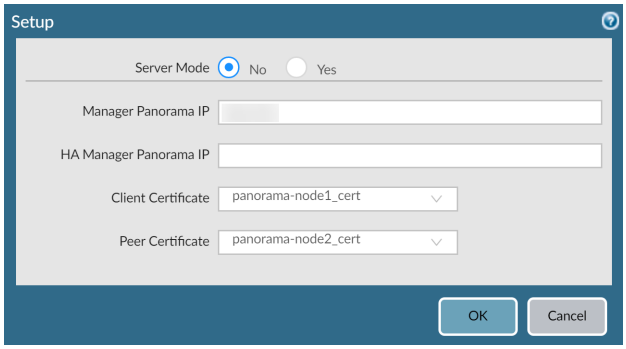


5. Cliquez sur **Commit (Valider)** et **Commit to Panorama (Validez sur Panorama)**.

STEP 4 | Configurez le plugiciel sur le nœud Panorama. Répétez cette étape pour tous les nœuds Panorama.

Si votre nœud Panorama est dans une configuration High Availability (haute disponibilité - HA), vous devez sélectionner le certificat du nœud Panorama que vous avez importé pour chaque homologue HA du nœud Panorama lors de la configuration du plug-in Panorama Interconnect sur chaque homologue.

1. Sélectionnez **Panorama** > **Interconnect** > **Setup (Configuration)**, puis modifiez la **Interconnect Plugin Setup (Configuration du plugiciel Interconnect)** :
   1. Dans le champ **Server Mode (Mode du serveur)**, sélectionnez **No (Non)**.
   2. **Manager Panorama IP (Adresse IP de gestion Panorama)** : saisissez l'adresse IP de gestion du contrôleur Panorama.
   3. **HA Manager IP (Adresse IP de gestion de l'homologue HA)** : Si le contrôleur Panorama est dans une configuration haute disponibilité, saisissez l'adresse IP de gestion de l'homologue HA du contrôleur Panorama.
   4. Sélectionnez le certificat du nœud Panorama que vous avez importé à l'étape 2.
   5. (HA uniquement) Sélectionnez le certificat du nœud Panorama homologue que vous avez importé à l'étape 2.
2. Cliquez sur **OK** pour enregistrer les paramètres.



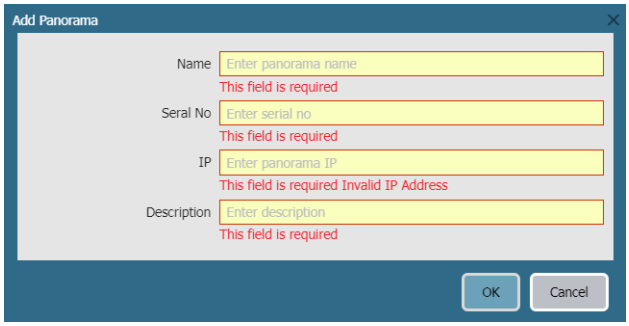
3. Cliquez sur **Commit (Valider)** et **Commit to Panorama (Validez sur Panorama)** pour finir de configurer le plugiciel sur le nœud Panorama.

© 2020 Palo Alto Networks, Inc.

STEP 5 | Ajoutez les nœuds Panorama au contrôleur Panorama.

1. Sélectionnez **Panorama** > **Interconnect** > **Panorama Nodes (Nœuds Panorama)** et **Add (Ajoutez)** le nœud Panorama.
   1. Donnez un **Name (Nom)** au nœud Panorama. Il n'a pas à correspondre au nom du périphérique qui est configuré sur le serveur de gestion Panorama.

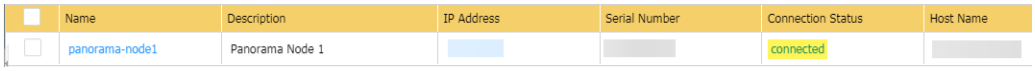
      Un point (.) dans le Name (Nom) du nœud Panorama n'est pas pris en charge.
   2. Saisissez le **Serial No (Numéro de série)** du nœud Panorama.
   3. Saisissez l'adresse **IP** du nœud Panorama. L'adresse IP doit être accessible au contrôleur Panorama.
   4. Saisissez une **Description** du nœud Panorama.
2. Cliquez sur **OK** pour ajouter le nœud Panorama.



3. Cliquez sur **Commit (Valider)** et sur **Commit to Panorama (Valider sur Panorama)** pour terminer l'ajout du nœud Panorama.

STEP 6 | Vérifiez que le nœud Panorama nouvellement ajouté est **`Connected`**.

1. Sélectionnez **Panorama** > **Interconnect** > **Panorama Nodes (Nœuds Panorama)**.
2. Trouvez le nœud Panorama que vous avez ajouté, puis vérifiez que la colonne Connection Status (État de la connexion) affiche `Connected`.



STEP 7 | Une fois le plugiciel installé sur le contrôleur Panorama et les nœuds Panorama, effectuez les étapes pour terminer la configuration de Panorama Interconnect :

1. Sur le contrôleur Panorama, Ajouter un groupe de périphériques. Répétez cette étape pour créer le nombre de groupes de périphériques dont vous avez besoin.
2. Sur le contrôleur Panorama, Configuration d'une pile de modèles. Répétez cette étape pour créer le nombre de piles de modèles dont vous avez besoin.
3. Synchroniser Panorama Interconnect pour appliquer la configuration propre à Panorama ainsi que les configurations de la pile de modèles et du groupe de périphériques, du contrôleur Panorama et des nœuds Panorama.
4. Sur le contrôleur Panorama, ajoutez un ou plusieurs pare-feu qui doivent être gérés par un nœud Panorama.
   - Ajouter un pare-feu à un nœud Panorama
   - Importer plusieurs pare-feu à un nœud Panorama
5. Appliquer la configuration du nœud Panorama aux périphériques gérés.

© 2020 Palo Alto Networks, Inc.

Synchroniser Panorama Interconnect

Pour appliquer les configurations de la pile de modèles et du groupe de périphériques depuis le contrôleur Panorama, synchronisez la configuration des nœuds Panorama aux le contrôleur Panorama pour synchroniser pour appliquer les configurations propres à Panorama et permettre au nœud Panorama de transmettre la configuration aux périphériques gérés.

- Appliquer la configuration courante de Panorama aux nœuds Panorama
- Synchroniser le nœud Panorama avec le contrôleur Panorama

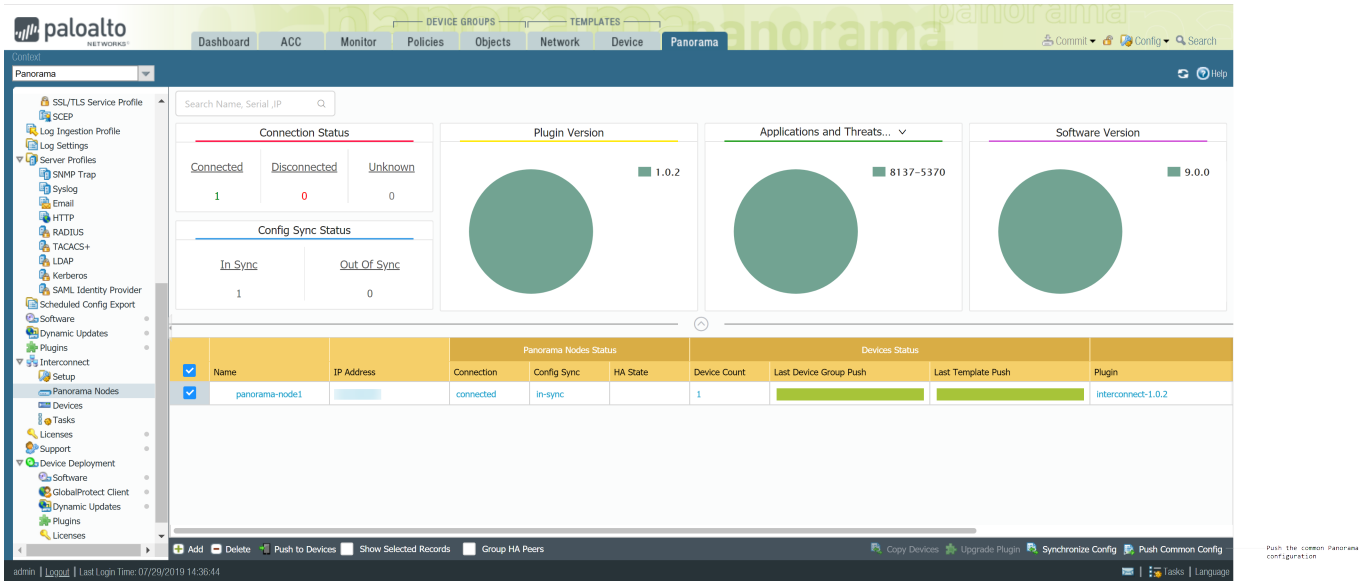
Appliquer la configuration courante de Panorama aux nœuds Panorama

Appliquez la configuration courante du contrôleur Panorama™ au nœud Panorama pour appliquer les configurations propres à Panorama aux nœuds Panorama. Pour synchroniser la configuration de la pile de modèles et du groupe de périphériques afin de l'appliquer aux périphériques gérés, reportez-vous à la section Synchroniser le nœud Panorama avec le contrôleur Panorama.

STEP 1 | Se connecter à l'interface Web Panorama du contrôleur Panorama.

STEP 2 | Sélectionnez **Panorama** > **Interconnect** > **Panorama Nodes (Nœuds Panorama)**, puis sélectionnez les nœuds Panorama qui gèrent les pare-feu pour leur transmettre la configuration.

STEP 3 | **Push Common Config (**Appliquez **la configuration courante)** pour appliquer les configurations propres à Panorama aux nœuds Panorama.



Synchroniser le nœud Panorama avec le contrôleur Panorama

Synchronisez la configuration du contrôleur Panorama™ sur les nœuds Panorama pour que le nœud Panorama puisse transmettre les configurations de la piles de modèles ou du groupe de périphériques aux périphériques gérés.

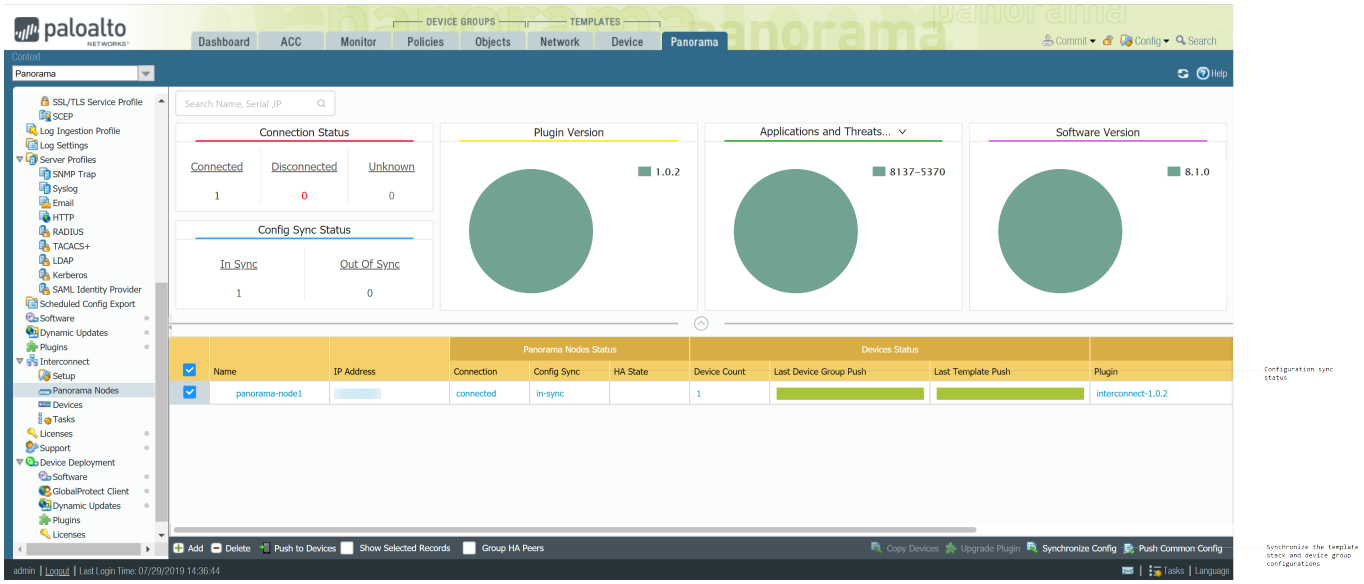
STEP 1 | Se connecter à l'interface Web Panorama du contrôleur Panorama.

STEP 2 | Sélectionnez **Panorama** > **Interconnect** > **Panorama Nodes (Nœuds Panorama)**, puis sélectionnez les nœuds Panorama à synchroniser avec le contrôleur Panorama.

© 2020 Palo Alto Networks, Inc.

STEP 3 | **Synchronize Config (Synchronisez la configuration)** pour appliquer les configurations du groupe de périphériques et de la pile de modèles sur les nœuds Panorama. Cette mesure est nécessaire pour transmettre la configuration aux périphériques gérés.

STEP 4 | Dans la colonne Sync Status (État de la synchronisation), vérifiez que le nœud Panorama est **in-sync**.



Gestion des pare-feu au moyen de Panorama Interconnect

Ajoutez un seul pare-feu ou importez plusieurs pare-feu en masse afin de les gérer sur un nœud Panorama™.

- Ajouter un pare-feu à un nœud Panorama
- Importer plusieurs pare-feu à un nœud Panorama
- Importer les variables des piles de modèles
- Gérer la clé principale avec Panorama Interconnect
- Appliquer la configuration du nœud Panorama aux périphériques gérés

Ajouter un pare-feu à un nœud Panorama

Ajoutez un seul pare-feu qui doit être géré par un nœud Panorama™ pour gérer la configuration de la pile de modèles et du groupe de périphériques à partir d'un contrôleur Panorama centralisé. Pour importer plusieurs pare-feu en masse, reportez-vous à la section Importer plusieurs pare-feu à un nœud Panorama.

STEP 1 | Configurez le pare-feu pour qu'il communique avec le nœud Panorama.

1. Effectuez la configuration initiale sur le pare-feu afin qu'il soit accessible et puisse communiquer avec Panorama sur le réseau.
2. Ajoutez l'adresse IP du nœud Panorama au pare-feu.
    1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et {0>Edit (Modifiez)<0} les paramètres de Panorama.
    2. Saisissez l'adresse IP de Panorama dans le premier champ.
    3. (Facultatif) Si vous avez configuré une paire haute disponibilité dans Panorama, entrez l'adresse IP du Panorama secondaire dans le deuxième champ.
    4. Cliquez sur **OK**.

© 2020 Palo Alto Networks, Inc.

3. Sélectionnez **Commit (Valider)** et **Commit (Valider)** pour enregistrer vos modifications.

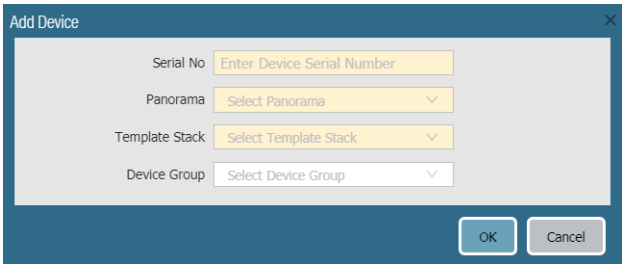
STEP 2 | Se connecter à l'interface Web Panorama du contrôleur Panorama.

STEP 3 | Sélectionnez **Panorama** > **Interconnect** > **Devices (Périphériques)**, puis **Add (Ajoutez)** le pare-feu.

STEP 4 | Saisissez les renseignements du pare-feu :

- Saisissez le **Serial No (Numéro de série)** du pare-feu.
- Sélectionnez le nœud **Panorama** qui doit gérer le pare-feu.
- Sélectionnez la **Template Stack (Pile de modèles)** avec laquelle gérer la configuration du pare-feu.
- Sélectionnez le **Device Group (Groupe de périphériques)** auquel associé le pare-feu.

STEP 5 | Cliquez sur **OK** pour ajouter le pare-feu en tant que périphérique géré.

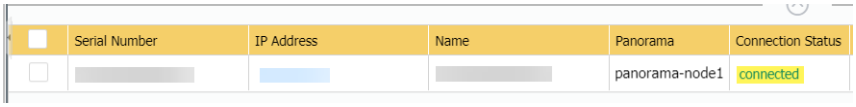


STEP 6 | Cliquez sur **Commit (Valider)** et sur **Commit to Panorama (Valider sur Panorama)** pour terminer l'ajout du pare-feu.

STEP 7 | Sélectionnez **Panorama** > **Interconnect** > **Panorama Nodes (Nœuds Panorama)**, puis **Synchronize Config (Synchroniser la configuration)**.

STEP 8 | Vérifiez que le pare-feu nouvellement ajouté est **`Connected`**.

1. Sélectionnez **Panorama** > **Interconnect** > **Devices (Périphériques)**.
2. Trouvez le pare-feu que vous avez ajouté, puis vérifiez que la colonne Connection Status (État de la connexion) affiche `Connected`.



Importer plusieurs pare-feu à un nœud Panorama

Vous pouvez importer plusieurs pare-feu pour les gérer par un nœud Panorama™ au moyen d'un modèle CSV qui vous est fourni lors de la procédure d'importation. L'importation de plusieurs pare-feu d'un seul coup vous permet d'ajouter rapidement plusieurs pare-feu à des nœuds Panorama et de les affecter à une pile de modèles et à un groupe de périphériques pour centraliser la gestion des configurations.

Lorsque vous importez plusieurs pare-feu, vous pouvez ajouter des pare-feu à différents nœuds Panorama, piles de modèles et groupes de périphériques. Par exemple, vous avez déployé le nœud Panorama A et le nœud Panorama B et chacun d'entre eux comprennent deux piles de modèles et deux groupes de périphériques. Si vous importez 100 pare-feu, vous pouvez les importer de l'une des manières suivantes :

- Ajouter 50 pare-feu au nœud Panorama A :
  - Affecter 25 pare-feu à la pile de modèle A1 et au groupe de périphériques A1.

© 2020 Palo Alto Networks, Inc.

- Affecter 25 pare-feu à la pile de modèle A2 et au groupe de périphériques A2.
- Ajouter 50 pare-feu au nœud Panorama B :
  - Affecter 30 pare-feu à la pile de modèle B1 et au groupe de périphériques B1.
  - Affecter 20 pare-feu à la pile de modèle B2 et au groupe de périphériques B2.

Pour ajouter un seul pare-feu, reportez-vous à la section Ajouter un pare-feu à un nœud Panorama.

STEP 1 | Configurez le pare-feu pour qu'il communique avec le nœud Panorama.

Répétez cette étape pour tous les pare-feu qui doivent être gérés par Panorama au moyen du plugiciel Interconnect.

1. Effectuez la configuration initiale sur le pare-feu afin qu'il soit accessible et puisse communiquer avec Panorama sur le réseau.
2. Ajoutez l'adresse IP du nœud Panorama au pare-feu.
   1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et Edit (Modifiez) les paramètres de Panorama.
   2. Saisissez l'adresse IP de Panorama dans le premier champ.
   3. (Facultatif) Si vous avez configuré une paire haute disponibilité dans Panorama, entrez l'adresse IP du Panorama secondaire dans le deuxième champ.
   4. Cliquez sur **OK**.
3. Sélectionnez **Commit (Valider)** et **Commit (Valider)** pour enregistrer vos modifications.

STEP 2 | Se connecter à l'interface Web Panorama du contrôleur Panorama.

STEP 3 | Cliquez sur **Commit (Valider)** et **Commit to Panorama (Validez sur Panorama)** les changements de configuration à apporter au contrôleur Panorama qui sont en attente. Pour importer plusieurs pare-feu, aucun changement à apporter au contrôleur Panorama ne doit être en attente, sinon l'importation échoue.

STEP 4 | Sélectionnez **Panorama** > **Interconnect** > **Devices (Périphériques)**, puis **Import (Importez)** les pare-feu.

STEP 5 | Cliquez sur **Download Sample CSV (Télécharger le modèle CSV)** pour télécharge un modèle de fichier CSV au bon format afin de charger plusieurs pare-feu.

STEP 6 | Remplissez le fichier CSV que vous avez téléchargé. Saisissez les valeurs appropriées dans les champs **serial (numéro de série)**, **panorama**, **device-group (Groupe de périphériques)** et **template-stack (pile de modèles)**. Le nœud Panorama, le groupe de périphériques et la pile de modèles doivent déjà être ajoutés et créés sur le contrôleur Panorama avant l'importation des pare-feu. Ils sont nécessaires pour ajouter le pare-feu. Lorsque vous avez terminé de saisir les renseignements concernant le pare-feu, **Save (Enregistrez)** le fichier.

Vous avez également la possibilité d'affecter des pare-feu à des horaires de contenu. Ils ne sont pas nécessaires à l'importation des pare-feu.



La modification de l'ordre des colonnes du fichier CSV n'est pas prise en charge. L'importation du pare-feu échoue si l'ordre des colonnes est modifié.

STEP 7 | Dans l'interface Web Panorama, **Select File (Sélectionnez le fichier)** à parcourir et sélectionnez le fichier CSV contenant les renseignements relatifs au pare-feu.

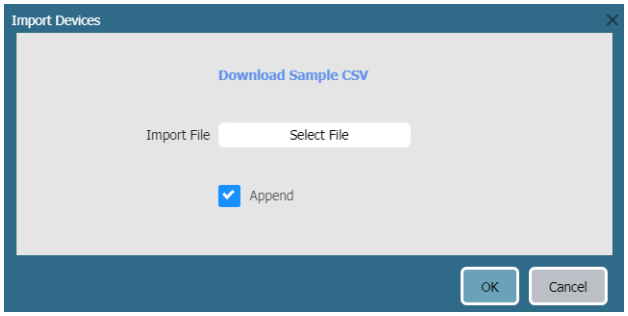
© 2020 Palo Alto Networks, Inc.

Si l'importation en masse contient un pare-feu pour lequel des renseignements nécessaires sont manquants, l'importation au complet échoue. Si une erreur survient, vous recevez un message d'erreur indiquant l'emplacement des problèmes dans le fichier d'importation.

STEP 8 | **Append (Ajoutez)** les nouveaux périphériques à la fin de la liste **Devices (Périphériques)**. Tous les périphériques importés doivent être des nouveaux périphériques. L'importation échoue si l'un des périphériques faisant l'objet de l'importation font partie de la configuration active du contrôleur Panorama.

Décochez la case Append (Ajouter) si vous souhaitez supprmer les périphériques existants de la liste et ajouter uniquement les nouveaux périphériques que vous ajouter.

STEP 9 | Cliquez sur **OK** pour ajouter les pare-feu en tant que périphériques gérés.

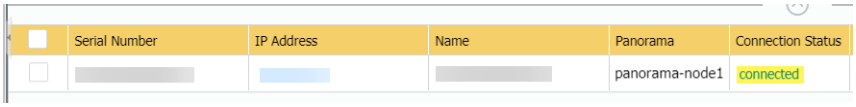


STEP 10 | Cliquez sur **Commit (Valider)** et sur **Commit to Panorama (Valider sur Panorama)** pour terminer l'ajout des pare-feu.

STEP 11 | Sélectionnez **Panorama** > **Interconnect** > **Panorama Nodes (Nœuds Panorama)**, puis **Synchronize Config (Synchroniser la configuration)**.

STEP 12 | Vérifiez que les pare-feu nouvellement ajoutés sont **`Connected`**.

1. Sélectionnez **Panorama** > **Interconnect** > **Devices (Périphériques)**.
2. Trouvez les pare-feu que vous avez importés, puis vérifiez que la colonne Connection Status (État de la connexion) affiche `Connected`.



Importer les variables des piles de modèles

Utilisez les variables des piles de modèles pour remplacer les adresses IP, les plages d'adresses IP, le FQDN, les interfaces dans les configurations IKE, VPN et HA et les ID de groupe de vos configurations de pare-feu. Les variables vous permettent de réduire le nombre total de modèles et de piles de modèles que vous devez gérer, tout en vous permettant de conserver les valeurs spécifiques au pare-feu.

L'importation des variables des piles de modèles vous permet de remplacer les valeurs de plusieurs variables existantes, et vous ne pouvez créer de nouvelles variables de piles de modèles lors de l'importation. Pour obtenir de plus amples renseignements sur la création d'une nouvelle variable de modèle ou de pile de modèles, consultez la section Configurer une variable de modèle ou de pile de modèles.

STEP 1 | Exportez les variables existantes d'une pile de modèles.

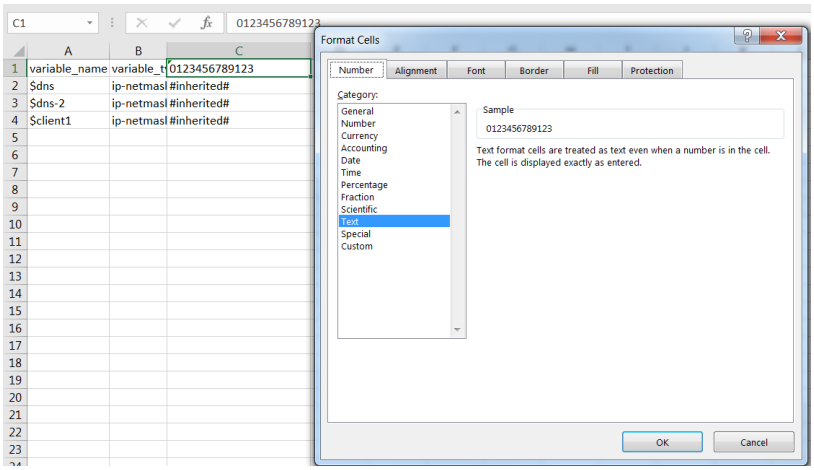
© 2020 Palo Alto Networks, Inc.

1. Connectez-vous à l'interface Web Panorama du contrôleur Panorama.
2. Sélectionnez **Panorama** > **Interconnect** > **Devices (Périphériques)**, puis **Export Variables (Exportez les variables)**.
3. Dans le menu déroulant, sélectionnez le **Name (Nom)** de la pile de modèles.
4. Cliquez sur **OK** et enregistrez le fichier CSV.

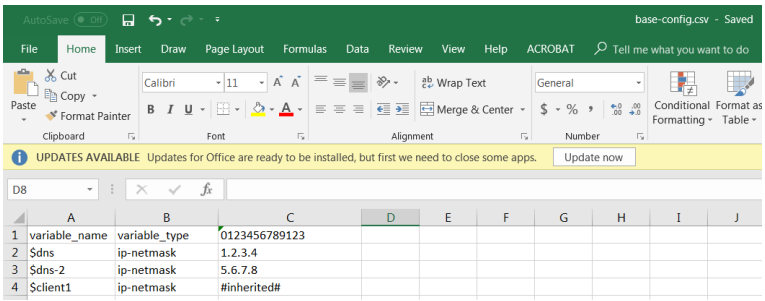
STEP 2 | Modifiez le fichier CSV contenant les variables de la pile de modèles à importer vers Panorama Interconnect au format suivant :

Les valeurs qui s'affichent en tant que `#inherited#` sont des valeurs qui sont définies dans la pile de modèles.

1. Corrigez le nombre de cellules contenant le numéro de série du pare-feu. Répétez cette étape pour tous les pare-feu du fichier CSV.
   1. Double-cliquez sur la cellule contenant le numéro de série du pare-feu, puis sélectionnez **Format Cells (Mettre en forme les cellules)**.
   2. Sélectionnez **Number (Numéro)** > **Text (Texte)**, puis cliquez sur **OK**.
   3. Ajoutez un **0** au début du numéro de série.



2. Saisissez une nouvelle valeur pour la variable du modèle souhaitée.
3. Sélectionnez **File (Fichier)** > **Save As (Enregistrer sous)**, puis enregistrez le fichier au format **CSV UTF-8**.

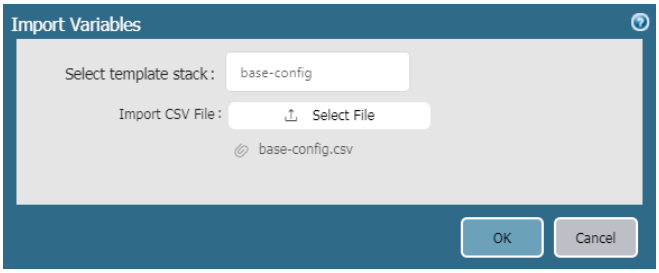


STEP 3 | Importez le fichier CSV vers la pile de modèles.

1. Connectez-vous à l'interface Web Panorama du contrôleur Panorama.
2. Sélectionnez **Panorama** > **Interconnect** > **Devices (Périphériques)**, puis **Import Variables (Importez les variables)**.
3. Dans la liste déroulante **Select template stack (Sélectionner la pile de modèles)**, sélectionnez la pile de modèles vers laquelle importer les variables.

© 2020 Palo Alto Networks, Inc.

4. Sous **Import CSV File (Importer le fichier CSV)**, cliquez sur **Select File (Sélectionner le fichier)**, puis sélectionnez le fichier CSV contenant les variables de la pile de modèles.
5. Cliquez sur **OK** pour importer les variables de la pile de modèles.



6. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

STEP 4 | Synchroniser le nœud Panorama avec le contrôleur Panorama.

STEP 5 | Appliquer la configuration du nœud Panorama aux périphériques gérés.

Gérer la clé principale avec Panorama Interconnect

Panorama, les pare-feu, les collecteurs de journaux et les appareils WF-500 utilisent une clé principale pour chiffrer les éléments de nature délicate de la configuration. Ils disposent d'une clé principale par défaut qu'ils utilisent pour chiffrer les mots de passe et les éléments de configuration.

Dans le cadre d'une pratique de sécurité standard, lors de l'expiration de votre clé principale, vous devez la renouveler sur chaque pare-feu, collecteur de journaux, appareil WildFire et Panorama individuel. La clé principale déployée sur vos périphériques gérés doit être identique pour le contrôleur Panorama, les nœuds Panorama et les périphériques gérés pour transmettre avec succès la configuration. Pour garantir le déploiement uniforme des clés, déployez une nouvelle clé principale ou renouvelez une clé principale venant à expiration sur plusieurs pare-feu, collecteurs de journaux et appareils WF-500 directement à partir de Panorama. Lorsque vous utilisez Panorama Interconnect, vous devez configurer et déployer la même clé principale pour le contrôleur Panorama et tous les nœuds Panorama et appareils gérés au cours d'une seule procédure. Pour déployer une clé principale aux périphériques gérés, vous devez configurer la clé principale sur chaque nœud Panorama, puis les déployer à tous les périphériques gérés par ce nœud. Reportez-vous à la rubrique Configuration de la clé principale pour obtenir de plus amples informations.

STEP 1 | Configurez la clé principale sur le contrôleur Panorama.

1. Sur le contrôleur Panorama, Se connecter à l'interface Web Panorama.
2. Sélectionnez **Panorama** > **Master Key and Diagnostics (Clé principale et diagnostics)**, puis modifiez la clé principale.
    1. Si vous renouvelez une clé principale, saisissez la **Current Master Key (Clé principale actuelle)**. Si vous remplacez la clé principale par défaut par une nouvelle clé principale, n'indiquez pas de **Current Master Key (Clé principale actuelle)**.
    2. Configurez la **New Master Key (Nouvelle clé principale)** et **Confirm Master Key (Confirmez la clé principale)**.
    3. Configurez la **Lifetime (Durée de vie)** de la clé principale et la **Time for Reminder (Durée du rappel)**.
    4. Configurez le contrôleur Panorama pour qu'il procède au **Auto Renew with Same Master Key (renouvellement automatique avec la même clé principale)** pendant un nombre de jours ou d'heures indiqués à l'issue de l'expiration de la clé.
    5. Cliquez sur **OK**.

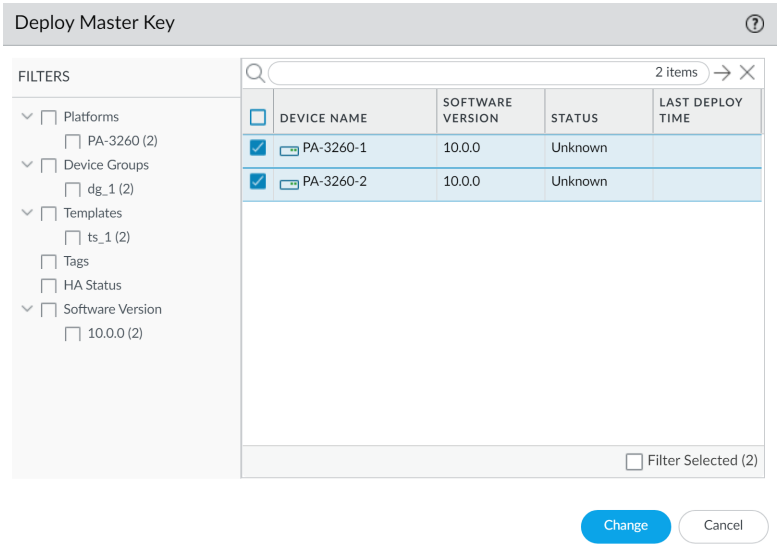
© 2020 Palo Alto Networks, Inc.

3. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

STEP 2 | Déployez la clé principale sur tous les périphériques gérés par le nœud Panorama.

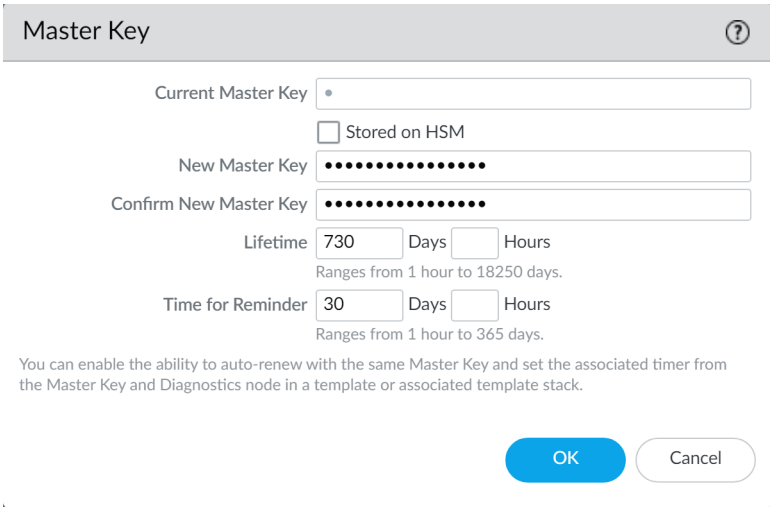
Répétez cette étape pour tous les nœuds Panorama.

1. Se connecter à l'interface Web Panorama du nœud Panorama.
2. Sélectionnez **Panorama** > **Master Key and Diagnostics (Clé principale et diagnostique)**, puis configurez la clé principale. La nouvelle clé principale doit être identique à celle que vous avez configurée sur le contrôleur Panorama à l'étape 1.
   1. Si vous renouvelez une clé principale, saisissez la **Current Master Key (Clé principale actuelle)**. Si vous remplacez la clé principale par défaut par une nouvelle clé principale, n'indiquez pas de **Current Master Key (Clé principale actuelle)**.
   2. Configurez la **New Master Key (Nouvelle clé principale)** et **Confirm Master Key (Confirmez la clé principale)**.
   3. Configurez la **Lifetime (Durée de vie)** de la clé principale et la **Time for Reminder (Durée du rappel)**.
   4. Configurez le contrôleur Panorama pour qu'il procède au **Auto Renew with Same Master Key (renouvellement automatique avec la même clé principale)** pendant un nombre de jours ou d'heures indiqués à l'issue de l'expiration de la clé.
   5. Cliquez sur **OK**.
3. Sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)** > **Summary (Récapitulatif)**, puis **Deploy Master Key (Déployer la clé principale)**.
4. Sélectionnez tous les périphériques, puis **Change (Modifiez)** la clé principale.



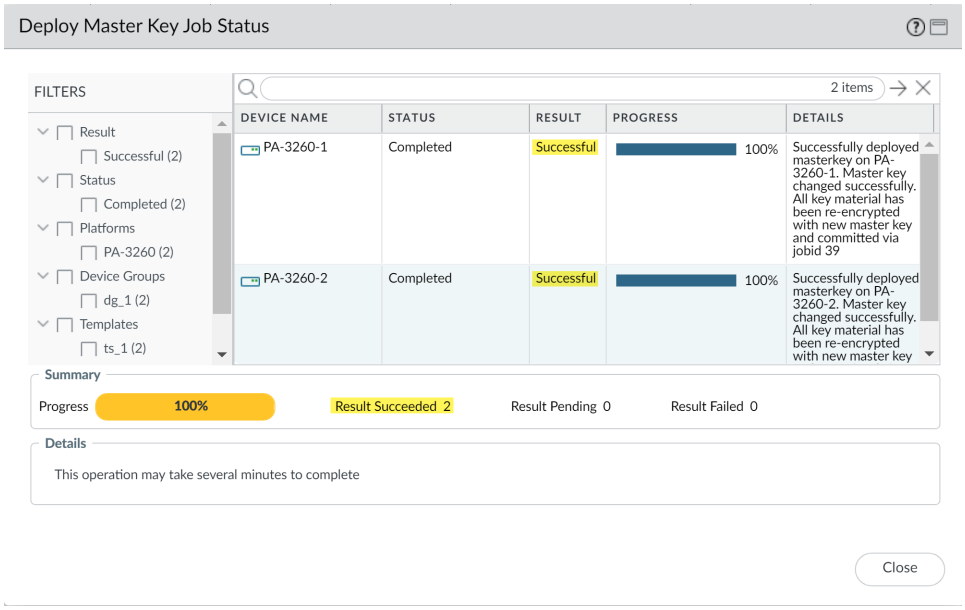
5. Configurez la clé principale La clé doit être identique à celle que vous avez configurée à l'étape 1 :
   1. Si vous renouvelez une clé principale, saisissez la **Current Master Key (Clé principale actuelle)**. Si vous remplacez la clé principale pas défaut par une nouvelle clé principale, n'indiquez pas de **Current Master Key (Clé principale actuelle)**.
   2. Configurez la **New Master Key (Nouvelle clé principale)** et **Confirm Master Key (Confirmez la clé principale)**.
   3. Configurez la **Lifetime (Durée de vie)** de la clé principale et la **Time for Reminder (Durée du rappel)**.
   4. Cliquez sur **OK**.

© 2020 Palo Alto Networks, Inc.



6. Vérifiez que la clé principale a été déployée avec succès à tous les périphériques sélectionnés.

   Un journal système est généré lorsque vous déployez une nouvelle clé principale à partir de Panorama.



STEP 3 | Déployez la clé principale aux collecteurs de journaux.

Répétez cette étape pour tous les nœuds Panorama. La nouvelle clé principale doit être identique à celle que vous avez configurée à l'étape 1.

1. Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)**, puis **Deploy Master Key (Déployer la clé principale)**.
2. Sélectionnez tous les périphériques, puis **Change (Modifiez)** la clé principale.
3. Configurez la clé principale :
   1. Si vous renouvelez une clé principale, saisissez la **Current Master Key (Clé principale actuelle)**. Si vous remplacez la clé principale par défaut par une nouvelle clé principale, n'indiquez pas de **Current Master Key (Clé principale actuelle)**.
   2. Précisez la **New Master Key (Nouvelle clé principale)** et **Confirm Master Key (Confirmez la clé principale)**.

© 2020 Palo Alto Networks, Inc.

3. Configurez la **Lifetime (Durée de vie)** de la clé principale et la **Time for Reminder (Durée du rappel)**.
4. Cliquez sur **OK**.

4. Vérifiez que la clé principale a été déployée avec succès à tous les périphériques sélectionnés.

   Un journal système est généré lorsque vous déployez une nouvelle clé principale à partir de Panorama.

STEP 4 | Déployez la clé principale aux appareils WildFire gérés.

Répétez cette étape pour tous les nœuds Panorama. La nouvelle clé principale doit être identique à celle que vous avez configurée à l'étape 1.

1. Sélectionnez **Panorama** > **Managed WildFire appliances (appareils WildFire gérés)**, puis **Deploy Master Key (Déployer la clé principale)**.
2. Sélectionnez tous les périphériques, puis **Change (Modifiez)** la clé principale.
3. Configurez la clé principale :
   1. Si vous renouvelez une clé principale, saisissez la **Current Master Key (Clé principale actuelle)**. Si vous remplacez la clé principale par défaut par une nouvelle clé principale, n'indiquez pas de **Current Master Key (Clé principale actuelle)**.
   2. Précisez la **New Master Key (Nouvelle clé principale)** et **Confirm Master Key (Confirmez la clé principale)**.
   3. Configurez la **Lifetime (Durée de vie)** de la clé principale et la **Time for Reminder (Durée du rappel)**.
   4. Cliquez sur **OK**.
4. Vérifiez que la clé principale a été déployée avec succès à tous les périphériques sélectionnés.

   Un journal système est généré lorsque vous déployez une nouvelle clé principale à partir de Panorama.

Appliquer la configuration du nœud Panorama aux périphériques gérés

Une fois que vous avez Synchroniser le nœud Panorama avec le contrôleur Panorama, les configurations de la pile de modèles et du groupe de périphériques, appliquez la configuration de la pile de modèles et du groupe de périphériques aux périphériques gérés.

STEP 1 | Se connecter à l'interface Web Panorama du contrôleur Panorama.

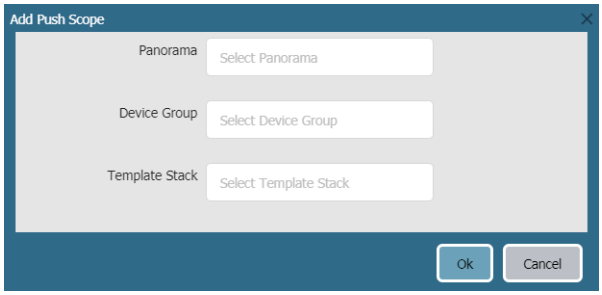
STEP 2 | Sélectionnez **Panorama** > **Interconnect** > **Devices (Périphériques)**.

STEP 3 | Cliquez sur **Push to Devices (Appliquer aux périphériques)** pour appliquer la configuration synchronisée des nœuds Panorama aux périphériques gérés.

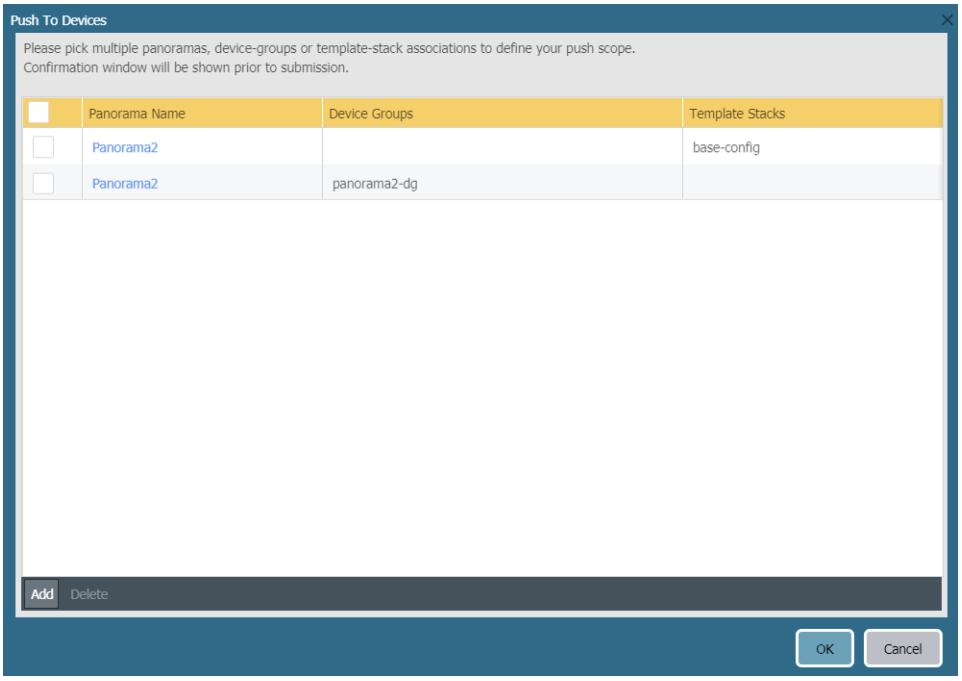
STEP 4 | **Add (Ajoutez)** le nœud de Panorama qui gère les périphériques pour y appliquer la configuration. Répétez cette étape pour appliquer la configuration à plusieurs nœuds Panorama, périphériques, groupes ou modèles, au besoin :

1. Sélectionnez le nœud **Panorama**.
2. Sélectionnez le **Device Group (Groupe de périphériques)** auquel appliquer les configurations du groupe de périphériques et de la pile de modèles ou sélectionnez une **Template Stack (pile de modèles)** si vous souhaitez uniquement appliquer la configuration de la pile de modèles.
3. Cliquez sur **OK** pour finir de définir la portée de la transmission.

© 2020 Palo Alto Networks, Inc.



STEP 5 | Cliquez sur **OK** pour appliquer la configuration aux périphériques gérés.



STEP 6 | Dans la colonne Device Group Push Status (État de l'application au groupe de périphériques), vérifiez que les applications sont **`in-sync`**.

Mettre à niveau le plugiciel (plug-in) Panorama Interconnect

Utilisez la procédure suivante pour mettre à niveau le plugiciel Panorama™ Interconnect sur le contrôleur Panorama et les nœuds Panorama. Lors de la mise à niveau du plugiciel Panorama Interconnect, vous devez procéder à la mise à niveau du contrôleur Panorama avant de faire passer les nœuds Panorama à la même version de plugiciel de le contrôleur. La nouvelle version du plugiciel que vous avez téléchargée et installée sur le nœud Panorama doit correspondre à la version du plugiciel que vous avez installée sur le contrôleur Panorama pour vous assurer que le contrôleur Panorama et les nœuds Panorama sélectionnés demeurent synchronisés.

Si c'est la première fois que vous installez le plugiciel, reportez-vous à la section Configurer le plugiciel (plug-in) Panorama Interconnect.

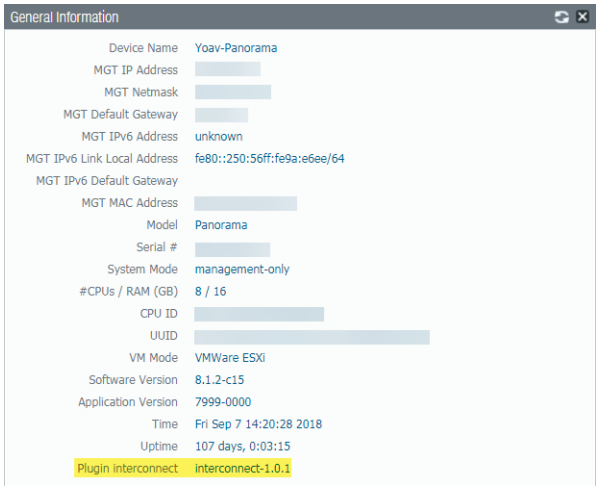
STEP 1 | Se connecter à l'interface Web Panorama du contrôleur Panorama.

STEP 2 | Mettez à niveau le plugiciel Panorama Interconnect sur le contrôleur Panorama.

1. Sélectionnez **Panorama** > **Plugins (Plugiciels)**, puis cherchez **`Interconnect`**.

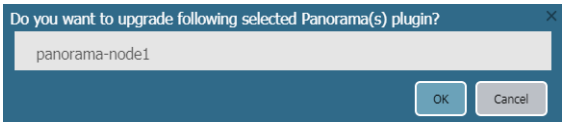
© 2020 Palo Alto Networks, Inc.

2. **Download (Téléchargez)**, puis **Install (Installez)** la nouvelle version du plugiciel Panorama Interconnect. Une invite vous avise que l'installation est terminée.
3. Vérifiez que le **Dashboard (Tableau de bord)** affiche la version nouvellement installée du plugiciel Interconnect.

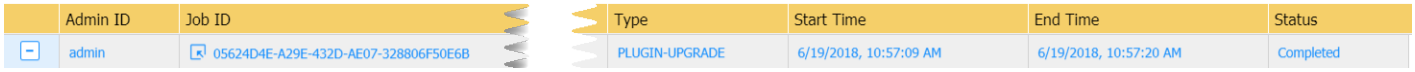


STEP 3 | Mettez à niveau le plugiciel Panorama Interconnect sur le nœud Panorama.

1. Sélectionnez **Panorama** > **Interconnect** > **Panorama Nodes (Nœuds Panorama)**, sélectionnez un ou plusieurs nœuds Panorama, puis **Upgrade Plugin (Mettre le plugiciel à niveau)**.
2. Vérifiez les nœuds Panorama sélectionnés, puis cliquez sur **OK** pour commencer la mise à niveau du plugiciel.



3. Attendez que la tâche de mise à niveau du plugiciel soit `Completed`. Cliquez sur **Panorama** > **Interconnect** > **Tasks (Tâches)** pour voir la progression du travail.



4. Une fois la mise à niveau terminée, sélectionnez **Panorama** > **Interconnect** > **Panorama Nodes (Nœuds Panorama)** pour vérifier que la version du **Plugin (Plugiciel)** est la bonne pour les nœuds Panorama sélectionnés.



© 2020 Palo Alto Networks, Inc.

Gérer la collecte des journaux

Tous les pare-feu de Palo Alto Networks peuvent générer des journaux qui fournissent une piste d'audit des activités du pare-feu. Pour la journalisation centralisée et la création de rapports, vous devez transférer les journaux générés sur les pare-feux vers votre infrastructure sur site incluant le serveur de gestion Panorama ™ ou les collecteurs de journaux ou envoyer les journaux à Cortex Data Lake basé sur le cloud. Facultativement, vous pouvez configurer Panorama pour transférer les journaux vers des destinations de journalisation externes (telles que les serveurs Syslog).

Si vous transférez des journaux vers un appareil virtuel Panorama en mode hérité, vous n'avez pas besoin d'effectuer de tâches supplémentaires pour activer la journalisation. Si vous transférez des journaux vers des collecteurs de journaux, vous devez les configurer en tant que collecteurs gérés et les affecter aux groupes de collecteurs. Un collecteur géré peut être local sur une appliance M-Series ou sur une appliance virtuelle Panorama en mode Panorama. En outre, un appareil M-Series ou un appareil virtuelle Panorama en mode Log Collector peut être des collecteurs de journaux dédiés. Pour déterminer si vous souhaitez déployer l'un des types de collecteurs gérés ou les deux, reportez-vous à la section Collecte des journaux locaux et distribués.

Pour gérer les journaux système et configuration que Panorama génère localement, voir Surveiller Panorama.

- Configurer un collecteur géré
- Configurer l'authentification pour un Collecteur de journaux dédié
- Gérer les groupes de collecteurs
- Configurer le transfert des journaux vers Panorama
- Configurez le transfert syslog vers des destinations extérieures.
- Transmettre les journaux à Cortex Data Lake
- Vérifier le transfert des journaux vers Panorama
- Modifier le journal de transfert et la mise en mémoire tampon par défaut
- Configurer le transfert des journaux de Panorama vers des destinations extérieures
- Déploiements de collecte de journaux

© 2020 Palo Alto Networks, Inc.

Configurer un collecteur géré

Pour activer le serveur de gestion de Panorama pour gérer un collecteur de journaux, vous devez l'ajouter comme un collecteur géré. Vous pouvez ajouter deux types de collecteurs gérés :

- **Collecteur de journaux dédié** : Pour configurer un nouvel appareil M-600, M-500, M-200 ou Panorama en tant que collecteur de journaux ou basculer d'un appareil M-Series existant ou d'un appareil virtuel Panorama du mode Panorama au mode collecteur de journaux, voir Configurer l'appareil de série M en tant que collecteur de journaux. Gardez à l'esprit que le passage du mode Panorama au mode collecteur de journaux supprime le collecteur de journaux local prédéfini sur l'appareil de série M en mode Panorama.
- **Collecteur de journal local** : un collecteur de journaux peut s'exécuter localement sur l'appareil M-600, M-500, M-200 ou sur l'appareil virtuel Panorama en mode Panorama. Sur les appareils de série M, le collecteur de journaux est prédéfini ; sur l'appareil virtuel, vous devez ajouter le collecteur de journaux. Lorsque le serveur de gestion Panorama a une configuration haute disponibilité (HD), chaque paire HD peut avoir un collecteur de journaux local. Toutefois, par rapport au Panorama principal, le collecteur de journaux sur le Panorama secondaire est distant et non local. Par conséquent, pour utiliser le collecteur de journaux sur le Panorama secondaire, vous devez l'ajouter manuellement au Panorama principal (pour plus de détails, voir Déployer les appareils de série M Panorama avec les collecteurs de journaux locaux ou Déployer les appareils virtuels Panorama avec les collecteurs de journaux locaux). Si vous supprimez un collecteur de journaux local, vous pouvez le rajouter ultérieurement. Les étapes suivantes décrivent comment ajouter un collecteur de journaux local.



Il est recommandé de conserver un collecteur de journaux local et un groupe de collecteurs sur le serveur de gestion Panorama, indépendamment de savoir s'il gère des collecteurs de journaux dédiés.



Si l'appareil virtuel Panorama est en mode hérité, vous devez passer en mode Panorama pour créer un collecteur de journaux. Pour plus de détails, consultez Configurer l'appareil virtuel Panorama avec le collecteur de journaux local*.*

STEP 1 | Enregistrez le numéro de série du collecteur de journaux.

Vous en aurez besoin lorsque vous ajouterez le collecteur de journaux comme collecteur géré.

1. Accédez à l'interface Web de Panorama.
2. Sélectionnez **Dashboard (Tableau de bord)** et enregistrez le **Serial # (Numéro de série)** dans la section General Information section (Informations générales).

STEP 2 | Ajoutez le collecteur de journaux en tant que collecteur géré.

1. Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** et **Add (Ajoutez)** un nouveau collecteur de journaux.
2. Dans les paramètres **General (Général)**, saisissez le numéro de série (**Collector S/N (N° de série du collecteur)**) que vous avez enregistré pour le collecteur de journaux.
3. Cliquez sur **OK** pour enregistrer vos modifications.
4. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)**.

STEP 3 | (Facultatif) Configurez l'authentification de l'administrateur du Collecteur de journaux.

1. Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** et modifiez le collecteur de journaux en cliquant sur son nom.
2. Configurez le mot de passe de l'administrateur du Collecteur de journaux :

© 2020 Palo Alto Networks, Inc.

1. Sélectionnez le **Mode** du mot de passe :
2. Si vous avez sélectionné **Password (Mot de passe)**, saisissez un **Password (Mot de passe)** en clair et **Confirm Password (Confirmez le mot de passe)**. Si vous avez sélectionné le mode de **Password Hash (Hachage du mot de passe)**, saisissez une chaîne de mot de passe hachée qui se compose d'un maximum de 63 caractères.

3. Configurez les exigences de sécurité de la connexion de l'administrateur :

   Si vous définissez le champ Failed Attempts (Tentatives échouées) sur une valeur non nulle, mais que vous laissez le champ Lockout Time (Durée de verrouillage) sur 0, l'administrateur est verrouillé indéfiniment jusqu'à ce qu'un autre administrateur déverrouille manuellement l'administrateur. Si aucun autre administrateur n'a été créé, vous devez reconfigurer les paramètres de Failed Attempts (Tentatives échouées) et de Lockout Time (Durée de verrouillage) sur et transmettre les changements de configuration au collecteur de journaux. Pour veiller à ce qu'un administrateur ne soit jamais verrouillé, utilisez la valeur 0 par défaut pour les Failed Attempts (Tentatives échouées) et la Lockout Time (Durée de verrouillage).

   1. Saisissez la valeur correspondant au nombre de **Failed Attempts (Tentatives échouées)** de connexion. La plage se situe entre la valeur par défaut de `0` et la valeur maximale de `10`, où la valeur `0` spécifie des tentatives de connexion illimitées.
   2. Saisissez la valeur de **Lockout Time (Durée de verrouillage)** entre la valeur par défaut de `0` et la valeur maximale de `60` minutes.

4. Cliquez sur **OK** pour enregistrer vos modifications.

STEP 4 | Activer les disques de journalisation.

1. Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** et modifiez le collecteur de journaux en cliquant sur son nom.

   Le nom du collecteur de journaux a la même valeur que le nom d'hôte du serveur de gestion Panorama.
2. Sélectionnez **Disks (Disques)** et **Add (Ajoutez)** chaque paire de disques.
3. Cliquez sur **OK** pour enregistrer vos modifications.
4. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)**.

STEP 5 | (Facultatif) Si votre déploiement utilise des certificats personnalisés pour l'authentification entre Panorama et les périphériques gérés, déployez le certificat de périphérique client personnalisé. Pour plus d'informations, consultez Configurer l'authentification à l'aide de certificats personnalisés.

1. Sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificat)** et choisissez le profil de certificat dans la liste déroulante ou cliquez sur **New Certificate Profile (Nouveau profil de certificat)** pour en créer un.
2. Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** et **Add (Ajoutez)** un nouveau collecteur de journaux ou sélectionnez un collecteur existant. Sélectionnez **Communication**.
3. Sélectionnez le type de certificat de périphérique dans la liste déroulante Type.
   - Si vous utilisez un certificat de périphérique local, sélectionnez **Certificate (Certificat)** et **Certificate Profile (Profil de certificat)** à partir des listes déroulantes respectives.
   - Si vous utilisez SCEP comme certificat de périphérique, sélectionnez **SCEP Profile (Profil SCEP)** et **Certificate Profile (Profil de certificat)** à partir des listes déroulantes respectives.
4. Cliquez sur **OK**.

© 2020 Palo Alto Networks, Inc.

STEP 6 | (Facultatif) Configurez **Secure Server Communication (Communication sécurisée avec le serveur)** sur un collecteur de journaux. Pour plus d'informations, consultez Configurer l'authentification à l'aide de certificats personnalisés.

1. Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** puis cliquez sur **Add (Ajouter)**. Sélectionnez **Communication**.
2. Vérifiez que la case **Custom Certificate Only (Certificat personnalisé uniquement)** n'est pas cochée. Cela vous permet de continuer à gérer tous les périphériques lors de la migration vers des certificats personnalisés.

   Lorsque la case Custom Certificate Only (Certificat personnalisé uniquement) est cochée, le collecteur de journaux ne s'authentifie pas et ne peut pas recevoir les journaux des périphériques à l'aide de certificats prédéfinis.
3. Sélectionnez le profil de service SSL/TLS depuis le menu déroulant **SSL/TLS Service Profile (Profil de service SSL/TLS)**. Ce profil de service SSL/TLS s'applique à toutes les connexions SSL entre le collecteur de journaux et les périphériques qu'il enregistre.
4. Sélectionnez le profil du certificat depuis la liste déroulante **Certificate Profile (Profil du certificat)**.
5. Sélectionnez **Authorize Client Based on Serial Number (Autoriser le client en fonction du numéro de série)** pour que le serveur vérifie les clients par rapport aux numéros de série des périphériques gérés. Le certificat client doit avoir le mot clé spécial $UDID défini en tant que CN à autoriser en fonction des numéros de série.
6. Dans **Disconnect Wait Time (min) (Délai d'attente de déconnexion (min))**, saisissez le nombre de minutes que Panorama doit attendre avant de mettre fin et de rétablir la connexion avec ses périphériques gérés. Ce champ est vide par défaut et la plage est comprise entre 0 et 44 640 minutes.

   Le délai d'attente de déconnexion de déconnexion ne commence pas à décompter tant que vous n'avez pas validé la nouvelle configuration.
7. (Facultatif) Configurez une liste d'autorisation.
   1. Cliquez sur **Add (Ajouter)** sous Authorization List (Liste d'autorisation).
   2. Sélectionnez **Subject (Objet)** ou **Subject Alt Name (Autre nom de l'objet)** comme type d'identifiant.
   3. Entrez un identifiant du type sélectionné.
   4. Cliquez sur **OK**.
   5. Sélectionnez **Check Authorization List (Vérifier la liste d'autorisation)** pour appliquer la liste d'autorisation.
8. Cliquez sur **OK**.
9. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)**.

STEP 7 | Validez vos modifications.

1. Vérifiez que la page **Panorama (Panorama)** > **Managed Collectors (collecteurs gérés)** répertorie le Collecteur de Journaux que vous avez ajouté. La colonne Connecté affiche une icône de coche pour indiquer que le collecteur de journaux est connecté à Panorama. Vous devrez peut-être attendre quelques minutes avant que la page affiche le statut de connexion actualisée.

   Jusqu'à ce que vous Configuration d'un groupe de collecteurs et que vous appliquiez les modifications de configuration au groupe de collecteurs, la colonne Configuration Status (État de configuration) affiche Out of sync (Désynchronisé), la colonne Run Time Status (État d'exécution) affiche Disconnected (Déconnecté), et la commande CLI **`show interface all`** *affiche les interfaces comme* `down`.
2. Cliquez sur **Statistics (statistiques)** dans la dernière colonne pour vérifier que les disques de journalisation sont activés.

STEP 8 | Étapes suivantes...

© 2020 Palo Alto Networks, Inc.

Avant qu'un collecteur de journaux puisse recevoir des journaux de pare-feu, vous devez :

1. Configurer le transfert des journaux vers Panorama.
2. Configuration d'un groupe de collecteurs : sur les appareils de série M, un groupe de collecteurs par défaut est prédéfini et contient déjà le collecteur de journaux local en tant que membre. Sur l'appareil virtuel Panorama, vous devez ajouter le groupe de collecteurs et ajouter le collecteur de journaux local en tant que membre. Sur les deux modèles, attribuez des pare-feu au collecteur de journaux local pour le transfert des journaux.

© 2020 Palo Alto Networks, Inc.

Configurer l'authentification pour un Collecteur de journaux dédié

Créez et configurez une meilleure authentification pour votre Collecteur de journaux dédié en configurant les utilisateurs administratifs locaux à l'aide de paramètres d'authentification granulaires ainsi qu'en exploitant RADIUS, TACAS+ ou LDAP pour l'autorisation et l'authentification.

Lorsque vous configurez et validez les administrateurs depuis Panorama, vous remplacez les administrateurs existants du Collecteur de journaux dédié par ceux que vous configurez dans Panorama.

- Configurez un Compte administratif pour un Collecteur de journaux dédié
- Configurer l'authentification RADIUS pour un Collecteur de journaux dédié
- Configurer l'authentification TACACS + pour un Collecteur de journaux dédié
- Configurer l'authentification LDAP pour un Collecteur de journaux dédié

Configurez un Compte administratif pour un Collecteur de journaux dédié

Créez un ou plusieurs administrateurs avec des paramètres d'authentification granulaires pour votre Collecteur de journaux dédié pour le gérer depuis un serveur de gestion Panorama™. De plus, vous pouvez configurer les administrateurs locaux depuis Panorama qui peuvent être configurés directement dans le CLI du Collecteur de journaux dédié. Cependant, la validation d'une nouvelle configuration pour passer au Collecteur de journaux dédié remplacera les administrateurs locaux configurés pour le Collecteur de journaux dédié.

STEP 1 | Se connecter à l'interface Web Panorama.

STEP 2 | Configurer un collecteur géré.

STEP 3 | (En option) Configure an authentication profile (Configurez un profil d'authentification) pour définir le service d'authentification qui valide les informations de connexion des administrateurs qui accèdent au CLI du Collecteur de journaux dédié.

STEP 4 | Configure one or more administrator accounts (Configurez un ou plusieurs comptes administrateurs) selon ce qui est nécessaire.

Les comptes administrateurs créés dans Panorama sont ensuite importés vers le Collecteur de journaux dédié et gérés depuis Panorama.

STEP 5 | Configurer l'authentification pour le Collecteur de journaux dédié

1. Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** et sélectionnez le collecteur de journaux dédié que vous avez préalablement ajouté.
2. (En option) Sélectionnez le A**uthentification Profile (Profil d'authentification)** que vous avez configuré au cours des étapes antérieures.
3. Configurez la **Timeout Configuration (Configuration du délai avant expiration)** d'authentification pour le Collecteur de journaux dédié.
    1. Saisissez le nombre de **Failed Attempt (Tentatives échouées)** avant que l'accès d'un utilisateur au CLI du Collecteur de journaux dédié ne soit bloqué.

© 2020 Palo Alto Networks, Inc.

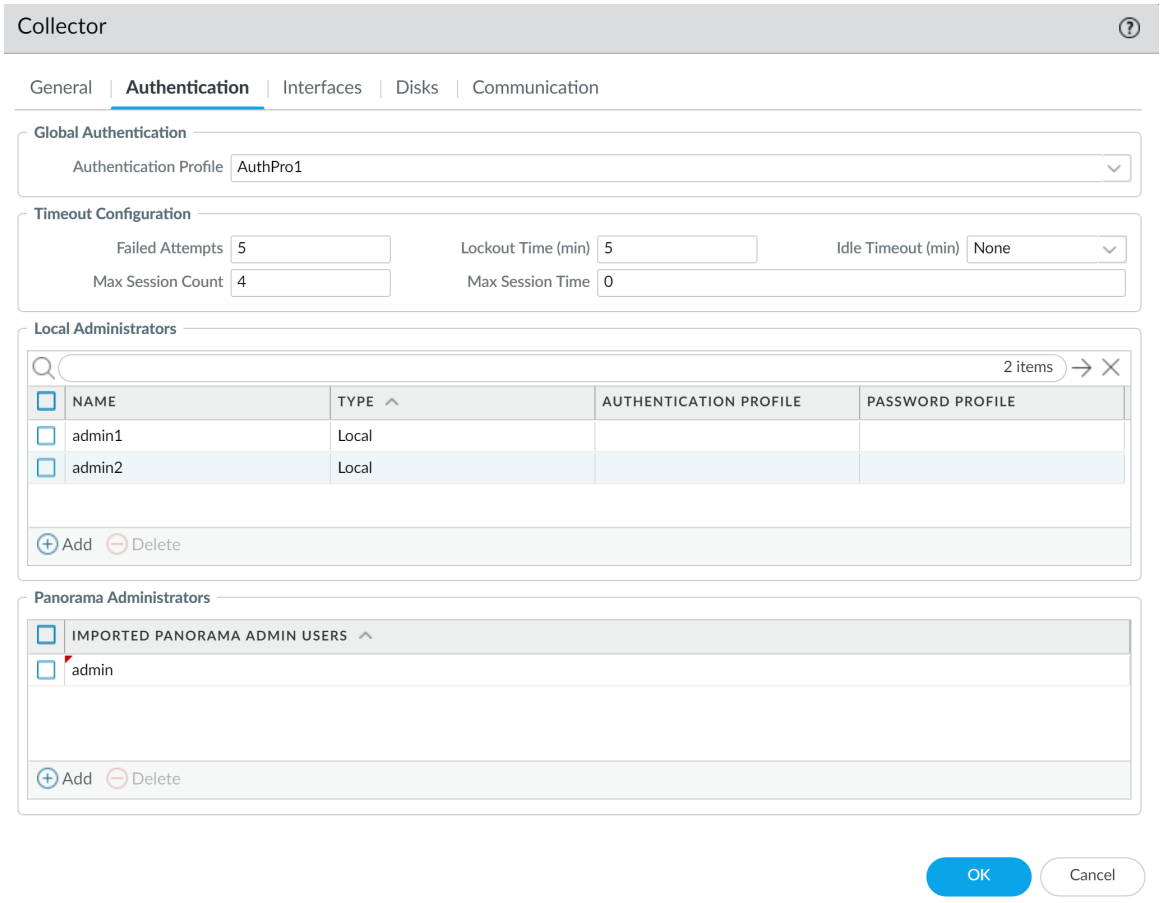
2. Saisissez la **Lockout Time (Durée de verrouillage)**, en minutes, selon laquelle le Collecteur de journaux dédié verrouille le compte d'un utilisateur après que celui-ci ait atteint le nombre de **Failed Attempts (Tentatives échouées)** configuré.
3. Saisissez le **Idle Timeout (délai d'expiration)**, en minutes, avant que le compte de l'utilisateur ne soit automatiquement déconnecté pour inactivité.
4. Saisissez le **Max Session Count (Compte de session max.)** pour indiquer combien de comptes d'utilisateur peuvent accéder simultanément au Collecteur de journaux dédié.
5. Saisissez la **Max Session Time (Durée de session max.)** pendant laquelle l'administrateur peut être connecté avant d'être automatiquement déconnecté.

4. Ajoutez les administrateurs du Collecteur de journaux dédié.

   Les administrateurs peuvent soit être ajoutés en tant qu'administrateur local ou en tant qu'administrateur Panorama importé, mais pas les deux. Ajouter le même administrateur en tant qu'administrateur local et en tant qu'administrateur Panorama importé n'est pas possible et peut entraîner une panne de validation de Panorama. Par exemple, la validation de Panorama échoue si vous ajoutez **`admin1`** en tant qu'administrateur local et administrateur Panorama.

   1. **Add (Ajoutez)** et configurez de nouveaux administrateurs uniques pour le Collecteur de journaux dédié. Ces administrateurs sont spécifiques au Collecteur de journaux dédié pour lequel ils sont créés et vous gérez ces administrateurs depuis ce tableau.
   2. **Add (Ajoutez)** n'importe quel administrateur configuré dans Panorama. Ces administrateurs sont créés dans Panorama et importés vers le Collecteur de journaux dédié.

5. Cliquez sur **OK** pour enregistrer la configuration de l'authentification du Collecteur de journaux dédié.



STEP 6 | **Commit (Validez)** et **Commit and Push (Validez et appliquez)** les modifications de votre configuration.

© 2020 Palo Alto Networks, Inc.

STEP 7 | Connectez-vous à l'ILC Panorama du Collecteur de journaux dédié afin de vérifier si vous pouvez accéder au Collecteur de journaux dédié en utilisant l'utilisateur admin local.

Configurer l'authentification RADIUS pour un Collecteur de journaux dédié

Utilisez un serveur RADIUS pour authentifier l'accès administratif à la CLI du Collecteur de journaux dédié. Vous pouvez également définir des attributs spécifiques au fournisseur (VSA) sur le serveur RADIUS pour gérer l'autorisation de l'administrateur. L'utilisation de VSA vous permet de changer les rôles rapidement, d'accéder aux domaines et aux groupes d'utilisateurs à travers votre service d'annuaire au lieu de reconfigurer les réglages dans le serveur de gestion Panorama™.



Vous pouvez importer le dictionnaire RADIUS de Palo Alto Networks dans le serveur RADIUS pour définir les attributs d'authentification nécessaires pour la communication entre Panorama et le serveur RADIUS.

STEP 1 | Se connecter à l'interface Web Panorama.

STEP 2 | Configurer un collecteur géré.

STEP 3 | Configuration de l'authentification RADIUS

1. Ajoutez un profil de serveur RADIUS.

   Le profil définit comment le Collecteur de journaux dédié se connecte au serveur RADIUS.

   1. Sélectionnez **Panorama** > **Server Profiles (Profils de serveur)** > **RADIUS** et **Add (Ajoutez)** un profil.
   2. Saisissez un **Profile Name (Nom de profil)** pour identifier le profil de serveur.
   3. Saisissez l'intervalle du **Timeout (Délai d'expiration)**, en secondes, après lequel une requête d'authentification arrive à expiration (plage de 1 à 20 ; par défaut 3).
   4. Sélectionnez l'**Authentication Protocol (Protocole d'authentification)** (par défaut, **CHAP**) que le collecteur de journaux dédié utilise pour s'authentifier au serveur RADIUS.

      Sélectionnez CHAP si le serveur RADIUS prend en charge ce protocole ; il est plus sécuritaire que PAP.

   5. **Add (Ajoutez)** chaque serveur RADIUS et saisissez les renseignements suivants :

      1. Le **Name (Nom)** qui permet d'identifier le serveur.
      2. L'adresse IP ou le FQDN du **RADIUS Server (Serveur RADIUS)**.
      3. Le **Secret**/**Confirm Secret (Phrase secrète / Confirmer une phrase secrète)**, une clé pour chiffrer les noms d'utilisateur et les mots de passe.
      4. Le **Port** du serveur pour les demandes d'authentification (1812 par défaut).

   6. Cliquez sur **OK** pour enregistrer le profil de serveur.
2. Affectez le profil de serveur RADIUS à un profil d'authentification.

   Le profil d'authentification définit les paramètres d'authentification qui sont communs à un ensemble d'administrateurs.

   1. Sélectionnez **Panorama** > **Authentication Profile (Profil d'authentification)** et **Add (Ajoutez)** un profil.
   2. Entrez un **Name (Nom)** pour identifier le profil d'authentification.
   3. Définissez le **Type** sur **RADIUS**.
   4. Sélectionnez le **Server Profile (Profil de serveur)** que vous avez créé.

© 2020 Palo Alto Networks, Inc.

5. Sélectionnez **Retrieve user group from RADIUS (Récupérer le groupe d'utilisateurs auprès de TACACS+)** pour recueillir de l'information sur le groupe d'utilisateurs auprès des VSA définis sur le serveur TACACS+.

   Panorama fait correspondre l'information sur le groupe avec les groupes que vous avez spécifiés dans la liste d'autorisation du profil d'authentification.
6. Sélectionnez **Advanced (Avancé)** et, dans la liste d'autorisation, **Add (Ajoutez)** les administrateurs qui sont autorisés à s'authentifier avec ce profil d'authentification.
7. Cliquez sur **OK** pour enregistrer le profil d'authentification.

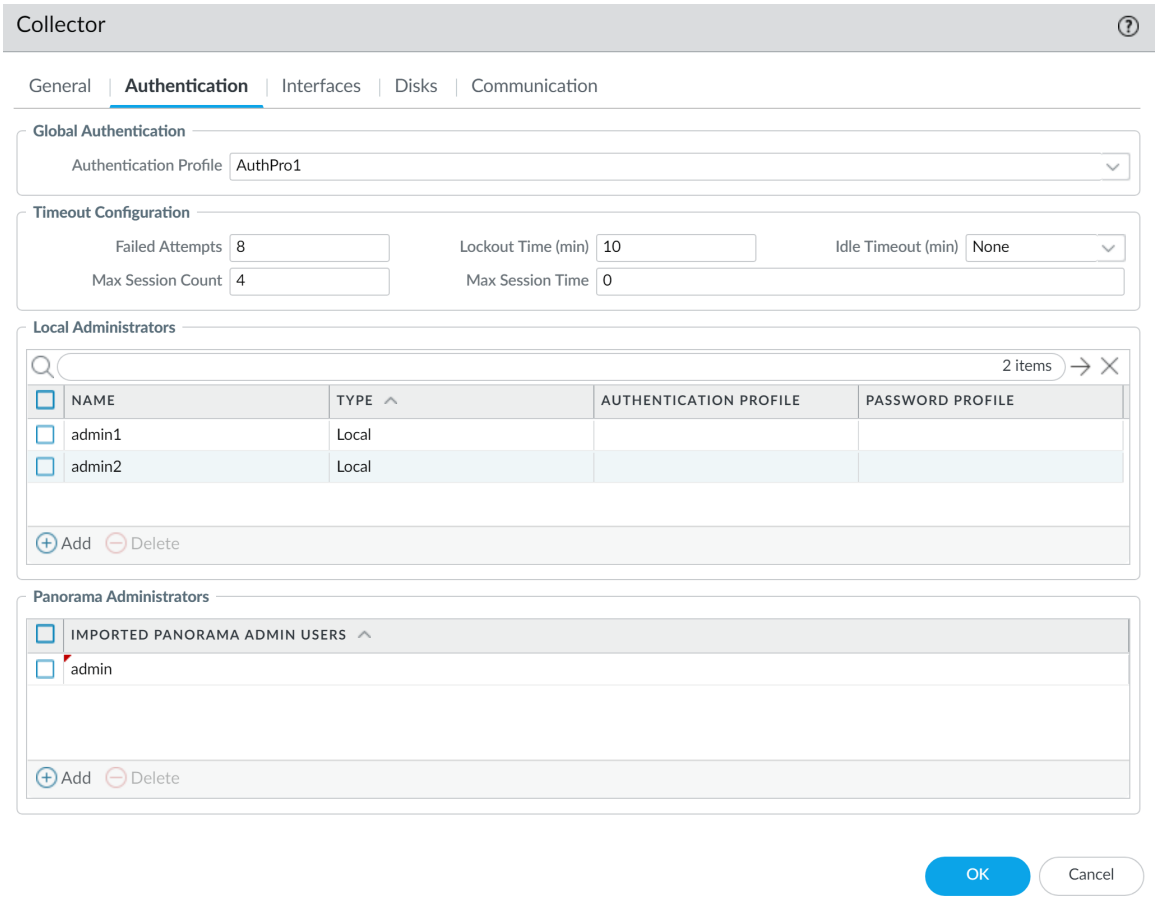
STEP 4 | Configurer l'authentification pour le Collecteur de journaux dédié

1. Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** et sélectionnez le collecteur de journaux dédié que vous avez préalablement ajouté.
2. Sélectionnez le **Authentification Profile (Profil d'authentification)** que vous avez configuré au cours des étapes antérieures.

   Si un profil d'authentification global n'est pas attribué, vous devez attribuer un profil d'authentification à chaque administrateur local individuel afin d'exploiter l'authentification à distance.
3. Configurez la **Timeout Configuration (Configuration du délai avant expiration)** d'authentification pour le Collecteur de journaux dédié.
   1. Saisissez le nombre de **Failed Attempt (Tentatives échouées)** avant que l'accès d'un utilisateur au CLI du Collecteur de journaux dédié ne soit bloqué.
   2. Saisissez la **Lockout Time (Durée de verrouillage)**, en minutes, selon laquelle le Collecteur de journaux dédié verrouille le compte d'un utilisateur après que celui-ci ait atteint le nombre de **Failed Attempts (Tentatives échouées)** configuré.
   3. Saisissez le **Idle Timeout (délai d'expiration)**, en minutes, avant que le compte de l'utilisateur ne soit automatiquement déconnecté pour inactivité.
   4. Saisissez le **Max Session Count (Compte de session max.)** pour indiquer combien de comptes d'utilisateur peuvent accéder simultanément au Collecteur de journaux dédié.
   5. Saisissez la **Max Session Time (Durée de session max.)** pendant laquelle l'administrateur peut être connecté avant d'être automatiquement déconnecté.
4. Ajoutez les administrateurs du Collecteur de journaux dédié.

   Les administrateurs peuvent soit être ajoutés en tant qu'administrateur local ou en tant qu'administrateur Panorama importé, mais pas les deux. Ajouter le même administrateur en tant qu'administrateur local et en tant qu'administrateur Panorama importé n'est pas possible et peut entraîner une panne de validation de Panorama. Par exemple, la validation de Panorama échoue si vous ajoutez `admin1` en tant qu'administrateur local et administrateur Panorama.
   1. **Add (Ajoutez)** et configurez de nouveaux administrateurs uniques pour le Collecteur de journaux dédié. Ces administrateurs sont spécifiques au Collecteur de journaux dédié pour lequel ils sont créés et vous gérez ces administrateurs depuis ce tableau.
   2. **Add (Ajoutez)** n'importe quel administrateur configuré dans Panorama. Ces administrateurs sont créés dans Panorama et importés vers le Collecteur de journaux dédié.
5. Cliquez sur **OK** pour enregistrer la configuration de l'authentification du Collecteur de journaux dédié.

© 2020 Palo Alto Networks, Inc.



STEP 5 | **Commit (Validez)** et **Commit and Push (Validez et appliquez)** les modifications de votre configuration.

STEP 6 | Connectez-vous à l'ILC Panorama du Collecteur de journaux dédié afin de vérifier si vous pouvez accéder au Collecteur de journaux dédié en utilisant l'utilisateur admin local.

Configurer l'authentification TACACS + pour un Collecteur de journaux dédié

Vous pouvez utiliser un serveur TACACS+ pour authentifier l'accès administratif au CLI du Collecteur de journaux dédié. Vous pouvez également définir des attributs spécifiques au fournisseur (VSA) sur le serveur TACACS+ pour gérer l'autorisation de l'administrateur. L'utilisation de VSA vous permet de changer les rôles rapidement, d'accéder aux domaines et aux groupes d'utilisateurs à travers votre service d'annuaire au lieu de reconfigurer les réglages dans Panorama.

STEP 1 | Se connecter à l'interface Web Panorama.

STEP 2 | Configurer un collecteur géré.

STEP 3 | Configuration de l'authentification TACACS+.

1. Ajoutez un profil de serveur TACACS+.

   Le profil définit comment le Collecteur de journaux dédié se connecte au serveur TACACS+.

© 2020 Palo Alto Networks, Inc.

1. Sélectionnez **Panorama** > **Server Profiles (Profils de serveur)** > **TACACS+** et **Add (Ajoutez)** un profil.
2. Saisissez un **Profile Name (Nom de profil)** pour identifier le profil de serveur.
3. Saisissez l'intervalle du **Timeout (Délai d'expiration)**, en secondes, après lequel une requête d'authentification arrive à expiration (plage de 1 à 20 ; par défaut 3).
4. Sélectionnez l'**Authentication Protocol (Protocole d'authentification)** (par défaut, **CHAP**) que Panorama utilise pour s'authentifier au serveur TACACS+.
5. Sélectionnez **CHAP** si le serveur TACACS+ prend en charge ce protocole ; il est plus sécuritaire que **PAP**.
6. **Add (Ajoutez)** chaque serveur TACACS+ et saisissez les renseignements suivants :
    1. Le **Name (Nom)** qui permet d'identifier le serveur.
    2. L'adresse IP ou le FQDN du **TACACS+ Server (Serveur TACACS+)**.
    3. **Le Secret / Confirm Secret (Phrase secrète / Confirmer une phrase secrète)**, une clé pour chiffrer les noms d'utilisateur et les mots de passe.
    4. Le **Port** du serveur pour les demandes d'authentification (49 par défaut).
7. Cliquez sur **OK** pour enregistrer le profil de serveur.

2. Affectez le profil de serveur TACACS+ à un profil d'authentification.

   Le profil d'authentification définit les paramètres d'authentification qui sont communs à un ensemble d'administrateurs.

   1. Sélectionnez **Panorama** > **Authentication Profile (Profil d'authentification)** et **Add (Ajoutez)** un profil.
   2. Saisissez un **Name (Nom)** pour identifier le profil.
   3. Définissez le **Type** sur **TACACS+**.
   4. Sélectionnez le **Server Profile (Profil de serveur)** que vous avez créé.
   5. Sélectionnez **Retrieve user group from TACACS+ (Récupérer le groupe d'utilisateurs auprès de TACACS+)** pour recueillir de l'information sur le groupe d'utilisateurs auprès des VSA définis sur le serveur TACACS+.

      Panorama fait correspondre l'information sur le groupe avec les groupes que vous avez spécifiés dans la liste d'autorisation du profil d'authentification.
   6. Sélectionnez **Advanced (Avancé)** et, dans la liste d'autorisation, **Add (Ajoutez)** les administrateurs qui sont autorisés à s'authentifier avec ce profil d'authentification.
   7. Cliquez sur **OK** pour enregistrer le profil d'authentification.

STEP 4 | Configurer l'authentification pour le Collecteur de journaux dédié

1. Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** et sélectionnez le collecteur de journaux dédié que vous avez préalablement ajouté.
2. Sélectionnez le **Authentification Profile (Profil d'authentification)** que vous avez configuré au cours des étapes antérieures.

   Si un profil d'authentification global n'est pas attribué, vous devez attribuer un profil d'authentification à chaque administrateur local individuel afin d'exploiter l'authentification à distance.
3. Configurez la **Timeout Configuration (Configuration du délai avant expiration)** d'authentification pour le Collecteur de journaux dédié.
   1. Saisissez le nombre de **Failed Attempt (Tentatives échouées)** avant que l'accès d'un utilisateur à la CLI du Collecteur de journaux dédié ne soit bloqué.
   2. Saisissez la **Lockout Time (Durée de verrouillage)**, en minutes, selon laquelle le Collecteur de journaux dédié verrouille le compte d'un utilisateur après que celui-ci ait atteint le nombre de **Failed Attempts (Tentatives échouées)** configuré.

© 2020 Palo Alto Networks, Inc.

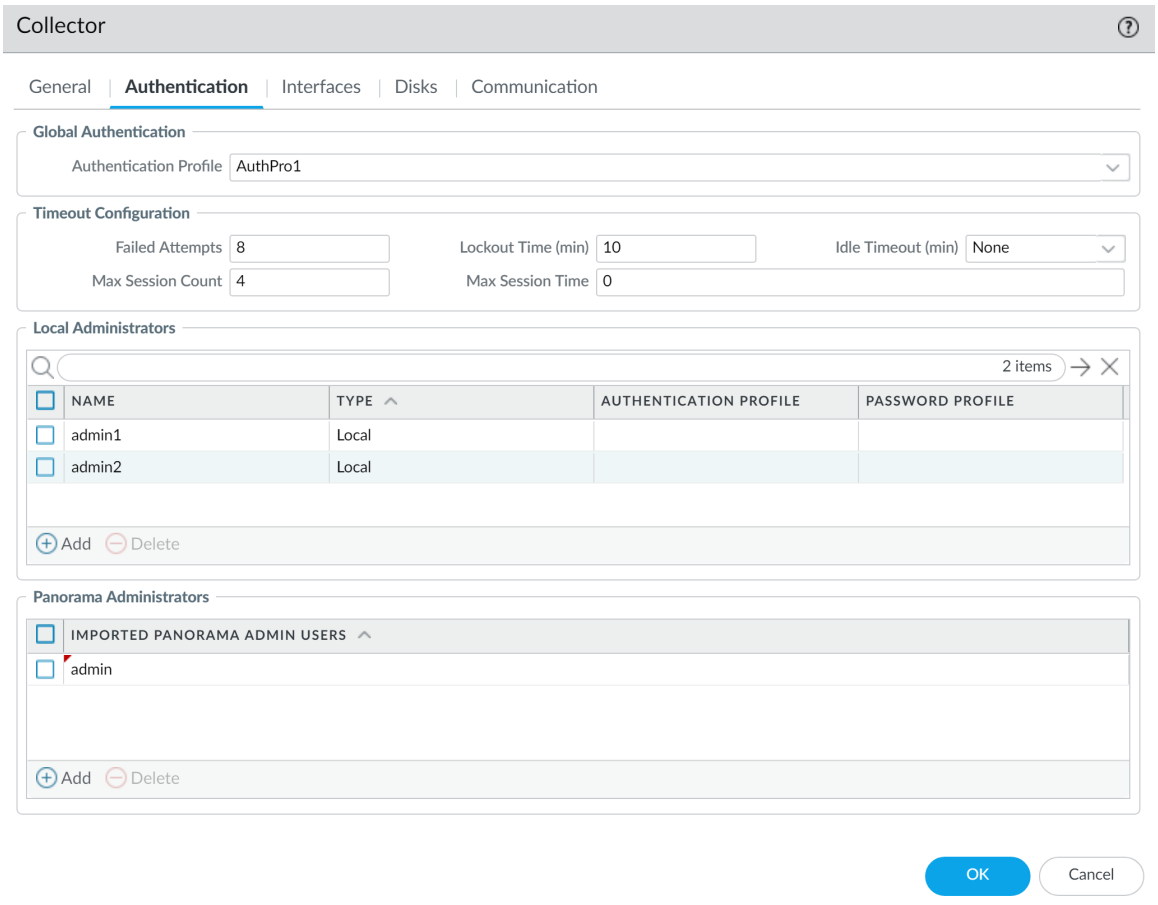
3. Saisissez le **Idle Timeout (délai d'expiration)**, en minutes, avant que le compte de l'utilisateur ne soit automatiquement déconnecté pour inactivité.
4. Saisissez le **Max Session Count (Compte de session max.)** pour indiquer combien de comptes d'utilisateur peuvent accéder simultanément au Collecteur de journaux dédié.
5. Saisissez la **Max Session Time (Durée de session max.)** pendant laquelle l'administrateur peut être connecté avant d'être automatiquement déconnecté.

4. Ajoutez les administrateurs du Collecteur de journaux dédié.

   Les administrateurs peuvent soit être ajoutés en tant qu'administrateur local ou en tant qu'administrateur Panorama importé, mais pas les deux. Ajouter le même administrateur en tant qu'administrateur local et en tant qu'administrateur Panorama importé n'est pas possible et peut entraîner une panne de validation de Panorama. Par exemple, la validation de Panorama échoue si vous ajoutez **`admin1`** en tant qu'administrateur local et administrateur Panorama.

   1. **Add (Ajoutez)** et configurez de nouveaux administrateurs uniques pour le Collecteur de journaux dédié. Ces administrateurs sont spécifiques au Collecteur de journaux dédié pour lequel ils sont créés et vous gérez ces administrateurs depuis ce tableau.
   2. **Add (Ajoutez)** n'importe quel administrateur configuré dans Panorama. Ces administrateurs sont créés dans Panorama et importés vers le Collecteur de journaux dédié.

5. Cliquez sur **OK** pour enregistrer la configuration de l'authentification du Collecteur de journaux dédié.



STEP 5 | **Commit (Validez)** et **Commit and Push (Validez et appliquez)** les modifications de votre configuration.

STEP 6 | Connectez-vous à la CLI du Collecteur de journaux dédié afin de vérifier si vous pouvez accéder au Collecteur de journaux dédié en utilisant l'utilisateur admin local.

© 2020 Palo Alto Networks, Inc.

Configurer l'authentification LDAP pour un Collecteur de journaux dédié

Vous pouvez utiliser LDAP pour authentifier les utilisateurs finaux qui accèdent à l'interface web du Collecteur de journaux dédié.

STEP 1 | Se connecter à l'interface Web Panorama.

STEP 2 | Configurer un collecteur géré.

STEP 3 | Ajoutez un profil de serveur LDAP.

Le profil définit comment le Collecteur de journaux dédié se connecte au serveur LDAP.

1. Sélectionnez **Panorama** > **Server Profiles (Profils de serveur)** > **LDAP** et **Add (Ajoutez)** un profil de serveur.
2. Saisissez un **Profile Name (Nom de profil)** pour identifier le profil de serveur.
3. **Add (Ajoutez)** les serveurs LDAP (maximum de quatre). Donnez un **Name (Nom)** à chaque serveur (pour l'identifier), ainsi qu'une adresse IP de **LDAP Server (Serveur LDAP)** ou un FQDN ainsi que le **Port (Port)** du serveur (valeur par défaut : 389).

   Si vous utilisez un objet d'adresse FQDN pour identifier le serveur et qu'ensuite vous changez l'adresse, vous devez valider le changement pour que la nouvelle adresse du serveur soit appliquée.
4. Sélectionnez le **Type (type)** de serveur.
5. Sélectionnez le **Base DN (DN de base)**.

   Pour déterminer le DN de base de votre répertoire, ouvrez les composants logiciels enfichables **Active Directory Domains and Trusts** de Microsoft Management Console et utilisez le nom du domaine de premier niveau.
6. Saisissez le **Bind DN (DN de liaison)** et le **Password (Mot de passe)** pour activer le service d'authentification permettant d'authentifier le pare-feu.

   Le compte Bind DN doit avoir l'autorisation nécessaire pour consulter le répertoire LDAP.
7. Entrez le **Bind Timeout (Délai de liaison)** et le **Délai de recherche** en secondes (la valeur par défaut est 30 pour les deux).
8. Saisissez la **Retry Interval (Intervalle de relance)** en secondes (valeur par défaut : 60).
9. (Facultatif) Si vous souhaitez que le point de terminaison utilise le protocole SSL ou TLS pour une connexion plus sécurisée au serveur d'annuaires, activez l'option **Require SSL/TLS secured connection (Exiger une connexion sécurisée SSL/TLS)** (activée par défaut). Le protocole utilisé par le point de terminaison varie selon le Port de serveur :
   - 389 (par défaut) : TLS (le Collecteur de journaux dédié utilise plus précisément l'opération StartTLS, qui met à niveau la connexion en texte brut initiale en TLS.)
   - 636 : SSL.
   - Tout autre port : le Collecteur de journaux dédié tente tout d'abord d'utiliser TLS. Si le serveur d'annuaires ne prend pas en charge TLS, le Collecteur de journaux dédié fera appel à SSL.
10. (Facultatif) Pour une sécurité supplémentaire, activez l'option **Verify Server Certificate for SSL sessions (Vérifier le certificat du serveur pour les sessions SSL)** afin que le point de terminaison vérifie le certificat que le serveur d'annuaire présente pour les connexions SSL/TLS. Pour activer la vérification, vous devez également activer l'option visant à **Require SSL/TLS secured connection (Exiger une connexion sécurisée SSL/TLS)**. Pour une vérification réussie, le certificat doit remplir l'une des conditions suivantes :

© 2020 Palo Alto Networks, Inc.

- Il se trouve dans la liste des certificats de Panorama : **Panorama** > **Certificate Management (Gestion de certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique).** Si nécessaire, importez le certificat dans Panorama.
- Le signataire du certificat figure dans la liste des autorités de certification de confiance : **Panorama** > **Certificate Management Gestion des certificats)** > **Certificates (Certificats)**.

11. Cliquez sur **OK** pour enregistrer le profil de serveur.

STEP 4 | Configurer l'authentification pour le Collecteur de journaux dédié

1. Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** et sélectionnez le collecteur de journaux dédié que vous avez préalablement ajouté.
2. Configurez la **Timeout Configuration (Configuration du délai avant expiration)** d'authentification pour le Collecteur de journaux dédié.
   1. Saisissez le nombre de **Failed Attempt (Tentatives échouées)** avant que l'accès d'un utilisateur au CLI du Collecteur de journaux dédié ne soit bloqué.
   2. Saisissez la **Lockout Time (Durée de verrouillage)**, en minutes, selon laquelle le Collecteur de journaux dédié verrouille le compte d'un utilisateur après que celui-ci ait atteint le nombre de **Failed Attempts (Tentatives échouées)** configuré.
   3. Saisissez le **Idle Timeout (délai d'expiration)**, en minutes, avant que le compte de l'utilisateur ne soit automatiquement déconnecté pour inactivité.
   4. Saisissez le **Max Session Count (Compte de session max.)** pour indiquer combien de comptes d'utilisateur peuvent accéder simultanément au Collecteur de journaux dédié.
   5. Saisissez la **Max Session Time (Durée de session max.)** pendant laquelle l'administrateur peut être connecté avant d'être automatiquement déconnecté.
3. Ajoutez les administrateurs du Collecteur de journaux dédié.

   Les administrateurs peuvent soit être ajoutés en tant qu'administrateur local ou en tant qu'administrateur Panorama importé, mais pas les deux. Ajouter le même administrateur en tant qu'administrateur local et en tant qu'administrateur Panorama importé n'est pas possible et peut entraîner une panne de validation de Panorama. Par exemple, la validation de Panorama échoue si vous ajoutez **`admin1`** en tant qu'administrateur local et administrateur Panorama.

   - Configurez les administrateurs locaux.

     Configurez de nouveaux administrateurs uniques pour le Collecteur de journaux dédié. Ces administrateurs sont spécifiques au Collecteur de journaux dédié pour lequel ils sont créés et vous gérez ces administrateurs depuis ce tableau.

     1. **Add (Ajoutez)** un ou plusieurs administrateurs locaux.
     2. Saisissez un **Name (Nom)** d'utilisateur pour l'administrateur local.
     3. Attribuez un**Authentication Profile (profile d'authentification)** que vous avez préalablement créé.

        Les profils d'authentification LDAP sont compatibles uniquement avec les administrateurs locaux individuels.
     4. Activez (cochez) **Use Public Key Authentication (SSH) (Utiliser l'authentification par clé publique (SSH)** pour importer un fichier de clé publique pour l'authentification.
     5. Sélectionnez un **Password Profile (profil de mot de passe)** pour définir les paramètres d'expiration.
   - Importez les administrateurs Panorama existants

     Importez des administrateurs existants configurés dans Panorama. Ces administrateurs sont configurés et gérés dans Panorama et importés vers le Collecteur de journaux dédié.

     1. **Add (Ajoutez)** un administrateur Panorama existant
4. Cliquez sur **OK** pour enregistrer la configuration de l'authentification du Collecteur de journaux dédié.

© 2020 Palo Alto Networks, Inc.

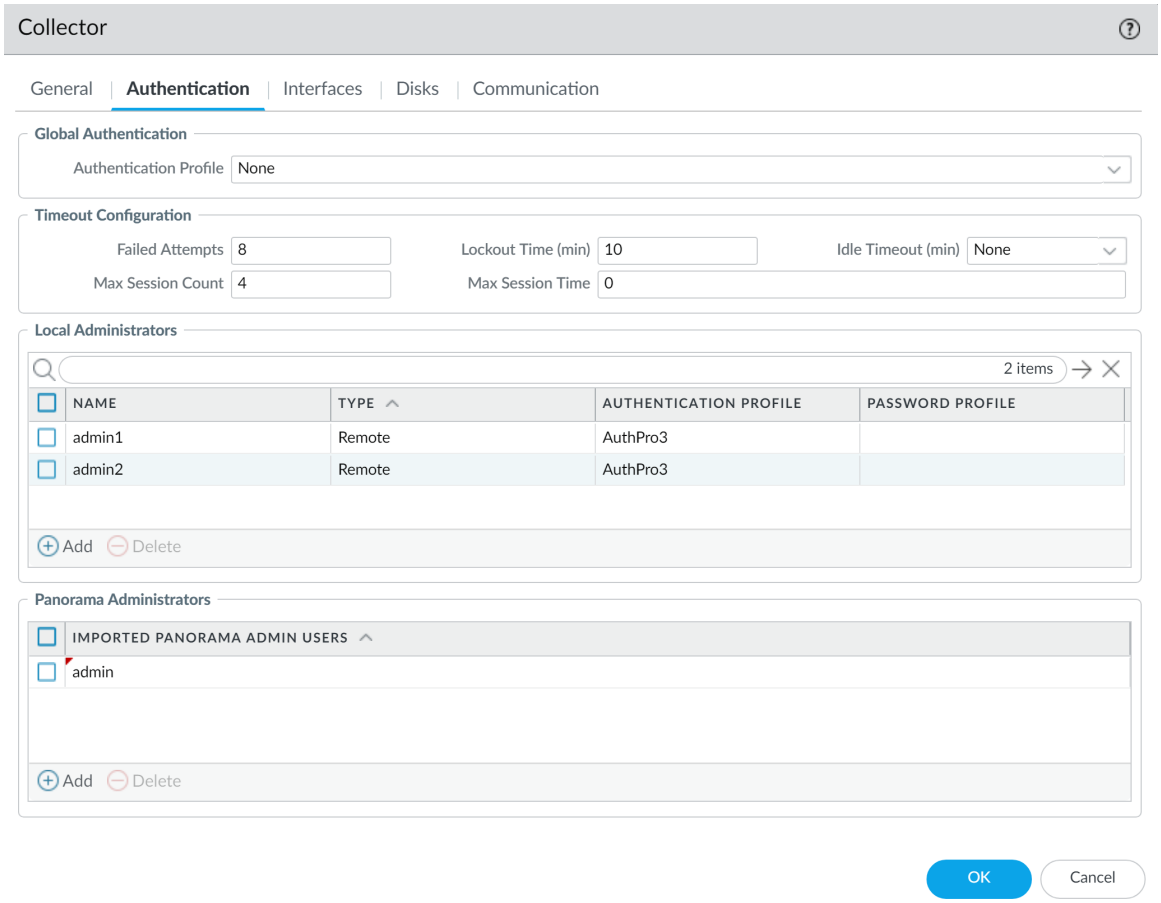
STEP 5 | Configurer l'authentification pour le Collecteur de journaux dédié

1. Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** et sélectionnez le collecteur de journaux dédié que vous avez préalablement ajouté.
2. Sélectionnez le **Authentification Profile (Profil d'authentification)** que vous avez configuré au cours des étapes antérieures.
3. Configurez la **Timeout Configuration (Configuration du délai avant expiration)** d'authentification pour le Collecteur de journaux dédié.
    1. Saisissez le nombre de **Failed Attempt (Tentatives échouées)** avant que l'accès d'un utilisateur au CLI du Collecteur de journaux dédié ne soit bloqué.
    2. Saisissez la **Lockout Time (Durée de verrouillage)**, en minutes, selon laquelle le Collecteur de journaux dédié verrouille le compte d'un utilisateur après que celui-ci ait atteint le nombre de **Failed Attempts (Tentatives échouées)** configuré.
    3. Saisissez le **Idle Timeout (délai d'expiration)**, en minutes, avant que le compte de l'utilisateur ne soit automatiquement déconnecté pour inactivité.
    4. Saisissez le **Max Session Count (Compte de session max.)** pour indiquer combien de comptes d'utilisateur peuvent accéder simultanément au Collecteur de journaux dédié.
    5. Saisissez la **Max Session Time (Durée de session max.)** pendant laquelle l'administrateur peut être connecté avant d'être automatiquement déconnecté.
4. Ajoutez les administrateurs du Collecteur de journaux dédié.

    Vous devez ajouter l'administrateur (**`admin`**) en tant qu'administrateur local ou en tant qu'administrateur Panorama importé, mais pas les deux. La validation des collecteurs gérés échoue si un administrateur n'est pas ajouté ou si l'administrateur est ajouté à la fois en tant qu'administrateur local et administrateur importé de Panorama.

    1. **Add (Ajoutez)** et configurez de nouveaux administrateurs uniques pour le Collecteur de journaux dédié. Ces administrateurs sont spécifiques au Collecteur de journaux dédié pour lequel ils sont créés et vous gérez ces administrateurs depuis ce tableau.
    2. **Add (Ajoutez)** n'importe quel administrateur configuré dans Panorama. Ces administrateurs sont créés dans Panorama et importés vers le Collecteur de journaux dédié.
5. Cliquez sur **OK** pour enregistrer la configuration de l'authentification du Collecteur de journaux dédié.

© 2020 Palo Alto Networks, Inc.



STEP 6 | **Commit (Validez)** et **Commit and Push (Validez et appliquez)** les modifications de votre configuration.

STEP 7 | Accédez au Collecteur de journaux dédié afin de vérifier si vous pouvez accéder au Collecteur de journaux dédié en utilisant l'utilisateur admin local.

© 2020 Palo Alto Networks, Inc.

Gérer les groupes de collecteurs

Un groupe de collecteurs contient entre 1 et 16 collecteurs de journaux qui fonctionnent comme une unité logique unique pour la collecte des journaux de pare-feu. Vous devez affecter au moins un collecteur de journaux à un groupe de collecteurs pour que les pare-feu envoient correctement des journaux à un collecteur de journaux. Les journaux de pare-feu sont supprimés si aucun groupe de collecteurs n'est configuré ou si aucun des collecteurs de journaux n'est affecté à un groupe de collecteurs. Vous pouvez configurer un groupe de collecteurs avec plusieurs collecteurs gérés pour assurer la redondance de journal ou pour tenir compte des taux de journalisation qui dépassent la capacité d'un seul collecteur géré (voir Modèles Panorama). Pour comprendre les exigences, les risques et les mesures d'atténuation recommandées, consultez les avertissements pour un groupe collecteur avec plusieurs collecteurs de journaux.

Les appareils M-600, M-500 et M-200 en mode Panorama ont un groupe de collecteurs prédéfini qui contient un collecteur de journaux local prédéfini. Vous pouvez modifier tous les paramètres du groupe de collecteurs prédéfini, sauf son nom (par défaut).

Si vous supprimez un groupe de collecteurs, vous perdrez les journaux.

Palo Alto Networks recommande de conserver le collecteur de journaux prédéfini et un groupe de collecteurs sur le serveur de gestion Panorama, indépendamment de savoir si Panorama gère également des collecteurs de journaux dédiés.

Si vous passez un appareil de série M du mode Panorama au mode collecteur de journaux, l'appareil perdra son groupe de collecteurs et son collecteur de journaux prédéfinis. Vous devrez alors configurer l'appareil de série M en tant que collecteur de journaux, ajoutez-le en tant que collecteur géré à Panorama et configurez un groupe de collecteurs pour qu'il contienne le collecteur géré.

- Configuration d'un groupe de collecteurs
- Configurer l'authentification avec des certificats personnalisés entre les collecteurs de journaux
- Déplacer un collecteur de journaux vers un autre groupe de collecteurs
- Supprimer un pare-feu d'un groupe de collecteurs

Configuration d'un groupe de collecteurs

Avant de configurer les groupes de collecteurs, décidez si chacun aura un seul collecteur de journaux ou plusieurs collecteurs de journaux (jusqu'à 16). Un groupe de collecteurs avec plusieurs collecteurs de journaux prend en charge des taux de journalisation et une redondance de journalisation supérieurs, mais présente les exigences suivantes :

- Dans un même groupe de collecteurs, tous les collecteurs de journaux doivent être exécutés sur le même modèle Panorama : uniquement des appareils M-600, uniquement des appareils M-500, uniquement des appareils M-200 ou uniquement des appareils virtuels Panorama.
- La redondance du journal n'est disponible que si chaque collecteur de journaux du groupe de collecteurs a le même nombre de disques de journalisation. Pour ajouter des disques à un collecteur de journaux, consultez la section Augmenter le stockage sur l'appareil de série M.
- (Pratique exemplaire) Tous les collecteurs de journaux du même groupe de collecteurs doivent se situer dans le même Local Area Network (Réseau local ; LAN). Évitez d'ajouter des collecteurs de journaux dans les mêmes réseaux ou dans des Wide Area Networks (Réseaux longue distance ; WAN) au même groupe de collecteurs comme les perturbations de réseau sont beaucoup plus courantes et peuvent entraîner la perte des données des journaux. De plus, il est recommandé que les collecteurs de journaux du même

© 2020 Palo Alto Networks, Inc.

groupe de collecteurs soient physiquement rapprochés les uns des autres pour permettre à Panorama d'interroger rapidement les collecteurs de journaux, lorsque cela s'avère nécessaire.

STEP 1 | Effectuez les tâches suivantes avant de configurer le groupe de collecteurs.

1. Ajoutez un pare-feu comme périphérique géré pour chaque pare-feu que vous affectez au groupe de collecteurs.
2. Configurez un collecteur géré pour chaque collecteur de journaux que vous allez attribuer au groupe de collecteurs.

STEP 2 | Ajoutez le groupe de collecteurs.

1. Accédez à l'interface Web de Panorama, sélectionnez **Panorama** > **Collector Groups (Groupes de collecteurs)** et **Add (Ajoutez)** un groupe de collecteur ou modifiez un collecteur existant.
2. Entrez un **Name (Nom)** pour le groupe de collecteurs si vous en ajoutez un.

   Vous ne pouvez pas renommer un groupe de collecteurs existant.
3. Entrez la **Minimum Retention Period (Période de conservation minimale)** en jours (1 à 2 000) pendant laquelle le groupe de collecteurs sera conservé pour les journaux de pare-feu.

   Par défaut, le champ est vide, ce qui signifie que le groupe de collecteurs conserve indéfiniment les journaux.
4. **Add (Ajoutez)** les collecteurs de journaux (1 à 16) à la liste des membres du groupe de collecteurs.
5. (Recommandé) **Enable log redundancy across collectors (Activez la redondance des journaux entre les collecteurs)** si vous ajoutez plusieurs collecteurs de journaux à un seul groupe de collecteurs.

   La redondance garantit qu'aucun journal n'est perdu si un collecteur de journaux devient indisponible. Chaque journal aura deux copies et chaque copie va résider sur un collecteur de journaux différent. Par exemple, si vous avez deux collecteurs de journaux dans le groupe de collecteurs, le journal est écrit aux deux collecteurs de journaux.

   Permettre la redondance crée plus de journaux et nécessite donc plus de capacité de stockage, ce qui réduit de moitié la capacité de stockage. Lorsque l'espace vient à manquer sur un groupe de collecteurs, il supprime les journaux les plus antérieurs. L'activation de la redondance multiplie par deux le trafic de traitement des journaux dans un groupe de collecteurs, réduisant ainsi de moitié son débit de journalisation maximum car chaque collecteur de journaux doit distribuer une copie de chaque journal qu'il reçoit.

STEP 3 | Assignez le collecteur de journaux et les pare-feu au groupe de collecteurs.

1. Sélectionnez **Device Log Forwarding (Transfert de journaux du périphérique)** et **Add (Ajouter)** des *listes de préférences de transfert de journaux* pour les pare-feu.

   Les données du journal sont transférées sur un canal TCP séparé. En ajoutant une préférence de transfert des journaux, la liste vous permet de créer des connexions TCP séparées pour le transfert des données de journal.

   Une liste de préférences détermine l'ordre dans lequel les collecteurs de journaux reçoivent les journaux d'un pare-feu. Si aucune liste de préférences de transfert des journaux n'est attribuée, vous pouvez être confronté à l'un des scénarios suivants :

   - *Si Panorama est en mode Gestion uniquement, Panorama supprime tous les journaux entrants.*
   - *Si le collecteur de journaux local n'est pas configuré comme un collecteur géré lorsque Panorama est en mode Panorama, Panorama supprime tous les journaux entrants.*
   - *Si le collecteur de journaux local est configuré comme un collecteur géré lorsque Panorama est en mode Panorama, les journaux entrants sont reçus mais le Panorama peut agir comme un goulot d'étranglement car tous les pare-feux gérés*

© 2020 Palo Alto Networks, Inc.

transmettent d'abord les journaux au collecteur de journaux local avant de les redistribuer aux autres collecteurs de journaux disponibles.

1. Dans la section Devices (Périphériques), cliquez sur **Modify (Modifier)**, sélectionnez les pare-feu et cliquez sur **OK**.
2. Dans la section Collectors (Collecteurs), **Add (Ajoutez)** les collecteurs de journaux à la liste de préférences.

   Si vous avez activé la redondance à l'étape 2, il est recommandé d'ajouter au moins deux collecteurs de journaux. Si vous affectez plusieurs collecteurs de journaux, le premier sera le principal ; ce n'est que si le principal devient inaccessible que les pare-feu envoient les journaux au collecteur de journaux suivant dans la liste. Pour modifier la priorité d'un collecteur de journaux, sélectionnez-le et cliquez sur **Move Up (Déplacer en haut)** (priorité plus élevée) ou **Move Down (Déplacer en bas)** (priorité inférieure).
3. Cliquez sur **OK**.

STEP 4 | Définir la capacité de stockage (Journal des quotas) et la période d'expiration pour chaque type de journal.

1. Retournez à l'onglet **General (Général)** et cliquez sur la valeur **Log Storage (Stockage des journaux)** .

   Si le champ affiche 0 MB, vérifiez que vous avez activé les paires de disques pour la journalisation et validé les changements (voir l'onglet Configurer un collecteur géré, Disks (Disques)).
2. Entrez le **Quota(%)** de stockage de journaux pour chaque type de journal.
3. Entrez les **Max Days (Jours maximum)** pour chaque type de journal (1 à 2 000).

   Par défaut, les champs sont vides, ce qui signifie que les journaux n'expirent jamais.

STEP 5 | Validez et vérifiez vos modifications.

1. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)**, puis **Commit and Push (Valider et appliquer)** vos modifications à Panorama et au groupe de collecteurs que vous avez configuré.
2. Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** pour vérifier que les collecteurs de journaux dans le groupe de collecteurs sont :

   - **Connecté à Panorama** : la colonne Connected (Connecté) affiche une icône de coche pour indiquer qu'un collecteur de journaux est connecté à Panorama.
   - **Synchronisé avec Panorama** : la colonne Configuration Status (État de configuration) indique si un collecteur de journaux est `In Sync` (icône verte) ou `Out of Sync` (icône rouge) avec Panorama.

STEP 6 | Résoudre les problèmes de connectivité aux ressources réseaux pour vérifier que vos pare-feu se connectent avec succès au collecteur de journaux.

STEP 7 | Étapes suivantes...

1. Configurer le transfert des journaux vers Panorama.

   Le groupe de collecteurs ne recevra pas les journaux de pare-feu tant que vous n'aurez pas configuré les pare-feu pour le transfert vers Panorama.
2. (Facultatif) Configurer le transfert de journal de Panorama vers des destinations externes.

   Vous pouvez configurer chaque groupe de collecteurs pour qu'il transfère les journaux vers des destinations distinctes (par exemple un serveur Syslog).

© 2020 Palo Alto Networks, Inc.

Configurer l'authentification avec des certificats personnalisés entre les collecteurs de journaux

Suivez la procédure suivante pour configurer des certificats personnalisés aux fins de la communication entre les collecteurs de journaux. Vous devez configurer la communication sécurisée avec le serveur et la communication client sécurisée sur chaque collecteur de journaux d'un groupe de collecteurs, car les rôles serveur et client sont choisis dynamiquement. Utilisez des certificats personnalisés pour créer une chaîne de confiance unique qui procure une authentification mutuelle entre les membres de votre groupe de collecteurs de journaux.

Pour plus d'informations sur l'utilisation de certificats personnalisés, voir Comment les connexions SSL / TLS sont-elles mutuellement authentifiées?

STEP 1 | Obtenez des paires de clés et des certificats d'autorité de certification (CA) pour chaque journal.

STEP 2 | Importez le certificat de l'autorité de certification pour valider l'identité du collecteur de journaux client, la paire de clés du serveur et la paire de clés client pour chaque collecteur de journaux du groupe de collecteurs.

1. Sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Import (Importer)**.
2. Importez le certificat de l'autorité de certification, la paire de clés du serveur et la paire de clés du client.
3. Répétez les étapes pour chaque collecteur de journaux.

STEP 3 | Configurez un profil de certificat qui inclut l'autorité de certification racine et l'autorité de certification intermédiaire pour la communication sécurisée avec le serveur. Ce profil de certificat définit l'authentification entre les collecteurs de journaux.

1. Sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificats)**.
2. Configurez un profil de certificat.

   Si vous configurez un CA intermédiaire dans le cadre du profil de certificat, vous devez également inclure la certification CA racine.

STEP 4 | Configurez le profil du certificat du périphérique client. Vous pouvez configurer ce profil sur chaque collecteur de journaux client individuellement ou vous pouvez transférer la configuration de Panorama™ vers des collecteurs de journaux gérés.

Si vous utilisez SCEP pour le certificat de client, configurez un profil SCEP *au lieu d'un certificat de profil.*

1. Sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificats)**.
2. Configuration d'un profil de certificat.

STEP 5 | Configurez un profil de service SSL/TLS.

1. Sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **SSL/TLS Service Profile (Profil de service SSL/TLS)**.
2. Configurez un profil SSL/TLS pour définir le certificat et le protocole que les collecteurs de journaux utilisent pour les services SSL / TLS.

© 2020 Palo Alto Networks, Inc.

STEP 6 | Après avoir déployé des certificats personnalisés sur tous les collecteurs de journaux, appliquez l'authentification par certificat personnalisé.

1. Sélectionner **Panorama (Panorama)** > **Collector Groups (Groupes de Collecteurs)** et sélectionnez le groupe de collecteurs.
2. À l'onglet Général, **Enable secure inter LC Communication (Activez la communication inter LC sécurisée)**.

   Si vous activez la communication inter-LC sécurisée et que votre groupe de collecteurs inclut un collecteur de journaux local, un lien doit apparaître indiquant que **Log Collector on local Panorama is using the secure client configuration from Panoramale** > **Secure Communication Settings (Le collecteur de journaux sur l'appareil Panorama local utilise la configuration client sécurisée à partir des paramètres de communication sécurisée de Panorama**). Vous pouvez cliquer sur ce lien pour ouvrir la boîte de dialogue Paramètres de communication sécurisée et configurer le serveur sécurisé et les paramètres du client sécurisés pour le collecteur de journaux local à partir de là.
3. Cliquez sur **OK**.
4. **Commit (Validez)** vos modifications.

STEP 7 | Configurez la Secure Server Communication (Communication sécurisée avec le serveur) sur chaque collecteur de journaux.

1. Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** pour les collecteurs de journaux dédiés ou **Panorama** > **Setup (Paramètres)** > **Management (Gestion)** et **Edit (Modifiez)** les paramètres de communication sécurisée pour un collecteur de journaux local.
2. Pour les collecteurs de journaux dédiés, cliquez sur le collecteur de journaux et sélectionnez **Communications**.
3. Activer la fonction **Customize Secure Server Communication (Personnaliser la communication sécurisée avec le serveur)**.
4. Sélectionnez le profil de service SSL/TLS depuis le menu déroulant **SSL/TLS Service Profile (Profil de service SSL/TLS)**. Ce profil de service SSL / TLS s'applique à toutes les connexions SSL entre les collecteurs de journaux.
5. Sélectionnez le **Certificate Profile (Profil de certificat)** dans le menu déroulant.
6. Vérifiez que la case **Custom Certificate Only (Certificat personnalisé uniquement)** n'est pas cochée. Cela permet à la communication entre collecteur de journaux de continuer à utiliser le certificat prédéfini tout en configurant des certificats personnalisés.
7. Définissez le délai d'attente de déconnexion : le nombre de minutes que les collecteurs de journaux attendent avant de mettre fin à la connexion et de la rétablir avec d'autres collecteurs de journaux. Ce champ est vide par défaut (plage comprise entre 0 et 44 640).
8. (Facultatif) Configurez une liste d'autorisation. La liste d'autorisation ajoute une couche de sécurité supplémentaire au-delà de l'authentification par certificat. La liste d'autorisation vérifie l'objet ou l'autre nom de l'objet du certificat client. Si l'objet ou l'autre nom de l'objet présenté avec le certificat client ne correspond pas à un identificateur de la liste d'autorisation, l'authentification est refusée.
   1. **Add (Ajoutez)** une liste d'autorisation.
   2. Sélectionnez le **Subject (Objet)** ou **Subject Alt Name (Autre nom de l'objet)** configuré dans le profil de certificat en tant que type d'identifiant.
   3. Entrez le nom commun si l'identifiant est `Subject` et l'adresse IP, le nom d'hôte ou l'e-mail si l'identificateur est `Subject Alt Name`.
   4. Cliquez sur **OK**.
   5. Activez l'option **Check Authorization List (Vérifier la liste d'autorisation)** pour configurer Panorama pour qu'il mette en œuvre la liste d'autorisation.
9. Cliquez sur **OK**.
10. **Commit (Validez)** vos modifications.

© 2020 Palo Alto Networks, Inc.

Après validation de ces modifications, le compte à rebours du temps d'attente de déconnexion commence. Lorsque le délai d'attente se termine, les collecteurs de journaux du groupe de collecteurs ne peuvent pas se connecter sans les certificats configurés.

STEP 8 | Configurez la communication client sécurisée sur chaque collecteur de journaux.

1. Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** pour les collecteurs de journaux dédiés ou **Panorama** > **Setup (Paramètres)** > **Management (Gestion)** et **Edit (Modifiez)** les paramètres de communication sécurisée pour un collecteur de journaux local.
2. Pour les collecteurs de journaux dédiés, cliquez sur le collecteur de journaux et sélectionnez **Communications**.
3. Sous Communications clients sécurisées, sélectionnez le **Certificate Type (type de certificat)**, le **Certificate (Certificat)**, et le **Certificate Profile (profil du certificat)** dans leurs menus déroulants respectifs.
4. Cliquez sur **OK**.
5. **Commit (Validez)** vos modifications.

Déplacer un collecteur de journaux vers un autre groupe de collecteurs

Les appareils M-600, M-500, M-200 et appareils virtuels Panorama peuvent disposer d'un ou plusieurs collecteurs de journaux dans chaque groupe de collecteurs. Vous attribuez des collecteurs de journaux à un groupe de collecteurs en fonction du taux de journalisation et des exigences de stockage de journaux de ce groupe de collecteurs. Si les taux et le stockage requis augmentent dans un groupe collecteur, il est recommandé d'augmenter le stockage sur l'appareil de Série M (voir la capacité de stockage du journal de la Série M) ou la configuration d'un groupe de collecteurs avec des collecteurs de journaux additionnels. Toutefois, dans certains déploiements, il peut être plus économique de déplacer des collecteur de journaux entre groupes de collecteurs.

Lorsqu'un collecteur de journaux est local pour un M-600, M-500 ou M-200 en mode Panorama, déplacez-le uniquement si l'appareil est l'homologue passif dans une configuration haute disponibilité (HA). La synchronisation HA applique les configurations associées au nouveau groupe de collecteurs. Ne déplacez jamais un collecteur de journaux qui est local à l'homologue actif HD.

Dans un même groupe de collecteurs, tous les collecteurs de journaux doivent être exécutés sur le même modèle Panorama : uniquement des appareils M-600, uniquement des appareils M-500, uniquement des appareils M-200 ou uniquement des appareils virtuels Panorama.

La redondance du journal n'est disponible que si chaque collecteur de journaux du groupe de collecteurs a le même nombre de disques de journalisation. Pour ajouter des disques à un collecteur de journaux, consultez la section Augmenter le stockage sur l'appareil de série M.

STEP 1 | Retirer le collecteur de journal de la gestion Panorama.

1. Sélectionnez **Panorama** > **Collector Groups (Groupes de collecteurs)** et modifiez le groupe de collecteurs contenant le collecteur de journaux que vous déplacerez.
2. Dans la section des membres du groupe de collecteurs, sélectionnez et **Delete (Supprimez)** le collecteur de journaux.

© 2020 Palo Alto Networks, Inc.

3. Sélectionnez **Device Log Forwarding (Transfert de journaux du périphérique)** et, dans la liste des préférences de transfert de journal, effectuez les opérations suivantes pour chaque ensemble de pare-feu assigné au collecteur de journaux que vous allez déplacer :
   1. Dans la colonne de périphériques, cliquez sur le lien pour les pare-feu assignés au collecteur de journaux.
   2. Dans la colonne des collecteurs, sélectionnez et **Delete (Supprimez)** le collecteur de journaux.

      Pour réaffecter les pare-feu, Add (Ajoutez) le nouveau collecteur de journaux auquel ils transmettront les journaux.
   3. Cliquez deux fois sur **OK** pour enregistrer vos modifications.
4. Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)**, puis sélectionnez et **Delete (Supprimez)** le collecteur de journaux que vous allez déplacer.

STEP 2 | Configurer un groupe de collecteurs.

Ajoutez le collecteur de journaux à son nouveau groupe de collecteur et assignez des pare-feu au collecteur de journaux.

Lorsque vous appliquez les modifications à la configuration du groupe de collecteurs, Panorama commence la redistribution des journaux dans le collecteur de journaux. Ce processus peut prendre des heures pour chaque téraoctets de journaux. Pendant le processus de redistribution, le débit de journalisation maximum est réduit. Dans la page Panorama > Collector Groups (Groupes de collecteurs), la colonne Log Redistribution State (État de la redistribution des journaux) indique l'état de la progression du processus en tant que pourcentage.

STEP 3 | Configurer le transfert des journaux vers Panorama pour le nouveau groupe de collecteurs que vous avez configuré.

STEP 4 | Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** pour valider vos modifications dans Panorama et appliquer les modifications aux groupes de périphériques, aux modèles et aux groupes de collecteurs, si vous ne l'avez pas déjà fait.

Supprimer un pare-feu d'un groupe de collecteurs

Si vous utilisez un appareil virtuel Panorama en mode hérité pour gérer les collecteurs de journaux dédiés, vous avez la possibilité de transférer les journaux du pare-feu vers Panorama au lieu de les transférer vers les collecteurs de journaux. Dans ce cas, vous devez supprimer le pare-feu du groupe de collecteurs ; le pare-feu transmettra automatiquement ses journaux à Panorama.

Pour supprimer temporairement la liste des préférences de transfert de journaux sur le pare-feu, vous pouvez le supprimer à l'aide de l'interface ILC sur le pare-feu. Toutefois, vous devez supprimer les pare-feux assignés dans la configuration du collecteur groupe sur Panorama. Sinon, la prochaine fois que vous appliquerez les modifications apportées au groupe de collecteurs, le périphérique sera reconfiguré pour envoyer des journaux au collecteur de journaux affecté.

STEP 1 | Sélectionnez **Panorama** > **Collector Groups (Groupes de collecteurs)** et modifiez le groupe de collecteurs.

© 2020 Palo Alto Networks, Inc.

STEP 2 | Sélectionnez **Device Log Forwarding (Transfert de journaux du périphérique)**, cliquez sur le pare-feu dans la liste des périphériques, **Modify (Modifiez)** la liste des périphériques, décochez la case du pare-feu et cliquez trois fois sur **OK**.

STEP 3 | Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)**, puis **Commit and Push (Valider et appliquer)** vos modifications apportées à Panorama et au groupe de collecteurs depuis lequel vous avez supprimé le pare-feu.

© 2020 Palo Alto Networks, Inc.

Configurer le transfert des journaux vers Panorama

Chaque pare-feu stocke ses fichiers journaux localement par défaut et ne peut pas afficher les journaux qui résident sur d'autres pare-feu. Par conséquent, pour obtenir une visibilité globale de l'activité réseau surveillée par tous vos pare-feu, vous devez transférer tous les journaux du pare-feu vers Panorama et utiliser Panorama pour la visibilité. Dans les situations où certaines équipes de votre entreprise peuvent être plus efficaces en surveillant uniquement les journaux qui concernent leurs activités, vous pouvez créer des filtres de transfert en fonction d'un attribut de journal (comme le type de menace ou l'utilisateur source). Par exemple, un analyste des activités liées à la sécurité qui examine les attaques menées par des logiciels malveillants pourrait être uniquement intéressé aux journaux des menaces dont l'attribut Type serait défini sur wildfire-virus.

Les étapes suivantes décrivent comment utiliser des modèles Panorama et des groupes de périphériques pour configurer plusieurs pare-feu pour transférer des journaux.

Si Panorama gère les pare-feu exécutant des versions antérieures à PAN-OS 7.0, spécifiez un serveur WildFire® à partir duquel Panorama peut collecter des informations d'analyse pour les échantillons WildFire soumis par ces pare-feu. Panorama utilise les informations pour remplir les journaux WildFire qui manquent de valeurs de champ introduites dans PAN-OS 7.0. Les pare-feu exécutant les versions antérieures ne remplissent pas ces champs. Pour spécifier le serveur, sélectionnez Panorama > Setup (Configuration) > WildFire, modifiez les paramètres généraux, puis entrez le nom du WildFire Private Cloud (Cloud Privé WildFire). La valeur par défaut est wildfire-public-cloud (cloud public WildFire), où le cloud WildFire est hébergé aux États-Unis.

Vous pouvez également transférer les journaux du pare-feu vers des services externes (tels qu'un serveur Syslog). Pour plus de détails, consultez la section Options de transfert des journaux.

STEP 1 | Ajoutez un groupe de périphériques pour les pare-feu qui transmettront les journaux.

Panorama requiert un groupe de périphériques pour transmettre un profil de journal vers les pare-feu. Créez un nouveau groupe de périphériques ou assignez les pare-feu à un groupe de périphériques existant.

STEP 2 | Ajoutez un Modèle pour les pare-feu qui transmettront les journaux.

Panorama requiert un modèle pour transmettre les paramètres du journal aux pare-feu. Créez un nouveau groupe de périphériques ou assignez les pare-feu à un groupe de périphériques existant.

STEP 3 | Création d'un profil de transfert des journaux.

Le profil définit les destinations des journaux du trafic, des menaces, des envois WildFire, de filtrage des URL, de filtrage des données, de tunnel et d'authentification.

1. Sélectionnez **Objects (Objets)** > **Log Forwarding (Journal de Transfert)**, sélectionnez le **Device Group (groupe de périphériques)** de pare-feu qui transmet les journaux et **Add (ajoutez)** un profil.
2. Entrez un **Name (Nom)** pour identifier le profil de transfert des journaux.
3. **Add (Ajoutez)** au moins un *profil de la liste de correspondance*.

   Les profils indiquent les filtres de requête de journal, les destinations de transfert et les actions automatiques, comme l'étiquetage. Pour chaque profil de la liste de correspondance :

© 2020 Palo Alto Networks, Inc.

1. Saisissez un **Name (Nom)** pour identifier le profil.
2. Sélectionnez le **Log Type (Type de journal)**.
3. Dans la liste déroulante **Filter (Filtre)**, sélectionnez **Filter Builder (Générateur de filtre)**. Indiquez les éléments suivants, puis **Add (Ajoutez)** chaque requête :

   Connector (Connecteur) logique (et/ou)

   Attribute (Attribut) du journal

   L'**Operator (Opérateur)** pour définir la logique d'inclusion ou d'exclusion

   La **Value (Valeur)** d'attribut à laquelle doit correspondre la requête
4. Sélectionnez **Panorama**.

4. Cliquez sur **OK** pour enregistrer le profil de transfert des journaux.

STEP 4 | Affectation du profil de transfert des journaux aux règles de politique et aux zones réseau.

Les règles de sécurité, d'authentification et de protection DoS prennent en charge le transfert des journaux. Dans cet exemple, vous associez le profil à une règle de sécurité.

Effectuez les étapes suivantes pour chaque règle qui déclenchera le transfert des journaux :

1. Sélectionnez la base de règles (par exemple, **Policies (Polices)** > **Security (Sécurité)** > **Pre Rules (Pré-règles)**), sélectionnez le **Device Group (Groupe de périphériques)** des pare-feu qui vont transmettre les journaux et modifiez la règle.
2. Sélectionnez **Actions** et sélectionnez le profil de **Log Forward (Transfert de journaux)** que vous avez créé.
3. Définissez le **Profile Type (Type de profil)** sur **Profiles (Profils)** ou sur **Group (Groupe)**, puis sélectionnez les profils de sécurité ou le **Group Profile (Profil de groupe)** requis pour déclencher la génération et le transfert des journaux suivants :
   - Journaux des menaces : le trafic doit correspondre à un profil de sécurité associé à une règle de sécurité.
   - Journaux WildFire : le trafic doit correspondre à un profil d'analyse WildFire associé à une règle.
4. Pour les journaux de trafic, sélectionnez **Log At Session Start (Connexion en début de session)** et/ou **Log At Session End (Connexion en fin de session)**.
5. Cliquez sur **OK** pour enregistrer la règle.

STEP 5 | Configurez les destinations pour les journaux système, les journaux de configuration, les journaux User-ID™ et les journaux de correspondance HIP.

Panorama génère des journaux de corrélation en fonction des journaux du pare-feu qu'il reçoit, plutôt que d'agréger les journaux de corrélation des pare-feu.

1. Sélectionnez **Device (Périphérique)** > **Log Settings (Paramètres du journal)** et sélectionnez le **Template (modèle)** des pare-feu qui transmettra les journaux.
2. Reportez-vous à l'étape Ajout d'un ou de plusieurs profils de la liste de correspondance pour chaque type de fichier que le pare-feu transférera.

STEP 6 | (Pare-feu PA-7000 Series uniquement) Configurez une interface de carte de journal pour le transfert des journaux.

Lorsque vous configurez un port de données sur l'une des cartes de traitement réseau (NPC) PA-7000 en tant qu'interface de la carte de journal, le pare-feu commence automatiquement à utiliser cette interface pour transférer les journaux vers les destinations de journalisation que vous configurez et transfère les fichiers pour l'analyse WildFire. Assurez-vous que l'interface que vous configurez peut atteindre les destinations de transfert de journaux et le cloud WildFire, l'appareil WildFire ou les deux.

© 2020 Palo Alto Networks, Inc.

Comme le pare-feu de la série PA-7000 peut désormais transférer les journaux vers Panorama, Panorama ne traite plus les pare-feu de la série PA-7000 qu'il gère en tant que collecteurs de journaux. Si vous n'avez pas configuré les pare-feu de la série PA-7000 pour transférer les journaux vers Panorama, tous les journaux générés par un pare-feu PA-7000 géré ne sont visibles que depuis le pare-feu local, et pas depuis Panorama. Si vous ne disposez pas encore d'une infrastructure de transfert de journaux capable de gérer le débit et le volume de journalisation des pare-feu PA-7000, vous pouvez, à partir de PAN-OS 8.0.8, permettre à Panorama d'interroger directement les pare-feu PA-7000 lors de la surveillance de journaux. Pour utiliser cette fonctionnalité, Panorama et les pare-feu de la série PA-7000 doivent utiliser PAN-OS 8.0.8 ou version ultérieure. Activez Panorama pour interroger directement les pare-feu de la série PA-7000 en entrant la commande suivante dans la CLI de Panorama :

```
> debug reportd send-request-to-7k yes
```

Après avoir exécuté cette commande, vous pourrez afficher les journaux des pare-feu de la série PA-7000 gérés sur l'onglet Monitor (Surveillance) de Panorama. En outre, comme pour tous les périphériques gérés, vous pouvez également générer des rapports incluant des données des journaux de la série PA-7000 en sélectionnant Remote Device Data (Données de périphérique distant) comme Data Source (Source de données). Si vous décidez par la suite d'activer les pare-feux de la série PA-7000 pour transférer les journaux vers Panorama, vous devez d'abord désactiver cette option en utilisant la commande ***debug-reportd send-request-to-7k no****.*

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**, sélectionnez le **Template (Modèle)** des pare-feu qui transmettront les journaux, et **Add Interface (Ajouter une interface)**.
2. Sélectionnez le **Slot (Logement)** et le **Interface Name (Nom de l'interface)**.
3. Définissez le **Interface Type (Type d'interface)** sur **Log Card (Carte de journal)**.
4. Saisissez l'**IP Address (Adresse IP)**, la **Default Gateway (Passerelle par défaut)** et, (pour IPv4 uniquement) le **Netmask (Masque réseau)**.
5. Sélectionnez **Advanced (Avancé)** et spécifiez la **Link Speed (Vitesse de liaison)**, le **Link Duplex (Duplex de la liaison)** et le **Link State (État de la liaison)**.

   La valeur par défaut de ces champs est auto, qui indique que le pare-feu détermine automatiquement les valeurs selon la connexion. Toutefois, la Link Speed (Vitesse de liaison) minimale recommandée pour toutes les connexions est 1000 (1 000) (Mbits/s).
6. Cliquez sur **OK** pour enregistrer vos modifications.

STEP 7 | Configurez Panorama pour recevoir les journaux.

Si vous souhaitez transférer les journaux vers un appareil virtuel Panorama en mode hérité, vous pouvez ignorer cette étape.

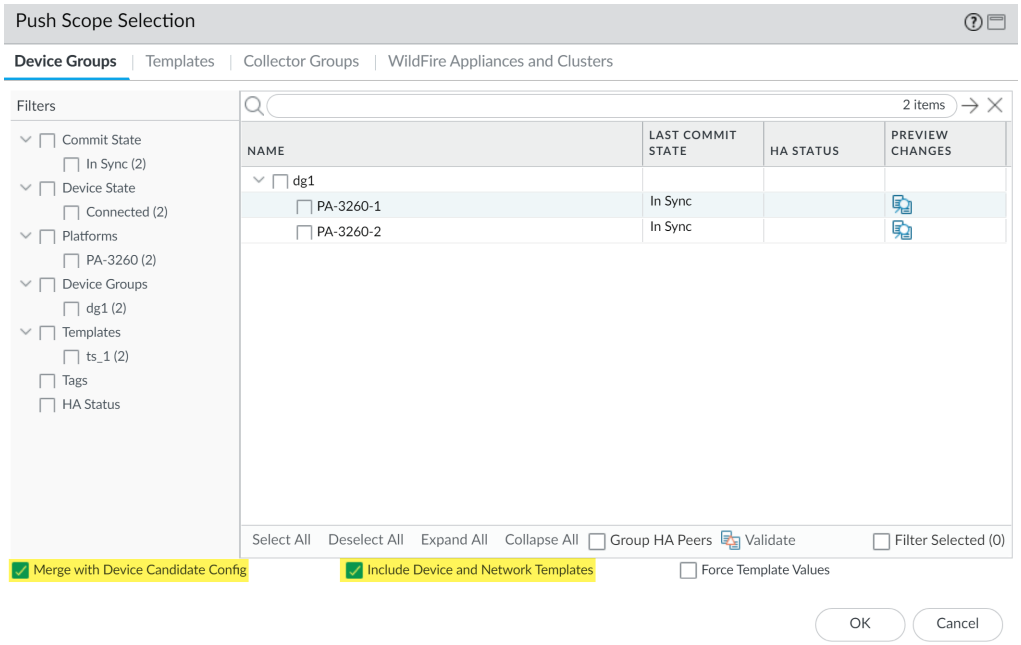
1. Pour chaque collecteur de journaux qui recevra des journaux, configurez un collecteur géré.
2. Configurez un groupe de collecteurs pour affecter des pare-feu à des collecteurs de journaux spécifiques pour le transfert de journaux.

STEP 8 | Validez vos modifications de configuration.

1. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** et **Edit Selections (Modifier les sélections)**.

© 2020 Palo Alto Networks, Inc.

2. Sélectionnez **Merge with Device Candidate Config (Fusionner avec la configuration candidate du périphérique)** et **Include Device and Network Templates (Inclure les modèles de périphérique et de réseau)**, puis cliquez sur **OK**.



3. **Commit and Push (Validez et appliquez)** vos modifications dans Panorama et appliquez les modifications aux groupes de périphériques, aux modèles et aux groupes de collecteurs.
4. Vérifiez le transfert de journal vers Panorama pour confirmer que votre configuration est réussie.

Pour modifier le mode de transfert de journaux que les pare-feu utilisent pour envoyer des journaux à Panorama, vous pouvez modifier les paramètres de transfert des journaux et de la mémoire tampon par défaut. *Vous pouvez aussi* gérer les quotas de stockage et de délais d'expiration pour les journaux et rapports.

© 2020 Palo Alto Networks, Inc.

Configurez le transfert syslog vers des destinations extérieures.

Dans le cas d'un déploiement avec un taux élevé de génération de journaux, vous pouvez transférer des journaux syslogs par une interface Ethernet afin d'éviter la perte de journaux et réduire la charge de l'interface de gestion ce qui optimise les opérations de gestion.

Le transfert de journaux syslog à l'aide d'une interface Ethernet est compatible uniquement avec un serveur de gestion Panorama™ en mode Panorama ou en mode Collecteur de journaux. En plus, vous pouvez activer le transfert de journaux syslog sur une interface unique que Panorama soit en mode Panorama ou en mode Collecteur de journaux.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Configurer un collecteur géré.

STEP 3 | Configuration d'un groupe de collecteurs.

Sur les appareils Panorama M-Series, un groupe de collecteurs par défaut est prédéfini et contient déjà le collecteur de journaux local en tant que membre. Cependant, sur l'appareil virtuel Panorama, vous devez ajouter le groupe de collecteurs et ajouter le collecteur de journaux local en tant que membre. Pour les deux configurations, vous devez attribuer des pare-feux à un Collecteur de journaux pour le transfert des journaux.

STEP 4 | Configurez un profil de serveur Syslog.

1. Sélectionnez **Panorama** > **Server Profiles (Profils de serveur)** > **Syslog** et **Add (Ajoutez)** un profil nouveau profil de serveur syslog.
2. Saisissez un **Name (Nom)** pour le profil du serveur Syslog.
3. Pour chaque serveur syslog, **Add (Ajouter)** les informations que Panorama ou le Collecteur de journaux dédié nécessite afin de s'y connecter :
   - **Name (Nom)** : nom unique du serveur syslog.
   - **Syslog Server (Serveur Syslog)** : adresse IP ou Fully Qualified Domaine Name (om de domaine complet ; FQDN) du serveur syslog.
   - **Transport** : sélectionnez **UDP**, **TCP**, ou **SSL** comme méthode de communication avec le serveur syslog.
   - **Port** : le numéro du port à utiliser lors d l'envoi de messages syslog (par défaut UDP sur le port 514) ; vous devez utiliser le même numéro de port sur Panorama et sur le Collecteur de journaux dédié.
   - **Format (Format)** : sélectionnez le format de message Syslog à utiliser : **BSD** (par défaut) ou **IETF**. Généralement, le format **BSD** est sur UDP et le format **IETF** est sur TCP ou SSL/TLS.
   - **Facility (Site)** : sélectionnez la valeur standard Syslog (par défaut **LOG_USER**) pour calculer le champ priority PRI (priorité) dans l'implémentation de votre serveur Syslog. Sélectionnez la valeur correspondant à l'utilisation du champ PRI pour gérer vos journaux syslog.
4. (En option) Pour personnaliser le format des messages syslog que Panorama ou le Collecteur de journaux dédié envoie, sélectionnez **Custom Log Format (Personnaliser le format des journaux)**. Pour plus d'informations sur comment créer des formats personnalisés pour les divers types de journaux, reportez-vous au Common Event Format Configuratiuon Guide (Guide de configuration des formats d'événements courants).
5. Cliquez sur **OK** pour enregistrer le profil de serveur syslog.

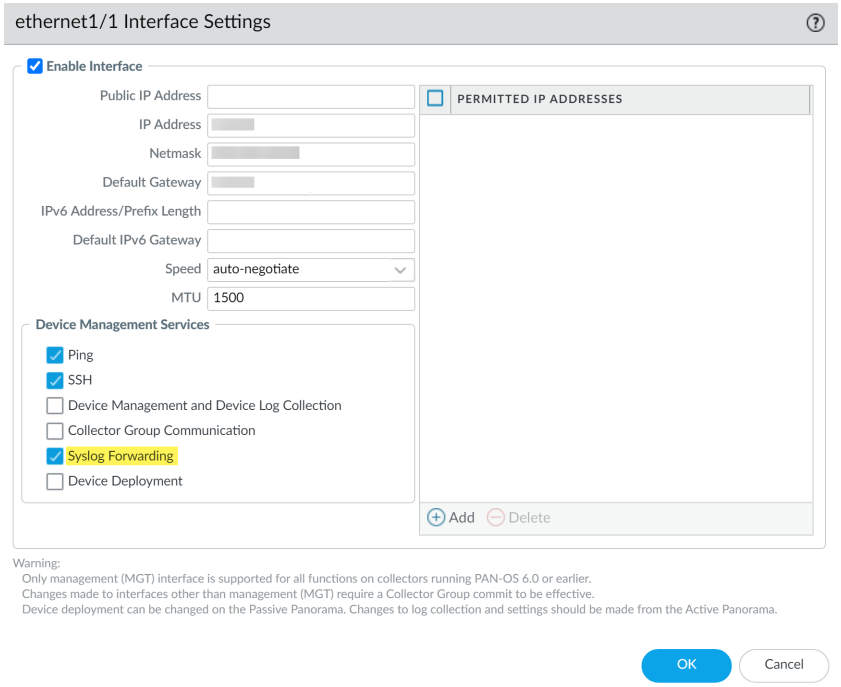
© 2020 Palo Alto Networks, Inc.

STEP 5 | Configurer une interface Ethernet pour transférer les syslogs.

Par défaut, le transfert de syslog est activé dans l'interface de gestion et est compatible sur une seule interface à la fois.

- Configurez une interface Ethernet sur le Collecteur de journaux local depuis l'interface web Panorama.
  1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Interfaces** et sélectionnez une interface Ethernet.
  2. **Enable Interface (Activez l'interface)**.
  3. Configurez l'interface Ethernet comme il convient.
  4. Dans la partie Services de gestion des périphériques, activez **Syslog Forwarding (Transférer Syslog)**.
  5. Sélectionnez **Yes (Oui)** pour confirmer votre modification du transfert syslog.

     Vous pouvez le faire sur une seule interface Ethernet sur le Collecteur de journaux local.
  6. Cliquez sur **OK** pour enregistrer vos modifications.
  7. **Commit (Validez)** et **Commit and Push (Validez et appliquez)** les modifications de votre configuration.

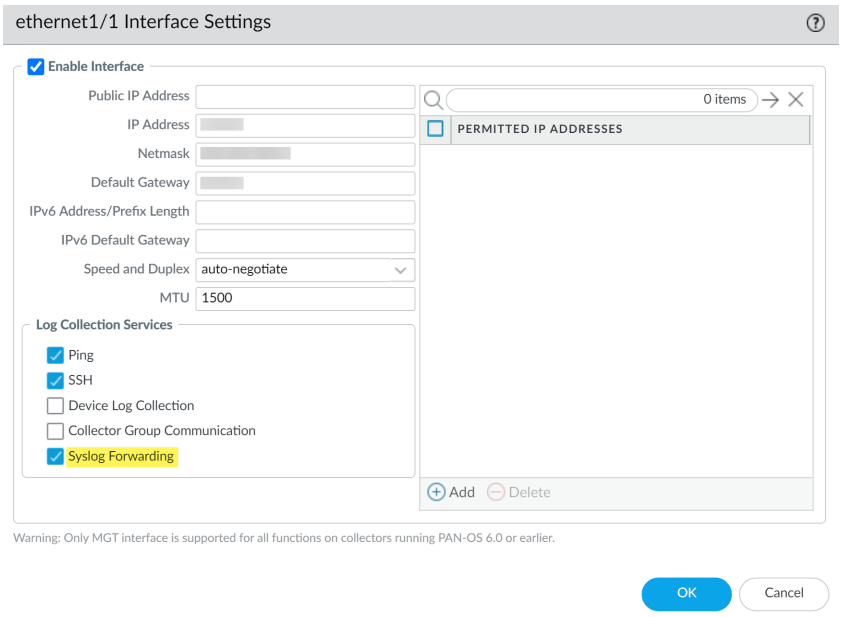


- Configurer une interface Ethernet sur un Collecteur de journaux dédié.
  1. Sélectionnez **Panorama (Panorama)** > **Managed Collectors (Collecteurs gérés)** et sélectionnez un Collecteur de journaux dédié.
  2. **Enable Interface (Activez l'interface)**.
  3. Configurez l'interface Ethernet comme il convient.
  4. Dans la partie Services de Collecteur de journaux, activez **Syslog Forwarding (Transférer Syslog)**.
  5. Sélectionnez **Yes (Oui)** pour confirmer votre modification du transfert syslog.

     Vous pouvez le faire sur une seule interface Ethernet sur le Collecteur de journaux dédié.
  6. Cliquez sur **OK** pour enregistrer vos modifications.

© 2020 Palo Alto Networks, Inc.

7. **Commit (Validez)** et **Commit and Push (Validez et appliquez)** les modifications de votre configuration.



- Configurez une interface Ethernet sur le Collecteur de journaux local ou le Collecteur de journaux dédié depuis le CLI de Panorama.

  Afin de bien configurer le transfert de syslog sur une interface Ethernet depuis le CLI, vous devez d'abord désactiver le transfert de syslog dans l'interface de gestion et ensuite activer le transfert de syslog sur l'interface Ethernet depuis le CLI ; Panorama ne désactive pas automatiquement le transfert de syslog sur l'interface de gestion sur laquelle vous activez le transfert de syslog sur une interface Ethernet depuis le CLI et le transfert de syslog se poursuit sur l'interface de gestion si vous l'activez sur les deux interfaces de gestion et Ethernet.

  1. Connectez-vous à l'ILC Panorama
  2. Désactivez le transfert de syslog dans l'interface de gestion :

     ```
     admin@Panorama> configure
     ```

     ```
     admin@Panorama> set log-collector <Log Collector Serial Number>
      deviceconfig system service disable-syslog-forwarding yes
     ```

  3. Activez le transfert de syslog dans l'interface Ethernet :

     ```
     admin@Panorama> configure
     ```

     ```
     admin@Panorama> set log-collector <Log Collector Serial Number>
      deviceconfig system eth<Interface Number>  service disable-syslog-
     forwarding no
     ```

     ```
     admin@Panorama> commit
     ```

  4. Validez vos modifications de configuration :

     ```
     admin@Panorama> run commit-all log-collector-config log-collector-
     group <Collector Group name>
     ```


© 2020 Palo Alto Networks, Inc.

STEP 6 | Configurer le transfert des journaux vers Panorama.

STEP 7 | Configure syslog forwarding from Panorama to a syslog server (Configurer le transfert de syslog depuis Panorama vers un serveur syslog.

© 2020 Palo Alto Networks, Inc.

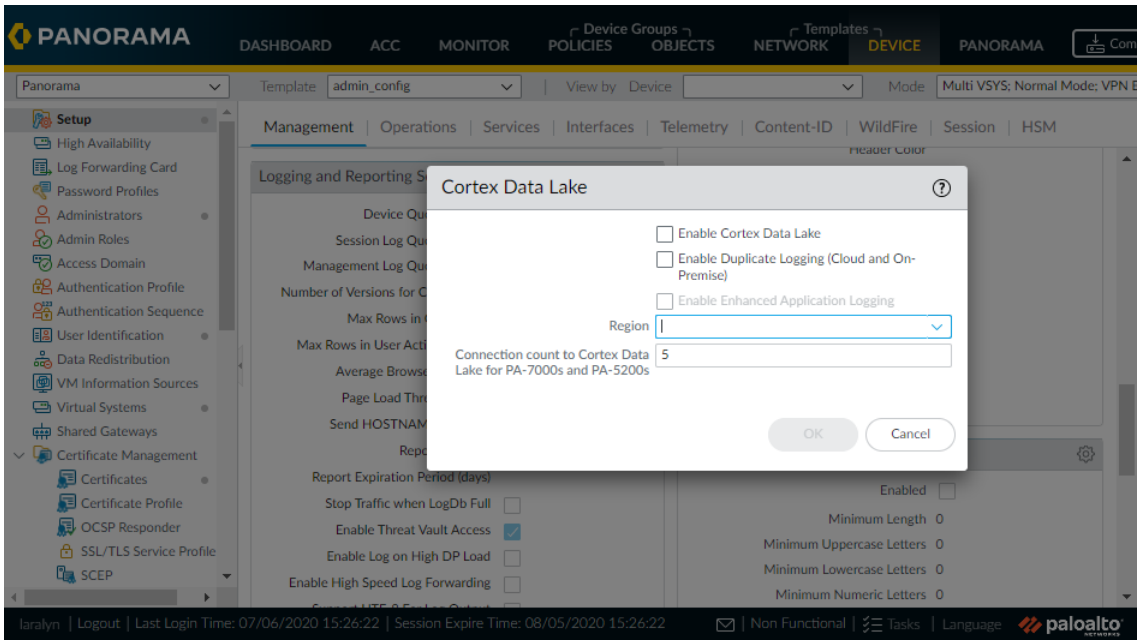
Transférer les journaux vers Cortex Data Lake

Cortex Data Lake est l'infrastructure de journalisation basée sur le cloud de Palo Alto Networks. Avant de pouvoir configurer vos pare-feux gérés pour envoyer des journaux vers Cortex Data Lake, auparavant appelé Service de journalisation, vous devez acheter une licence pour le volume de journaux de votre déploiement et installer le plug-in de services cloud. Si vous avez déjà installé Log Collectors, vous pouvez utiliser Cortex Data Lake pour compléter et augmenter votre configuration existante.

STEP 1 | Installez les plug-ins Panorama.

STEP 2 | Configurez les pare-feux pour envoyer des journaux vers Cortex Data Lake.

Pour les pare-feu exécutant PAN-OS 8.1 ou des versions ultérieures, vous pouvez choisir d'envoyer des journaux vers Cortex Data Lake et à votre installation de collecte de journaux Panorama et sur site lorsque vous sélectionnez **Enable Duplicate Logging (Cloud and On-Premise) (Activer la journalisation dupliquée (Cloud et sur site))**. Lorsque cette option est activée, les pare-feu appartenant au modèle sélectionné enregistrent une copie des journaux dans les deux emplacements. Vous pouvez choisir soit **Enable Duplicate Logging (Cloud and On-Premise) (Activer la journalisation double (Cloud et Sur site))** ou **Enable Logging Service (Activer le Service de journalisation)**, mais pas les deux.



© 2020 Palo Alto Networks, Inc.

Vérifier le transfert des journaux vers Panorama

Vérifiez le transfert des journaux vers Panorama après avoir configuré le transfert de journal vers Panorama ou versCortex Data Lake pour tester que votre configuration a réussi.

Après avoir configuré le transfert des journaux vers des collecteurs de journaux, les pare-feu gérés ouvrent une connexion TCP à tous les collecteurs de journaux configurés. Ces connexions expirent aux soixante (60) secondes et n'indiquent pas que le pare-feu a perdu la connexion aux collecteurs de journaux. Lorsque vous configurez le transfert des journaux vers un collecteur de journaux local ou dédié via une interface ethernet prise en charge, les journaux du trafic du pare-feu affiche des sessions `incomplete` même si le pare-feu arrive à se connecter aux collecteur de journaux. Si vous configurez le transfert des journaux via le port de gestion, aucun journal de trafic affichant des sessions `incomplete` n'est généré. Les journaux du trafic affichant des sessions `incomplete` sont générés par tous les pare-feu, sauf les pare-feu PA-5200 et PA-7000 Series.

STEP 1 | Accédez à la CLI du pare-feu.

STEP 2 | Si vous avez configuré des collecteurs de journaux, vérifiez que chaque pare-feu a une liste de préférence de transfert de journaux.

```
> show log-collector preference-list
```

Si le groupe collecteur n'a qu'un seul collecteur de journaux, la sortie ressemblera à ceci :

```
Forward to all: No
Log collector Preference List
Serial Number: 003001000024
IP Address: 10.2.133.48
IPV6 Address: unknown
```

STEP 3 | Vérifiez que chaque pare-feu transfère les journaux.

```
> show logging-status
```

Pour le transfert réussi, la sortie indique que l'agent de transfert de journal est activé.

- Pour un appareil virtuel Panorama, l'agent est `Panorama`.
- Pour un appareil de Série M, l'agent est un `LogCollector`.
- Pour le Cortex Data Lake, l'agent est `Log CollectionService` (Service de collecte de journaux). Et

```
'Log Collection log forwarding agent' is active and connected
 to <IP_address>.
```

STEP 4 | Afficher le taux moyen de journalisation. Le taux affiché sera la moyenne de journaux/seconde pour les cinq dernières minutes.

© 2020 Palo Alto Networks, Inc.

- Si le Collecteur de journaux reçoit les journaux, accédez à l'interface web de Panorama, sélectionnez **Panorama (Panorama)** > **Managed Collectors (Collecteurs gérés)** et cliquez sur le lien **Statistics (statistiques)** dans la colonne la plus à droite.
- Si un appareil virtuel Panorama en mode hérité reçoit les journaux, accédez à l'ILC de Panorama et exécutez la commande suivante : **`debug log-collector log-collection-stats show incoming-logs`**.



Cette commande fonctionne aussi sur un appareil de la série M.

© 2020 Palo Alto Networks, Inc.

Modifier le journal de transfert et la mise en mémoire tampon par défaut

Vous pouvez définir le mode d'expédition de journal qui permet aux pare-feux d'envoyer les journaux vers Panorama et, lorsqu'il est configuré dans une configuration de haute disponibilité (HD), spécifiez l'homologue Panorama qui peut recevoir les journaux. Pour accéder à ces options, sélectionnez **Panorama** > **Setup (Configuration)** > **Management (Gestion)**, modifiez les paramètres de journalisation et de génération de rapports, et sélectionnez **Log Export and Reporting (Exportation de journaux et génération de rapports)**.

- Définissez le mode de transfert des journaux sur le pare-feu : Les pare-feux peuvent transférer des journaux à Panorama (s'applique à la fois à l'appareil de la série M et à l'appareil virtuel Panorama) soit en mémoire tampon du journal en mode transfert ou en mode transfert de journaux Live.

Options de journalisation	Description
(Pratique exemplaire) **Buffered Log Forwarding from Device (Transfert des journaux en mémoire tampon depuis le périphérique)** Par défaut : Activé	Permet à chaque pare-feu géré de mettre les journaux en mémoire tampon et d'envoyer les journaux à des intervalles de 30 secondes vers Panorama (non configurable par l'utilisateur). Le transfert des journaux en mémoire tampon est appréciable lorsque le pare-feu perd sa connectivité à Panorama. Le pare-feu met les entrées de journal en mémoire tampon sur son disque dur local et conserve un pointeur pour enregistrer la dernière entrée de journal qui a été envoyée à Panorama. Lorsque la connectivité est rétablie, le pare-feu reprend le transfert des journaux là où il s'est arrêté. L'espace disque disponible pour la mise en mémoire tampon dépend du quota de stockage de journal pour le modèle de pare-feu et du volume de journaux en attente de routage. Dans le cas où un pare-feu a été déconnecté longtemps et où le dernier journal transmis a été renouvelé, tous les journaux du disque dur local sont transmis à Panorama dès le rétablissement de la connexion. Si l'espace disque disponible sur le disque dur local du pare-feu est utilisé, les entrées les plus anciennes sont supprimées pour permettre la journalisation des nouveaux événements.
Transfert des journaux en mode direct depuis le périphérique Cette option est activée lorsque la case à cocher **Buffered Log Forwarding from Device (Transfert des journaux en mémoire tampon depuis le périphérique)** n'est pas sélectionnée.	En mode direct, le pare-feu géré envoie chaque transaction de journal vers Panorama au moment de l'enregistrement sur le pare-feu.

- Définissez les préférences de transfert des journaux sur un appareil virtuel Panorama en mode hérité qui est déployé en configuration haute disponibilité (HD) :

© 2020 Palo Alto Networks, Inc.

- Lorsque vous vous connectez à un disque virtuel, activez la journalisation sur le disque local sur l'homologue Panorama principal seulement. Par défaut, les deux homologues Panorama dans la configuration HD reçoivent les journaux.

  Pour les pare-feu des séries PA-7000 et PA-5200, seul l'homologue actif reçoit les journaux.
- Lorsque vous vous connectez en NFS (serveur ESXi uniquement), activez les pare-feu pour n'envoyer que les journaux récemment générés vers un homologue Panorama secondaire, qui est alors promu principal après un basculement.

Options de journalisation	Appartient à	Description
Seulement les journaux actifs primaires sur le disque Local Par défaut : Désactivé	Appareil virtuel Panorama en mode hérité se connectant à un disque virtuel et déployé dans une configuration haute disponibilité (HD).	Permet de configurer uniquement l'homologue Panorama primaire pour enregistrer les journaux sur le disque local.
Obtenir uniquement de nouveaux journaux à convertir au primaire Par défaut : Désactivé	Appareil virtuel Panorama en mode hérité monté sur un magasin de données NFS (système de fichiers réseau), exécuté sur un serveur VMware ESXi et déployé dans une configuration haute disponibilité	Avec la journalisation NFS, lorsque vous disposez d'une paire de serveurs Panorama configurée en haute disponibilité, seul l'homologue Panorama principal est monté sur la base de données NFS. Les pare-feux ne peuvent donc envoyer les journaux qu'à l'homologue Panorama primaire, qui peut écrire dans la base de données NFS. Lorsqu'un basculement HD se produit, l'option **Get Only New Logs on Convert to Primary (Obtenir uniquement les nouveaux journaux lors de la conversion vers le périphérique primaire)** permet à l'administrateur de configurer les pare-feux gérés pour n'envoyer que les journaux récemment générés à Panorama. Cet événement est déclenché lorsque la priorité de Panorama passe de secondaire active à primaire, et lorsqu'il peut commencer la journalisation au NFS. Ce comportement est en général activé pour éviter aux pare-feux d'envoyer de gros volumes de journaux placés en mémoire tampon une fois la connectivité vers Panorama restaurée après une période significative.

© 2020 Palo Alto Networks, Inc.

Configurer le transfert des journaux de Panorama vers des destinations extérieures

Panorama vous permet de transmettre les journaux à des services externes, y compris les services Syslog, e-mail, interruption SNMP et HTTP. L'utilisation d'un service externe vous permet de recevoir des alertes d'événements importants, d'archiver des informations surveillées sur des systèmes disposant d'un stockage à long terme dédié, et d'intégrer des outils de surveillance de sécurité tiers. En plus de transférer les journaux des pare-feu, vous pouvez transférer les journaux générés par le serveur de gestion Panorama et les collecteurs de journaux. Le serveur de gestion Panorama ou le collecteur de journaux qui transfère les journaux les convertit au format approprié pour la destination (message Syslog, notification par e-mail, interruption SNMP ou charge utile HTTP).



Si votre serveur de gestion Panorama est un appareil virtuel Panorama en mode hérité, il convertit et transmet les journaux aux services externes sans utiliser les collecteurs de journaux.

Vous pouvez également transférer les journaux directement depuis les pare-feu vers des services externes : consultez la section Options de transfert des journaux*.*

Sur une application virtuelle Panorama exécutant Panorama 5.1 ou versions antérieures, vous pouvez utiliser les commandes Secure Copy (SCP) de l'ILC *pour exporter la base de données de journal complète sur un serveur SCP et l'importer dans un autre appareil virtuel Panorama. Une application virtuelle Panorama exécutant Panorama 6.0 ou versions ultérieures et les appareils de série M exécutant toute version, ne supportent pas ces options, car la base de données de journal sur ces modèles est trop importante pour une exportation ou importation pragmatique.*

Pour transférer les journaux vers des services externes, commencez par configurer les pare-feu pour qu'ils transfèrent les journaux à Panorama. Vous devez ensuite configurer les profils de serveur qui définissent la manière dont Panorama et les collecteurs de journaux se connectent aux services. Enfin, vous affectez les profils de serveur aux paramètres de journaux de Panorama et aux groupes de collecteurs.

STEP 1 | Configurez les pare-feu pour transmettre les journaux à Panorama.

Configurer le transfert des journaux vers Panorama.

STEP 2 | Configurez un profil de serveur pour chaque service externe qui recevra des informations des journaux.

1. Sélectionnez **Panorama** > **Server Profiles (profils de serveur)** et sélectionnez le type de serveur qui recevra les données du journal : **SNMP Trap (Interruption SNMP)**, **Syslog**, **Email (E-mail)** ou **HTTP**.
2. Configurez le profil de serveur :
   - Configurez un profil de serveur d'interruption SNMP. Pour plus de détails sur la façon dont SNMP fonctionne pour Panorama et les collecteurs de journaux, reportez-vous au support SNMP.
   - Configurez un profil de serveur Syslog. Si le serveur syslog requiert l'authentification du client, utilisez la page **Panorama** > **Certificate Management (Gestion de certificat)** > **Certificates (Certificats)** pour créer un certificat pour sécuriser la communication syslog sur SSL.
   - Configurez un profil de serveur de messagerie.
   - Configurez un profil de serveur HTTP.

STEP 3 | Configurez les destinations pour :

© 2020 Palo Alto Networks, Inc.

- Les journaux générés par le serveur de gestion Panorama et les collecteurs de journaux.
- Les journaux de pare-feu que recueille une application virtuelle Panorama en mode hérité.

1. **Panorama** > **Log Settings (Paramètres des journaux)**.
2. **Add (Ajoutez)** un ou plus *profils de liste de correspondance* pour chaque type de journal.

   Les profils indiquent les filtres de requête de journal, les destinations de transfert et les actions automatiques, comme l'étiquetage. Pour chaque profil de la liste de correspondance :

   1. Saisissez un **Name (Nom)** pour identifier le profil.
   2. Sélectionnez le **Log Type (Type de journal)**.
   3. Dans la liste déroulante **Filter (Filtre)**, sélectionnez **Filter Builder (Générateur de filtre)**. Indiquez les éléments suivants, puis **Add (Ajoutez)** chaque requête :

      Connector (Connecteur) logique (et/ou)

      Attribute (Attribut) du journal

      L'**Operator (Opérateur)** pour définir la logique d'inclusion ou d'exclusion

      La **Value (Valeur)** d'attribut à laquelle doit correspondre la requête
   4. **Add (Ajoutez)** les profils de serveur que vous avez configurés pour chaque service externe.
   5. Cliquez sur **OK** pour enregistrer le profil.

STEP 4 | Configurez les destinations des journaux des pare-feu que les collecteurs de journaux reçoivent.



Chaque groupe de collecteur peut transmettre les journaux vers différentes destinations. Si les collecteurs de journaux sont locaux dans une paire de haute disponibilité (HD) de serveurs de gestion Panorama, vous devez vous connecter à chaque homologue HD pour configurer le transfert de journal pour son groupe de collecteur.

1. Sélectionnez **Panorama** > **Collector Groups (Groupes de collecteurs)** et modifiez le groupe de collecteurs qui va recevoir les journaux du pare-feu.
2. (Facultatif, transfert par interruption SNMP uniquement) Sélectionnez **Monitoring (Surveillance)** et configurez les paramètres SNMP.
3. Sélectionnez **Collector Log Forwarding (Transfert des journaux)** et **Add (Ajoutez)** des profils de liste de correspondance configurés si nécessaire.
4. Cliquez sur **OK** pour enregistrer les modifications au groupe de collecteurs.

STEP 5 | (Transfert Syslog uniquement) Si le serveur Syslog requiert l'authentification du client, et que les pare-feu transmettent les journaux aux collecteurs de journaux dédiés, affectez un certificat qui assure la communication Syslog sur SSL.

Effectuez les étapes suivantes pour chaque type de journal dédié :

1. Sélectionnez **Panorama (Panorama)** > **Managed Collectors (Collecteurs gérés)** et modifiez le collecteur de journaux.
2. Sélectionnez le **Certificate for Secure Syslog (Certificat pour sécuriser Syslog)** et cliquez sur **OK**.

STEP 6 | (Transfert par interruption SNMP uniquement) Activez votre gestionnaire SNMP pour interpréter les interruptions.

Chargez les MIB prises en charge et, si nécessaire, compilez-les. Pour les étapes spécifiques, reportez-vous à la documentation de votre gestionnaire SNMP.

STEP 7 | Validez et vérifiez vos modifications de configuration.

© 2020 Palo Alto Networks, Inc.

1. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** pour valider vos modifications dans Panorama et appliquer les modifications aux groupes de périphériques, aux modèles et aux groupes de collecteurs.
2. Vérifiez que les services extérieurs reçoivent les informations des journaux :
   - **Serveur de messagerie** : vérifiez que les destinataires spécifiés reçoivent les journaux sous forme de notifications par e-mail.
   - **Serveur Syslog** : reportez-vous à la documentation de votre serveur Syslog pour vérifier s'il reçoit les journaux sous forme de messages Syslog.
   - **Gestionnaire SNMP** : reportez-vous à la documentation de votre serveur d'interruption SNMP pour vérifier qu'il reçoit les journaux en tant qu'interruptions SNMP.
   - **Serveur HTTP** : vérifiez que le serveur HTTP reçoit les journaux au format de charge utile correct.

© 2020 Palo Alto Networks, Inc.

Déploiements de collecte de journaux

Les rubriques qui suivent décrivent comment configurer la collecte des journaux dans les déploiements les plus caractéristiques. Avant de commencer, Planification de votre déploiement Panorama en fonction de vos besoins d'exploitation actuels et futurs.



Les déploiements dans ces rubriques décrivent tous Panorama dans une configuration de haute disponibilité (HD). Palo Alto Networks recommande HD parce qu'elle permet la récupération automatique (en cas de défaillance du serveur) des composants qui ne sont pas enregistrés dans le cadre des sauvegardes de configuration. Dans les déploiements HD, le serveur de gestion Panorama ne prend en charge que la configuration active/passive.

- Déployer Panorama avec des collecteurs de journaux dédiés
- Déployer les appareils de série M Panorama avec les collecteurs de journaux locaux
- Déployer les appareils virtuels Panorama avec les collecteurs de journaux locaux
- Déployer les appareils virtuels Panorama en mode hérité avec la collecte de journaux locale

Déployer Panorama avec des collecteurs de journaux dédiés

Les figures suivantes illustrent Panorama dans un déploiement de collecte de journaux distribués. Dans ces exemples, le serveur d'administration de Panorama se compose de deux appareils virtuels de série M ou Panorama en mode Panorama qui sont déployés dans une configuration actif/passif haute disponibilité (HA). Les pare-feux envoient les journaux aux Collecteurs de Journaux dédiés (appareils virtuels de série M ou Panorama en mode Collecteur de Journaux). Il s'agit de la configuration recommandée si les pare-feu produisent plus de 10.000 journaux/seconde.



Si vous affectez plus d'un collecteur de journaux à un groupe de collecteurs, consultez Mises en garde pour un groupe de collecteurs comportant plusieurs collecteurs de journaux *pour comprendre les exigences, les risques et les mesures d'atténuation recommandées.*

© 2020 Palo Alto Networks, Inc.

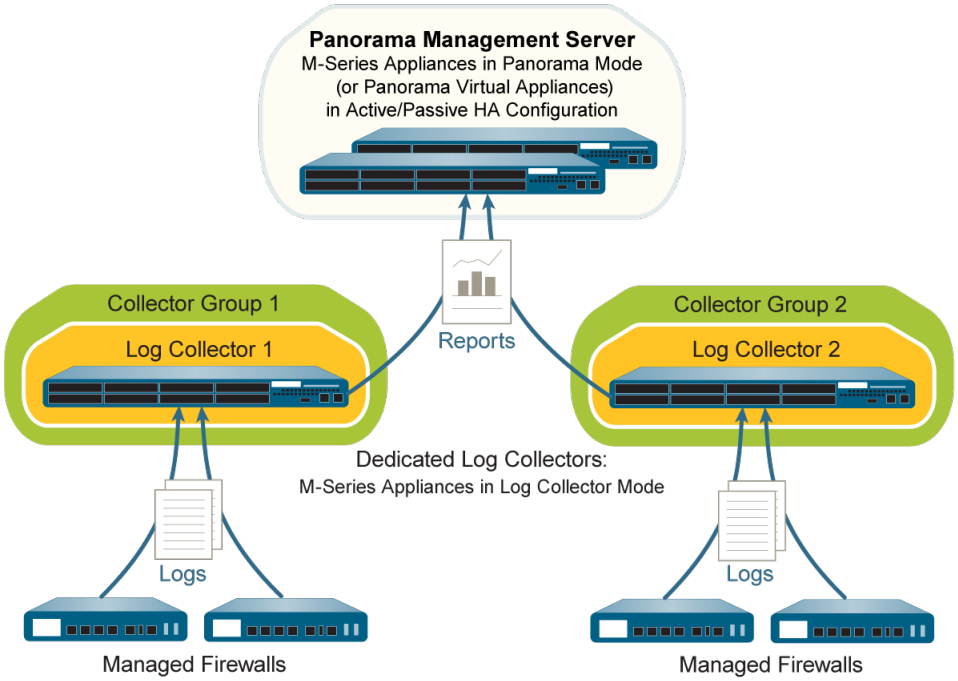


Figure 17: Collecteur de journaux dédié unique par groupe de collecteurs

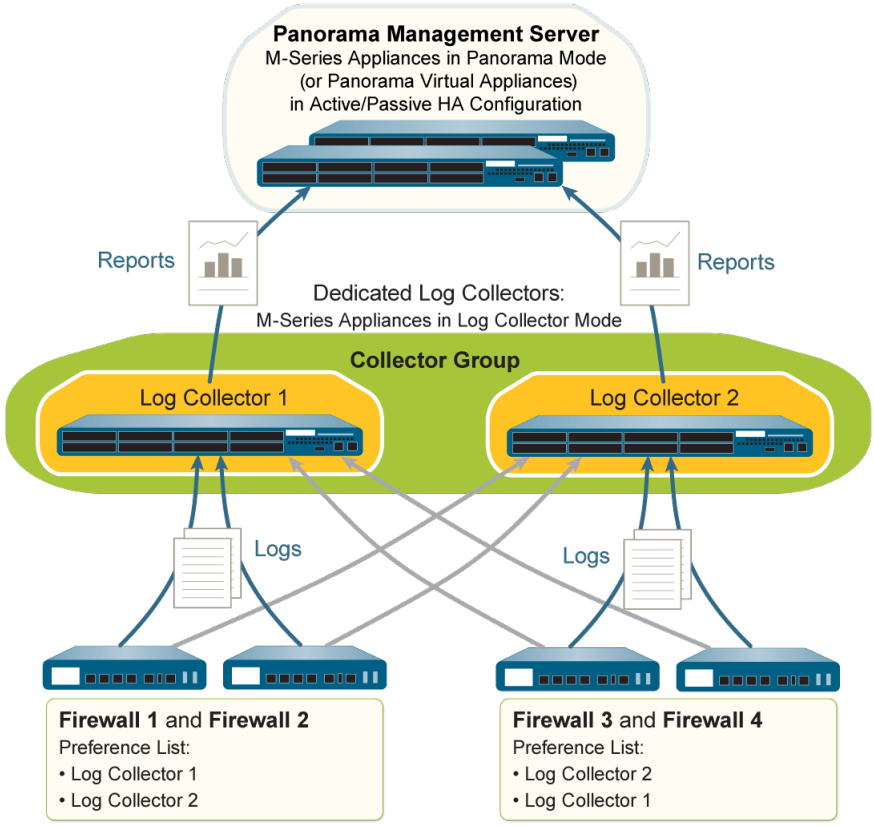


Figure 18: Plusieurs collecteurs de journaux dédiés par groupe de collecteurs

Effectuez les étapes suivantes pour déployer Panorama avec des collecteurs de journaux dédiés. Ignorez les étapes que vous avez déjà effectuées (par exemple, la configuration initiale).

© 2020 Palo Alto Networks, Inc.

STEP 1 | Effectuer la configuration initiale du serveur de gestion Panorama (applications virtuelles ou appareils de la série M) et les collecteurs de journal dédiés.

Pour chaque appareil de la série M :

1. Montez l'appareil de série M dans une baie. Se référer au Guide de référence du matériel de la série-M pour obtenir des instructions.
2. Effectuez la configuration initiale de l'appareil de série M.

   Palo Alto Networks recommande de réserver l'interface de gestion (MGT) à l'accès administratif à Panorama et de dédier séparément les interfaces de l'appareil de série M aux autres services Panorama.
3. Configurez chaque baie. Cette tâche est nécessaire pour rendre les disques RAID disponibles pour la journalisation. Vous pouvez éventuellement ajouter des disques pour augmenter la capacité de stockage sur l'appareil de série M.
4. Enregistrer Panorama et installer les licences.
5. Installer les mises à jour de contenu et logicielles pour Panorama.

Pour chaque appareil virtuel (le cas échéant) :

1. Installez l'application virtuelle Panorama.
2. Effectuez la configuration initiale de l'application virtuelle Panorama.
3. Enregistrer Panorama et installer les licences.
4. Installer les mises à jour de contenu et logicielles pour Panorama.

Pour le serveur de gestion du Panorama (application virtuelle ou appareil de la série M), vous devez également configurer la HD sur la Panorama.

STEP 2 | Basculez du mode panorama en mode collecteur de journaux sur chaque serveur de gestion Panorama qui sera un collecteur de journaux dédié.

Changer le mode d'un appareil virtuel de série M ou Panorama supprime toutes les données des journaux existantes et supprime toutes les configurations sauf les paramètres de gestion d'accès. Après la bascule, l'appareil virtuel de série M ou Panorama garde l'accès à la CLI mais perd l'accès à l'interface web.

1. Connectez-vous à Panorama d'une des façons suivantes :
   - (appareils de série M uniquement) Fixez un câble série à partir d'un ordinateur au port console sur l'appareil de série M. Utilisez ensuite le logiciel d'émulation de terminal (9600-8-N-1) pour vous connecter.
   - Utilisez un logiciel d'émulation de terminal tel que PuTTY pour ouvrir une session SSH à l'adresse IP que vous avez spécifiée pour l'interface MGT du serveur de gestion Panorama lors de la configuration initiale.
2. Connectez-vous à l'ILC lorsque vous y êtes invité. Utilisez le compte admin par défaut et le mot de passe affecté lors de la configuration initiale.
3. Pour passer à une session en mode collecteur de journaux, entrez la commande suivante :

```
> request system system-mode logger
```

4. Entrez **Y** pour confirmer le changement de mode. Le serveur de gestion Panorama redémarre. Si le processus de redémarrage met fin à votre session du logiciel d'émulation de terminal, reconnectez-vous à Panorama pour afficher l'invite de connexion Panorama.

© 2020 Palo Alto Networks, Inc.

Si vous voyez une invite de ***connexion CMS****, cela signifie que le collecteur de journaux n'a pas terminé le redémarrage. Appuyez sur ENTER à l'invite sans taper un nom d'utilisateur ou un mot de passe.*

5. Connectez-vous à l'ILC.
6. Vérifiez que la bascule en mode collecteur de journaux a réussi :

```
> show system info | match system-mode
```

Si le changement de mode a réussi, la sortie affiche :

```
system-mode: logger
```

STEP 3 | Activez la connectivité entre chaque collecteur de journaux et le serveur de gestion de Panorama.

Cette étape est requise avant de pouvoir activer les disques de journalisation sur le collecteur de journaux.

Saisissez les commandes suivantes dans l'ILC du collecteur de journaux,où <*adresseIP1*> est pour l'interface de gestion de Panorama actif et <*adresseIP2*> est pour l'interface de gestion de Panorama passif.

```
> configure
# set deviceconfig system panorama-server <IPaddress1> panorama-server-2
 <IPaddress2>
# commit
# exit
```

STEP 4 | Enregistrez le numéro de série de chaque collecteur de journaux.

Vous avez besoin des numéros de série pour ajouter les collecteurs de journaux en tant que collecteurs gérés sur le serveur de gestion de Panorama.

1. Dans l'ICL de chaque collecteur de journaux, saisissez la commande suivante pour afficher son numéro de série.

```
> show system info | match serial
```

2. Enregistrez le numéro de série.

STEP 5 | Ajoutez chaque collecteur de journaux comme collecteur géré.

Utilisez l'interface Web de l'homologue du serveur de gestion du Panorama principal pour configurer un collecteur géré :

1. Sélectionnez **Panorama (Panorama)** > **Managed Collectors (Collecteurs gérés)** et **Add (ajoutez)** le collecteur géré.
2. Dans l'onglet **General (général)**, saisissez le numéro de série (**Collector s/n (S/N du Collecteur)**) que vous avez enregistré pour le collecteur de journaux.
3. Entrez l'adresse IP ou le nom de domaine complet des homologues HD Panorama principaux et secondaires dans les champs **Panorama Server IP (IP serveur Panorama)** et **Panorama Server IP 2 (IP serveur Panorama 2)** respectivement. Ces champs sont obligatoires.
4. Sélectionnez **Interfaces**, cliquez sur **Management (Gestion)** et remplissez un ou les deux ensembles de champs suivants pour l'interface de gestion, selon les protocoles IP de votre réseau.

© 2020 Palo Alto Networks, Inc.

- IPv4 : **IP Address (Adresse IP)**, **Netmask (Masque de sous-réseau)** et **Default Gateway (Passerelle par défaut)**
- IPv6 : **IPv6 Address/Prefix Length (Longueur du préfixe / de l'adresse IPv6)** et **Default IPv6 Gateway (Passerelle IPv6 par défaut)**

5. (Facultatif) Sélectionnez **SNMP** si vous utilisez un gestionnaire SNMP pour surveiller les statistiques du Collecteur de journaux.

   L'utilisation de SNMP nécessite des étapes supplémentaires en plus de la configuration du collecteur de journaux (voir Surveiller Panorama et les statistiques des collecteurs de journaux en utilisant SNMP).
6. Cliquez sur **OK** pour enregistrer vos modifications.
7. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

   Cette étape est requise avant de pouvoir activer les disques de journalisation sur le collecteur de journaux.
8. Vérifiez que la page **Panorama (Panorama)** > **Managed Collectors (collecteurs gérés)** répertorie le Collecteur de Journaux que vous avez ajouté. La colonne Connecté affiche une icône de coche pour indiquer que le collecteur de journaux est connecté à Panorama. Vous devrez peut-être attendre quelques minutes avant que la page affiche le statut de connexion actualisée.

   À ce stade, la colonne État de configuration affiche Désynchronisé et la colonne État d'exécution affiche Déconnecté. L'état passera à Synchronisé et Connecté une fois que vous aurez configuré un groupe de collecteurs (étape 9).

STEP 6 | Activez les disques de journalisation sur chaque collecteur de journaux.

Utilisez l'interface Web de l'homologue du serveur de gestion du Panorama principal pour exécuter ces étapes :

1. Sélectionnez **Panorama (Panorama)** > **Managed Collectors (Collecteurs gérés)** et modifiez le collecteur de journaux.
2. Sélectionnez **Disks (Disques)**, **Add (Ajoutez)** chaque paire de disques et cliquez sur **OK**.
3. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

STEP 7 | (Recommandé) Configurez les interfaces **Ethernet1**, **Ethernet2**, **Ethernet3**, **Ethernet4**, et **Ethernet5** si le collecteur de journaux les utilisera pour la **Device Log Collection (Collecte de journaux de périphériques)** (réception des journaux des pare-feu) et la **Collector Group Communication (Communication du groupe de collecteurs)**.

Par défaut, le collecteur de journaux utilise l'interface de gestion pour la collecte de journaux et la communication du groupe de collecteurs. L'attribution d'autres interfaces à ces fonctions vous permet de réserver l'interface de gestion pour le trafic de gestion. Dans un environnement où le trafic de journaux est important, envisagez d'utiliser les interfaces de 10 Gbit/s (**Ethernet4** et **Ethernet5**) sur l'appareil M-500 pour la collecte de journaux et la communication de groupe de collecteurs. Pour équilibrer le trafic de journalisation entre les interfaces, vous pouvez activer **Device Log Collection (Collecte de journaux de périphériques)** sur plusieurs interfaces.

Utilisez l'interface Web du serveur de gestion Panorama principal pour effectuer ces étapes pour chaque collecteur de journaux.

1. Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)**, modifiez le collecteur de journaux, et sélectionnez **Interfaces**.
2. Exécutez les étapes suivantes pour chaque interface :
   1. Cliquez sur le nom de l'interface pour la modifier.

© 2020 Palo Alto Networks, Inc.

2. Sélectionnez **<interface-name> (nom de l'interface)** pour activer l'interface.
3. Remplissez un ou les deux des ensembles de champs suivants, selon les protocoles IP de votre réseau :

   IPv4 : **IP Address (Adresse IP)**, **Netmask (Masque de sous-réseau)** et **Default Gateway (Passerelle par défaut)**

   IPv6 : **IPv6 Address/Prefix Length (Longueur du préfixe / de l'adresse IPv6)** et **Default IPv6 Gateway (Passerelle IPv6 par défaut)**
4. Sélectionnez les services de gestion de périphériques pris en charge par l'interface :

   Device Log Collection (Collecte de journaux de périphériques) : vous pouvez assigner une ou plusieurs interfaces.

   Collector Group Communication (Communication du groupe de collecteurs) : vous ne pouvez attribuer qu'une seule interface.
5. Cliquez sur **OK** pour enregistrer vos modifications d'interface.

3. Cliquez sur **OK** pour enregistrer les modifications au collecteur de journaux.
4. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos modifications à la configuration Panorama.

STEP 8 | Ajouter un pare-feu en tant que périphérique géré.

Utilisez l'interface Web de l'homologue du serveur de gestion du Panorama principal pour effectuer cette tâche pour chaque pare-feu qui transmettra les journaux aux collecteurs de journaux.

STEP 9 | Configurez le groupe de collecteurs.

Si chaque groupe de collecteur aura un collecteur de journaux, répétez cette étape pour chaque groupe de collecteurs avant de continuer.

Si vous voulez assigner tous les collecteurs de journaux à un seul groupe de collecteur, ne l'effectuez qu'une seule fois.

Utilisez l'interface Web de l'homologue du serveur de gestion Panorama principal pour configurer un groupe de collecteurs.

1. Sélectionnez **Panorama (Panorama)** > **Collector Groups (Groupes de Collecteurs)** et **Add (ajoutez)** le groupe de collecteurs.
2. Entrez un **Name (Nom)** pour identifier le domaine d'accès.
3. **Add (Ajoutez)** un ou plusieurs collecteurs de journaux dans la liste des membres du groupe de collecteurs.

   Dans un même groupe de collecteurs, tous les collecteurs de journaux doivent être exécutés sur le même modèle Panorama : uniquement des appareils M-600, uniquement des appareils M-500, uniquement des appareils M-200 ou uniquement des appareils virtuels Panorama.
4. (Recommandé) **Enable log redundancy across collectors (Activez la redondance des journaux entre les collecteurs)** si vous ajoutez plusieurs collecteurs de journaux à un seul groupe de collecteurs. Cette option nécessite que chaque collecteur de journaux ait le même nombre de disques de journalisation.
5. (Facultatif) Sélectionnez **Monitoring (Surveillance)** et configurez les paramètres si vous allez utiliser SNMP pour surveiller les statistiques des collecteurs de journaux et les interruptions.
6. Sélectionnez **Device Log Forwarding (Transfert de journaux du périphérique)** et configurez la liste des préférences de transfert de journaux. Cette liste définit quels pare-feu transmettent les journaux à quels collecteurs de journaux. Affectez des pare-feu selon le nombre de collecteurs de journaux que contient ce groupe de collecteurs :

© 2020 Palo Alto Networks, Inc.

- **Unique** : assignez les pare-feu qui transmettront les journaux à ce collecteur de journaux, comme illustré dans Collecteur de journaux dédié unique par groupe de collecteurs.
- **Plusieurs** : assignez chaque pare-feu aux deux collecteurs de journaux pour la redondance. Lorsque vous configurez les préférences, donnez la première priorité au collecteur de journaux 1 pour la moitié des pare-feu et donnez la première priorité au collecteur de journaux 2 pour l'autre moitié des pare-feu, comme illustré dans Plusieurs collecteurs de journaux dédiés par groupe de collecteurs.

7. Cliquez sur **OK** pour enregistrer les modifications au groupe de collecteurs.
8. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)**, puis **Commit and Push (Valider et appliquer)** vos modifications à Panorama et aux groupes de collecteurs que vous avez ajoutés.
9. Sélectionnez **Panorama (Panorama)** > **Managed Collectors (Collecteurs gérés)** pour vérifier que la configuration de Collecteur de journaux est synchronisée avec Panorama.

   La colonne Configuration Status (État de configuration) doit afficher In Sync (synchronisation) et la colonne Run Time Status (État d'exécution) doit afficher Connected (Connecté).

STEP 10 | Configurez le transfert de journaux depuis les pare-feu vers Panorama.

Utiliser l'interface Web de l'homologue du serveur de gestion du Panorama principal pour exécuter ces étapes :

1. Configurer le transfert des journaux vers Panorama.
2. Vérifier le transfert des journaux vers Panorama.
3. (Facultatif) Configurer le transfert de journal de Panorama vers des destinations externes.

Déployer les appareils de série M Panorama avec les collecteurs de journaux locaux

Les figures suivantes illustrent Panorama dans un déploiement de collecte de journaux centralisée. Dans ces exemples, le serveur d'administration de Panorama se compose de deux appareils de série M en mode Panorama qui sont déployés dans une configuration actif/passif haute disponibilité (HD). Les pare-feu envoient les journaux à un collecteur de journal local (par défaut) prédéfini sur chaque appareil Panorama de Série M . Il s'agit de la configuration recommandée si les pare-feu produisent plus de 10 000 journaux/seconde.

Si vous affectez plus d'un collecteur de journaux à un groupe de collecteurs, consultez Mises en garde pour un groupe de collecteurs comportant plusieurs collecteurs de journaux *pour comprendre les exigences, les risques et les mesures d'atténuation recommandées.*

Après la mise en œuvre de ce déploiement, si la fréquence d'enregistrement augmente au-delà de 10 000 journaux par seconde, Palo Alto Networks recommande que vous ajoutiez des collecteurs de journaux dédiés (appareils de série M en mode collecteurs de journaux) comme décrit dans Déployer Panorama avec des collecteurs de journaux dédiés*. Une telle expansion peut nécessiter une réaffectation des pare-feu, depuis les collecteurs de journaux locaux aux collecteurs de journaux dédiés.*

© 2020 Palo Alto Networks, Inc.

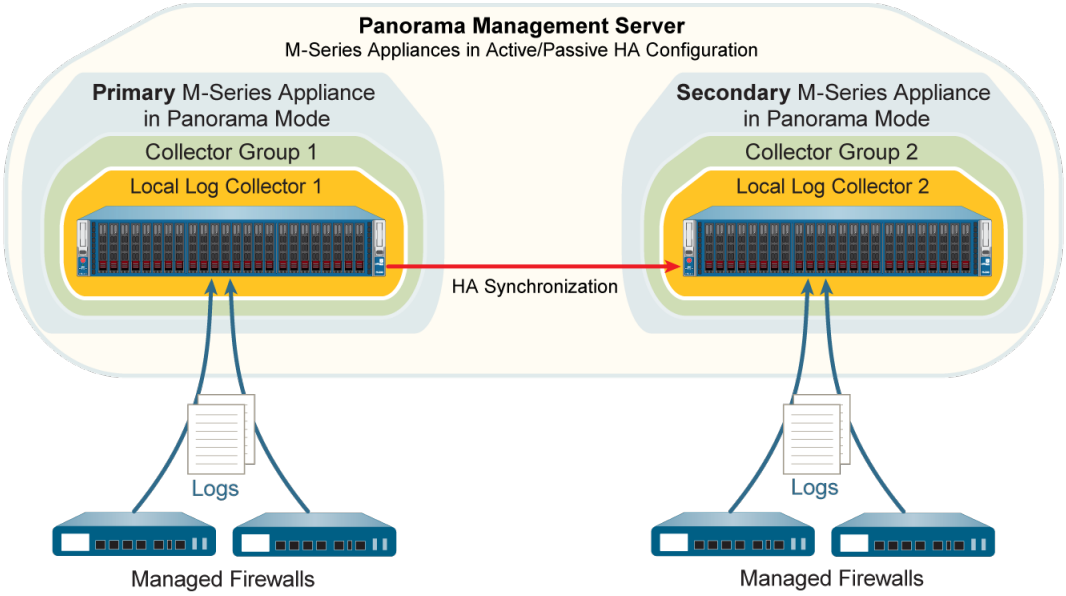


Figure 19: Collecteur de journaux local unique par groupe de collecteurs

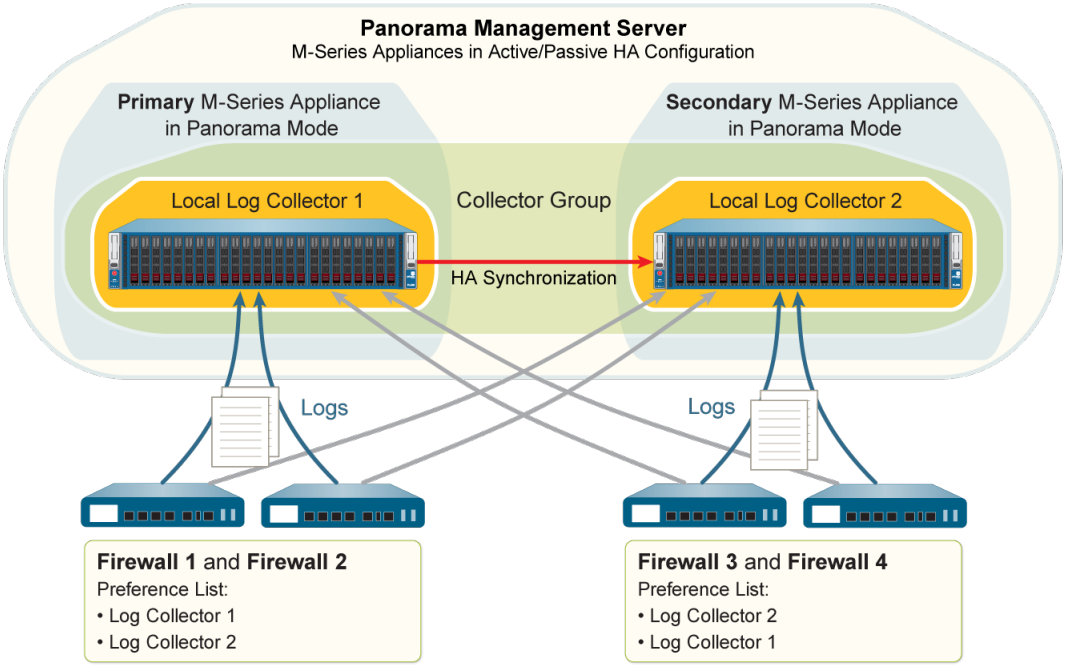


Figure 20: Plusieurs collecteurs de journaux locaux par groupe de collecteurs

Effectuez les étapes suivantes pour déployer Panorama avec des collecteurs de journaux locaux. Ignorez les étapes que vous avez déjà effectuées (par exemple, la configuration initiale).

STEP 1 | Effectuez la configuration initiale de chaque appareil virtuel de série M.

1. Montez l'appareil de série M dans une baie. Se référer au Guide de référence du matériel de la série-M pour obtenir des instructions.
2. Effectuez la configuration initiale de l'appareil de série M.

© 2020 Palo Alto Networks, Inc.

Palo Alto Networks recommande de réserver l'interface de gestion (MGT) à l'accès administratif à Panorama et de dédier séparément les interfaces de l'appareil de série M *aux autres services Panorama.*

3. Configurez chaque baie. Cette tâche est nécessaire pour rendre les disques RAID disponibles pour la journalisation. Vous pouvez éventuellement ajouter des disques pour augmenter la capacité de stockage sur l'appareil de série M.
4. Enregistrer Panorama et installer les licences.
5. Installer les mises à jour de contenu et logicielles pour Panorama.
6. Définir la HD (haute disponibilité) sur Panorama.

STEP 2 | Effectuez les étapes suivantes pour préparer Panorama pour la collecte de journaux.

1. Connectez-vous au Panorama principal d'une des façons suivantes :
   - Fixez un câble série à partir d'un ordinateur au port console du Panorama principal. Utilisez ensuite le logiciel d'émulation de terminal (9600-8-N-1) pour vous connecter.
   - Utilisez un logiciel d'émulation de terminal tel que PuTTY pour ouvrir une session SSH à l'adresse IP que vous avez spécifiée pour l'interface MGT du Panorama principal lors de la configuration initiale.
2. Connectez-vous à l'ILC lorsque vous y êtes invité. Utilisez le compte admin par défaut et le mot de passe affecté lors de la configuration initiale.
3. Activer le Panorama principal pour se connecter au Panorama secondaire en entrant la commande suivante, où *<adresse IP 2>* représente l'interface de gestion du Panorama secondaire :

```
> configure
# set deviceconfig system panorama-server <IPaddress2>
# commit
```

4. Connectez-vous à l'ILC du collecteur de journaux.
5. Activer le Panorama principal pour se connecter au Panorama secondaire en entrant la commande suivante, où *<adresse IP 2>* représente l'interface de gestion du Panorama primaire :

```
> configure
# set deviceconfig system panorama-server <IPaddress1>
# commit
# exit
```

6. Dans l'ILC du Panorama secondaire, saisissez la commande suivante pour afficher le numéro de série, puis enregistrez-le :

```
> show system info | match serial
```

   Vous avez besoin du numéro de série pour ajouter le collecteur de journaux du Panorama secondaire en tant que collecteur managé au Panorama principal.

STEP 3 | Modifiez le collecteur de journaux qui est local pour le Panorama principal.

Utilisez l'interface Web du Panorama principal pour effectuer ces étapes :

1. Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** et sélectionnez le collecteur de journaux par défaut (local).
2. Sélectionnez **Disks (Disques)** et **Add (Ajoutez)** chaque paire de disques.
3. Cliquez sur **OK** pour enregistrer vos modifications.

© 2020 Palo Alto Networks, Inc.

STEP 4 | Configurez le collecteur de journaux qui est local pour le Panorama secondaire.

Panorama traite ce collecteur de journaux comme distant, parce qu'il n'est pas local au Panorama principal. C'est pourquoi vous devez l'ajouter manuellement sur le Panorama principal.

Utilisez l'interface Web du Panorama principal pour configurer un collecteur géré :

1. Sélectionnez **Panorama (Panorama)** > **Managed Collectors (Collecteurs gérés)** et **Add (ajoutez)** le collecteur de journaux.
2. Saisissez le numéro de série (**Collector S/N (N° de série du collecteur)**) que vous avez enregistré pour le collecteur de journaux du Panorama secondaire.
3. Entrez l'adresse IP ou le nom de domaine complet des homologues HD Panorama principaux et secondaires dans les champs **Panorama Server IP (IP serveur Panorama)** et **Panorama Server IP 2 (IP serveur Panorama 2)** respectivement.

   Ces deux champs sont obligatoires.
4. Sélectionnez **Interfaces** et configurez chaque interface que le collecteur de journaux utilisera. L'interface **Management (Gestion)** est nécessaire. Exécutez les étapes suivantes pour chaque interface :
   1. Cliquez sur le nom de l'interface.
   2. Configurez un ou les deux des ensembles de champs suivants selon les protocoles IP de votre réseau.

      IPv4 : **IP Address (Adresse IP)**, **Netmask (Masque de sous-réseau)** et **Default Gateway (Passerelle par défaut)**

      IPv6 : **IPv6 Address/Prefix Length (Longueur du préfixe / de l'adresse IPv6)** et **Default IPv6 Gateway (Passerelle IPv6 par défaut)**
   3. (Interface de gestion uniquement) Sélectionnez **SNMP** si vous utilisez un gestionnaire SNMP pour surveiller les statistiques du collecteur de journaux.

      L'utilisation de SNMP nécessite des étapes supplémentaires en plus de la configuration du collecteur de journaux (voir Surveiller Panorama et les statistiques des collecteurs de journaux en utilisant SNMP).
   4. Cliquez sur **OK** pour enregistrer vos modifications d'interface.
5. Cliquez sur **OK** pour enregistrer les modifications au collecteur de journaux.
6. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

   Cette étape est requise avant de pouvoir activer les disques de journalisation.
7. Modifiez le collecteur de journaux en cliquant sur son nom.
8. Sélectionnez **Disks (Disques)** et **Add (Ajoutez)** chaque paire de disques RAID, puis cliquez sur **OK**.
9. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

STEP 5 | Ajouter un pare-feu en tant que périphérique géré.

Utilisez l'interface Web du Panorama principal pour effectuer cette tâche pour chaque pare-feu qui transmettra les journaux aux collecteurs de journaux.

STEP 6 | Modifier le collecteur de journaux qui est prédéfini pour le Panorama principal.

Utilisez l'interface Web du Panorama principal pour configurer un groupe de collecteurs :

1. Sélectionnez **Panorama** > **Collectors Groups (Groupes de collecteurs)** et modifiez le groupe de collecteurs **default (Par défaut)**.

© 2020 Palo Alto Networks, Inc.

2. **Add (Ajoutez)** le collecteur de journaux local du Panorama secondaire à la liste des membres du groupe de collecteurs si vous ajoutez plusieurs collecteurs de journaux à un seul groupe de collecteurs. Par défaut, la liste affiche le collecteur de journaux local du Panorama principal parce qu'il est pré-attribué au groupe de collecteurs par défaut.

   Dans un même groupe de collecteurs, tous les collecteurs de journaux doivent être exécutés sur le même modèle Panorama : uniquement des appareils M-600, uniquement des appareils M-500, uniquement des appareils M-200 ou uniquement des appareils virtuels Panorama.
3. (Recommandé) **Enable log redundancy across collectors (Activez la redondance des journaux entre les collecteurs)** si vous ajoutez plusieurs collecteurs de journaux à un seul groupe de collecteurs. Cette option nécessite que chaque collecteur de journaux ait le même nombre de disques de journalisation.
4. (Facultatif) Sélectionnez **Monitoring (Surveillance)** et configurez les paramètres si vous allez utiliser SNMP pour surveiller les statistiques des collecteurs de journaux et les interruptions.
5. Sélectionnez **Device Log Forwarding (Transfert de journaux du périphérique)** et configurez la liste des préférences de transfert de journaux. Cette liste définit quels pare-feu transmettent les journaux à quels collecteurs de journaux. Affectez des pare-feu selon le nombre de collecteurs de journaux que contient ce groupe de collecteurs :
   - **Unique** : assignez les pare-feu qui transmettront les journaux au collecteur de journaux local du Panorama principal, comme illustré dans Collecteur de journaux local unique par groupe de collecteurs.
   - **Plusieurs** : assignez chaque pare-feu aux deux collecteurs de journaux pour la redondance. Lorsque vous configurez les préférences, donnez la première priorité au collecteur de journaux 1 pour la moitié des pare-feu et donnez la première priorité au collecteur de journaux 2 pour l'autre moitié des pare-feu, comme illustré dans Plusieurs collecteurs de journaux locaux par groupe de collecteurs.
6. Cliquez sur **OK** pour enregistrer vos modifications.

STEP 7 | Configurez un groupe de collecteurs contenant le collecteur de journaux du Panorama secondaire.

Requis si chaque groupe de collecteurs n'a qu'un seul collecteur de journaux.

Utilisez l'interface Web du Panorama principal pour configurer un groupe de collecteurs :

1. Sélectionnez **Panorama (Panorama)** > **Collector Groups (Groupes de Collecteurs)** et **Add (ajoutez)** le groupe de collecteurs.
2. Entrez un **Name (Nom)** pour identifier le domaine d'accès.
3. **Add (Ajoutez)** le collecteur de journaux local du Panorama secondaire à la liste des membres du groupe de collecteurs.
4. (Facultatif) Cliquez sur l'onglet **Monitoring (Surveillance)** et configurez les paramètres si vous allez utiliser un gestionnaire SNMP pour surveiller les statistiques des collecteurs de journaux et les interruptions.
5. Sélectionnez **Device Log Forwarding (Transfert de journaux du périphérique)** et **Add (Ajoutez)** une entrée dans la liste des préférences de transfert de journaux.
   1. **Modify (Modifiez)** la liste des périphériques, sélectionnez les pare-feu qui transmettent les journaux vers le collecteur de journaux local du Panorama secondaire (voir Collecteur de journal local unique par groupe de collecteurs), et cliquez sur **OK**.
   2. **Add (Ajoutez)** le collecteur de journaux local du Panorama secondaire à la liste des collecteurs et cliquez sur **OK**.
6. Cliquez sur **OK** pour enregistrer vos modifications.

© 2020 Palo Alto Networks, Inc.

STEP 8 | Validez et modifiez vos modifications à la configuration Panorama et aux groupes de collecteurs.

Dans l'interface Web du Panorama principal, sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)**, puis **Commit and Push (Valider et appliquer)** vos modifications à Panorama et aux groupes de collecteurs que vous avez ajoutés.

STEP 9 | Opérez un basculement manuel pour que le Panorama secondaire devienne actif.

Utilisez l'interface Web du Panorama principal pour effectuer les étapes suivantes :

1. Sélectionnez **Panorama** > **High Availability (Haute Disponibilité)**.
2. Cliquez sur **Suspend local Panorama (Suspendre le Panorama local)** dans la section de commandes opérationnelles.

STEP 10 | Sur le Panorama secondaire, configurez les paramètres réseau du collecteur de journaux qui est local sur le Panorama principal.

Utilisez l'interface Web du Panorama secondaire pour effectuer les étapes suivantes :

1. Dans l'interface Web Panorama, sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** et sélectionnez le collecteur de journaux qui est local sur le Panorama principal.
2. Entrez l'adresse IP ou le nom de domaine complet des homologues HD Panorama principaux et secondaires dans les champs **Panorama Server IP (IP serveur Panorama)** et **Panorama Server IP 2 (IP serveur Panorama 2)** respectivement.

   Ces deux champs sont obligatoires.
3. Sélectionnez **Interfaces**, cliquez sur **Management (Gestion)** et remplissez un ou les deux ensembles de champs suivants (selon les protocoles IP de votre réseau) avec les valeurs d'interface de gestion du Panorama principal :
   - **IPv4** : **IP Address (Adresse IP)**, **Netmask (Masque de sous-réseau)** et **Default Gateway (Passerelle par défaut)**
   - **IPv6** : **IPv6 Address/Prefix Length (Longueur du préfixe / de l'adresse IPv6)** et **Default IPv6 Gateway (Passerelle IPv6 par défaut)**
4. Cliquez sur **OK** pour enregistrer vos modifications.
5. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)**, puis **Commit and Push (Valider et appliquer)** vos modifications à Panorama et aux groupes de collecteurs que vous avez ajoutés.

STEP 11 | Opérez un basculement manuel pour que le Panorama principal devienne actif.

Utilisez l'interface Web du Panorama secondaire pour effectuer les étapes suivantes :

1. Sélectionnez **Panorama** > **High Availability (Haute Disponibilité)**.
2. Cliquez sur **Suspend local Panorama (Suspendre le Panorama local)** dans la section de commandes opérationnelles.

STEP 12 | Configurez le transfert de journaux depuis les pare-feu vers Panorama.

Utilisez l'interface Web du serveur de gestion du Panorama principal pour :

1. Configurer le transfert des journaux vers Panorama.
2. Vérifier le transfert des journaux vers Panorama.
3. (Facultatif) Configurer le transfert de journal de Panorama vers des destinations externes.



Vous pouvez affecter des profils de serveur externes distincts à chaque homologue HD de Panorama. Par exemple, vous pouvez vouloir que chaque homologue HD transmette les journaux à un serveur syslog différent. Pour que chaque paire

© 2020 Palo Alto Networks, Inc.

Panorama transfère les journaux vers différents services externes, connectez-vous à l'interface Web de chaque paire, sélectionnez Panorama (Panorama) > Collector Groups (Groupes de collecteurs), sélectionnez le groupe de collecteurs, sélectionnez Collector Log Forwarding (Transfert de journal des collecteurs), affectez les profils du serveur et cliquez sur OK (OK).

Déployer les appareils virtuels Panorama avec les collecteurs de journaux locaux

Vous pouvez configurer des pare-feu pour envoyer des journaux à un collecteur de journaux qui s'exécute localement sur un appareil virtuel Panorama en mode Panorama. Dans une configuration haute disponibilité (HD), chaque homologue HD peut avoir un collecteur de journaux local. Vous pouvez affecter les collecteurs de journaux locaux sur les homologues HD au même groupe de collecteurs ou séparer les groupes de collecteurs, comme illustré dans les figures suivantes. Reportez-vous au Définir la configuration requise pour l'appareil virtuel Panorama pour consulter le nombre de logs par seconde supporté lors du déploiement de l'appareil virtuel Panorama avec des collecteurs de journaux locaux dans une infrastructure virtuelle VMware.

Si vous affectez plus d'un collecteur de journaux à un groupe de collecteurs, consultez Mises en garde pour un groupe de collecteurs comportant plusieurs collecteurs de journaux *pour comprendre les exigences, les risques et les mesures d'atténuation recommandées.*

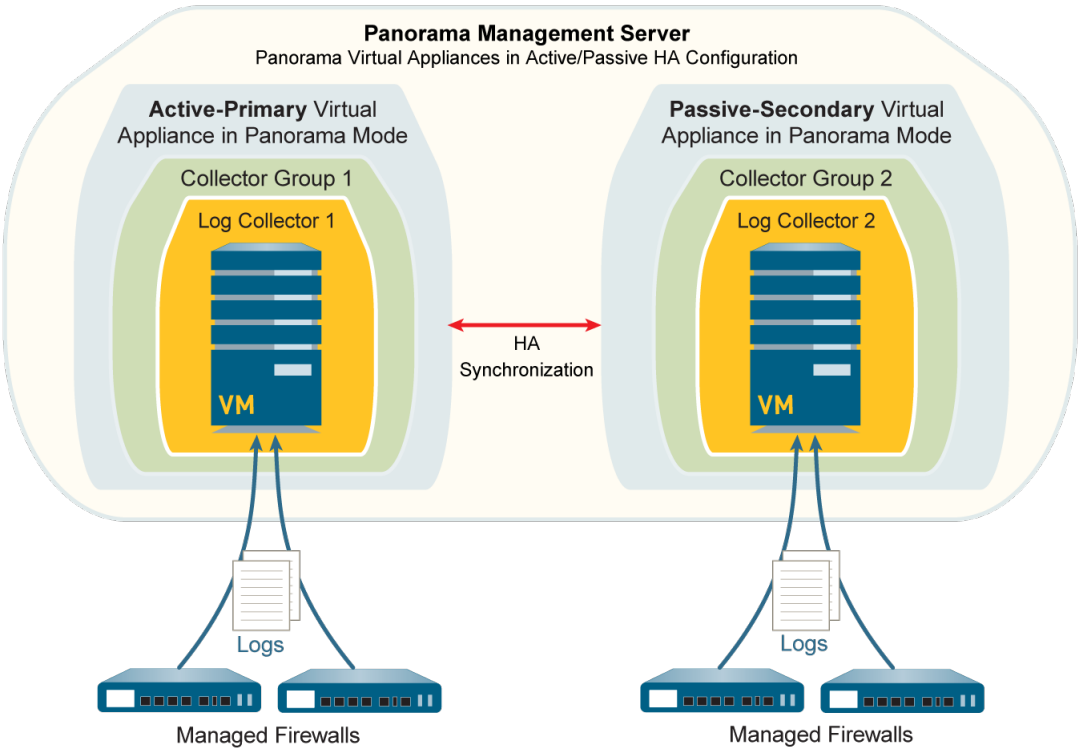


Figure 21: Collecteur de journaux unique par groupe de collecteurs

© 2020 Palo Alto Networks, Inc.

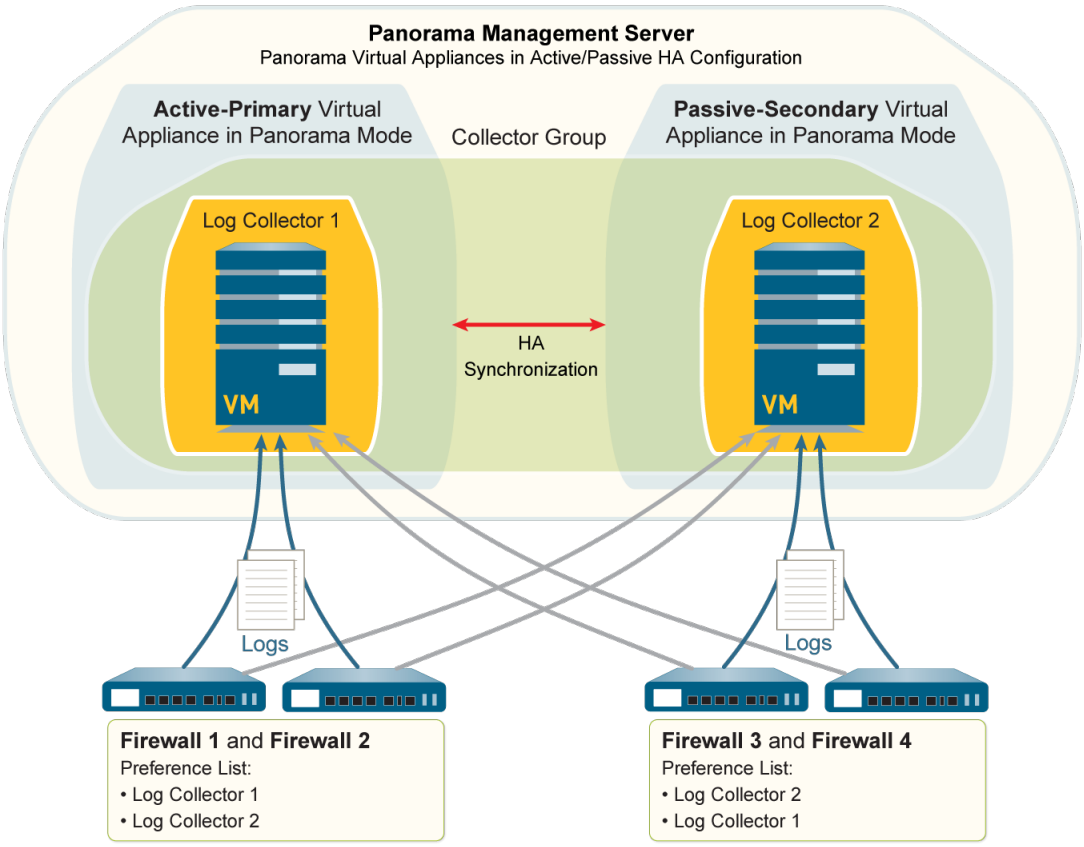


Figure 22: Plusieurs collecteurs de journaux par groupe de collecteurs

Effectuez les étapes suivantes pour déployer Panorama avec des collecteurs de journaux locaux. Ignorez les étapes que vous avez déjà effectuées (par exemple, la configuration initiale).

STEP 1 | Effectuez la configuration initiale de chaque application virtuelle Panorama.

1. Installez l'application virtuelle Panorama. Vous devez configurer les ressources suivantes pour vous assurer que l'appareil virtuel démarre en mode Panorama :
   - Disque système avec exactement 81 Go de stockage.
   - Processeurs et mémoire suffisants pour la quantité de journaux que Panorama va recevoir et stocker.
   - Disque de journalisation virtuel avec 2 à 24 To de stockage.

   Panorama divise automatiquement le nouveau disque en partitions de 2 To, chacune fonctionnant comme un disque virtuel distinct.
2. Effectuez la configuration initiale de l'application virtuelle Panorama.
3. Enregistrer Panorama et installer les licences.
4. Installer les mises à jour de contenu et logicielles pour Panorama.

STEP 2 | Placez les appareils virtuels Panorama dans une configuration HD.

1. Définir la HD (haute disponibilité) sur Panorama.
2. Testez le basculement HD de Panorama.

STEP 3 | Ajoutez un collecteur de journaux qui est local pour le Panorama principal.

Sur le Panorama principal :

© 2020 Palo Alto Networks, Inc.

1. Enregistrez le numéro de série de Panorama.
    1. Accédez à l'interface Web de Panorama.
    2. Sélectionnez **Dashboard (Tableau de bord)** et enregistrez le **Serial # (Numéro de série)** dans la section General Information section (Informations générales).
2. Ajoutez le collecteur de journaux en tant que collecteur géré.
    1. Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** et **Add (Ajoutez)** un nouveau collecteur de journaux.
    2. Dans les paramètres **General (Général)**, saisissez le numéro de série (**Collector S/N (N° de série du collecteur)**) que vous avez enregistré pour Panorama.
    3. Cliquez sur **OK** pour enregistrer vos modifications.
    4. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)**.

        Cette étape est requise avant de pouvoir ajouter les disques de journalisation virtuels.
3. Ajoutez les disques de journalisation virtuels.
    1. Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** et modifiez le collecteur de journaux en cliquant sur son nom.

        Le nom du collecteur de journaux a la même valeur que le nom d'hôte du Panorama principal.
    2. Sélectionnez **Disks (Disques)** et **Add (Ajoutez)** les disques de journalisation virtuels.
    3. Cliquez sur **OK** pour enregistrer vos modifications.
    4. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)**.

STEP 4 | Ajoutez un collecteur de journaux qui est local pour le Panorama secondaire.



Panorama traite ce collecteur de journaux comme distant, car il ne s'exécute pas localement sur le Panorama principal.

1. Enregistrez le numéro de série du Panorama secondaire.
    1. Accédez à l'interface Web du Panorama secondaire.
    2. Sélectionnez **Dashboard (Tableau de bord)** et enregistrez le **Serial # (Numéro de série)** dans la section General Information section (Informations générales).
2. Accédez à l'interface Web du Panorama principal.
3. Sélectionnez **Panorama (Panorama)** > **Managed Collectors (Collecteurs gérés)** et **Add (ajoutez)** le collecteur de journaux.
4. Dans les paramètres **General (Général)**, saisissez le numéro de série (**Collector S/N (N° de série du collecteur)**) que vous avez enregistré pour le Panorama secondaire.
5. Entrez l'adresse IP ou le nom de domaine complet des homologues HD Panorama principaux et secondaires dans les champs **Panorama Server IP (IP serveur Panorama)** et **Panorama Server IP 2 (IP serveur Panorama 2)** respectivement.

    Ces deux champs sont obligatoires.
6. Cliquez sur **OK** pour enregistrer les modifications au collecteur de journaux.
7. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

    Cette étape est requise avant de pouvoir ajouter les disques de journalisation virtuels.
8. Modifiez le collecteur de journaux en cliquant sur son nom.

    Le nom du collecteur de journaux a la même valeur que le nom d'hôte du Panorama secondaire.
9. Sélectionnez **Disks (Disques)**, **Add (Ajoutez)** les disques de journalisation virtuels, et cliquez **OK**.
10. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

© 2020 Palo Alto Networks, Inc.

STEP 5 | Ajouter un pare-feu en tant que périphérique géré.

Utilisez l'appareil Panorama principal pour effectuer cette tâche pour chaque pare-feu qui transmettra les journaux aux collecteurs de journaux.

STEP 6 | Configurez le groupe de collecteurs.

Effectuez cette étape une seule fois si vous affectez les deux collecteurs de journaux au même groupe de collecteurs. Sinon, configurez un groupe de collecteurs pour chaque collecteur de journaux.

Sur le Panorama principal :

1. Sélectionnez **Panorama** > **Collector Groups (Groupes de collecteurs)** et **Add (Ajoutez)** un groupe de collecteurs.
2. **Add (Ajoutez)** un ou les deux collecteurs de journaux en tant que membres du groupe de collecteurs.

   Dans un même groupe de collecteurs, tous les collecteurs de journaux doivent être exécutés sur le même modèle Panorama : uniquement des appareils M-600, uniquement des appareils M-500, uniquement des appareils M-200 ou uniquement des appareils virtuels Panorama.
3. (Recommandé) **Enable log redundancy across collectors (Activez la redondance des journaux entre les collecteurs)** si vous ajoutez plusieurs collecteurs de journaux à un seul groupe de collecteurs. Cette option nécessite que chaque collecteur de journaux ait le même nombre de disques de journalisation virtuels.

   L'activation de la redondance double la quantité de journaux et le trafic de traitement des journaux dans un groupe de collecteurs. Si nécessaire, augmentez la capacité de stockage de journaux sur l'appareil virtuel Panorama.
4. Sélectionnez **Device Log Forwarding (Transfert de journaux du périphérique)** et configurez la liste des préférences de transfert de journaux. Cette liste définit quels pare-feu transmettent les journaux à quels collecteurs de journaux. Affectez des pare-feu selon le nombre de collecteurs de journaux que contient ce groupe de collecteurs :
   - **Unique** : assignez les pare-feu qui transmettront les journaux au collecteur de journaux local du Panorama principal, comme illustré dans Collecteur de journaux local unique par groupe de collecteurs.
   - **Plusieurs** : assignez chaque pare-feu aux deux collecteurs de journaux pour la redondance. Lorsque vous configurez la liste de préférences, donnez la première priorité au collecteur de journaux 1 pour la moitié des pare-feu et donnez la première priorité au collecteur de journaux 2 pour l'autre moitié des pare-feu, comme illustré dans Multiple collecteurs de journaux dédiés par groupe de collecteurs.
5. Cliquez sur **OK** pour enregistrer vos modifications.
6. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)**, puis **Commit and Push (Valider et appliquer)** vos modifications à Panorama et aux groupes de collecteurs que vous avez ajoutés.

STEP 7 | Déclenchez le basculement sur l'appareil Panorama principal pour que l'appareil Panorama secondaire devienne actif.

Sur le Panorama principal :

1. Sélectionnez **Panorama** > **High Availability (Haute Disponibilité)**.
2. Cliquez sur **Suspend local Panorama (Suspendre le Panorama local)** dans la section de commandes opérationnelles.

STEP 8 | Configurer la connexion depuis le Panorama secondaire vers le collecteur de journaux qui est local sur le Panorama principal.

© 2020 Palo Alto Networks, Inc.

Sur le Panorama secondaire :

1. Dans l'interface Web Panorama, sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** et sélectionnez le collecteur de journaux qui est local sur le Panorama principal.
2. Entrez l'adresse IP ou le nom de domaine complet des homologues HD Panorama principaux et secondaires dans les champs **Panorama Server IP (IP serveur Panorama)** et **Panorama Server IP 2 (IP serveur Panorama 2)** respectivement.

   Ces deux champs sont obligatoires.
3. Cliquez sur **OK** pour enregistrer vos modifications.
4. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)**, puis **Commit and Push (Valider et appliquer)** vos modifications à Panorama et aux groupes de collecteurs.

STEP 9 | Déclenchez la restauration sur le Panorama secondaire pour que le Panorama principal devienne actif.

Sur le Panorama secondaire :

1. Sélectionnez **Panorama** > **High Availability (Haute Disponibilité)**.
2. Cliquez sur **Suspend local Panorama (Suspendre le Panorama local)** dans la section de commandes opérationnelles.

STEP 10 | Configurez le transfert de journaux depuis les pare-feu vers Panorama.

Sur le Panorama principal pour :

1. Configurer le transfert des journaux vers Panorama à partir du pare-feu.
2. Vérifier le transfert des journaux vers Panorama.

Déployer les appareils virtuels Panorama en mode hérité avec la collecte de journaux locale

La figure suivante illustre Panorama dans un déploiement de collecte de journaux centralisée. Dans cet exemple, le serveur de gestion Panorama comprend deux applications virtuelles Panorama en mode hérité qui sont déployées dans une configuration active / passive haute disponibilité (HD). Cette configuration convient pour la gestion de pare-feu dans une infrastructure virtuelle VMware dans laquelle Panorama traite jusqu'à 10 000 journaux/seconde. Les pare-feu envoient des journaux au magasin de données NFS (serveur ESXi uniquement) ou au disque virtuel sur le serveur de gestion Panorama. Par défaut, les homologues actifs et passifs reçoivent les journaux, même si vous pouvez modifier les paramètres de transfert de journaux et de la mémoire tampon par défaut afin que seul l'homologue actif ne les reçoive. Pour les pare-feu des séries PA-7000 et PA-5200, seul l'homologue actif reçoit les journaux. Par défaut, l'application virtuelle Panorama en mode hérité utilise approximativement 11 Go sur sa partition de disque interne pour le stockage des journaux, bien que vous puissiez augmenter la capacité de stockage de journaux sur l'appareil virtuel Panorama si nécessaire.

Si le taux de journalisation dépasse 10 000 journaux par seconde, il vous est recommandé de déployer Panorama avec des collecteurs de journaux dédiés.

© 2020 Palo Alto Networks, Inc.

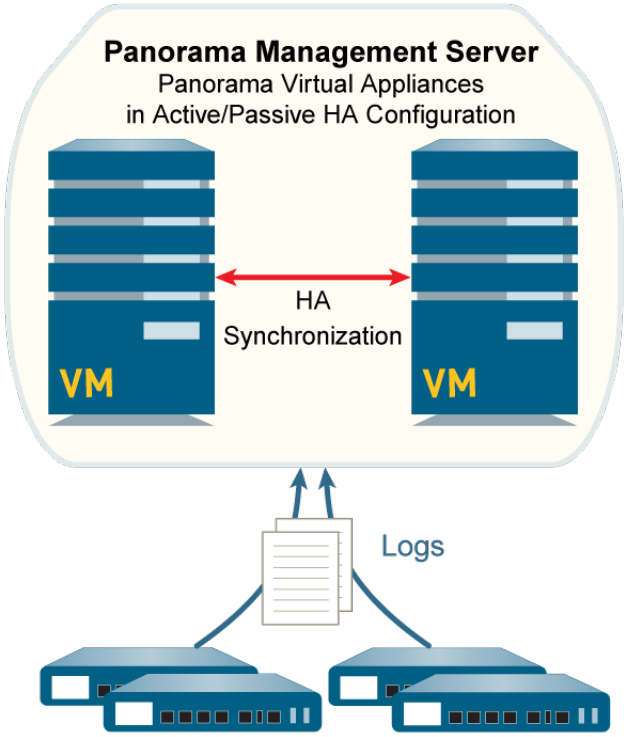


Figure 23: Appareils virtuels Panorama en mode hérité avec la collecte de journaux locale

Effectuez les étapes suivantes pour déployer les applications virtuelles Panorama avec collecte des journaux. Ignorez les étapes que vous avez déjà effectuées (par exemple, la configuration initiale).

STEP 1 | Effectuez la configuration initiale de chaque application virtuelle Panorama.

1. Installez l'application virtuelle Panorama. Pour vous assurer que l'appareil virtuel démarre en mode Panorama, n'ajoutez pas de disque de journalisation virtuel lors de l'installation.

   Par défaut, Panorama utilise une partition de 11 Go sur son disque système pour le stockage des journaux. Si vous souhaitez plus de stockage, vous pouvez ajouter un disque de journalisation virtuel dédié de 8 To maximum après l'installation.
2. Effectuez la configuration initiale de l'application virtuelle Panorama.
3. Enregistrer Panorama et installer les licences.
4. Installer les mises à jour de contenu et logicielles pour Panorama.

STEP 2 | Placez les appareils virtuels Panorama dans une configuration HD.

1. Définir la HD (haute disponibilité) sur Panorama.
2. Testez le basculement HD de Panorama.

STEP 3 | Effectuez les étapes suivantes pour préparer Panorama pour la collecte de journaux.

1. Ajoutez un pare-feu comme un périphérique géré pour chacune qui transmettra les journaux à Panorama.
2. Configurer le transfert des journaux vers Panorama.

STEP 4 | Validez vos modifications.

Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

© 2020 Palo Alto Networks, Inc.

Gérer les appareils WildFire

Vous pouvez gérer jusqu'à 200 appareils WildFire autonomes et nœuds de cluster d'appareils WildFire centralisés à l'aide d'un appareil Panorama de série M ou virtuel. Par rapport à la gestion individuelle des appareils et des clusters d'appareils WildFire à l'aide de la CLI locale, l'utilisation de Panorama permet une gestion et une surveillance centralisées de plusieurs appareils et clusters d'appareils. La gestion centralisée vous permet d'appliquer des configurations courantes, des mises à jour de configuration et des mises à niveau logicielles à tout ou partie des appareils WildFire gérés, ce qui facilite la configuration uniforme des appareils et des clusters d'appareils WildFire.

Lorsque vous utilisez Panorama pour gérer des clusters d'appareils WildFire, Panorama doit exécuter une version égale ou ultérieure à celle des appareils WildFire gérés.

- Ajouter des appareils WildFire autonomes à gérer avec Panorama
- Configurer les paramètres de l'appareil WildFire de base sur Panorama
- Configurer l'authentification à l'aide de certificats personnalisés sur les appareils et clusters WildFire
- Supprimer un appareil WildFire de la gestion Panorama
- Gérer les clusters Wildfire

© 2020 Palo Alto Networks, Inc.

Ajouter des appareils WildFire autonomes à gérer avec Panorama

Vous pouvez gérer jusqu'à 200 appareils WildFire avec un appareil Panorama virtuel ou de série M. La limite de 200 appareils WildFire correspond au total combiné des nœuds de cluster des appareils WildFire et autonomes (si vous configurez un cluster et ajoutez des nœuds sur Panorama).

Assurez-vous que Panorama exécute au moins la version 8.0.1 et que tout appareil WildFire que vous ajoutez à Panorama exécute également au moins la version 8.0.1.

STEP 1 | À l'aide de l'interface de ligne de commande locale, vérifiez que chaque appareil WildFire que vous souhaitez gérer avec Panorama exécute PAN-OS 8.0.1 ou version ultérieure.

```
admin@qa16> show system info | match version
sw-version: 8.0.1-c45
wf-content-version: 702-283
logdb-version: 8.0.15
```

STEP 2 | Sur chaque appareil Panorama que vous souhaitez utiliser pour gérer les appareils WildFire, vérifiez que Panorama exécute la version 8.0.1 ou ultérieure :

Dashboard (Tableau de bord) > **General Information (Informations générales)** > **Software Version (Version du logiciel)** affiche la version du logiciel en cours d'exécution.

STEP 3 | Si vous n'êtes pas sûr si un appareil WildFire appartient à un cluster d'appareils WildFire ou est un appareil autonome sur la CLI de l'appareil WildFire local, vérifiez **`Node mode`** pour vous assurer que le statut est **`stand_alone`**, et vérifiez **`Application status`** pour vous assurer que **`global-db-service`** et **`global-file-service`** indiquent **`ReadyStandalone`**.

```
admin@WF-500> show cluster membership
Service Summary:  wfpc signature
Cluster name:
Address:          10.10.10.100
Host name:        WF-500
Node name:        wfpc-012345678901-internal
Serial number:    012345678901
Node mode:     stand_alone
Server role:      True
HA priority:
Last changed:     Mon, 06 Mar 2017 16:34:25 -0800
Services:         wfcore signature wfpc infra
Monitor status:
                  Serf Health Status: passing
                      Agent alive and reachable
Application status:
                  global-db-service: ReadyStandalone
        wildfire-apps-service: Ready
        global-queue-service: ReadyStandalone
        wildfire-management-service: Done
        siggen-db: ReadyMaster
Diag report:
                  10.10.10.100: reported leader '10.10.10.100', age 0.
                  10.10.10.100: local node passed sanity check.
```


© 2020 Palo Alto Networks, Inc.

STEP 4 | Si les appareils WildFire que vous souhaitez gérer avec Panorama sont nouveaux, consultez Premiers pas avec WildFire pour vous assurer que vous effectuez les étapes de base, telles que la confirmation de l'activation de votre licence WildFire, l'activation de la journalisation, la connexion de pare-feu aux appareils WildFire et la configuration des fonctionnalités de base de WildFire.

STEP 5 | Sur la CLI locale de chaque appareil WildFire que le serveur Panorama gérera, configurez l'adresse IP du serveur Panorama.

Avant d'enregistrer des appareils WildFire autonomes sur un appareil Panorama, vous devez d'abord configurer l'adresse IP de Panorama ou le nom de domaine complet sur chaque appareil WildFire. C'est ainsi que chaque appareil WildFire sait quel appareil Panorama le gère.

1. Configurez l'adresse IP ou le nom de domaine complet de l'interface de gestion de l'appareil Panorama principal :

```
admin@WF-500# set deviceconfig system panorama-server <ip-address | FQDN>
```

2. Si vous utilisez un appareil Panorama de sauvegarde pour une haute disponibilité (recommandé), configurez l'adresse IP ou le nom de domaine complet de l'interface de gestion de l'appareil Panorama de sauvegarde :

```
admin@WF-500# set deviceconfig system panorama-server-2 <ip-address |
 FQDN>
```

STEP 6 | Enregistrez les appareils WildFire sur l'appareil Panorama principal.

1. Depuis l'interface Web de Panorama, **Panorama** > **Managed WildFire Appliances (Appareils WildFire gérés)** et **Add Appliance (Ajouter un appareil)**.
2. Saisissez le numéro de série de chaque appareil WildFire sur une ligne séparée. Si vous n'avez pas de liste de numéros de série sur chaque appareil WildFire, exécutez :

```
admin@WF-500> show system info | match serial
serial: 012345678901
```

Plusieurs commandes CLI locales affichent le numéro de série de l'appareil WildFire, notamment **show cluster membership**.

3. Cliquez sur **OK**.

Si elles sont disponibles, les informations sur la configuration déjà validée sur les appareils WildFire s'affichent, telles que l'adresse IP et la version du logiciel.

STEP 7 | (Facultatif) Importer les configurations d'appareils WildFire dans l'appareil Panorama.

1. Sélectionnez les appareils dont vous souhaitez importer les configurations dans la liste des appareils WildFire gérés.
2. **Import Config (Importer la configuration)**.
3. Sélectionnez **Oui**.

L'importation de configurations met à jour les informations affichées et intègre les configurations importées dans la configuration candidate de l'appareil Panorama.

4. **Commit to Panorama (Valider sur Panorama)** pour que les configurations de l'appareil WildFire importées fassent partie de la configuration en cours d'exécution de Panorama.

STEP 8 | Configurez ou confirmez la configuration des interfaces de l'appareil WildFire.

© 2020 Palo Alto Networks, Inc.

L'appareil WildFire dispose de quatre interfaces : **Management (Gestion)** (Ethernet0), **Analysis Network Environment (Environnement de réseau d'analyse)** (Ethernet1), **Ethernet2**, et **Ethernet3**.

1. Sélectionnez **Panorama** > **Managed WildFire Appliances (Appareils WildFire gérés)** et sélectionnez un appareil WildFire.
2. Sélectionnez **Interfaces**.
3. Sélectionnez une interface pour la configurer ou l'éditer. Vous pouvez activer l'interface, définir la vitesse et le duplex, l'adresse IP et le masque de réseau, la passerelle par défaut, le MTU, le serveur DNS, l'état de la liaison et les **Management Services (Services de gestion)** pour chaque interface. Vous pouvez aussi **Add (Ajouter)** adresses IP autorisées de sorte qu'une interface n'accepte que le trafic provenant d'adresses spécifiées.

   Les interfaces **Analysis Network Environment (Environnement de réseau d'analyse)**, **Ethernet2**, et **Ethernet3** prennent uniquement en charge **Ping** comme option de **Management Services (Services de gestion)** .

   L'interface **Management (Gestion)** prend en charge **Ping**, **SSH**, et **SNMP** comme options de **Management Services (Services de gestion)**. En outre, l'interface **Management (Gestion)** prend en charge la configuration du serveur proxy dans le cas où une connexion directe à Internet n'est pas possible.
4. Cliquez sur **OK** après avoir configuré ou confirmé les paramètres.

STEP 9 | Validez la configuration sur l'appareil Panorama et appliquez-la à l'appareil ou à plusieurs appareils.

1. **Commit and Push (Valider et appliquer)**.
2. S'il y a des configurations sur l'appareil Panorama que vous ne voulez pas appliquer, **Edit Selections (Modifier les sélections)** pour choisir les appareils sur lesquels vous appliquez les configurations. La configuration appliquée écrase la configuration en cours d'exécution sur l'appareil WildFire.

STEP 10 | Vérifiez la configuration.

1. Sélectionnez **Panorama** > **Managed WildFire Appliances (Appareils WildFire gérés)**.
2. Vérifiez les champs suivants :
   - **Connected (Connecté)** : l'état est **Connected (Connecté)**.
   - **Role (Rôle)** : le rôle de chaque appareil WildFire est **Standalone (Autonome)**.
   - **Config Status (État de la configuration)** : l'état est `In Sync`.
   - **Last Commit State (État de la dernière validation)** : `Commit succeeded`.

© 2020 Palo Alto Networks, Inc.

Configurer les paramètres de l'appareil WildFire de base sur Panorama

La configuration des paramètres de base tels que la mise à jour du contenu et les serveurs cloud WildFire, les services cloud WildFire, la journalisation, l'authentification, etc. est similaire à la configuration des paramètres de cluster généraux sur Panorama. Au lieu de sélectionner un cluster et de configurer les paramètres sur le cluster, sélectionnez un appareil WildFire et configurez les paramètres individuels de cet appareil. Sélectionnez et configurez chaque appareil WildFire que vous ajoutez à Panorama.

La section Configuration de l'appareil WildFire décrit comment intégrer un appareil WildFire à un réseau et effectuer une configuration de base avec l'interface de ligne de commande, mais les concepts sont identiques à ceux d'une configuration de base avec Panorama.

De nombreux paramètres sont prédéfinis avec des valeurs par défaut, des informations provenant de paramètres existants sur l'appareil WildFire ou les paramètres que vous avez configurés lors de l'ajout de l'appareil WildFire à Panorama.

- Configurer l'authentification pour un appareil WildFire

Configurer l'authentification pour un appareil WildFire

Créez et configurez une meilleure authentification pour votre appareil WildFire en configurant les utilisateurs administratifs locaux à l'aide de paramètres d'authentification granulaires ainsi qu'en exploitant RADIUS, TACAS+ ou LDAP pour l'autorisation et l'authentification.

Lorsque vous configurez et validez les administrateurs depuis Panorama, vous remplacez les administrateurs existants de l'appareil WildFire par ceux que vous configurez dans Panorama.

- Configurez un Compte administratif pour un appareil WildFire.
- Configurer l'authentification RADIUS pour un appareil WildFire
- Configurer l'authentification TACACS + pour un appareil WildFire
- Configurer l'authentification LDAP pour un appareil WildFire

Configurez un Compte administratif pour un appareil WildFire.

Créez un ou plusieurs administrateurs avec des paramètres d'authentification granulaires pour votre appareil WildFire pour le gérer depuis un serveur de gestion Panorama. De plus, vous pouvez configurer les administrateurs locaux depuis Panorama qui peuvent être configurés directement dans le CLI de l'appareil WildFire. Cependant, la validation d'une nouvelle configuration pour passer à l'appareil WildFire remplacera les administrateurs locaux configurés pour l'appareil WildFire.

STEP 1 | Se connecter à l'interface Web Panorama.

STEP 2 | Ajouter des appareils WildFire autonomes à gérer avec Panorama.

STEP 3 | (En option) Configure an authentication profile (Configurez un profil d'authentification) pour définir le service d'authentification qui valide les informations de connexion des administrateurs de qui accèdent au CLI de l'appareil WildFire.

STEP 4 | Configure one or more administrator accounts (Configurez un ou plusieurs comptes administrateurs) selon ce qui est nécessaire.

© 2020 Palo Alto Networks, Inc.

Les comptes administrateurs créés dans Panorama sont ensuite importés vers les appareils WildFire et gérés depuis Panorama.

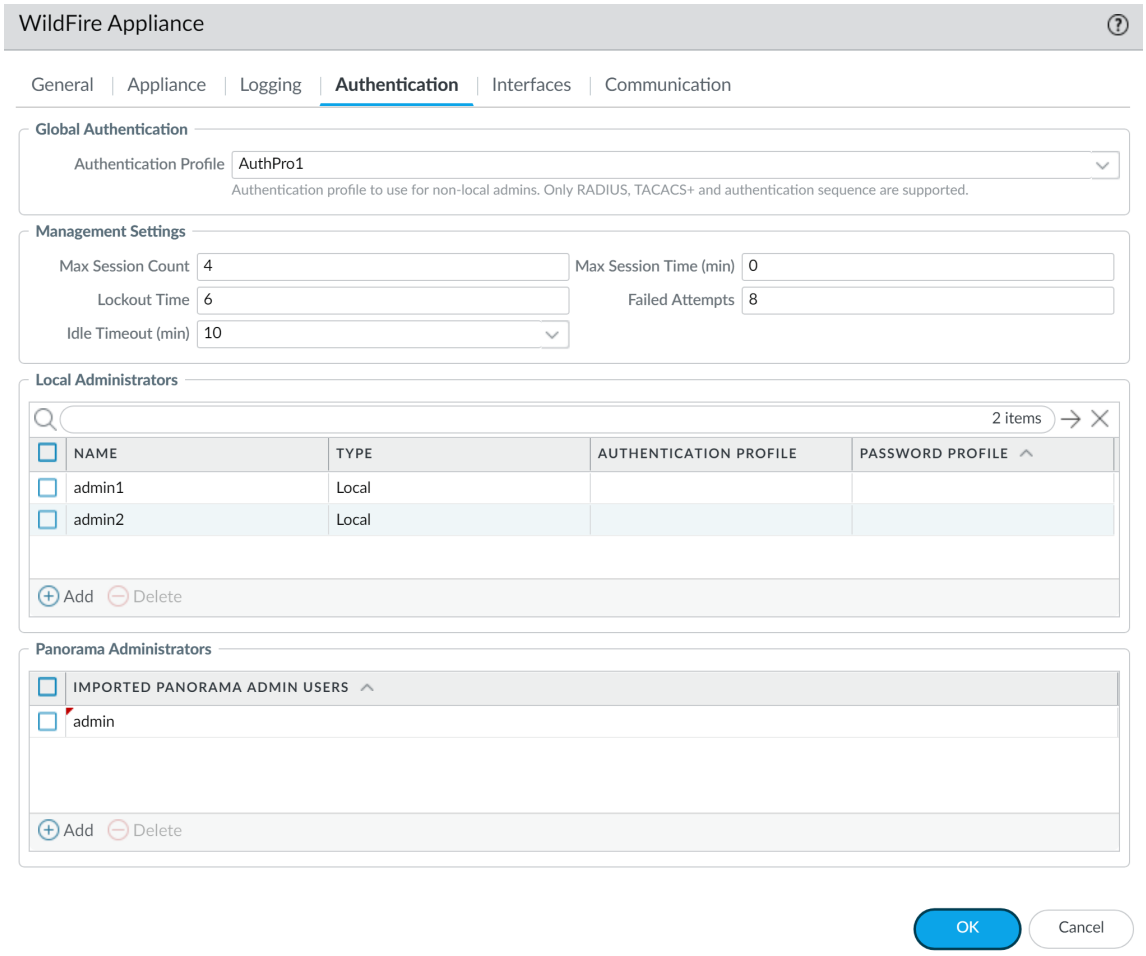
STEP 5 | Configurer l'authentification pour l’appareil WildFire.

1. Sélectionnez**Panorama** > **Managed WildFire Appliance (Appareil WildFire géré)** et sélectionnez l’appareil WildFire géré que vous venez d’ajouter.
2. (En option) Sélectionnez le A**uthentification Profile (Profil d’authentification)** que vous avez configuré au cours des étapes antérieures.
3. Configurez la **Timeout Configuration (Configuration du délai avant expiration)** d’authentification pour l’appareil WildFire.
   1. Saisissez le nombre de **Failed Attempt (Tentatives échouées)** avant que l’accès d’un utilisateur au CLI de l’appareil WildFire ne soit bloqué.
   2. Saisissez la **Lockout Time (Durée de verrouillage)**, en minutes, selon l’appareil WildFire verrouille le compte d’un utilisateur après que celui-ci ait atteint le nombre de **Failed Attempts (Tentatives échouées)** configuré.
   3. Saisissez le **Idle Timeout (délai d'expiration)**, en minutes, avant que le compte de l’utilisateur ne soit automatiquement déconnecté pour inactivité.
   4. Saisissez le **Max Session Count (Compte de session max.)** pour indiquer combien de comptes d’utilisateur peuvent accéder simultanément à l’appareil WildFire.
   5. Saisissez la **Max Session Time (Durée de session max.)** pendant laquelle l’administrateur peut être connecté avant d’être automatiquement déconnecté.
4. Ajoutez les administrateurs de l’appareil WildFire.

   Les administrateurs peuvent soit être ajoutés en tant qu’administrateur local ou en tant qu’administrateur Panorama importé, mais pas les deux. Ajouter le même administrateur en tant qu’administrateur local et en tant qu’administrateur Panorama importé n’est pas possible et peut entraîner une panne de validation de Panorama. Par exemple, la validation de Panorama échoue si vous ajoutez `admin1` en tant qu’administrateur local et administrateur Panorama.

   1. **Add (Ajoutez)** et configurez de nouveaux administrateurs uniques pour l’appareil WildFire. Ces administrateurs sont spécifiques à l’appareil WildFire pour lequel ils sont créés et vous gérez ces administrateurs depuis ce tableau.
   2. **Add (Ajoutez)** n’importe quel administrateur configuré dans Panorama. Ces administrateurs sont créés dans Panorama et importés vers l’appareil WildFire.
5. Cliquez sur **OK** pour enregistrer la configuration de l’authentification de l’appareil WildFire.

© 2020 Palo Alto Networks, Inc.



STEP 6 | **Commit (Validez)** et **Commit and Push (Validez et appliquez)** les modifications de votre configuration.

STEP 7 | Access the WildFire appliance CLI (Accédez au CLI de l'appareil WildFire) afin de pouvoir vérifier que vous pouvez accéder à l'appareil WildFire en utilisant l'utilisateur admin local.

Configurer l'authentification RADIUS pour un appareil WildFire

Utilisez RADIUS pour authentifier l'accès administratif à la CLI de l'appareil WildFire. Vous pouvez également définir des attributs spécifiques au fournisseur (VSA) sur le serveur RADIUS pour gérer l'autorisation de l'administrateur. L'utilisation de VSA vous permet de changer les rôles rapidement, d'accéder aux domaines et aux groupes d'utilisateurs à travers votre service d'annuaire au lieu de reconfigurer les réglages dans le serveur de gestion Panorama™.

Vous pouvez importer le dictionnaire RADIUS de Palo Alto Networks dans le serveur RADIUS pour définir les attributs d'authentification nécessaires pour la communication entre Panorama et le serveur RADIUS.

STEP 1 | Se connecter à l'interface Web Panorama.

STEP 2 | Ajouter des appareils WildFire autonomes à gérer avec Panorama.

© 2020 Palo Alto Networks, Inc.

STEP 3 | Configuration de l'authentification RADIUS

1. Ajoutez un profil de serveur RADIUS.

   Le profil définit comment l'appareil WildFire se connecte au serveur RADIUS.

   1. Sélectionnez **Panorama** > **Server Profiles (Profils de serveur)** > **RADIUS** et **Add (Ajoutez)** un profil.
   2. Saisissez un **Profile Name (Nom de profil)** pour identifier le profil de serveur.
   3. Saisissez l'intervalle du **Timeout (Délai d'expiration)**, en secondes, après lequel une requête d'authentification arrive à expiration (plage de 1 à 20 ; par défaut 3).
   4. Sélectionnez l'**Authentication Protocol (Protocole d'authentification)** (par défaut, **CHAP**) que l'appareil WildFire utilise pour s'authentifier au serveur RADIUS.

      Sélectionnez CHAP si le serveur RADIUS prend en charge ce protocole ; il est plus sécuritaire que PAP.

   5. **Add (Ajoutez)** chaque serveur RADIUS et saisissez les renseignements suivants :

      1. Le **Name (Nom)** qui permet d'identifier le serveur.
      2. L'adresse IP ou le FQDN du **RADIUS Server (Serveur RADIUS)**.
      3. Le **Secret/Confirm Secret (Phrase secrète / Confirmer une phrase secrète)**, une clé pour chiffrer les noms d'utilisateur et les mots de passe.
      4. Le **Port** du serveur pour les demandes d'authentification (1812 par défaut).
   6. Cliquez sur **OK** pour enregistrer le profil de serveur.
2. Affectez le profil de serveur RADIUS à un profil d'authentification.

   Le profil d'authentification définit les paramètres d'authentification qui sont communs à un ensemble d'administrateurs.

   1. Sélectionnez **Panorama** > **Authentication Profile (Profil d'authentification)** et **Add (Ajoutez)** un profil.
   2. Entrez un **Name (Nom)** pour identifier le profil d'authentification.
   3. Définissez le **Type** sur **RADIUS**.
   4. Sélectionnez le **Server Profile (Profil de serveur)** que vous avez créé.
   5. Sélectionnez **Retrieve user group from RADIUS (Récupérer le groupe d'utilisateurs auprès de TACACS+)** pour recueillir de l'information sur le groupe d'utilisateurs auprès des VSA définis sur le serveur TACACS+.

      Panorama fait correspondre l'information sur le groupe avec les groupes que vous avez spécifiés dans la liste d'autorisation du profil d'authentification.
   6. Sélectionnez **Advanced (Avancé)** et, dans la liste d'autorisation, **Add (Ajoutez)** les administrateurs qui sont autorisés à s'authentifier avec ce profil d'authentification.
   7. Cliquez sur **OK** pour enregistrer le profil d'authentification.

STEP 4 | Configurer l'authentification pour l'appareil WildFire.

1. Sélectionnez**Panorama** > **Managed WildFire Appliance (Appareil WildFire géré)** et sélectionnez l'appareil WildFire géré que vous venez d'ajouter.
2. Sélectionnez le **Authentification Profile (Profil d'authentification)** que vous avez configuré au cours des étapes antérieures.

   Si un profil d'authentification global n'est pas attribué, vous devez attribuer un profil d'authentification à chaque administrateur local individuel afin d'exploiter l'authentification à distance.
3. Configurez la **Timeout Configuration (Configuration du délai avant expiration)** d'authentification pour l'appareil WildFire.

   1. Saisissez le nombre de **Failed Attempt (Tentatives échouées)** avant que l'accès d'un utilisateur au CLI de l'appareil WildFire ne soit bloqué.

© 2020 Palo Alto Networks, Inc.

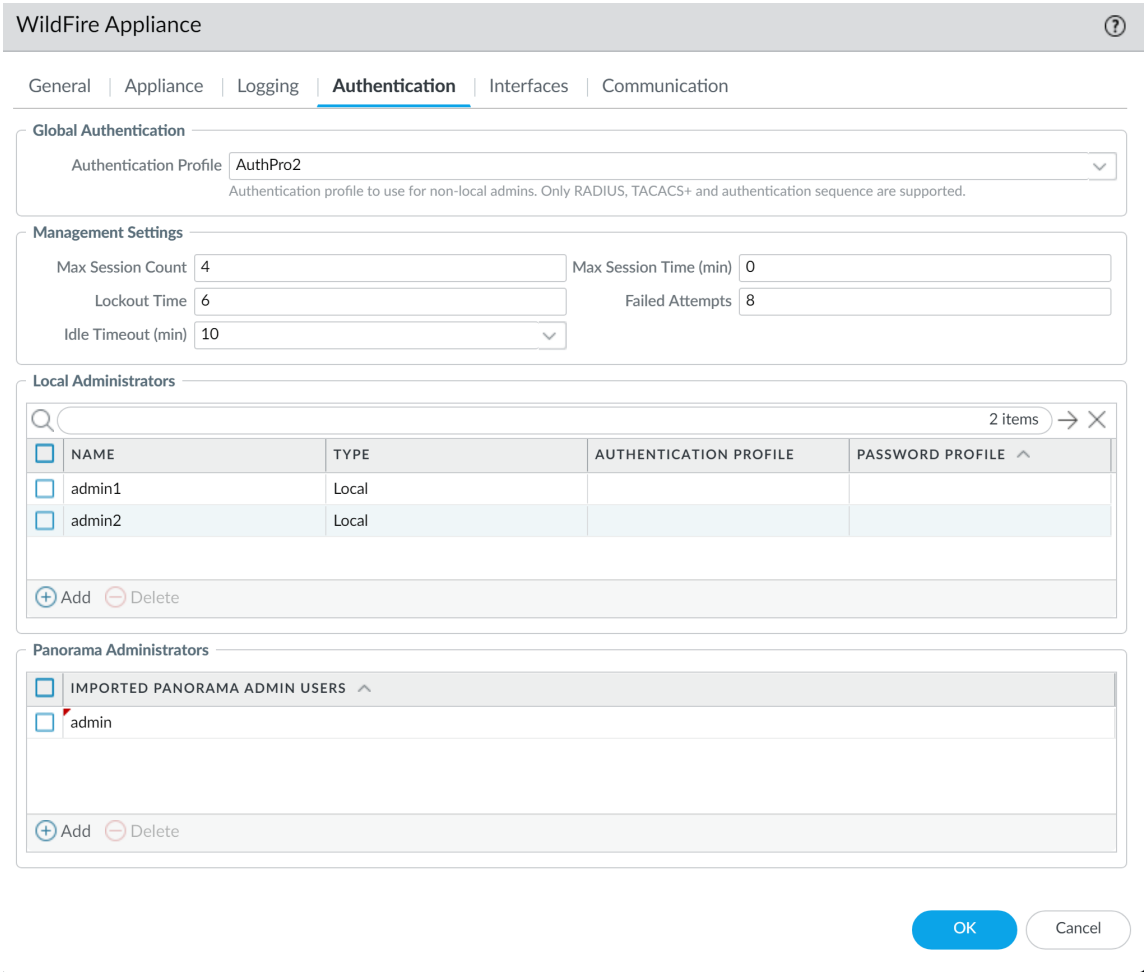
2. Saisissez la **Lockout Time (Durée de verrouillage)**, en minutes, selon l'appareil WildFire verrouille le compte d'un utilisateur après que celui-ci ait atteint le nombre de **Failed Attempts (Tentatives échouées)** configuré.
3. Saisissez le **Idle Timeout (délai d'expiration)**, en minutes, avant que le compte de l'utilisateur ne soit automatiquement déconnecté pour inactivité.
4. Saisissez le **Max Session Count (Compte de session max.)** pour indiquer combien de comptes d'utilisateur peuvent accéder simultanément à l'appareil WildFire.
5. Saisissez la **Max Session Time (Durée de session max.)** pendant laquelle l'administrateur peut être connecté avant d'être automatiquement déconnecté.

4. Ajoutez les administrateurs de l'appareil WildFire.

   Les administrateurs peuvent soit être ajoutés en tant qu'administrateur local ou en tant qu'administrateur Panorama importé, mais pas les deux. Ajouter le même administrateur en tant qu'administrateur local et en tant qu'administrateur Panorama importé n'est pas possible et peut entraîner une panne de validation de Panorama. Par exemple, la validation de Panorama échoue si vous ajoutez `admin1` en tant qu'administrateur local et administrateur Panorama.

   1. **Add (Ajoutez)** et configurez de nouveaux administrateurs uniques pour l'appareil WildFire. Ces administrateurs sont spécifiques à l'appareil WildFire pour lequel ils sont créés et vous gérez ces administrateurs depuis ce tableau.
   2. **Add (Ajoutez)** n'importe quel administrateur configuré dans Panorama. Ces administrateurs sont créés dans Panorama et importés vers l'appareil WildFire.

5. Cliquez sur **OK** pour enregistrer la configuration de l'authentification de l'appareil WildFire.



© 2020 Palo Alto Networks, Inc.

STEP 5 | **Commit (Validez)** et **Commit and Push (Validez et appliquez)** les modifications de votre configuration.

STEP 6 | Access the WildFire appliance CLI (Accédez au CLI de l'appareil WildFire) afin de pouvoir vérifier que vous pouvez accéder à l'appareil WildFire en utilisant l'utilisateur admin local.

Configurer l'authentification TACACS + pour un appareil WildFire

Vous pouvez utiliser un serveur TACACS+ pour authentifier l'accès administratif à la CLI de l'appareil WildFire. Vous pouvez également définir des attributs spécifiques au fournisseur (VSA) sur le serveur TACACS+ pour gérer l'autorisation de l'administrateur. L'utilisation de VSA vous permet de changer les rôles rapidement, d'accéder aux domaines et aux groupes d'utilisateurs à travers votre service d'annuaire au lieu de reconfigurer les réglages dans Panorama.

STEP 1 | Se connecter à l'interface Web Panorama.

STEP 2 | Ajouter des appareils WildFire autonomes à gérer avec Panorama.

STEP 3 | Configurer l'authentification TACACS+

1. Ajoutez un profil de serveur TACACS+.

   Le profil définit comment l'appareil WildFire se connecte au serveur TACACS+.

   1. Sélectionnez **Panorama** > **Server Profiles (Profils de serveur)** > **TACACS+** et **Add (Ajoutez)** un profil.
   2. Saisissez un **Profile Name (Nom de profil)** pour identifier le profil de serveur.
   3. Saisissez l'intervalle du **Timeout (Délai d'expiration)**, en secondes, après lequel une requête d'authentification arrive à expiration (plage de 1 à 20 ; par défaut 3).
   4. Sélectionnez l'**Authentication Protocol (Protocole d'authentification)** (par défaut, **CHAP**) que Panorama utilise pour s'authentifier au serveur TACACS+.
   5. Sélectionnez **CHAP** si le serveur TACACS+ prend en charge ce protocole ; il est plus sécuritaire que **PAP**.
   6. **Add (Ajoutez)** chaque serveur TACACS+ et saisissez les renseignements suivants :

      1. Le **Name (Nom)** qui permet d'identifier le serveur.
      2. L'adresse IP ou le FQDN du **TACACS+ Server (Serveur TACACS+)**.
      3. **La Secret / Confirm Secret (Phrase secrète / Confirmer une phrase secrète)**, une clé pour chiffrer les noms d'utilisateur et les mots de passe.
      4. Le **Port** du serveur pour les demandes d'authentification (49 par défaut).
   7. Cliquez sur **OK** pour enregistrer le profil de serveur.
2. Affectez le profil de serveur TACACS+ à un profil d'authentification.

   Le profil d'authentification définit les paramètres d'authentification qui sont communs à un ensemble d'administrateurs.

   1. Sélectionnez **Panorama** > **Authentication Profile (Profil d'authentification)** et **Add (Ajoutez)** un profil.
   2. Saisissez un **Name (Nom)** pour identifier le profil.
   3. Définissez le **Type** sur **TACACS+**.
   4. Sélectionnez le **Server Profile (Profil de serveur)** que vous avez créé.
   5. Sélectionnez **Retrieve user group from TACACS+ (Récupérer le groupe d'utilisateurs auprès de TACACS+)** pour recueillir de l'information sur le groupe d'utilisateurs auprès des VSA définis sur le serveur TACACS+.

© 2020 Palo Alto Networks, Inc.

Panorama fait correspondre l'information sur le groupe avec les groupes que vous avez spécifiés dans la liste d'autorisation du profil d'authentification.

6. Sélectionnez **Advanced (Avancé)** et, dans la liste d'autorisation, **Add (Ajoutez)** les administrateurs qui sont autorisés à s'authentifier avec ce profil d'authentification.
7. Cliquez sur **OK** pour enregistrer le profil d'authentification.

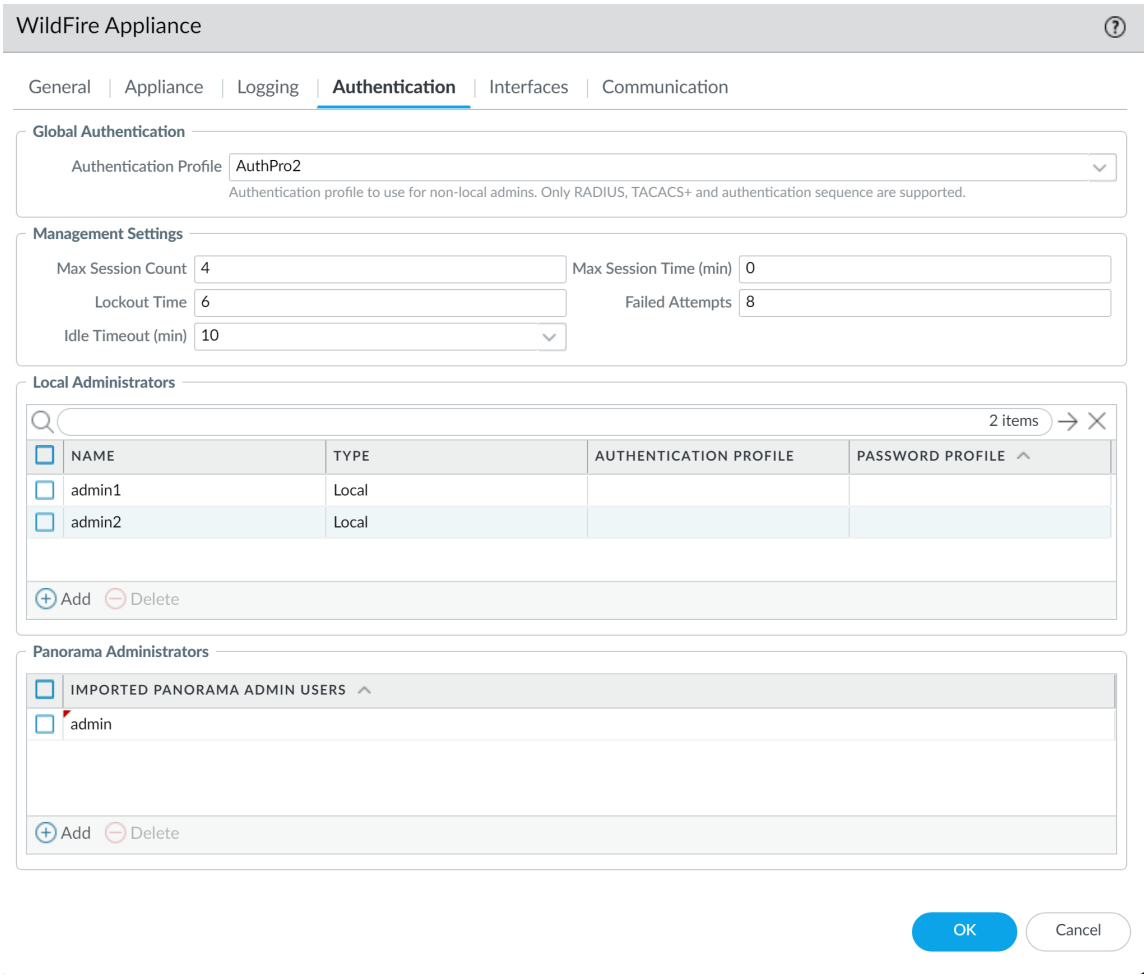
STEP 4 | Configurer l'authentification pour l'appareil WildFire.

1. Sélectionnez**Panorama** > **Managed WildFire Appliance (Appareil WildFire géré)** et sélectionnez l'appareil WildFire géré que vous venez d'ajouter.
2. Sélectionnez le **Authentification Profile (Profil d'authentification)** que vous avez configuré au cours des étapes antérieures.

   Si un profil d'authentification global n'est pas attribué, vous devez attribuer un profil d'authentification à chaque administrateur local individuel afin d'exploiter l'authentification à distance.
3. Configurez la **Timeout Configuration (Configuration du délai avant expiration)** d'authentification pour l'appareil WildFire.
   1. Saisissez le nombre de **Failed Attempt (Tentatives échouées)** avant que l'accès d'un utilisateur à la CLI de l'appareil WildFire ne soit bloqué.
   2. Saisissez la **Lockout Time (Durée de verrouillage)**, en minutes, selon l'appareil WildFire verrouille le compte d'un utilisateur après que celui-ci ait atteint le nombre de **Failed Attempts (Tentatives échouées)** configuré.
   3. Saisissez le **Idle Timeout (délai d'expiration)**, en minutes, avant que le compte de l'utilisateur ne soit automatiquement déconnecté pour inactivité.
   4. Saisissez le **Max Session Count (Compte de session max.)** pour indiquer combien de comptes d'utilisateur peuvent accéder simultanément à l'appareil WildFire.
   5. Saisissez la **Max Session Time (Durée de session max.)** pendant laquelle l'administrateur peut être connecté avant d'être automatiquement déconnecté.
4. Ajoutez les administrateurs de l'appareil WildFire.

   Les administrateurs peuvent soit être ajoutés en tant qu'administrateur local ou en tant qu'administrateur Panorama importé, mais pas les deux. Ajouter le même administrateur en tant qu'administrateur local et en tant qu'administrateur Panorama importé n'est pas possible et peut entraîner une panne de validation de Panorama. Par exemple, la validation de Panorama échoue si vous ajoutez `admin1` en tant qu'administrateur local et administrateur Panorama.
   1. **Add (Ajoutez)** et configurez de nouveaux administrateurs uniques pour l'appareil WildFire. Ces administrateurs sont spécifiques à l'appareil WildFire pour lequel ils sont créés et vous gérez ces administrateurs depuis ce tableau.
   2. **Add (Ajoutez)** n'importe quel administrateur configuré dans Panorama. Ces administrateurs sont créés dans Panorama et importés vers l'appareil WildFire.
5. Cliquez sur **OK** pour enregistrer la configuration de l'authentification de l'appareil WildFire.

© 2020 Palo Alto Networks, Inc.



STEP 5 | **Commit (Validez)** et **Commit and Push (Validez et appliquez)** les modifications de votre configuration.

STEP 6 | Accédez au CLI de l'appareil WildFire afin de pouvoir vérifier que vous pouvez accéder à l'appareil WildFire en utilisant l'utilisateur admin local.

Configurer l'authentification LDAP pour un appareil WildFire

Vous pouvez utiliser LDAP pour authentifier les utilisateurs qui accèdent à la CLI des appareils WildFire d'un cluster WildFire.

STEP 1 | Se connecter à l'interface Web Panorama.

STEP 2 | Ajouter des appareils WildFire autonomes à gérer avec Panorama.

STEP 3 | Ajoutez un profil de serveur LDAP.

Le profil définit comment l'appareil WildFire se connecte au serveur LDAP.

1. Sélectionnez **Panorama** > **Server Profiles (Profils de serveur)** > **LDAP** et **Add (Ajoutez)** un profil de serveur.
2. Saisissez un **Profile Name (Nom de profil)** pour identifier le profil de serveur.

© 2020 Palo Alto Networks, Inc.

3. **Add (Ajoutez)** les serveurs LDAP (maximum de quatre). Donnez un **Name (Nom)** à chaque serveur (pour l'identifier), ainsi qu'une adresse IP de **LDAP Server (Serveur LDAP)** ou un FQDN ainsi que le **Port (Port)** du serveur (valeur par défaut : 389).

   Si vous utilisez un objet d'adresse FQDN pour identifier le serveur et qu'ensuite vous changez l'adresse, vous devez valider le changement pour que la nouvelle adresse du serveur soit appliquée.
4. Sélectionnez le **Type (type)** de serveur.
5. Sélectionnez le **Base DN (DN de base)**.

   Pour déterminer le DN de base de votre répertoire, ouvrez les composants logiciels enfichables **Active Directory Domains and Trusts** de Microsoft Management Console et utilisez le nom du domaine de premier niveau.
6. Saisissez le **Bind DN (DN de liaison)** et le **Password (Mot de passe)** pour activer le service d'authentification permettant d'authentifier le pare-feu.

   Le compte Bind DN doit avoir l'autorisation nécessaire pour consulter le répertoire LDAP.
7. Entrez le **Bind Timeout (Délai de liaison)** et le **Délai de recherche** en secondes (la valeur par défaut est 30 pour les deux).
8. Saisissez la **Retry Interval (Intervalle de relance)** en secondes (valeur par défaut : 60).
9. (Facultatif) Si vous souhaitez que le point de terminaison utilise le protocole SSL ou TLS pour une connexion plus sécurisée au serveur d'annuaires, activez l'option **Require SSL/TLS secured connection (Exiger une connexion sécurisée SSL/TLS)** (activée par défaut). Le protocole utilisé par le point de terminaison varie selon le Port de serveur :
   - 389 (par défaut) : TLS (l'appareil WildFire utilise plus précisément l'opération StartTLS, qui met à niveau la connexion en texte brut initiale en TLS.)
   - 636 : SSL.
   - Tout autre port : l'appareil WildFire tente tout d'abord d'utiliser TLS. Si le serveur d'annuaires ne prend pas en charge TLS, l'appareil WildFire fera appel à SSL.
10. (Facultatif) Pour une sécurité supplémentaire, activez l'option **Verify Server Certificate for SSL sessions (Vérifier le certificat du serveur pour les sessions SSL)** afin que le point de terminaison vérifie le certificat que le serveur d'annuaire présente pour les connexions SSL/TLS. Pour activer la vérification, vous devez également activer l'option visant à **Require SSL/TLS secured connection (Exiger une connexion sécurisée SSL/TLS)**. Pour une vérification réussie, le certificat doit remplir l'une des conditions suivantes :
    - Il se trouve dans la liste des certificats de Panorama : **Panorama** > **Certificate Management (Gestion de certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique).** Si nécessaire, importez le certificat dans Panorama.
    - Le signataire du certificat figure dans la liste des autorités de certification de confiance : **Panorama** > **Certificate Management Gestion des certificats)** > **Certificates (Certificats)**.
11. Cliquez sur **OK** pour enregistrer le profil de serveur.

STEP 4 | Configurer l'authentification pour l'appareil WildFire.

1. Sélectionnez**Panorama** > **Managed WildFire Appliance (Appareil WildFire géré)** et sélectionnez l'appareil WildFire géré que vous venez d'ajouter.
2. Configurez la **Timeout Configuration (Configuration du délai avant expiration)** d'authentification pour l'appareil WildFire.
   1. Saisissez le nombre de **Failed Attempt (Tentatives échouées)** avant que l'accès d'un utilisateur au CLI de l'appareil WildFire ne soit bloqué.

© 2020 Palo Alto Networks, Inc.

2. Saisissez la **Lockout Time (Durée de verrouillage)**, en minutes, selon l'appareil WildFire verrouille le compte d'un utilisateur après que celui-ci ait atteint le nombre de **Failed Attempts (Tentatives échouées)** configuré.
3. Saisissez le **Idle Timeout (délai d'expiration)**, en minutes, avant que le compte de l'utilisateur ne soit automatiquement déconnecté pour inactivité.
4. Saisissez le **Max Session Count (Compte de session max.)** pour indiquer combien de comptes d'utilisateur peuvent accéder simultanément à l'appareil WildFire.
5. Saisissez la **Max Session Time (Durée de session max.)** pendant laquelle l'administrateur peut être connecté avant d'être automatiquement déconnecté.

3. Ajoutez les administrateurs de l'appareil WildFire.

   Les administrateurs peuvent soit être ajoutés en tant qu'administrateur local ou en tant qu'administrateur Panorama importé, mais pas les deux. Ajouter le même administrateur en tant qu'administrateur local et en tant qu'administrateur Panorama importé n'est pas possible et peut entraîner une panne de validation de Panorama. Par exemple, la validation de Panorama échoue si vous ajoutez **`admin1`** en tant qu'administrateur local et administrateur Panorama.

   - Configurez les administrateurs locaux.

     Configurez de nouveaux administrateurs uniques pour les appareils WildFire. Ces administrateurs sont spécifiques à l'appareil WildFire pour lequel ils sont créés et vous gérez ces administrateurs depuis ce tableau.

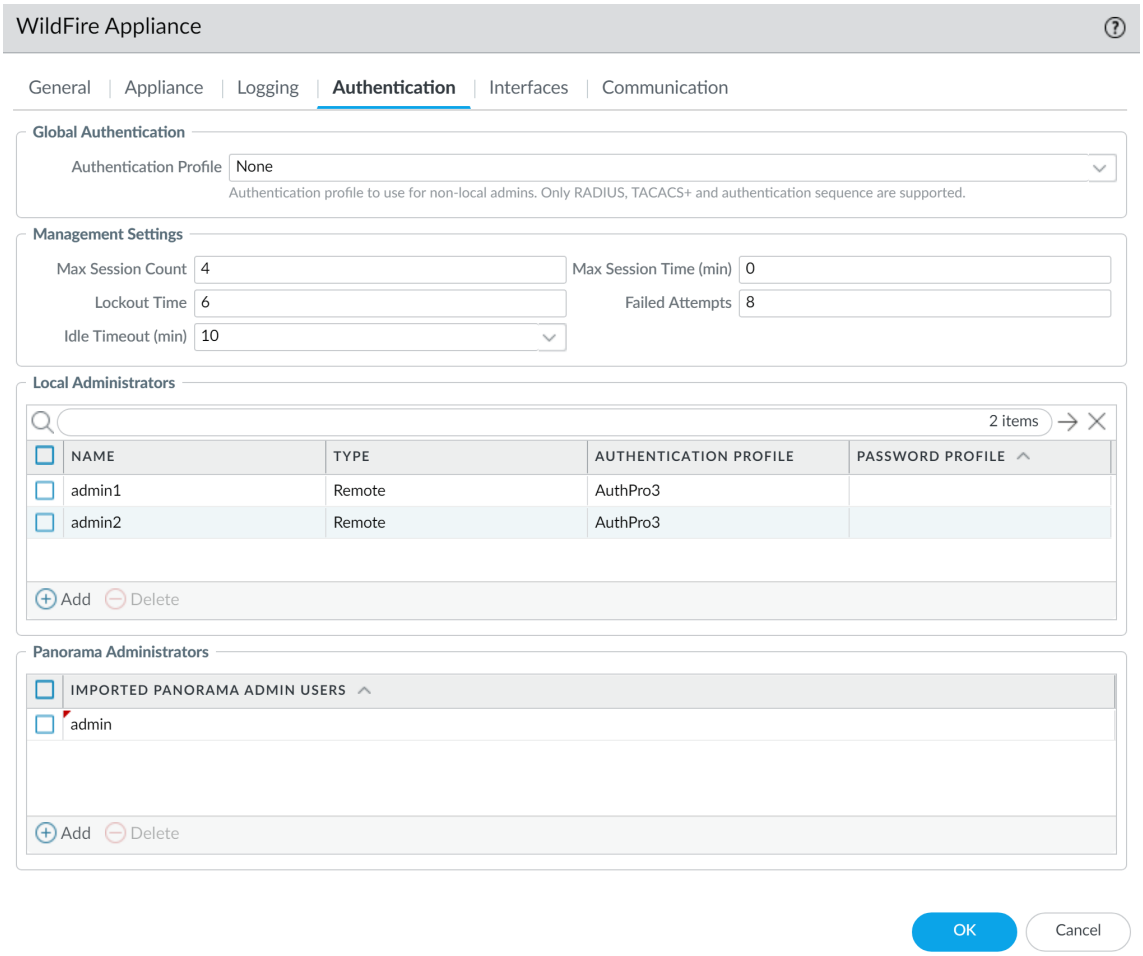
     1. **Add (Ajoutez)** un ou plusieurs administrateurs locaux.
     2. Saisissez un **Name (Nom)** d'utilisateur pour l'administrateur local.
     3. Attribuez un**Authentication Profile (profile d'authentification)** que vous avez préalablement créé.

        Les profils d'authentification LDAP sont compatibles uniquement avec les administrateurs locaux individuels.
     4. Activez (cochez) **Use Public Key Authentication (SSH) (Utiliser l'authentification par clé publique (SSH)** pour importer un fichier de clé publique pour l'authentification.
     5. Sélectionnez un **Password Profile (profil de mot de passe)** pour définir les paramètres d'expiration.
   - Importez les administrateurs Panorama existants

     Importez des administrateurs existants configurés dans Panorama. Ces administrateurs sont configurés et gérés dans Panorama et importés vers l'appareil WildFire.

     1. **Add (Ajoutez)** un administrateur Panorama existant
4. Cliquez sur **OK** pour enregistrer la configuration de l'authentification de l'appareil WildFire.

© 2020 Palo Alto Networks, Inc.



STEP 5 | **Commit (Validez)** et **Commit and Push (Validez et appliquez)** les modifications de votre configuration.

STEP 6 | Accédez au CLI de l'appareil WildFire afin de pouvoir vérifier que vous pouvez accéder à l'appareil WildFire en utilisant l'utilisateur admin local.

© 2020 Palo Alto Networks, Inc.

Configurer l'authentification à l'aide de certificats personnalisés sur les appareils et clusters WildFire

Par défaut, un appareil WildFire® utilise des certificats prédéfinis pour une authentification mutuelle avec d'autres pare-feu et appareils Palo Alto Networks® afin d'établir les connexions SSL utilisées pour l'accès de gestion et la communication inter-dispositifs. Cependant, vous pouvez configurer l'authentification à l'aide de certificats personnalisés. Les certificats personnalisés vous permettent d'établir une chaîne de confiance unique pour garantir une authentification mutuelle entre votre appareil WildFire ou votre cluster WildFire géré par Panorama ™ et les pare-feu. Vous pouvez générer ces certificats localement sur Panorama ou le pare-feu, les obtenir auprès d'une autorité de certification (CA) tierce approuvée ou obtenir des certificats auprès d'une infrastructure de clés privées (PKI) d'entreprise.

Pour plus d'informations sur l'utilisation de certificats personnalisés, voir Comment les connexions SSL / TLS sont-elles mutuellement authentifiées?

- Configurer un certificat personnalisé pour un appareil WildFire géré par Panorama
- Configurer l'authentification avec un certificat personnalisé unique pour un cluster WildFire
- Appliquer des certificats personnalisés sur un appareil WildFire configuré via Panorama

Configurer un certificat personnalisé pour un appareil WildFire géré par Panorama

Si vous utilisez Panorama ™ pour gérer votre appareil WildFire® ou votre cluster WildFire, vous pouvez configurer l'authentification par certificat personnalisé via l'interface Web de Panorama au lieu d'utiliser de la CLI de l'appareil WildFire. Le pare-feu ou Panorama utilisent également cette connexion pour transférer des échantillons de fichiers/e-mails vers WildFire pour analyse.

Cette procédure décrit l'installation d'un certificat unique sur un seul appareil WildFire. Si l'appareil WildFire fait partie d'un cluster, ce périphérique et chaque membre du cluster possèdent un certificat client unique. Pour déployer un seul certificat sur toutes les appareils WildFire du cluster, consultez Configuration de l'authentification avec un certificat personnalisé unique pour un cluster WildFire.

STEP 1 | Obtenez des paires de clés et des certificats d'autorité de certification (CA) pour l'appareil et le pare-feu.

STEP 2 | Importez le certificat CA pour valider l'identité du pare-feu et la paire de clés pour le dispositif WildFire.

1. Sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Import (Importer)**.
2. Importez le certificat CA et la paire de clés sur Panorama.

STEP 3 | Configurez un profil de certificat incluant l'autorité de certification racine et l'autorité de certification intermédiaire. Ce profil de certificat définit l'authentification mutuelle entre l'appareil WildFire et les pare-feu.

1. Sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificats)**.
2. Configurez un profil de certificat.

© 2020 Palo Alto Networks, Inc.

Si vous configurez un CA intermédiaire dans le cadre du profil de certificat, vous devez également inclure la certification CA racine.

STEP 4 | Configurez un profil SSL / TLS pour l'appareil WildFire.

Les versions 8.0 et ultérieures de PAN-OS prennent uniquement en charge TLS 1.2 et les versions ultérieures. Vous devez donc définir la version maximale sur TLS 1.2 ou une version ultérieure.

1. Sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **SSL/TLS Service Profile (Profil de service SSL/TLS)**.
2. Configurez un profil SSL/TLS pour définir le certificat et le protocole utilisés par l'appareil WildFire et ses pare-feu pour les services SSL / TLS.

STEP 5 | Configurez la communication sécurisée avec le serveur sur Wildfire.

1. Sélectionnez**Panorama** > **Managed WildFire Clusters (Clusters WildFire gérés)** ou **Panorama** > **Managed WildFire Appliances (Appareils WildFire gérés)** et sélectionnez un cluster ou un appareil.
2. Sélectionnez **Communication**.
3. Activer la fonction **Customize Secure Server Communication (Personnaliser la communication sécurisée avec le serveur)**.
4. Sélectionnez le **SSL/TLS Service Profile (Profil de service SSL/TLS)**. Ce profil de service SSL / TLS s'applique à toutes les connexions SSL entre l'appareil WildFire et le pare-feu ou Panorama.
5. Sélectionnez le **Certificate Profile (Profil de certificat)** que vous avez configuré pour la communication entre l'appareil WildFire et le pare-feu ou Panorama.
6. Vérifiez que la case **Custom Certificate Only (Certificat personnalisé uniquement)** n'est pas cochée. Cela permet au dispositif WildFire de continuer à communiquer avec les pare-feu en utilisant le certificat prédéfini lors de la migration vers des certificats personnalisés.
7. (Facultatif) Configurez une liste d'autorisation.
    1. **Add (Ajoutez)** une liste d'autorisation.
    2. Sélectionnez le **Subject (Objet)** ou **Subject Alt Name (Autre nom de l'objet)** configuré dans le profil de certificat en tant que type d'identifiant.
    3. Entrez le nom commun si l'identifiant est Subject (Objet) et l'adresse IP, le nom d'hôte ou l'e-mail si l'identificateur est Subject Alt Name (Autre nom de l'objet).
    4. Cliquez sur **OK**.
    5. Activez l'option **Check Authorization List (Vérifiez la liste d'authorisation)** pour mettre en œuvre la liste d'autorisation.
8. Cliquez sur **OK**.
9. **Commit (Validez)** vos modifications.

STEP 6 | Importez le certificat d'autorité de certification pour valider le certificat de l'appareil WildFire.

1. Connectez-vous à l'interface Web du pare-feu.
2. Importez le certificat de l'autorité de certification.

STEP 7 | Configurez un certificat local ou SCEP pour le pare-feu.

- Si vous utilisez un certificat local, importez la paire de clés pour le pare-feu.
- Si vous utilisez SCEP pour le certificat du pare-feu, configurez un profil SCEP.

STEP 8 | Configurez le profil de certificat pour le pare-feu ou Panorama. Vous pouvez configurer ce profil sur chaque pare-feu client ou sur appareil Panorama individuellement ou vous pouvez utiliser un modèle pour transmettre la configuration de Panorama vers des pare-feu gérés.

© 2020 Palo Alto Networks, Inc.

1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil du certificat)** pour les pare-feu ou **Panorama** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil du certificat)** pour Panorama.
2. Configuration d'un profil de certificat.

STEP 9 | Déployez des certificats personnalisés sur chaque pare-feu ou appareil Panorama.

1. Connectez-vous à l'interface Web du pare-feu.
2. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** pour les pare-feu ou **Panorama** > **Setup (Configuration)** > **Management (Gestion)** pour Panorama, puis **Edit (Modifiez)** les paramètres de la communication sécurisée.
3. Sélectionnez le **Certificate Type (Type de certificat)**, le **Certificate (Certificat)** et le **Certificate Profile (Profil du certificat)**.
4. Sous Customize Communication (Personnaliser la communication), sélectionnez **WildFire Communication (Communication WildFire)**.
5. Cliquez sur **OK**.
6. **Commit (Validez)** vos modifications.

STEP 10 | Après avoir déployé des certificats personnalisés sur tous les périphériques gérés, appliquez l'authentification par certificat personnalisé.

1. Connectez-vous à Panorama.
2. Sélectionnez**Panorama** > **Managed WildFire Clusters (Clusters WildFire gérés)** ou **Panorama** > **Managed WildFire Appliances (Appareils WildFire gérés)** et sélectionnez un cluster ou un appareil.
3. Sélectionnez **Communication**.
4. Cochez **Custom Certificate Only (Certificat personnalisé uniquement)**.
5. Cliquez sur **OK**.
6. **Commit (Validez)** vos modifications.

Après avoir validé cette modification, WildFire commence immédiatement à appliquer les certificats personnalisés.

Configurer l'authentification avec un certificat personnalisé unique pour un cluster WildFire

Au lieu d'attribuer des certificats uniques à chaque appareil WildFire® faisant partie d'un cluster, vous pouvez affecter un seul certificat client partagé à l'ensemble du cluster WildFire, ce qui vous permet de transmettre un seul certificat à tous les appareils WildFire du cluster au lieu de configurer des certificats séparés pour chaque membre du cluster. Étant donné que les appareils WildFire individuels partagent un certificat client, vous devez configurer un nom d'hôte unique (nom DNS) pour chaque appareil WildFire. Vous pouvez ensuite ajouter tous les noms d'hôte en tant qu'attributs de certificat au certificat partagé ou utiliser une chaîne générique unique qui correspond à tous les noms d'hôtes personnalisés sur tous les appareils WildFire du cluster.

Pour configurer un certificat personnalisé unique à utiliser pour votre cluster WildFire lors de la communication avec Panorama™, procédez comme suit.

STEP 1 | Procurez-vous une paire de clés de serveur et un certificat CA pour Panorama.

STEP 2 | Configurez un profil de certificat qui inclut l'autorité de certification racine (CA) et l'autorité de certification intermédiaire. Ce profil de certificat définit l'authentification entre le cluster WildFire (client) et l'appareil Panorama (serveur).

1. Sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificats)**.

© 2020 Palo Alto Networks, Inc.

2. Configurez un profil de certificat.

   Si vous configurez un CA intermédiaire dans le cadre du profil de certificat, vous devez également inclure la certification CA racine.

STEP 3 | Configurez un profil de service SSL/TLS.

1. Sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **SSL/TLS Service Profile (Profil de service SSL/TLS)**.
2. Configurez un profil SSL/TLS pour définir le certificat et le protocole utilisés par le cluster WildFire et l'appareil Panorama pour les services SSL / TLS.

STEP 4 | Connectez chaque noeud du cluster à Panorama..

STEP 5 | Configurez un nom d'hôte unique (nom DNS) sur chaque nœud du cluster ou utilisez une chaîne avec un seul caractère générique qui correspond à tous les noms DNS personnalisés définis sur les appareils WildFire du cluster.

Si vous utilisez une chaîne à caractère générique unique, consultez RFC-6125,Section 6.4.3 pour connaître les exigences et les limitations des valeurs de chaînes génériques. Assurez-vous de bien comprendre ces exigences et limitations lors de la configuration de vos noms DNS personnalisés.

1. Connectez-vous à la CLI WildFire sur un nœud.
2. Utilisez la commande suivante pour attribuer un nom DNS personnalisé unique au nœud.

```
admin@WF-500> configure
```

```
admin@WF-500# set deviceconfig setting wildfire custom-dns-name <dns-name>
```

3. **Commit (Validez)** la modification.
4. Répétez ce processus pour chaque nœud du cluster.

STEP 6 | Sur Panorama, générez un certificat client pour tous les nœuds du cluster. Sous Attributs de certificat, ajoutez une entrée de nom d'hôte pour chaque nom DNS personnalisé que vous avez attribué aux nœuds de cluster ou ajoutez une entrée de nom d'hôte avec une chaîne générique unique correspondant à tous les noms d'hôte de nœud, tels que * .example.com ; vous pouvez le faire uniquement si chaque nom DNS personnalisé partage une chaîne commune.

STEP 7 | Sur Panorama, configurez le profil du certificat du périphérique client.

1. Sélectionnez**Panorama** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil des certificats)** pour Panorama.
2. Configuration d'un profil de certificat.

STEP 8 | Déployez des certificats personnalisés sur chaque nœud. Ce profil de certificat doit contenir le certificat de l'autorité de certification qui a signé le certificat du serveur Panorama.

1. Sélectionnez **Panorama** > **Managed WildFire Clusters (Clusters WildFire gérés)** et cliquez sur le nom du cluster.
2. Sélectionnez **Communications**.
3. Sous Communications clients sécurisées, sélectionnez le **Certificate Type (Type de certificat)**, le **Certificate (Certificat)**, et le **Certificate Profile (Profil du certificat)**.
4. Cliquez sur **OK**.
5. **Commit (Validez)** vos modifications.

STEP 9 | Configurez la communication sécurisée du serveur sur Panorama.

© 2020 Palo Alto Networks, Inc.

1. Sélectionnez **Panorama** > **Setup (Paramètres)** > **Management (Gestion)**, puis **Edit (Modifier)** pour sélectionner **Customize Secure Server Communication (Personnaliser la communication sécurisée avec le serveur)**.
2. Cliquez sur **Customize Secure Server Communication (Personnaliser la communication sécurisée avec le serveur)** pour l'activer.
3. Sélectionnez le **SSL/TLS Service Profile (Profil de service SSL/TLS)**. Ce profil de service SSL / TLS s'applique à toutes les connexions SSL entre WildFire et Panorama.
4. Sélectionnez le **Certificate Profile (Profil de certificat)** de Panorama.
5. Cochez **Custom Certificate Only (Certificat personnalisé uniquement)** pour activer cette option.
6. Cliquez sur **OK**.
7. **Commit (Validez)** vos modifications.

Appliquer des certificats personnalisés sur un appareil WildFire configuré via Panorama

Par défaut, Panorama ™ utilise un certificat prédéfini lors de la communication avec un appareil WildFire® afin de transmettre des configurations. Vous pouvez également configurer des certificats personnalisés pour établir une authentification mutuelle pour la connexion que Panorama utilise pour transmettre des configurations à un appareil ou à un cluster WildFire géré. Suivez la procédure suivante pour configurer le certificat de serveur sur Panorama et le certificat client sur l'appareil WildFire.

STEP 1 | Obtenez des paires de clés et des certificats d'autorité de certification (CA) pour Panorama et le dispositif de WildFire.

STEP 2 | Importez le certificat CA pour valider l'identité le dispositif WildFire et la paire de clés pour Panorama.

1. Sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Import (Importer)**.
2. Importez le certificat CA et la paire de clés sur Panorama.

STEP 3 | Configurez un profil de certificat incluant l'autorité de certification racine et l'autorité de certification intermédiaire. Ce profil de certificat définit l'authentification entre l'appareil WildFire (client) et l'appareil virtuel Panorama ou M-Series (serveur).

1. Sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificats)**.
2. Configurez un profil de certificat.

   Si vous configurez un CA intermédiaire dans le cadre du profil de certificat, vous devez également inclure la certification CA racine.

STEP 4 | Configurez un profil de service SSL/TLS.

1. Sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **SSL/TLS Service Profile (Profil de service SSL/TLS)**.
2. Configurez un profil SSL/TLS pour définir le certificat et le protocole utilisés par le cluster WildFire et le dispositif Panorama pour les services SSL / TLS.

STEP 5 | Configurez la communication sécurisée du serveur sur Panorama.

1. Sélectionnez **Panorama** > **Setup (Paramètres)** > **Management (Gestion)**, puis **Edit (Modifier)** pour sélectionner **Customize Secure Server Communication (Personnaliser la communication sécurisée avec le serveur)**.

© 2020 Palo Alto Networks, Inc.

2. Activer la fonction **Customize Secure Server Communication (Personnaliser la communication sécurisée avec le serveur)**.
3. Sélectionnez le **SSL/TLS Service Profile (Profil de service SSL/TLS)**.
4. Sélectionnez le profil du certificat depuis la liste déroulante **Certificate Profile (Profil du certificat)**.
5. Vérifiez que la case **Custom Certificate Only (Certificat personnalisé uniquement)** n'est pas cochée. Cela permet au dispositif Panorama de continuer à communiquer avec WildFire avec le certificat prédéfini lors de la migration vers des certificats personnalisés.
6. (Facultatif) Configurez une liste d'autorisation.
    1. **Add (Ajoutez)** une liste d'autorisation.
    2. Sélectionnez le **Subject (Objet)** ou **Subject Alt Name (Autre nom de l'objet)** configuré dans le profil de certificat en tant que type d'identifiant.
    3. Entrez le **Common Name (Nom common)** si l'identifiant est `Subject` ou une **IP address (Adresse IPL**, le **hostname (nom d'hôte)**, ou le **email** si l'identifiant les `Subject Alt Name`.
    4. Cliquez sur **OK**.
    5. Activez l'option **Check Authorization List (Vérifier la liste d'autorisation)** pour configurer Panorama pour qu'il mette en œuvre la liste d'autorisation.
7. Cliquez sur **OK**.
8. **Commit (Validez)** vos modifications.

STEP 6 | Importez le certificat d'autorité de certification pour valider le certificat pour Panorama.

1. Connectez-vous à l'interface utilisateur de Panorama.
2. Importez le certificat de l'autorité de certification.

STEP 7 | Configurez un certificat local ou SCEP pour l'appareil WildFire.

1. Si vous utilisez un certificat local, importez la paire de clés pour l'appareil WF-500.
2. Si vous utilisez SCEP pour le certificat de l'appareil WildFire, configurez un profil SCEP.

STEP 8 | Configurez le profil du certificat du dispositif WildFire.

1. Sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificats)**.
2. Configurez un profil de certificat.

STEP 9 | Déployez des certificats personnalisés sur chaque appareil Wildfire.

1. Connectez-vous à Panorama.
2. Sélectionnez **Panorama** > **Managed WildFire Appliances (Clusters d'appareils WildFire)** et cliquez sur le nom du collecteur ou de l'appareil.
3. Sélectionnez **Communications**.
4. Sous Communications clients sécurisées, sélectionnez le **Certificate Type (type de certificat)**, le **Certificate (Certificat)**, et le **Certificate Profile (profil du certificat)** dans leurs menus déroulants respectifs.
5. Cliquez sur **OK**.
6. **Commit (Validez)** vos modifications.

STEP 10 | Après avoir déployé des certificats personnalisés sur tous les périphériques gérés, appliquez l'authentification par certificat personnalisé.

1. Sélectionnez **Panorama (Panorama)** > **Setup (Paramétrage)** > **Management (Gestion)** et **Edit (Modifiez)** les paramètres de communication sécurisée.
2. **Allow Custom Certificate Only (Autoriser un certificat personnalisé uniquement)**.
3. Cliquez sur **OK**.
4. **Commit (Validez)** vos modifications.

© 2020 Palo Alto Networks, Inc.

Après validation de ces modifications, le compte à rebours du temps d'attente de déconnexion commence. Lorsque le délai d'attente se termine, Panorama et les appareils WildFire gérés ne peuvent pas se connecter sans les certificats configurés.

© 2020 Palo Alto Networks, Inc.

Supprimer un appareil WildFire de la gestion Panorama

Vous pouvez supprimer des appareils autonomes WildFire de la gestion Panorama. Lorsque vous supprimez un appareil WildFire autonome de la gestion Panorama, vous ne bénéficiez plus des avantages de la gestion centralisée et devez gérer l'appareil à l'aide de sa CLI locale et de ses scripts.

STEP 1 | Sélectionnez **Panorama** > **Managed WildFire Appliances (Appareils WildFire gérés)**.

STEP 2 | Sélectionnez le ou les appareils WildFire que vous souhaitez supprimer de la gestion Panorama en cochant à côté de chaque appareil ou en cliquant sur la ligne d'un appareil.

STEP 3 | **Remove (Retirez)** les appareils WildFire sélectionnés de la gestion Panorama.

© 2020 Palo Alto Networks, Inc.

Gérer les clusters Wildfire

Un cluster d'appareils WildFire est un groupe d'appareils WildFire interconnectés qui mettent en commun les ressources afin d'accroître la capacité de stockage et d'analyse d'échantillons, de soutenir des groupes plus importants de pare-feu et de simplifier la configuration et la gestion de nombreux appareils WildFire. Pour renforcer la sécurité et maintenir la confidentialité du contenu transmis, vous pouvez également chiffrer les communications entre les dispositifs WildFire d'un cluster. Pour plus d'informations sur les clusters et les processus de déploiement WildFire, reportez-vous à Clusters WildFire Appliance.

The following tasks can be performed using Panorama to manage your WildFire cluster.

- Configuration centralisée d'un cluster sur Panorama
- Affichage de l'état du cluster d'appareils WildFire au moyen de Panorama
- Mise à niveau centrale d'un cluster sur Panorama à partir d'une connexion Internet
- Mise à niveau centrale d'un cluster sur Panorama sans connexion Internet
- Configurer le chiffrement d'appareil à appareil à l'aide de certificats prédéfinis centralisés sur Panorama
- Configurer le chiffrement d'appareil à appareil à l'aide de certificats personnalisés de manière centralisée sur Panorama

Configuration centralisée d'un cluster sur Panorama

Avant de configurer un cluster d'appareils WildFire sur un appareil Panorama M-Series ou virtuel, vous devez disposer de deux appareils WildFire qui peuvent être configurés en tant que paire de nœuds de contrôle à haute disponibilité ainsi que des autres appareils WildFire nécessaires pour devenir des nœuds esclaves en vue d'améliorer l'analyse, la capacité de stockage et la résilience du cluster.

S'il s'agit de nouveaux appareils WildFire, consultez la section Premiers pas avec WildFire pour vous assurer d'effectuer les étapes de base, par exemple, confirmer que votre licence WildFire est active, activer la journalisation, connecter les pare-feu aux appareils WildFire et configurer les fonctionnalités de base de WildFire.

Pour créer des clusters d'appareils WildFire, vous devez mettre à niveau tous les appareils WildFire *que vous souhaitez ajouter au cluster à Panorama 8.0.1 ou à toute version ultérieure. Si vous vous servez de Panorama pour gérer les clusters d'appareils WildFire, Panorama doit également utiliser PAN-OS 8.0.1 ou toute version ultérieure. Sur chaque appareil WildFire que vous voulez ajouter à un cluster, exécutez la commande* **`show system info | match version`** *sur la CLI de l'appareil WildFire pour vérifier que l'appareil utilise bien PAN-OS 8.0.1 ou une version ultérieure. Sur chaque appareil Panorama que vous utilisez pour gérer des clusters (*ou des appareils autonomes*), vous devez sélectionner Dashboard (Tableau de bord) > General Information (Informations générales) > Software Version (Version du logiciel) pour afficher la version logicielle en cours d'exécution.*

Lorsque vos appareils WildFire sont disponibles, effectuez les tâches appropriées :

- Configuration d'un cluster et ajout de nœuds sur Panorama
- Configuration des paramètres généraux d'un cluster sur Panorama
- Configurer l'authentification pour un cluster WildFire
- Suppression d'un cluster de la gestion Panorama

La suppression d'un nœud d'un cluster à l'aide de Panorama n'est pas prise en charge. Procédez plutôt à la suppression locale d'un nœud d'un cluster *au moyen de la CLI locale de WildFire.*

© 2020 Palo Alto Networks, Inc.

Configuration d'un cluster et ajout de nœuds sur Panorama

Avant de configurer un cluster d'appareils WildFire depuis Panorama, vous devez mettre à niveau Panorama vers la version 8.0.1 ou vers une version ultérieure et procédez à la mise à niveau de tous les appareils WildFire que vous prévoyez d'ajouter au cluster vers Panorama 8.0.1 ou toute version ultérieure. Tous les appareils WildFire doivent utiliser la même version de PAN-OS .

Vous pouvez gérer jusqu'à 200 appareils WildFire avec un appareil Panorama virtuel ou de série M. La limite de 200 appareils WildFire correspond au total combiné d'appareils autonomes et de nœuds de cluster d'appareils WildFire (si vous procédez également à l'ajout d'appareils WildFire autonomes à gérer au moyen de Panorama). Sauf indication contraire, la configuration se fait sur Panorama.



Chaque nœud du cluster d'appareils WildFire doit posséder une adresse IP statique du même sous-réseau et des connexions à faible latence.

STEP 1 | Au moyen de la CLI locale, configurez l'adresse IP du serveur Panorama qui gérera le cluster d'appareils WildFire.

Avant d'enregistrer un cluster ou des appareils WildFire autonomes sur un appareil Panorama, vous devez d'abord configurer l'adresse IP ou le FQDN de Panorama sur chaque appareil WildFire en utilisant la CLI locale de WildFire. C'est ainsi que chaque appareil WildFire sait quel appareil Panorama le gère.

1. Sur chaque appareil WildFire, configurez l'adresse IP ou le FQDN de l'interface de gestion de l'appareil Panorama principal :

```
admin@WF-500# set deviceconfig system panorama-server <ip-address | FQDN>
```

2. Sur chaque appareil WildFire, si vous utilisez un appareil Panorama de secours pour la haute disponibilité (recommandé), configurez l'adresse IP ou le FQDN de l'interface de gestion de l'appareil Panorama de secours :

```
admin@WF-500# set deviceconfig system panorama-server-2 <ip-address |
 FQDN>
```

3. Validez la configuration sur chaque appareil WildFire :

```
admin@WF-500# commit
```

STEP 2 | Enregistrez les appareils WildFire sur l'appareil Panorama principal.

Les appareils nouvellement enregistrés sont en mode autonome, sauf s'ils appartiennent déjà à un cluster en raison d'une configuration de cluster locale.

1. Sélectionnez **Panorama (Panorama)** > **Managed WildFire Appliances (Appareils WildFire gérés)** et **Add Appliance (Ajouter l'appareil)**.
2. Saisissez le numéro de série de chaque appareil WildFire sur une ligne séparée. Si vous n'avez pas la liste des numéros de série des appareils WildFire, à l'aide de la CLI, exécutez la commande **`show system info`** sur chaque appareil WildFire pour en obtenir le numéro de série.
3. Cliquez sur **OK**.

   Si elles sont disponibles, les informations sur la configuration déjà validée sur les appareils WildFire s'affichent, telles que l'adresse IP et la version du logiciel. Les appareils WildFire qui appartiennent déjà à un cluster (par exemple, en raison d'une configuration d'un cluster locale) affichent les informations relatives à leur cluster ainsi que leur état de connexion.

STEP 3 | (Facultatif) Importer les configurations d'appareils WildFire dans l'appareil Panorama.

© 2020 Palo Alto Networks, Inc.

L'importation des configurations vous permet de gagner du temps, car vous pouvez les réutiliser ou les modifier sur Panorama, puis les transmettre à un ou plusieurs clusters d'appareils WildFire ou à des appareils WildFire autonomes. Si vous ne souhaitez pas importer de configurations, sautez cette étape. Lorsque vous transmettez une configuration depuis Panorama, la configuration transmise remplace la configuration locale.

1. Sélectionnez **Panorama (Panorama)** > **Managed WildFire Appliances (Appareils WildFire gérés)**, puis, dans la liste des appareils WildFire gérés, sélectionnez ceux dont vous souhaitez importer les configurations.
2. **Import Config (Importer la configuration)**.
3. Sélectionnez **Oui**.

   L'importation de configurations met à jour les informations affichées et intègre les configurations importées dans la configuration candidate de l'appareil Panorama.
4. **Commit to Panorama (Valider sur Panorama)** pour que les configurations de l'appareil WildFire importées fassent partie de la configuration en cours d'exécution de Panorama.

STEP 4 | Créez un nouveau cluster d'appareils WildFire.

1. Sélectionnez **Managed WildFire Clusters (Clusters WildFire gérés)**.

   Sélectionnez **Appliance (Appareil)** > **No Cluster Assigned (Aucun cluster affecté)** pour afficher les appareils (nœuds) WildFire autonomes et connaître le nombre de nœuds disponibles qui ne sont pas encore affectés à un cluster.
2. **Create Cluster (Créer un cluster)**.
3. Saisissez un **Name (Nom)** de cluster alphanumérique qui compte un maximum de 63 caractères. Le **Name (Nom)** peut comprendre des caractères en lettre minuscule et des chiffres, de même que des tirets et des points si ces derniers ne sont pas le premier ni le dernier caractère. Les espaces et autres caractères ne sont pas permis.
4. Cliquez sur **OK**.

   Le nouveau nom de cluster s'affiche, mais aucun nœud WildFire ne lui est affecté.

STEP 5 | Ajoutez des appareils WildFire au nouveau cluster.

Le premier appareil WildFire ajouté au cluster devient automatiquement le nœud de contrôle et le deuxième appareil WildFire ajouté au cluster devient automatiquement le nœud de contrôle de secours. Tous les autres appareils WildFire qui sont ajoutés au cluster deviennent des nœuds esclaves. Les nœuds esclaves utilisent les paramètres du nœud de contrôle pour assurer l'uniformité de la configuration du cluster.

1. Sélectionnez le nouveau cluster.
2. Sélectionnez **Clustering (Mise en cluster)**.
3. **Browse (Parcourez)** la liste d'appareils WildFire qui n'appartiennent pas à un cluster.
4. Ajoutez (⊕) chaque appareil WildFire que vous souhaitez inclure dans le cluster. Vous pouvez ajouter jusqu'à 20 nœuds à un cluster. Chaque appareil WildFire que vous ajoutez au cluster s'affiche de même que le rôle qui lui est automatique attribué.
5. Cliquez sur **OK**.

STEP 6 | Configurez les interfaces **Management (De gestion)**, **Analysis Environment Network (Du réseau de l'environnement d'analyse)**, HA (HA) et de gestion du cluster.

Configurez les interfaces **Management (De gestion)**, **Analysis Environment Network (Du réseau de l'environnement d'analyse)** et de gestion du cluster sur chaque membre du cluster (nœuds de contrôle et esclaves) si elles ne sont pas déjà configurées. L'interface de gestion du cluster est une interface dédiée à la gestion et à la communication au sein du cluster ; ce n'est pas la même interface que l'interface de gestion.

© 2020 Palo Alto Networks, Inc.

Configurez les interfaces HA individuellement sur le nœud de contrôle et sur le nœud de contrôle de secours. Les interfaces HA relient le noeud principal et le noeud de contrôle de secours et leur permettent de rester synchronisés et prêts à faire face à un basculement.

Les nœuds du cluster ont besoin d'adresses IP pour chacune des quatre interfaces des appareils WildFire. Vous ne pouvez pas configurez les services HA sur les nœuds esclaves.

1. Sélectionnez le nouveau cluster.
2. Sélectionnez **Clustering (Mise en cluster)**.
3. Si l'interface de gestion n'est pas configurée sur un nœud du cluster, sélectionnez **Interface Name (Nom de l'interface)** > **Management (Gestion)**, puis saisissez l'adresse IP, le masque réseau, les services et les autres informations relatives à l'interface.
4. Si l'interface du réseau de l'environnement d'analyse n'est pas configurée sur un nœud du cluster, sélectionnez **Interface Name (Nom de l'interface)** > **Analysis Environment Network (Réseau de l'environnement d'analyse)**, puis saisissez l'adresse IP, le masque réseau, les services et les autres informations relatives à l'interface.
5. Sur le nœud de contrôle et le nœud de contrôle de secours, sélectionnez l'interface à utiliser pour la liaison de contrôle HA. Vous devez configurer la même interface pour le service HA sur les deux nœuds de contrôle. Par exemple, sur le nœud de contrôle, puis sur le nœud de contrôle de secours, sélectionnez **Ethernet3**.
6. Pour chaque nœud de contrôle, sélectionnez **Clustering Services (Services de mise en cluster)** > **HA (HA)**. (L'option **HA (HA)** n'est pas disponible pour les nœuds esclaves.) Si vous souhaitez également disposer de la possibilité d'envoyer des requêtes ping à l'interface, sélectionnez **Management Services (Services de gestion)** > **Ping**.
7. Cliquez sur **OK**.
8. (Recommandé) Sélectionnez l'interface à utiliser en tant que liaison de contrôle HA de secours entre le nœud de contrôle et le nœud de contrôle de secours. Vous devez utiliser la même interface pour le service de secours HA sur les deux nœuds. Par exemple, sur les deux nœuds, sélectionnez **Management (Gestion)**.

   Sélectionnez **Clustering Services (Services de mise en cluster)** > **HA Backup (HA de secours)** sur les deux nœuds. Vous pouvez également sélectionner **Ping (Ping)**, **SSH (SSH)** et **SNMP (SNMP)** si vous souhaitez disposer de ces **Management Services (Services de gestion)** sur l'interface.

   L'interface du Analysis Environment Network (Réseau de l'environnement d'analyse) ne peut être une interface HA, ni une interface HA de secours, ni une interface de gestion du cluster .
9. Sélectionnez l'interface dédiée à utiliser pour la gestion et la communication au sein du cluster. Vous devez utiliser la même interface sur les deux nœuds, par exemple, **Ethernet2 (Ethernet2)**.
10. Sélectionnez **Clustering Services (Services de mise en cluster)** > **Cluster Management (Gestion du cluster)** sur les deux nœuds. Si vous souhaitez également disposer de la possibilité d'envoyer des requêtes ping à l'interface, sélectionnez **Management Services (Services de gestion)** > **Ping**.

    Les nœuds esclaves du cluster héritent automatiquement des paramètres du nœud de contrôle pour l'interface de gestion et de communication dédiée.

STEP 7 | Validez la configuration sur l'appareil Panorama et transmettez-la au cluster.

1. **Commit and Push (Valider et appliquer)**.
2. S'il y a des configurations sur l'appareil Panorama que vous ne voulez pas appliquer, **Edit Selections (Modifier les sélections)** pour choisir les appareils sur lesquels vous appliquez les configurations. La configuration transmise remplace la configuration active sur les nœuds du cluster. Tous les nœuds du cluster utilisent ainsi la même configuration.

© 2020 Palo Alto Networks, Inc.

STEP 8 | Vérifiez la configuration.

1. Sélectionnez **Panorama** > **Managed WildFire Clusters (Clusters WildFire gérés)**.
2. Vérifiez les champs suivants :
   - **Appliance (Appareil)** : au lieu de s'afficher en tant qu'appareils autonomes, les nœuds WildFire qui ont été ajoutés au cluster s'affichent sous le nom du cluster.
   - **Cluster Name (Nom du cluster)** : le nom du cluster s'affiche pour chaque nœud.
   - **Role (Rôle)** : le rôle approprié (**Controller (Contrôleur)**, **Controller Backup (Contrôleur de secours)** ou **Worker (Esclave)**) s'affiche pour chaque nœud.
   - **Config Status (État de la configuration)** : l'état est `In Sync`.
   - **Last Commit State (État de la dernière validation)** : `Commit succeeded`.

STEP 9 | En utilisant la CLI locale sur le nœud de contrôle principal (et non par l'interface Web de Panorama), vérifiez que les configurations sont synchronisées.

Si ce n'est pas le cas, synchronisez manuellement les configurations haute disponibilité sur les nœuds de contrôle et validez la configuration.

Bien que vous puissiez effectuer la plupart des autres configurations sur Panorama, vous devez synchroniser les configurations haute disponibilité des nœuds de contrôle sur la CLI du nœud de contrôle principal.

1. Sur le nœud de contrôle principal, vérifiez que les configurations sont synchronisées :

```
admin@WF-500(active-controller)> show high-availability all
```

   À la fin du résultat, cherchez la mention `Configuration Synchronization` :

```
Configuration Synchronization:
    Enabled: yes
    Running Configuration: synchronized
```

   Si la configuration active est synchronisée, vous n'avez pas à manuellement synchroniser la configuration. Cependant, si la configuration n'est pas synchronisée, vous devez la synchroniser manuellement.
2. Si elle n'est pas synchronisée, sur le nœud de contrôle principal, synchronisez la configuration de la haute disponibilité au nœud de contrôle de l'homologue distant :

```
admin@WF-500(active-controller)> request high-availability sync-to-remote
 running-config
```

   Si la configuration du nœud de contrôle principal ne concorde pas avec celle du nœud de contrôle de secours, c'est la première qui a préséance sur la seconde.
3. Validez la configuration :

```
admin@WF-500# commit
```

Configuration des paramètres généraux d'un cluster sur Panorama

Certains paramètres généraux sont facultatifs, tandis que d'autres sont pré-renseignés avec des valeurs par défaut. Vous devriez au moins prendre le temps de vérifier ces paramètres pour vous assurer que la configuration du cluster correspond à vos besoins. Voici certains paramètres généraux :

© 2020 Palo Alto Networks, Inc.

- Connexion au cloud WildFire public et envoi d'échantillons au cloud public.
- Configuration des politiques de conservation des données.
- Configuration de la journalisation.
- Paramétrage de l'environnement d'analyse (l'image VM qui correspond le mieux à votre environnement) et personnalisation de l'environnement d'analyse pour servir au mieux les types de fichiers que les pare-feu transmettent à WildFire.
- Établissez les adresses IP du serveur DNS, du serveur NTP, etc.

STEP 1 | Configuration des paramètres des nœuds du cluster d'appareils WildFire.

Bon nombre de paramètres sont pré-renseignés à partir des paramètres par défaut, des informations tirées des paramètres qui existaient auparavant sur le nœud de contrôle ou des paramètres que vous venez de configurer.

1. Sélectionnez le cluster.
2. Sélectionnez **Appliance (Appareil)**.
3. Saisissez les nouvelles informations, conservez les informations pré-renseignées à partir du nœud de contrôle du cluster ou modifiez les informations pré-renseignées, notamment :
   - Le nom de **Domain (domaine)**.
   - L'adresse IP du **Primary DNS Server (Serveur DNS principal)** et du **Secondary DNS Server (Serveur DNS secondaire)**.
   - La **NTP Server Address (Adresse du serveur NTP)** et le **Authentication Type (Type d'authentification)** du **Primary DNS Server (Serveur DNS principal)** et du **Secondary DNS Server (Serveur DNS secondaire)**. Les options applicables au **Authentication Type (Type d'authentification)** sont **None (Aucun)**, **Symmetric Key (Clé symétrique)** et **AutoKey (Clé automatique)**.

STEP 2 | Configurez les paramètres généraux du cluster.

Bon nombre de paramètres sont pré-renseignés à partir des paramètres par défaut, des informations tirées des paramètres qui existaient auparavant sur le nœud de contrôle ou des paramètres que vous venez de configurer.

1. Sélectionnez le nouveau cluster > **General (Général)**.
2. (Facultatif) **Enable DNS (Activez le protocole DNS)** pour le nœud de contrôle pour qu'il publie l'état du service au moyen du protocole DNS. Le contrôleur du cluster offre des services DNS sur le port de l'interface de gestion (MGT).
3. **Register Firewall To (Enregistrer le pare-feu pour)** l'utilisation du service publié par le ou les contrôleurs du cluster. Palo Alto Networks recommande d'ajouter les deux contrôleurs en tant que serveurs de l'autorité, puisque vous pourrez ainsi profiter des avantages de la haute disponibilité. Servez-vous de la forme suivante :

   ```
   wfpc.service.<cluster-name>.<domain>
   ```

   Par exemple, un cluster nommé *mycluster* dans le domaine *paloaltonetworks.com* posséderait le nom de domaine suivant :

   ```
   wfpc.service.mycluster.paloaltonetworks.com
   ```

4. Saisissez le **Content Update Server (Serveur de mises à jour de contenu)** du cluster. Utilisez le FQDN `updates.paloaltonetworks.com` par défaut pour vous connecter au serveur le plus près. **Check Server Identity (Vérifiez l'identité du serveur)** pour confirmer l'identité du serveur de mise à jour en faisant correspondre le nom commun (CN) dans le certificat avec l'adresse IP ou FQDN du serveur (cette vérification s'effectue par défaut).

© 2020 Palo Alto Networks, Inc.

5. (Facultatif) Saisissez l'emplacement du **WildFire Cloud Server (Serveur de cloud WildFire)** global ou utilisez la valeur par défaut `wildfire.paloaltonetworks.com` pour que le cluster (ou l'appareil autonome géré par Panorama) puisse envoyer des informations au serveur de cloud WildFire le plus proche. Si vous laissez ce champ en blanc sans vous connecter à un serveur de cloud WildFire, le cluster ne peut recevoir les mises à jour des signatures directement du cloud WildFire public et ne peut envoyer des échantillons pour analyse ni ne transmettre de données au cloud public.
6. Si vous connectez le cluster au cloud WildFire public, sélectionnez les services de cloud que vous souhaitez activer :
   - **Send Analysis Data (Envoyer les données d'analyse)** : envoyez un rapport XML concernant l'analyse locale des échantillons malveillants. Si vous envoyez les échantillons, le cluster n'envoie pas de rapports.
   - **Send Malicious Samples (Envoyer les échantillons malveillants)** : envoyez les échantillons malveillants.
   - **Send Diagnostics (Envoyer les diagnostics)** : envoyez les données sur les diagnostics.
   - **Verdict Lookup (Recherche de verdicts)** : interrogez automatiquement le cloud WildFire public pour savoir s'il existe des verdicts avant d'effectuer une analyse locale dans le but de réduire la charge sur le cluster d'appareils WildFire local.
7. Sélectionnez la **Sample Analysis Image (Image pour l'analyse d'échantillon)** à utiliser, en fonction des types d'échantillons que le cluster analysera.
8. Configurez la durée de temps pendant laquelle le cluster doit conserver les données d'échantillons **Benign/Grayware (Bénins/indésirables)** (plage de 1 à 90 jours ; 14 jours par défaut) et les données d'échantillons **Malicious (Malveillants)** (minimum 1 jour, aucun maximum (indéfinie) ; indéfinie par défaut). Les données des échantillons malveillants comprennent les verdicts d'hameçonnage.
9. (Facultatif) Sélectionnez **Preferred Analysis Environment (Environnement d'analyse préféré)** pour allouer davantage de ressources à **Executables (Exécutables)** ou à **Documents** selon votre environnement. L'allocation **Default (Par défaut)** est répartie entre **Executables (Exécutables)** et **Documents**. La quantité de ressources disponibles dépend du nombre de nœuds WildFire qui composent le cluster.

STEP 3 | Vérifiez que les serveurs Panorama principal et de secours sont configurés.

Si vous n'avez pas configuré de serveur Panorama de secours, mais que vous aimeriez le faire, vous pouvez l'ajouter.

1. Sélectionnez le cluster.
2. Sélectionnez **Appliance (Appareil)**.
3. Vérifiez (ou saisissez) l'adresse IP ou le FQDN du **Panorama Server (Serveur Panorama)** principal et du **Panorama Server 2 (Serveur 2 de Panorama)** de secours si vous utilisez une configuration haute disponibilité pour la gestion centralisée du cluster.

STEP 4 | (Facultatif) Configurez les paramètres système et les paramètres du journal de configuration du cluster, y compris le transfert des journaux.

1. Sélectionnez le cluster.
2. Sélectionnez **Logging (Journalisation)**.
3. Sélectionnez **System (Système)** ou **Configuration (Configuration)** pour configurer un système ou un journal de configuration, respectivement. Leur processus de configuration est similaire.
4. **Add (Ajoutez)** (⊕) et donnez un **Name (Nom)** à l'instance de transfert des journaux, sélectionnez le **Filter (Filtre)** et configurez la **Forward Method (Méthode de transfert)** (**SNMP (SNMP)**, **Email (E-mail)**, **Syslog (Syslog)** ou **HTTP (HTTP)**).

STEP 5 | Configurez l'authentification administrative.

1. Sélectionnez le cluster.
2. Sélectionnez **Authentication (Authentification)**.

© 2020 Palo Alto Networks, Inc.

3. Sélectionnez le **Authentication Profile (Profil d'authentification)**, soit **None (Aucun)** ou **radius (radius)**. RADIUS est la seule méthode d'authentification externe qui est prise en charge.
4. Définissez le mode **Local Authentication (Authentification locale)** des utilisateurs administrateurs sur **Password (Mot de passe)** ou **Password Hash (Hachage du mot de passe)**, puis saisissez le **Password (Mot de passe)**.

STEP 6 | Validez la configuration sur l'appareil Panorama et transmettez-la au cluster.

1. **Commit and Push (Valider et appliquer)**.
2. S'il y a des configurations sur l'appareil Panorama que vous ne voulez pas appliquer, **Edit Selections (Modifier les sélections)** pour choisir les appareils sur lesquels vous appliquez les configurations. La configuration transmise remplace la configuration active sur les nœuds du cluster. Tous les nœuds du cluster utilisent ainsi la même configuration.

Configurer l'authentification pour un cluster WildFire

Créez et configurez une meilleure authentification pour tous les appareils WildFire d'un cluster WildFire en configurant les utilisateurs administratifs locaux à l'aide de paramètres d'authentification granulaires ainsi qu'en exploitant RADIUS, TACAS+ ou LDAP pour l'autorisation et l'authentification.

Lorsque vous configurez et validez les administrateurs depuis Panorama, vous remplacez les administrateurs existants de tous les appareils WildFire dans le cluster WildFire par ceux que vous configurez dans Panorama.

- Configurez un Compte administratif pour un cluster WildFire.
- Configurer l'authentification RADIUS pour un cluster WildFire
- Configurer l'authentification TACACS + pour un cluster WildFire
- Configurer l'authentification LDAP pour un cluster WildFire

Configurez un Compte administratif pour un cluster WildFire.

Créez un ou plusieurs administrateurs avec des paramètres d'authentification granulaires pour tous les appareils WildFire dans un cluster pour les gérer depuis un serveur de gestion Panorama. De plus, vous pouvez configurer les administrateurs locaux depuis Panorama qui peuvent être configurés directement dans le CLI de l'appareil WildFire. Cependant, la validation d'une nouvelle configuration pour passer à l'appareil WildFire remplacera les administrateurs locaux configurés pour l'appareil WildFire.

STEP 1 | Se connecter à l'interface Web Panorama.

STEP 2 | Configuration centralisée d'un cluster sur Panorama.

STEP 3 | (En option) Configure an authentication profile (Configurez un profil d'authentification) pour définir le service d'authentification qui valide les informations de connexion des administrateurs de qui accèdent au CLI de l'appareil WildFire.

STEP 4 | Configure one or more administrator accounts (Configurez un ou plusieurs comptes administrateurs) selon ce qui est nécessaire.

Les comptes administrateurs créés dans Panorama sont ensuite importés vers les appareils WildFire dans le cluster WildFire et gérés depuis Panorama.

STEP 5 | Configurer l'authentification pour tous les appareils WildFire du cluster WildFire.

1. Sélectionnez**Panorama** > **Managed WildFire Clusters (Clusters WildFire gérés)** et sélectionnez le cluster WildFire géré que vous venez d configurer.
2. (En option) Sélectionnez le **Authentification Profile (Profil d'authentification)** que vous avez configuré au cours des étapes antérieures.

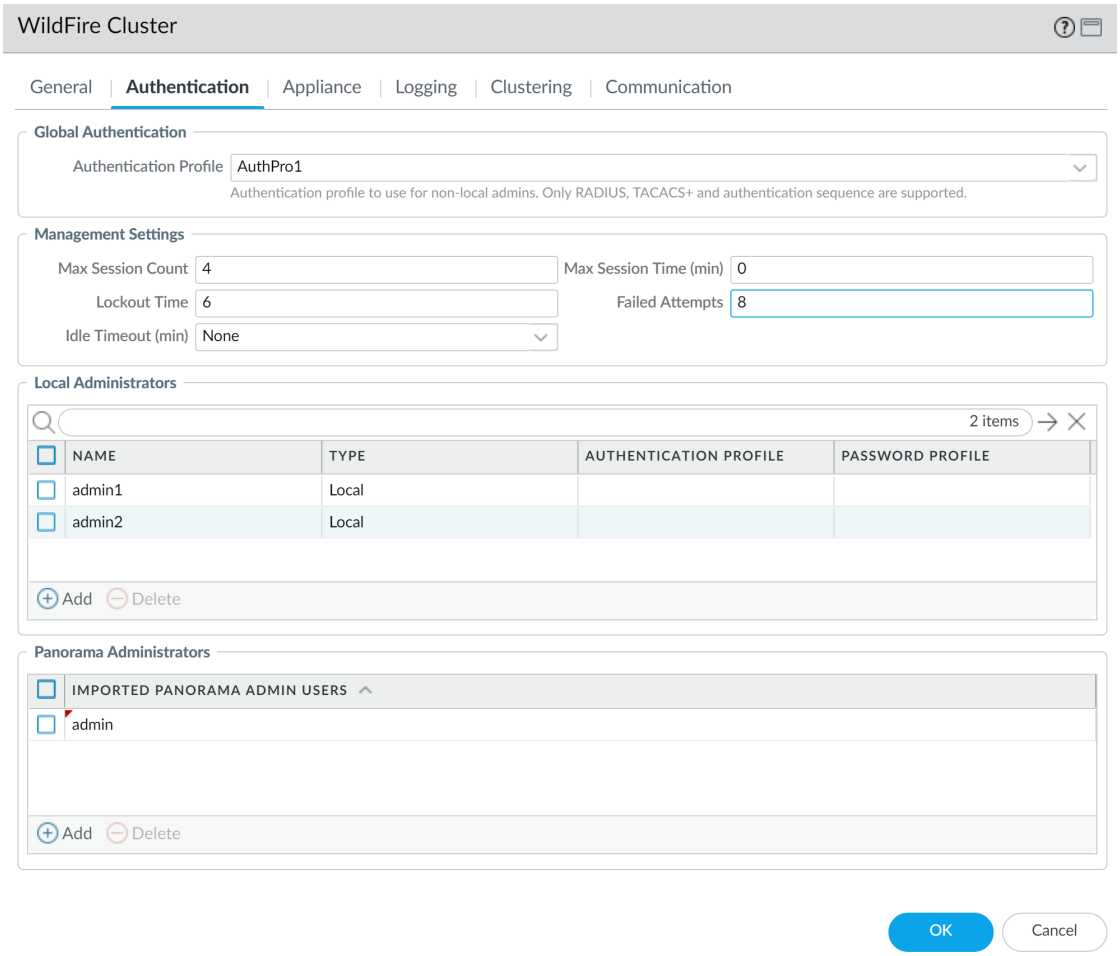
© 2020 Palo Alto Networks, Inc.

3. Configurez la **Timeout Configuration (Configuration du délai avant expiration)** d'authentification pour les appareils WildFire.
    1. Saisissez le nombre de **Failed Attempt (Tentatives échouées)** avant que l'accès d'un utilisateur au CLI de l'appareil WildFire ne soit bloqué.
    2. Saisissez la **Lockout Time (Durée de verrouillage)**, en minutes, selon l'appareil WildFire verrouille le compte d'un utilisateur après que celui-ci ait atteint le nombre de **Failed Attempts (Tentatives échouées)**.
    3. Saisissez le **Idle Timeout (délai d'expiration)**, en minutes, avant que le compte de l'utilisateur ne soit automatiquement déconnecté pour inactivité.
    4. Saisissez le **Max Session Count (Compte de session max.)** pour indiquer combien de comptes d'utilisateur peuvent accéder simultanément à un appareil WildFire.
    5. Saisissez la **Max Session Time (Durée de session max.)** pendant laquelle l'administrateur peut être connecté avant d'être automatiquement déconnecté.
4. Ajoutez les administrateurs de l'appareil WildFire.

    Les administrateurs peuvent soit être ajoutés en tant qu'administrateur local ou en tant qu'administrateur Panorama importé, mais pas les deux. Ajouter le même administrateur en tant qu'administrateur local et en tant qu'administrateur Panorama importé n'est pas possible et peut entraîner une panne de validation de Panorama. Par exemple, la validation de Panorama échoue si vous ajoutez **`admin1`** en tant qu'administrateur local et administrateur Panorama.

    1. **Add (Ajoutez)** et configurez de nouveaux administrateurs uniques pour les appareils WildFire dans le cluster WildFire. Ces administrateurs sont spécifiques aux appareils WildFire dans le cluster WildFire pour lequel ils sont créés et vous gérez ces administrateurs depuis ce tableau.
    2. **Add (Ajoutez)** n'importe quel administrateur configuré dans Panorama. Ces administrateurs sont créés dans Panorama et importés vers les appareils WildFire dans le cluster WildFire.
5. Cliquez sur **OK** pour enregistrer la configuration de l'authentification du cluster WildFire.

© 2020 Palo Alto Networks, Inc.



STEP 6 | **Commit (Validez)** et **Commit and Push (Validez et appliquez)** les modifications de votre configuration.

STEP 7 | Access the WildFire appliance CLI (Accédez au CLI de l'appareil WildFire) afin de pouvoir vérifier que vous pouvez accéder à l'appareil WildFire en utilisant l'utilisateur admin local.

Configurer l'authentification RADIUS pour un cluster WildFire

Utilisez un serveur RADIUS pour autoriser l'accès administratif à la CLI des appareils WildFire d'un cluster WildFire. Vous pouvez également définir des attributs spécifiques au fournisseur (VSA) sur le serveur RADIUS pour gérer l'autorisation de l'administrateur. L'utilisation de VSA vous permet de changer les rôles rapidement, d'accéder aux domaines et aux groupes d'utilisateurs à travers votre service d'annuaire au lieu de reconfigurer les réglages dans le serveur de gestion Panorama™.

Vous pouvez importer le dictionnaire RADIUS de Palo Alto Networks dans le serveur RADIUS pour définir les attributs d'authentification nécessaires pour la communication entre Panorama et le serveur RADIUS.

STEP 1 | Se connecter à l'interface Web Panorama.

STEP 2 | Configuration centralisée d'un cluster sur Panorama.

STEP 3 | Configuration de l'authentification RADIUS

© 2020 Palo Alto Networks, Inc.

1. Ajoutez un profil de serveur RADIUS.

   Le profil définit la façon dont les périphériques WildFire dans le cluster WildFire se connectent au serveur RADIUS.

   1. Sélectionnez **Panorama** > **Server Profiles (Profils de serveur)** > **RADIUS** et **Add (Ajoutez)** un profil.
   2. Saisissez un **Profile Name (Nom de profil)** pour identifier le profil de serveur.
   3. Saisissez l'intervalle du **Timeout (Délai d'expiration)**, en secondes, après lequel une requête d'authentification arrive à expiration (plage de 1 à 20 ; par défaut 3).
   4. Sélectionnez l'**Authentication Protocol (Protocole d'authentification)** (par défaut, **CHAP**) que l'appareil WildFire utilise pour s'authentifier au serveur RADIUS.

      Sélectionnez CHAP si le serveur RADIUS prend en charge ce protocole ; il est plus sécuritaire que PAP.

   5. **Add (Ajoutez)** chaque serveur RADIUS et saisissez les renseignements suivants :

      1. Le **Name (Nom)** qui permet d'identifier le serveur.
      2. L'adresse IP ou le FQDN du **RADIUS Server (Serveur RADIUS)**.
      3. Le **Secret/Confirm Secret (Phrase secrète / Confirmer une phrase secrète)**, une clé pour chiffrer les noms d'utilisateur et les mots de passe.
      4. Le **Port** du serveur pour les demandes d'authentification (1812 par défaut).
   6. Cliquez sur **OK** pour enregistrer le profil de serveur.
2. Affectez le profil de serveur RADIUS à un profil d'authentification.

   Le profil d'authentification définit les paramètres d'authentification qui sont communs à un ensemble d'administrateurs.

   1. Sélectionnez **Panorama** > **Authentication Profile (Profil d'authentification)** et **Add (Ajoutez)** un profil.
   2. Entrez un **Name (Nom)** pour identifier le profil d'authentification.
   3. Définissez le **Type** sur **RADIUS**.
   4. Sélectionnez le **Server Profile (Profil de serveur)** que vous avez créé.
   5. Sélectionnez **Retrieve user group from RADIUS (Récupérer le groupe d'utilisateurs auprès de TACACS+)** pour recueillir de l'information sur le groupe d'utilisateurs auprès des VSA définis sur le serveur TACACS+.

      Panorama fait correspondre l'information sur le groupe avec les groupes que vous avez spécifiés dans la liste d'autorisation du profil d'authentification.
   6. Sélectionnez **Advanced (Avancé)** et, dans la liste d'autorisation, **Add (Ajoutez)** les administrateurs qui sont autorisés à s'authentifier avec ce profil d'authentification.
   7. Cliquez sur **OK** pour enregistrer le profil d'authentification.

STEP 4 | Configurer l'authentification pour le cluster WildFire.

1. Sélectionnez**Panorama** > **Managed WildFire Clusters (Clusters WildFire gérés)** et sélectionnez le cluster WildFire géré que vous venez d'ajouter.
2. Sélectionnez le **Authentification Profile (Profil d'authentification)** que vous avez configuré au cours des étapes antérieures.

   Si un profil d'authentification global n'est pas attribué, vous devez attribuer un profil d'authentification à chaque administrateur local individuel afin d'exploiter l'authentification à distance.
3. Configurez la **Timeout Configuration (Configuration du délai avant expiration)** d'authentification pour un appareil WildFire.

   1. Saisissez le nombre de **Failed Attempt (Tentatives échouées)** avant que l'accès d'un utilisateur au CLI de l'appareil WildFire ne soit bloqué.

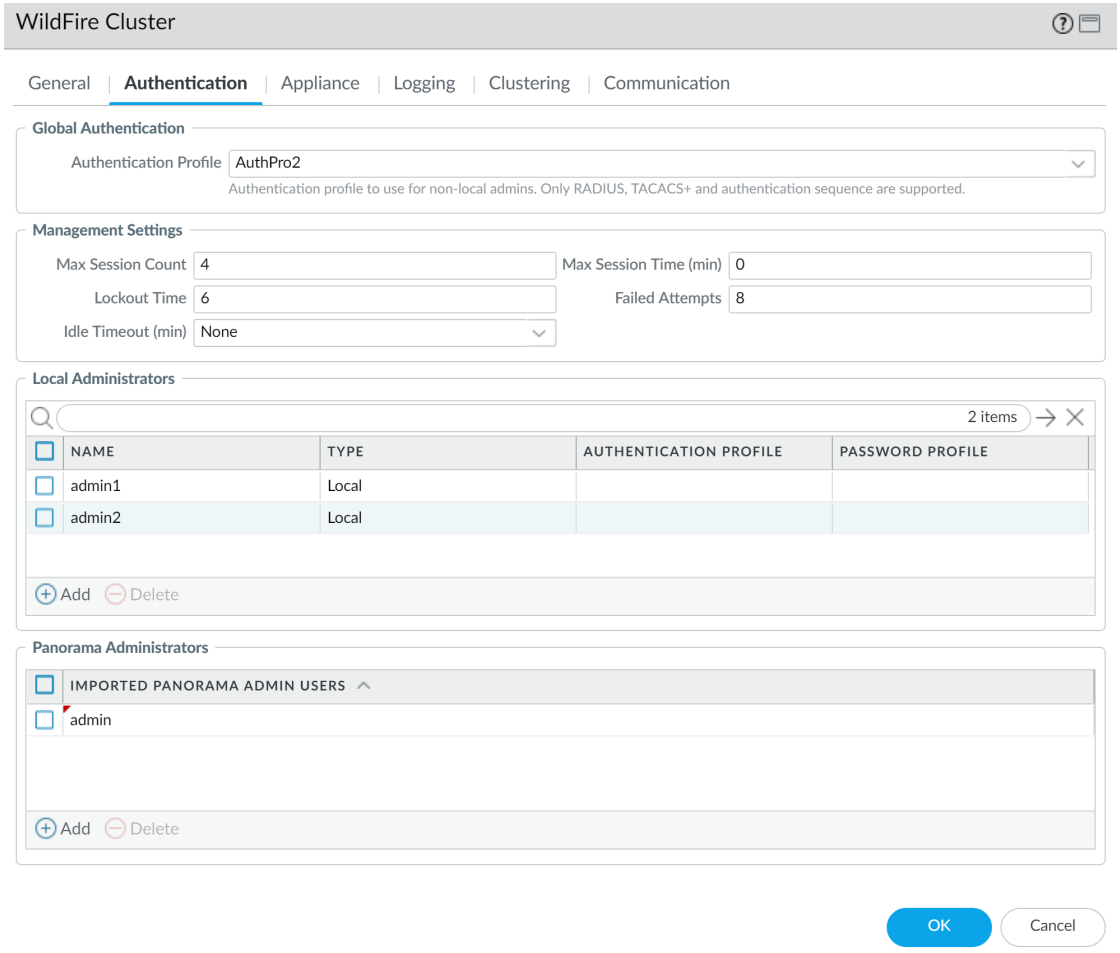
© 2020 Palo Alto Networks, Inc.

2. Saisissez la **Lockout Time (Durée de verrouillage)**, en minutes, selon l'appareil WildFire verrouille le compte d'un utilisateur après que celui-ci ait atteint le nombre de **Failed Attempts (Tentatives échouées)**.
3. Saisissez le **Idle Timeout (délai d'expiration)**, en minutes, avant que le compte de l'utilisateur ne soit automatiquement déconnecté pour inactivité.
4. Saisissez le **Max Session Count (Compte de session max.)** pour indiquer combien de comptes d'utilisateur peuvent accéder simultanément à un appareil WildFire.
5. Saisissez la **Max Session Time (Durée de session max.)** pendant laquelle l'administrateur peut être connecté avant d'être automatiquement déconnecté.

4. Ajoutez les administrateurs de l'appareil WildFire.

   Les administrateurs peuvent soit être ajoutés en tant qu'administrateur local ou en tant qu'administrateur Panorama importé, mais pas les deux. Ajouter le même administrateur en tant qu'administrateur local et en tant qu'administrateur Panorama importé n'est pas possible et peut entraîner une panne de validation de Panorama. Par exemple, la validation de Panorama échoue si vous ajoutez `admin1` en tant qu'administrateur local et administrateur Panorama.

   1. **Add (Ajoutez)** et configurez de nouveaux administrateurs uniques pour les appareils WildFire dans le cluster WildFire. Ces administrateurs sont spécifiques aux appareils WildFire dans le cluster WildFire pour lequel ils sont créés et vous gérez ces administrateurs depuis ce tableau.
   2. **Add (Ajoutez)** n'importe quel administrateur configuré dans Panorama. Ces administrateurs sont créés dans Panorama et importés vers les appareils WildFire dans le cluster WildFire.
5. Cliquez sur **OK** pour enregistrer la configuration de l'authentification du cluster WildFire.



© 2020 Palo Alto Networks, Inc.

STEP 5 | **Commit (Validez)** et **Commit and Push (Validez et appliquez)** les modifications de votre configuration.

STEP 6 | Access the WildFire appliance CLI (Accédez au CLI de l'appareil WildFire) afin de pouvoir vérifier que vous pouvez accéder à l'appareil WildFire en utilisant l'utilisateur admin local.

Configurer l'authentification TACACS + pour un cluster WildFire

Vous pouvez utiliser un serveur TACACS+ pour autoriser l'accès administratif à la CLI des appareils WildFire d'un cluster WildFire. Vous pouvez également définir des attributs spécifiques au fournisseur (VSA) sur le serveur TACACS+ pour gérer l'autorisation de l'administrateur. L'utilisation de VSA vous permet de changer les rôles rapidement, d'accéder aux domaines et aux groupes d'utilisateurs à travers votre service d'annuaire au lieu de reconfigurer les réglages dans Panorama.

STEP 1 | Se connecter à l'interface Web Panorama.

STEP 2 | Configuration centralisée d'un cluster sur Panorama.

STEP 3 | Configurer l'authentification TACACS+

1. Ajoutez un profil de serveur TACACS+.

   Le profil définit comment un appareil WildFire se connecte au serveur TACACS+.

   1. Sélectionnez **Panorama** > **Server Profiles (Profils de serveur)** > **TACACS+** et **Add (Ajoutez)** un profil.
   2. Saisissez un **Profile Name (Nom de profil)** pour identifier le profil de serveur.
   3. Saisissez l'intervalle du **Timeout (Délai d'expiration)**, en secondes, après lequel une requête d'authentification arrive à expiration (plage de 1 à 20 ; par défaut 3).
   4. Sélectionnez l'**Authentication Protocol (Protocole d'authentification)** (par défaut, **CHAP**) que Panorama utilise pour s'authentifier au serveur TACACS+.
   5. Sélectionnez **CHAP** si le serveur TACACS+ prend en charge ce protocole ; il est plus sécuritaire que **PAP**.
   6. **Add (Ajoutez)** chaque serveur TACACS+ et saisissez les renseignements suivants :
      1. Le **Name (Nom)** qui permet d'identifier le serveur.
      2. L'adresse IP ou le FQDN du **TACACS+ Server (Serveur TACACS+)**.
      3. **La Secret / Confirm Secret (Phrase secrète / Confirmer une phrase secrète)**, une clé pour chiffrer les noms d'utilisateur et les mots de passe.
      4. Le **Port** du serveur pour les demandes d'authentification (49 par défaut).
   7. Cliquez sur **OK** pour enregistrer le profil de serveur.
2. Affectez le profil de serveur TACACS+ à un profil d'authentification.

   Le profil d'authentification définit les paramètres d'authentification qui sont communs à un ensemble d'administrateurs.

   1. Sélectionnez **Panorama** > **Authentication Profile (Profil d'authentification)** et **Add (Ajoutez)** un profil.
   2. Saisissez un **Name (Nom)** pour identifier le profil.
   3. Définissez le **Type** sur **TACACS+**.
   4. Sélectionnez le **Server Profile (Profil de serveur)** que vous avez créé.
   5. Sélectionnez **Retrieve user group from TACACS+ (Récupérer le groupe d'utilisateurs auprès de TACACS+)** pour recueillir de l'information sur le groupe d'utilisateurs auprès des VSA définis sur le serveur TACACS+.

      Panorama fait correspondre l'information sur le groupe avec les groupes que vous avez spécifiés dans la liste d'autorisation du profil d'authentification.

© 2020 Palo Alto Networks, Inc.

6. Sélectionnez **Advanced (Avancé)** et, dans la liste d'autorisation, **Add (Ajoutez)** les administrateurs qui sont autorisés à s'authentifier avec ce profil d'authentification.
7. Cliquez sur **OK** pour enregistrer le profil d'authentification.

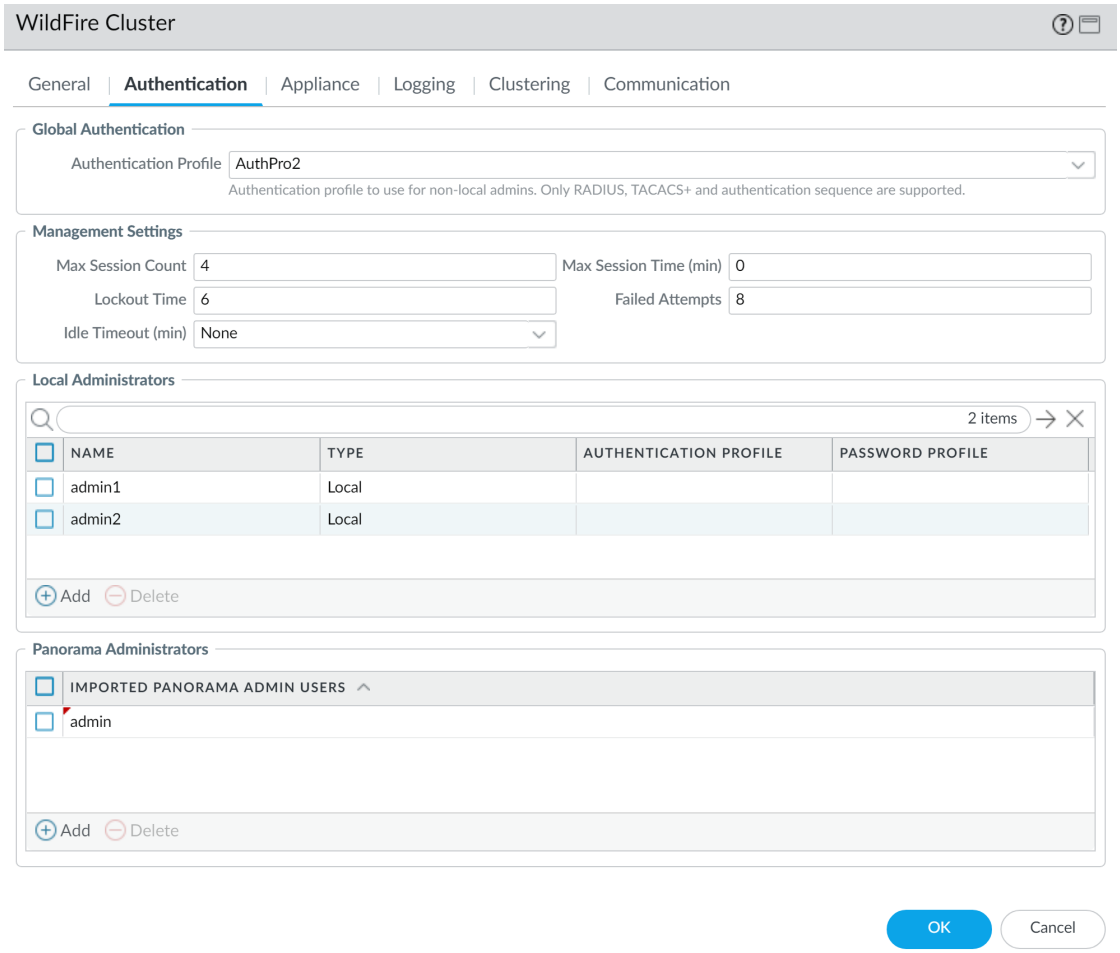
STEP 4 | Configurer l'authentification pour le cluster WildFire.

1. Sélectionnez**Panorama** > **Managed WildFire Clusters (Clusters WildFire gérés)** et sélectionnez le cluster WildFire géré que vous venez d'ajouter.
2. Sélectionnez le **Authentification Profile (Profil d'authentification)** que vous avez configuré au cours des étapes antérieures.

   Si un profil d'authentification global n'est pas attribué, vous devez attribuer un profil d'authentification à chaque administrateur local individuel afin d'exploiter l'authentification à distance.
3. Configurez la **Timeout Configuration (Configuration du délai avant expiration)** d'authentification pour un appareil WildFire.
   1. Saisissez le nombre de **Failed Attempt (Tentatives échouées)** avant que l'accès d'un utilisateur au CLI de l'appareil WildFire ne soit bloqué.
   2. Saisissez la **Lockout Time (Durée de verrouillage)**, en minutes, pour laquelle l'appareil WildFire verrouille le compte d'un utilisateur après que celui-ci ait atteint le nombre de **Failed Attempts (Tentatives échouées)**.
   3. Saisissez le **Idle Timeout (délai d'expiration)**, en minutes, avant que le compte de l'utilisateur ne soit automatiquement déconnecté pour inactivité.
   4. Saisissez le **Max Session Count (Compte de session max.)** pour indiquer combien de comptes d'utilisateur peuvent accéder simultanément à un appareil WildFire.
   5. Saisissez la **Max Session Time (Durée de session max.)** pendant laquelle l'administrateur peut être connecté avant d'être automatiquement déconnecté.
4. Ajoutez les administrateurs de l'appareil WildFire.

   Les administrateurs peuvent soit être ajoutés en tant qu'administrateur local ou en tant qu'administrateur Panorama importé, mais pas les deux. Ajouter le même administrateur en tant qu'administrateur local et en tant qu'administrateur Panorama importé n'est pas possible et peut entraîner une panne de validation de Panorama. Par exemple, la validation de Panorama échoue si vous ajoutez **`admin1`** en tant qu'administrateur local et administrateur Panorama.
   1. **Add (Ajoutez)** et configurez de nouveaux administrateurs uniques pour les appareils WildFire dans le cluster WildFire. Ces administrateurs sont spécifiques aux appareils WildFire dans le cluster WildFire pour lequel ils sont créés et vous gérez ces administrateurs depuis ce tableau.
   2. **Add (Ajoutez)** n'importe quel administrateur configuré dans Panorama. Ces administrateurs sont créés dans Panorama et importés vers les appareils WildFire dans le cluster WildFire.
5. Cliquez sur **OK** pour enregistrer la configuration de l'authentification du cluster WildFire.

© 2020 Palo Alto Networks, Inc.



STEP 5 | **Commit (Validez)** et **Commit and Push (Validez et appliquez)** les modifications de votre configuration.

STEP 6 | Accédez à la CLI de l'appareil WildFire afin de pouvoir vérifier que vous pouvez accéder à l'appareil WildFire en utilisant l'utilisateur admin local.

Configurer l'authentification LDAP pour un cluster WildFire

Vous pouvez utiliser LDAP pour authentifier les utilisateurs qui accèdent à la CLI des appareils WildFire d'un cluster WildFire.

STEP 1 | Se connecter à l'interface Web Panorama.

STEP 2 | Configuration centralisée d'un cluster sur Panorama.

STEP 3 | Ajoutez un profil de serveur LDAP.

Le profil définit comment un appareil WildFire se connecte au serveur LDAP.

1. Sélectionnez **Panorama** > **Server Profiles (Profils de serveur)** > **LDAP** et **Add (Ajoutez)** un profil de serveur.
2. Saisissez un **Profile Name (Nom de profil)** pour identifier le profil de serveur.

© 2020 Palo Alto Networks, Inc.

3. **Add (Ajoutez)** les serveurs LDAP (maximum de quatre). Donnez un **Name (Nom)** à chaque serveur (pour l'identifier), ainsi qu'une adresse IP de **LDAP Server (Serveur LDAP)** ou un FQDN ainsi que le **Port (Port)** du serveur (valeur par défaut : 389).

   Si vous utilisez un objet d'adresse FQDN pour identifier le serveur et qu'ensuite vous changez l'adresse, vous devez valider le changement pour que la nouvelle adresse du serveur soit appliquée.
4. Sélectionnez le **Type (type)** de serveur.
5. Sélectionnez le **Base DN (DN de base)**.

   Pour déterminer le DN de base de votre répertoire, ouvrez les composants logiciels enfichables **Active Directory Domains and Trusts** de Microsoft Management Console et utilisez le nom du domaine de premier niveau.
6. Saisissez le **Bind DN (DN de liaison)** et le **Password (Mot de passe)** pour activer le service d'authentification permettant d'authentifier le pare-feu.

   Le compte Bind DN doit avoir l'autorisation nécessaire pour consulter le répertoire LDAP.
7. Entrez le **Bind Timeout (Délai de liaison)** et le **Délai de recherche** en secondes (la valeur par défaut est 30 pour les deux).
8. Saisissez la **Retry Interval (Intervalle de relance)** en secondes (valeur par défaut : 60).
9. (Facultatif) Si vous souhaitez que le point de terminaison utilise le protocole SSL ou TLS pour une connexion plus sécurisée au serveur d'annuaires, activez l'option **Require SSL/TLS secured connection (Exiger une connexion sécurisée SSL/TLS)** (activée par défaut). Le protocole utilisé par le point de terminaison varie selon le Port de serveur :
   - 389 (par défaut) : TLS (l'appareil WildFire utilise plus précisément l'opération StartTLS, qui met à niveau la connexion en texte brut initiale en TLS.)
   - 636 : SSL.
   - Tout autre port : l'appareil WildFire tente tout d'abord d'utiliser TLS. Si le serveur d'annuaires ne prend pas en charge TLS, l'appareil WildFire fera appel à SSL.
10. (Facultatif) Pour une sécurité supplémentaire, activez l'option **Verify Server Certificate for SSL sessions (Vérifier le certificat du serveur pour les sessions SSL)** afin que le point de terminaison vérifie le certificat que le serveur d'annuaire présente pour les connexions SSL/TLS. Pour activer la vérification, vous devez également activer l'option visant à **Require SSL/TLS secured connection (Exiger une connexion sécurisée SSL/TLS)**. Pour une vérification réussie, le certificat doit remplir l'une des conditions suivantes :
    - Il se trouve dans la liste des certificats de Panorama : **Panorama** > **Certificate Management (Gestion de certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique).** Si nécessaire, importez le certificat dans Panorama.
    - Le signataire du certificat figure dans la liste des autorités de certification de confiance : **Panorama** > **Certificate Management Gestion des certificats)** > **Certificates (Certificats)**.
11. Cliquez sur **OK** pour enregistrer le profil de serveur.

STEP 4 | Configurer l'authentification pour le cluster WildFire.

1. Sélectionnez**Panorama** > **Managed WildFire Clusters (Clusters WildFire gérés)** et sélectionnez le cluster WildFire géré que vous venez d'ajouter.
2. Configurez la **Timeout Configuration (Configuration du délai avant expiration)** d'authentification pour un appareil WildFire.
   1. Saisissez le nombre de **Failed Attempt (Tentatives échouées)** avant que l'accès d'un utilisateur au CLI de l'appareil WildFire ne soit bloqué.

© 2020 Palo Alto Networks, Inc.

2. Saisissez la **Lockout Time (Durée de verrouillage)**, en minutes, selon l'appareil WildFire verrouille le compte d'un utilisateur après que celui-ci ait atteint le nombre de **Failed Attempts (Tentatives échouées)**.
3. Saisissez le **Idle Timeout (délai d'expiration)**, en minutes, avant que le compte de l'utilisateur ne soit automatiquement déconnecté pour inactivité.
4. Saisissez le **Max Session Count (Compte de session max.)** pour indiquer combien de comptes d'utilisateur peuvent accéder simultanément à un appareil WildFire.
5. Saisissez la **Max Session Time (Durée de session max.)** pendant laquelle l'administrateur peut être connecté avant d'être automatiquement déconnecté.

3. Ajoutez les administrateurs de l'appareil WildFire.

   Les administrateurs peuvent soit être ajoutés en tant qu'administrateur local ou en tant qu'administrateur Panorama importé, mais pas les deux. Ajouter le même administrateur en tant qu'administrateur local et en tant qu'administrateur Panorama importé n'est pas possible et peut entraîner une panne de validation de Panorama. Par exemple, la validation de Panorama échoue si vous ajoutez **`admin1`** en tant qu'administrateur local et administrateur Panorama.

   - Configurez les administrateurs locaux.

     Configurez de nouveaux administrateurs uniques pour les appareils WildFire dans le cluster WildFire. Ces administrateurs sont spécifiques aux appareils WildFire dans le cluster WildFire pour lequel ils sont créés et vous gérez ces administrateurs depuis ce tableau.

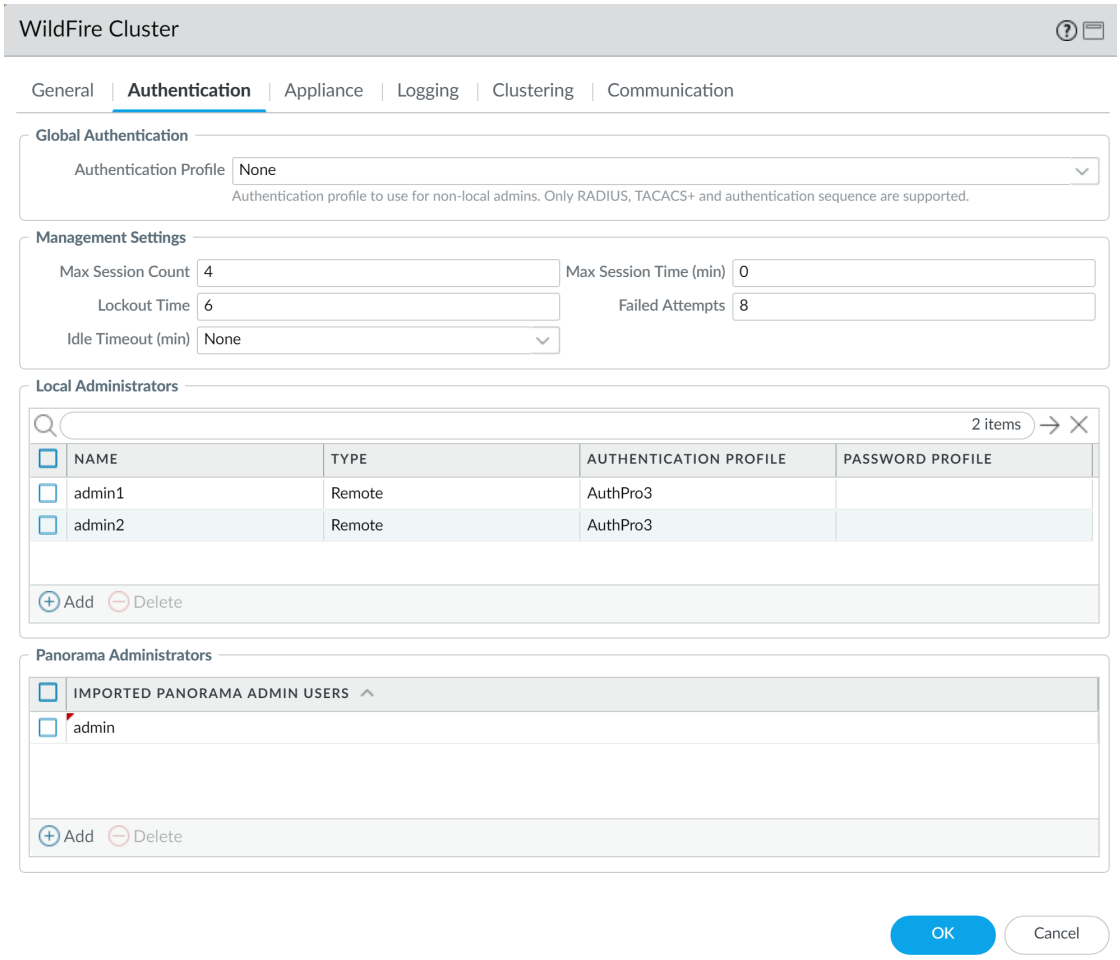
     1. **Add (Ajoutez)** un ou plusieurs administrateurs locaux.
     2. Saisissez un **Name (Nom)** d'utilisateur pour l'administrateur local.
     3. Attribuez un**Authentication Profile (profile d'authentification)** que vous avez préalablement créé.

        Les profils d'authentification LDAP sont compatibles uniquement avec les administrateurs locaux individuels.
     4. Activez (cochez) **Use Public Key Authentication (SSH) (Utiliser l'authentification par clé publique (SSH)** pour importer un fichier de clé publique pour l'authentification.
     5. Sélectionnez un **Password Profile (profil de mot de passe)** pour définir les paramètres d'expiration.
   - Importez les administrateurs Panorama existants

     Importez des administrateurs existants configurés dans Panorama. Ces administrateurs sont configurés et gérés dans Panorama et importés vers tous les appareils WildFire dans le cluster WildFire.

     1. **Add (Ajoutez)** un administrateur Panorama existant
4. Cliquez sur **OK** pour enregistrer la configuration de l'authentification du cluster WildFire.

© 2020 Palo Alto Networks, Inc.



STEP 5 | **Commit (Validez)** et **Commit and Push (Validez et appliquez)** les modifications de votre configuration.

STEP 6 | Accédez à la CLI de l'appareil WildFire afin de pouvoir vérifier que vous pouvez accéder à l'appareil WildFire en utilisant l'utilisateur admin local.

Suppression d'un cluster de la gestion Panorama

Pour supprimer un cluster de la gestion Panorama, sélectionnez **Panorama (Panorama)** > **Managed WildFire Clusters (Clusters WildFire gérés)**, sélectionnez la ligne correspondant au cluster que vous souhaitez supprimer (ne cliquez pas sur le nom du cluster), puis **Remove From Panorama (Supprimer de Panorama)**.

Si vous supprimez un cluster d'appareils WildFire de la gestion Panorama, l'interface Web de Panorama place les appareils WildFire de ce cluster en mode lecture seule. Bien que les appareils WildFire du cluster supprimé s'affichent dans l'interface Web de Panorama, vous ne pouvez transmettre de configurations aux appareils WildFire ou les gérer à l'aide de Panorama lorsqu'ils sont en mode lecture seule. Après avoir été supprimés de la gestion Panorama, les membres du cluster d'appareils WildFire utilisent la configuration locale du cluster. Vous pouvez gérer le cluster à l'aide de la CLI locale.

Pour gérer les appareils WildFire du cluster au moyen de Panorama après avoir supprimé le cluster de la gestion Panorama, réimportez le cluster dans Panorama (**Panorama (Panorama)** > **Managed WildFire Clusters (Clusters WildFire gérés)** > **Import Cluster Config (Importer la configuration du cluster)**).

© 2020 Palo Alto Networks, Inc.

STEP 1 | Sélectionnez le nœud contrôleur du cluster. Le nom **Cluster (Cluster)** se renseigne automatiquement.

STEP 2 | Cliquez sur **OK**. Le nœud contrôleur de secours et les nœuds esclaves sont renseignés automatiquement.

STEP 3 | Cliquez sur **OK (OK)** pour importer le cluster.

STEP 4 | **Commit (Validez)** les modifications.

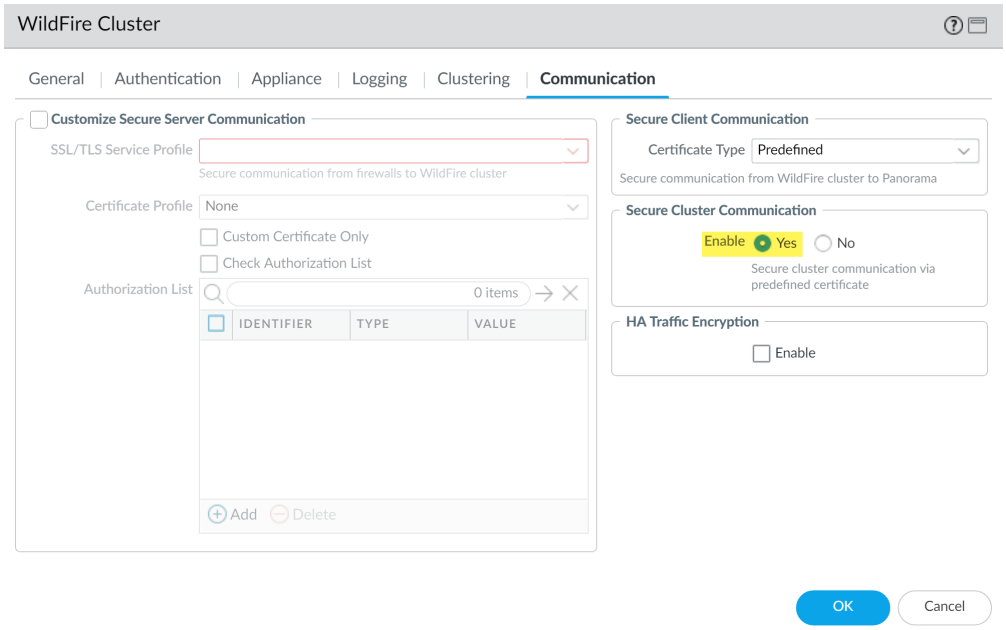
Configurer le chiffrement d'appareil à appareil à l'aide de certificats prédéfinis centralisés sur Panorama

STEP 1 | Mettez à jour chaque appareil WildFire géré vers la version 8.1.x de PAN-OS. Tous les appareils gérés doivent exécuter PAN-OS 8.1 ou une version ultérieure pour activer le cryptage d'appareil à appareil.

STEP 2 | Vérifiez que votre cluster d'appareils WildFire a été correctement configuré et qu'il fonctionne correctement.

STEP 3 | Dans Panorama, sélectionnez **Panorama >Managed WildFire Clusters (Clusters Wildfire gérés)**> *WF_cluster_name (nom du cluster WildFire)*> **Communication.**

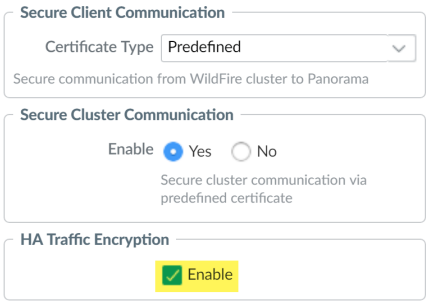
STEP 4 | **Enable (Activez)** la communication sécurisée avec le cluster.



STEP 5 | (Recommandé) **Enable (Activez)** le chiffrement du trafic HD. Ce paramètre facultatif déchiffre le trafic HD entre la paire HD. C'est une pratique exemplaire recommandée par Palo Alto Networks.

Le chiffrement du trafic HD ne peut être désactivé lorsque le mode FIPS/CC est utilisé.

© 2020 Palo Alto Networks, Inc.



STEP 6 | Cliquez sur **OK** pour enregistrer les paramètres du **WildFire Cluster (Cluster WildFire)**.

STEP 7 | **Commit (Validez)** vos modifications.

Configurer le chiffrement d'appareil à appareil à l'aide de certificats personnalisés de manière centralisée sur Panorama

STEP 1 | Mettez à jour chaque appareil WildFire géré vers la version 8.1.x de PAN-OS. Tous les appareils gérés doivent exécuter PAN-OS 8.1 ou une version ultérieure pour activer le cryptage d'appareil à appareil.

STEP 2 | Vérifiez que votre cluster d'appareils WildFire a été correctement configuré et qu'il fonctionne correctement.

STEP 3 | Vérifiez votre configuration de communication sécurisée WildFire existante. Gardez à l'esprit que si vous avez précédemment configuré l'appareil WildFire et le pare-feu pour procurer des communications sécurisées à l'aide d'un certificat personnalisé, vous pouvez également utiliser ce certificat personnalisé pour sécuriser les communications entre les appareils WildFire.

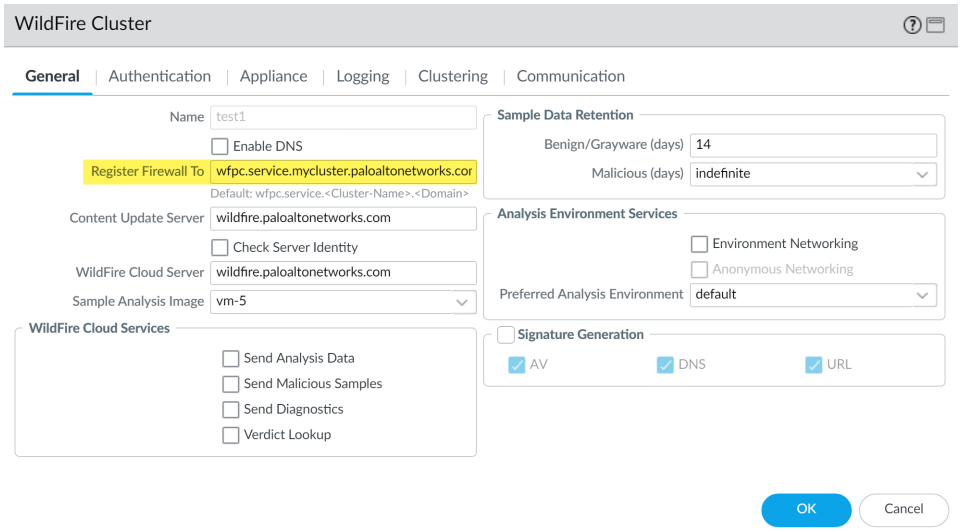
1. Sélectionnez **Panorama >Managed WildFire Clusters (Clusters Wildfire gérés)**> *WF_cluster_name (nom du cluster WildFire)*> **Communication.**
2. Si l'option **Customize Secure Server Communication (Personnaliser la communication du serveur sécurisé)** a été activée et que vous souhaitez utiliser ce certificat, identifiez les détails du certificat personnalisé à utiliser. Sinon, passez à l'étape 5 pour commencer le processus d'installation d'un nouveau certificat personnalisé.
3. Déterminez le nom de domaine complet (FQDN / nom DNS) du certificat personnalisé qui sera utilisé pour définir l'adresse d'enregistrement du pare-feu à l'Étape4.

Assurez-vous de noter le nom du certificat personnalisé et le nom de domaine complet associé. Ceux-ci sont référencés plusieurs fois au cours du processus de configuration.

STEP 4 | Configurez l'adresse d'enregistrement du pare-feu sur Panorama.

1. Dans Panorama, sélectionnez **Panorama >Managed WildFire Clusters (Clusters Wildfire gérés)**> *WF_cluster_name (nom du cluster WildFire)*> **General (Général)**.
2. Dans le champ **Register Firewall To (Enregistrer le pare-feu vers)** spécifiez le nom DNS utilisé pour l'authentification qui figure dans le certificat personnalisé (généralement le SubjectName ou le SubjectAltName). Par exemple, le nom de domaine par défaut est **`wfpc.service.mycluster.paloaltonetworks.com`**.

© 2020 Palo Alto Networks, Inc.

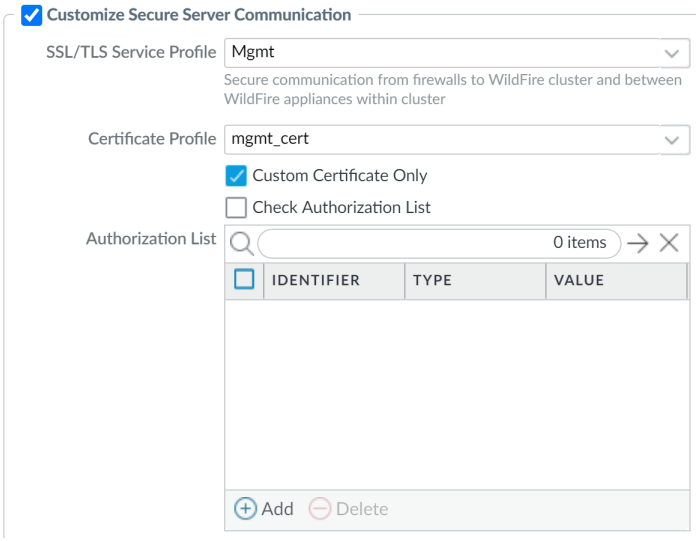


STEP 5 | Configurez les paramètres de **Secure Server Communication (Communication du serveur sécurisée)** WildFire sur Panorama. Si vous avez déjà configuré des communications sécurisées entre le pare-feu et le cluster WildFire et que vous utilisez le certificat personnalisé existant, passez à l'Étape 4 ci-dessous.

1. Dans Panorama, sélectionnez **Panorama >Managed WildFire Clusters (Clusters Wildfire gérés)**> *WF_cluster_name (nom du cluster WildFire)*> **Communication.**
2. Cliquez sur **Customize Secure Server Communication (Personnaliser la communication sécurisée avec le serveur)**.
3. Configurez et déployez des certificats personnalisés utilisés par les appareils WildFire et le pare-feu associé. Le profil de service SSL / TLS définit le certificat personnalisé utilisé par les appareils WildFire pour communiquer avec les homologues de l'appareil WildFire et le pare-feu. Vous devez également configurer les paramètres du certificat personnalisé sur le pare-feu associé au cluster de l'appareil WildFire. La configuration sera effectuée ultérieurement à l'Étape 9.
   1. Ouvrez la liste déroulante Profil de service SSL / TLS et cliquez sur Profil de service SSL / TLS. Configurez un profil de service SSL / TLS avec le certificat personnalisé que vous souhaitez utiliser. Après avoir configuré le profil de service SSL / TLS, cliquez sur OK et sélectionnez le profil de service SSL / TLS nouvellement créé.
   2. Ouvrez la liste déroulante Profil de certificat et cliquez sur Profil de certificat. Configurez un profil de certificat qui identifie le certificat personnalisé utilisé pour établir des connexions sécurisées entre le pare-feu et les appareils WildFire, ainsi qu'entre les appareils WildFire homologues. Après avoir configuré le profil de certificat, cliquez sur OK et sélectionnez le profil nouvellement créé.
4. Cochez la case **Custom Certificate Only (Certificat personnalisé seulement)**. Cela vous permet d'utiliser les certificats personnalisés que vous avez configurés à la place des certificats préconfigurés par défaut.
5. (Facultatif) Configurez une liste d'autorisation. La liste d'autorisation vérifie le nom de l'objet ou l'autre nom de l'objet ; si le nom du **Subject (Objet)** ou le **Subject Alt Name (Autre nom de l'objet)** présenté avec le certificat personnalisé ne correspond pas à un identifiant de la liste d'autorisation, l'authentification sera refusée.
   1. **Add (Ajoutez)** une liste d'autorisation.
   2. Sélectionnez le **Subject (Objet)** ou le **Subject Alt Name (Autre nom de l'objet)** configuré dans le profil de certificat en tant que type d'identifiant.
   3. Entrez le nom commun si l'identifiant est Subject (Objet) et l'adresse IP, le nom d'hôte ou l'e-mail si l'identificateur est Subject Alt Name (Autre nom de l'objet).
   4. Cliquez sur **OK**.

© 2020 Palo Alto Networks, Inc.

5. Sélectionnez **Check Authorization List (Vérifier la liste d'autorisation)** pour appliquer la liste d'autorisation.
6. Cliquez sur **OK**.



STEP 6 | **Enable (Activez)** la communication sécurisée avec le cluster.

STEP 7 | (Recommandé) **Enable (Activez)** le chiffrement du trafic HD. Ce paramètre facultatif déchiffre le trafic HD entre la paire HD. C'est une pratique exemplaire recommandée par Palo Alto Networks.

Le chiffrement du trafic HD ne peut être désactivé lorsque le mode FIPS/CC est utilisé.

STEP 8 | Cliquez sur **OK** pour enregistrer les paramètres du **WildFire Cluster (Cluster WildFire)**.

STEP 9 | Configurez les **paramètres de communication sécurisée** du pare-feu sur Panorama pour associer le cluster d'appareils WildFire au certificat personnalisé du pare-feu. Ce faisant, vous profiterez d'un canal de communications sécurisées entre le pare-feu et le cluster d'appareils WildFire. Si vous avez déjà configuré des communications sécurisées entre le pare-feu et le cluster d'appareils WildFire et que vous utilisez le certificat personnalisé existant, passez à l'Étape suivante.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management Secure Communication Settings (Gestion des paramètres de communication sécurisée)**, puis cliquez sur l'icône de **Edit (Modification)** qui se trouve dans les **Secure Communication Settings (Paramètres de communication sécurisée)** pour configurer les paramètres du certificat personnalisé du pare-feu.
2. Sélectionnez le **Certificate Type (Type de certificat)**, le **Certificate (Certificat)** et le **Certificate Profile (Profil de certificat)** dans les menus déroulants respectifs et configurez-les pour qu'ils utilisent le certificat personnalisé.
3. Sous Customize Communication (Personnaliser la communication), sélectionnez **WildFire Communication (Communication WildFire)**.
4. Cliquez sur **OK**.

STEP 10 | **Commit (Validez)** vos modifications.

© 2020 Palo Alto Networks, Inc.

Affichage de l'état du cluster d'appareils WildFire au moyen de Panorama

Pour confirmer le bon fonctionnement d'un cluster d'appareils WildFire configuré, vous pouvez afficher son état actuel en vous servant de l'appareil Panorama.

Palo Alto Networks recommande d'utiliser la CLI de l'appareil WildFire pour vérifier l'état de votre cluster d'appareils WildFire. Les autres détails sur le statut qui ne sont pas visibles depuis Panorama s'affichent dans le résultat de la commande.

STEP 1 | Sur l'appareil Panorama principal, sélectionnez **Panorama (Panorama) > Managed WildFire Clusters (Clusters WildFire gérés)**.

STEP 2 | Dans la colonne **Cluster Status (État du cluster)**, vérifiez ce qui suit :

1. Les services wfpc et de signature sont actifs.
2. Aucune autre opération n'est présente. Voici certaines opérations anormales et leurs conditions d'état :
   - Decommission [requested / ongoing / denied / success / fail]
   - Suspend [requested / ongoing / denied / success / fail]
   - Reboot [requested / ongoing / denied / success / fail]
   - Cluster [offline / splitbrain / unready]
   - Service [suspended / none]
   - HA [peer-offline / cfg-not-sync / cfg-sync-off]

STEP 3 | Dans la colonne **Config Status (État de la configuration)**, vérifiez ce qui suit :

1. La configuration de l'appareil est **In Sync (Synchronisée)** avec la configuration qui est stockée sur l'appareil Panorama.
2. Aucun autre état n'est présent. Voici certaines conditions d'état anormales :
   - **Out of Sync (Désynchronisées)** : [la configuration de l'appareil n'est pas synchronisée avec sa configuration enregistrée sur Panorama. Vous pouvez placer votre souris sur la loupe pour afficher la cause de l'échec de la synchronisation].

STEP 4 | Dans la colonne **Connected (Connecté)**, vérifiez que l'état des appareils WildFire configurés est **Connected (Connecté)**.

Mise à niveau centrale d'un cluster sur Panorama à partir d'une connexion Internet

Les appareils WildFire d'un cluster peuvent être mis à niveau parallèlement lorsqu'ils sont gérés par Panorama. Si Panorama dispose d'une connexion directe à l'Internet, vous pouvez vérifier l'existence de nouvelles versions et les télécharger directement de Panorama.

Panorama ne peut gérer que des appareils et des clusters d'appareils WildFire qui utilisent la même version logicielle ou une version logicielle ultérieure.

STEP 1 | Faites passer Panorama à une version équivalente ou ultérieure que la version logicielle que vous souhaitez installer sur le cluster WildFire.

Pour plus de renseignements sur la mise à jour de Panorama, reportez-vous à la section Installer les mises à jour de contenu et logicielles pour Panorama.

© 2020 Palo Alto Networks, Inc.

STEP 2 | Suspendez temporairement les analyses des échantillons.

1. Cessez le transfert, par les pare-feu, des nouveaux échantillons vers l'appareil WildFire.
    1. Connectez-vous à l'interface Web du pare-feu.
    2. Sélectionnez **Device > Setup > WildFire (Périphérique > Configuration > WildFire)** et modifiez les **General Settings (Paramètres généraux)**.
    3. Décochez le champ **WildFire Private Cloud (Cloud WildFire privé)**.
    4. Cliquez sur **OK**, puis sur **Commit (Valider)**.
2. Confirmez que l'analyse des échantillons que le pare-feu a déjà soumis à l'appareil est terminée :
    1. Connectez-vous à l'interface Web Panorama.
    2. Sélectionnez **Panorama (Panorama) > Managed WildFire Clusters (Clusters WildFire gérés)** et **View (Afficher)** l'**Utilization (Utilisation)** de l'environnement d'analyse des clusters.
    3. Vérifiez qu'aucune analyse d'échantillons n'est en cours dans la **Virtual Machine Usage (Utilisation de la machine virtuelle)**.

    Si vous ne voulez pas attendre que l'appareil WildFire termine d'analyser les échantillons récemment envoyés, vous pouvez passer à l'étape suivante. Sachez toutefois que l'appareil WildFire abandonnera alors les échantillons en attente dans la file d'attente pour analyse.

STEP 3 | Installez la dernière mise à jour de contenu pour l'appareil WildFire.

Grâce à ces mises à jour, l'appareil dispose des renseignements sur les menaces les plus récentes, ce qui lui permet de bien détecter les logiciels malveillants.

Vous devez installer les mises à jour de contenu avant d'installer les mises à jour logicielles. Consultez les Notes de version pour la version de contenu minimale que vous devez installer pour une version de Panorama.

1. Téléchargez la mise à jour du contenu pour WildFire :
    1. Sélectionnez **Panorama (Panorama) > Device Deployment (Déploiement du périphérique) > Dynamic Updates (Mises à jour dynamiques)**.
    2. Sélectionnez un module de mise à jour du contenu WildFire, puis cliquez sur **Download (Télécharger)**.
2. Cliquez sur **Install (Installer)**.
3. Sélectionnez le ou les clusters d'appareils WildFire ou les appareils individuels que vous souhaitez mettre à niveau.
4. Cliquez sur **OK** pour démarrer l'installation.

STEP 4 | Téléchargez la version PAN-OS du logiciel sur l'appareil WildFire.

Lorsque vous mettez à jour l'appareil WildFire, vous ne pouvez sauter de versions principales. Par exemple, si vous souhaitez passer de la PAN-OS 6.1 à PAN-OS 7.1, vous devez d'abord télécharger la PAN-OS 7.0 et l'installer.

1. Téléchargez la mise à niveau logicielle pour WildFire :
    1. Sélectionnez **Panorama > Device Deployment > Software (Panorama > Déploiement de périphérique > Logiciel)**.
    2. Cliquez sur **Check Now (Vérifier maintenant)** pour récupérer une liste à jour des versions.
    3. Sélectionnez la version de WildFire que vous souhaitez installer et cliquez sur **Download (Télécharger)**.
    4. Cliquez sur **Close (Fermer)** pour sortir de la fenêtre **Download Software (Télécharger le logiciel)**.
2. Cliquez sur **Install (Installer)**.

© 2020 Palo Alto Networks, Inc.

3. Sélectionnez le ou les clusters d'appareils WildFire que vous souhaitez mettre à niveau.
4. Sélectionnez un mode d'installation :
   - (8.0.2 et version ultérieure) **Select Reboot device after install (Sélectionner Redémarrer après chaque installation)**.
   - (8.0.1 et version ultérieure) Sélectionnez **Upload only (Charger seulement)**.
5. Cliquez sur **OK** pour démarrer l'installation.
6. (Facultatif) Surveillez la progression de l'installation sur Panorama.
7. (8.0.1 uniquement) Une fois le module de mise à niveau téléchargé, installez la mise à niveau sur chaque nœud :
   1.
```
admin@WF-500 (passive-controller)> request system software install
 version 8.0.2
```
   2. Confirmez que la mise à niveau est terminée. Exécutez la commande suivante et consultez le type de tâche **Install** et l'état **FIN** :

```
admin@WF-500(passive-controller)> show jobs all

Enqueued Dequeued ID Type Status Result Completed
------------------------------------------------------
14:53:15 14:53:15 5 Install FIN    OK   14:53:19
```
   3. Redémarrez l'appareil en douceur :

```
admin@WF-500(passive-controller)> request cluster reboot-local-node
```

   Le processus de mise à niveau peut prendre de 10 minutes à plus d'une heure, selon le nombre d'échantillons stockés sur l'appareil WildFire.
   4. Reprenez cette étape pour chaque nœud esclave du cluster.

STEP 5 | (Facultatif) Affichez l'état des tâches de redémarrage du nœud de contrôle WildFire.

Sur le contrôleur du cluster WildFire, exécutez la commande suivante et consultez le type de tâche **Install** et l'état **FIN** :

```
admin@WF-500(active-controller)> show cluster task pending
```

STEP 6 | Vérifiez que l'appareil WildFire est prêt à reprendre l'analyse des échantillons.

1. Vérifiez que le champ sw-version indique 8.0.1 :

```
admin@WF-500(passive-controller)> show system info | match sw-version
```

2. Confirmez que tous les processus fonctionnent :

```
admin@WF-500(passive-controller)> show system software status
```

3. Confirmez que la tâche d'auto-validation(**AutoCom**) est terminée :

```
admin@WF-500(passive-controller)> show jobs all
```


© 2020 Palo Alto Networks, Inc.

Mise à niveau centrale d'un cluster sur Panorama sans connexion Internet

Les appareils WildFire d'un cluster peuvent être mis à niveau parallèlement lorsqu'ils sont gérés par Panorama. Si Panorama ne dispose pas d'une connexion directe à l'Internet, vous devez télécharger les mises à jour de contenu et logicielles sur le site de support Palo Alto Networks et les héberger sur un serveur interne avant qu'elles ne puissent être distribuées par Panorama.

Panorama ne peut gérer que des appareils et des clusters d'appareils WildFire qui utilisent la même version logicielle ou une version logicielle ultérieure.

STEP 1 | Faites passer Panorama à une version équivalente ou ultérieure que la version logicielle que vous souhaitez installer sur le cluster WildFire.

Pour plus de renseignements sur la mise à jour de Panorama, reportez-vous à la section Installer les mises à jour de contenu et logicielles pour Panorama.

STEP 2 | Suspendez temporairement les analyses des échantillons.

1. Cessez le transfert, par les pare-feu, des nouveaux échantillons vers l'appareil WildFire.
    1. Connectez-vous à l'interface Web du pare-feu.
    2. Sélectionnez **Device > Setup > WildFire (Périphérique > Configuration > WildFire)** et modifiez les **General Settings (Paramètres généraux)**.
    3. Décochez le champ **WildFire Private Cloud (Cloud WildFire privé)**.
    4. Cliquez sur **OK**, puis sur **Commit (Valider)**.
2. Confirmez que l'analyse des échantillons que le pare-feu a déjà soumis à l'appareil est terminée :
    1. Connectez-vous à l'interface Web Panorama.
    2. Sélectionnez **Panorama (Panorama) > Managed WildFire Clusters (Clusters WildFire gérés)** et **View (Afficher)** l'**Utilization (Utilisation)** de l'environnement d'analyse des clusters.
    3. Vérifiez qu'aucune analyse d'échantillons n'est en cours dans la **Virtual Machine Usage (Utilisation de la machine virtuelle)**.

    Si vous ne voulez pas attendre que l'appareil WildFire termine d'analyser les échantillons récemment envoyés, vous pouvez passer à l'étape suivante. Sachez toutefois que l'appareil WildFire abandonnera alors les échantillons en attente dans la file d'attente pour analyse.

STEP 3 | Téléchargez les mises à jour de contenu et logicielles de WildFire sur un hôte avec un accès Internet. Panorama doit avoir accès à l'hôte.

1. Utilisez un hôte avec accès à Internet pour ouvrir une session sur le site Web d'assistance client de Palo Alto Networks.
2. Téléchargez les mises à jour de contenu :
    1. Cliquez sur **Dynamic Updates (Mises à jour dynamique)** dans la section Tools (Outils).
    2. **Download (Téléchargez)** le contenu souhaité et enregistrez le fichier sur l'hôte. Effectuez cette étape pour chaque type de contenu que vous allez mettre à jour.
3. Télécharger les mises à jour logicielles :
    1. Revenez à la page principale du site de Support Clients de Palo Alto Networks et cliquez sur **Software Updates (Mises à jour de logiciel)** dans la section Tools (Outils).
    2. Consultez la colonne Télécharger pour déterminer la version à installer. Le nom de fichier du module de mise à jour indique le modèle et la version de la mise à niveau : WildFire_<version>.
    3. Cliquez sur le nom du fichier et enregistrez le fichier sur l'hôte.

© 2020 Palo Alto Networks, Inc.

STEP 4 | Installez la dernière mise à jour de contenu pour l'appareil WildFire.

Grâce à ces mises à jour, l'appareil dispose des renseignements sur les menaces les plus récentes, ce qui lui permet de bien détecter les logiciels malveillants.

Vous devez installer les mises à jour de contenu avant d'installer les mises à jour logicielles. Consultez les Notes de version pour la version de contenu minimale que vous devez installer pour une version de Panorama.

1. Téléchargez la mise à jour du contenu pour WildFire :
   1. Sélectionnez **Panorama (Panorama) > Device Deployment (Déploiement du périphérique) > Dynamic Updates (Mises à jour dynamiques)**.
   2. Cliquez sur **Upload (Télécharger)**, sélectionnez le **Type (Type)** de contenu, **Browse (Recherchez)** le fichier de mise à jour de contenu WildFire, puis cliquez sur **OK (OK)**.
   3. Cliquez sur **Install From File (Installer depuis le fichier)**, sélectionnez le **Type (Type)** de module, le **File Name (Nom de fichier)** et les appareils WildFire du cluster que vous souhaitez mettre à niveau, puis cliquez sur **OK (OK)**.
2. Cliquez sur **OK** pour démarrer l'installation.

STEP 5 | Téléchargez la version PAN-OS du logiciel sur l'appareil WildFire.

Lorsque vous mettez à jour l'appareil WildFire, vous ne pouvez sauter de versions principales. Par exemple, si vous souhaitez passer de la PAN-OS 6.1 à PAN-OS 7.1, vous devez d'abord télécharger la PAN-OS 7.0 et l'installer.

1. Téléchargez la mise à niveau logicielle pour WildFire :
   1. Sélectionnez **Panorama > Device Deployment > Software (Panorama > Déploiement de périphérique > Logiciel)**.
   2. Cliquez sur **Check Now (Vérifier maintenant)** pour récupérer une liste à jour des versions.
   3. Sélectionnez la version de WildFire que vous souhaitez installer et cliquez sur **Download (Télécharger)**.
   4. Cliquez sur **Close (Fermer)** pour sortir de la fenêtre **Download Software (Télécharger le logiciel)**.
2. Cliquez sur **Install (Installer)**.
3. Sélectionnez le ou les clusters d'appareils WildFire que vous souhaitez mettre à niveau.
4. Sélectionnez un mode d'installation :
   - (8.0.2 et version ultérieure) **Select Reboot device after install (Sélectionner Redémarrer après chaque installation)**.
   - (8.0.1 et version ultérieure) Sélectionnez **Upload only (Charger seulement)**.
5. Cliquez sur **OK** pour démarrer l'installation.
6. (Facultatif) Surveillez la progression de l'installation sur Panorama.
7. (8.0.1 uniquement) Une fois le module de mise à niveau téléchargé, installez la mise à niveau sur chaque nœud :
   1. ```
      admin@WF-500 (passive-controller)> request system software install
       version 8.0.2
      ```
   2. Confirmez que la mise à niveau est terminée. Exécutez la commande suivante et consultez le type de tâche **`Install`** et l'état **`FIN`** :

      ```
      admin@WF-500(passive-controller)> show jobs all

      Enqueued Dequeued ID Type Status Result Completed
      ---------------------------------------------------
      ```


© 2020 Palo Alto Networks, Inc.
      ```

```
14:53:15 14:53:15 5 Install FIN    OK   14:53:19
```

3. Redémarrez l'appareil en douceur :

```
admin@WF-500(passive-controller)> request cluster reboot-local-node
```

Le processus de mise à niveau peut prendre de 10 minutes à plus d'une heure, selon le nombre d'échantillons stockés sur l'appareil WildFire.

4. Reprenez l'étape 7 pour chaque nœud esclave du cluster.

STEP 6 | (Facultatif) Affichez l'état des tâches de redémarrage du nœud de contrôle WildFire.

Sur le contrôleur du cluster WildFire, exécutez la commande suivante et consultez le type de tâche **`Install`** et l'état **`FIN`** :

```
admin@WF-500(active-controller)> show cluster task pending
```

STEP 7 | Vérifiez que l'appareil WildFire est prêt à reprendre l'analyse des échantillons.

1. Vérifiez que le champ sw-version indique 8.0.1 :

```
admin@WF-500(passive-controller)> show system info | match sw-version
```

2. Confirmez que tous les processus fonctionnent :
   admin@WF-500(passive-controller)> **`show system software status`**
3. Confirmez que la tâche d'auto-validation(**`AutoCom`**) est terminée :

```
admin@WF-500(passive-controller)> show jobs all
```

Gestion des licences et des mises à jour

Vous pouvez utiliser le serveur de gestion Panorama™ pour gérer de manière centralisée les licences, les mises à jour logicielles et les mises à jour de contenu sur les pare-feu et les collecteurs de journaux dédiés. Lorsque vous déployez des licences ou des mises à jour, Panorama vérifie avec le serveur de licences de Palo Alto Networks® ou le serveur de mises à jour la validité de la demande et permet ensuite l'extraction et l'installation de la licence/mise à jour. Cette fonctionnalité facilite le déploiement en éliminant la nécessité de répéter les mêmes tâches sur chaque pare-feu ou Collecteur de journaux dédié. C'est particulièrement utile pour la gestion des pare-feux qui ne disposent pas d'un accès Internet direct ou pour la gestion des collecteurs de journaux dédiés, qui ne disposent pas d'une interface web.

Avant de déployer des mises à jour, reportez-vous à Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire pour des détails importants sur la compatibilité de mise à jour de version .

Vous devez activer un abonnement d'assistance directement sur chaque pare-feu ; Panorama ne peut pas être utilisé pour déployer les abonnements d'assistance.

Pour activer les licences ou installer des mises à jour sur le serveur de gestion Panorama, voir Enregistrer Panorama et installer les licences et installer le contenu et les mises à jour logicielles pour Panorama.

- Gestion des licences des pare-feux à l'aide de Panorama
- Déployer des mises à niveau vers des pare-feu, des collecteurs de journaux et des appareils WildFire à l'aide de Panorama

© 2020 Palo Alto Networks, Inc.

Gestion des licences des pare-feux à l'aide de Panorama

Les étapes suivantes décrivent comment faire pour récupérer de nouvelles licences à l'aide d'un code d'authentification (*auth*) et appliquer les clés de licence pour les pare-feu gérés. Elles décrivent également comment mettre à jour (actualiser) manuellement l'état de la licence sur les pare-feu n'ayant pas d'accès direct à Internet. Dans le cas de pare-feu qui disposent d'un accès direct à Internet, Panorama™ effectue automatiquement une vérification quotidienne sur le serveur de licences, obtient les mises à jour et les renouvellements des licences et les applique aux pare-feu. La vérification est codée strictement pour s'effectuer entre 1 h et 2 h ; vous ne pouvez pas changer cet horaire.



Vous ne pouvez pas utiliser Panorama pour activer la licence d'assistance des pare-feu. Vous devez accéder à chaque pare-feu individuellement pour activer leurs licences d'assistance.

Pour activer les licences pour Panorama, voir Enregistrer Panorama et installer des licences.

- Activez les licences nouvellement achetées.
  1. Sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Licenses (Licences)** et **Activate (Activer)**.
  2. Entrez le **Auth Code (Code d'authentification)** que Palo Alto Networks® fournit pour chaque pare-feu qui a une nouvelle licence.
  3. **Activate (Activez)** la licence.
  4. (Abonnements Wildfire® uniquement) Effectuez une validation sur chaque pare-feu doté d'un nouvel abonnement Wildfire pour terminer l'activation :
     - **Commit (Validez)** les modifications en attente. Vous devez accéder à chaque interface Web de pare-feu pour le faire.
     - Si aucune modification de configuration n'est en attente, effectuez une modification mineure et cliquez sur **Commit (Valider)**. Par exemple, mettez à jour une description de la règle et validez la modification. Si les pare-feux appartiennent au même groupe de périphériques, vous pouvez pousser la modification de la règle à partir de panorama pour initier une validation sur tous ces pare-feux au lieu d'accéder à chaque pare-feu séparément.

     Vérifiez que les règles du profil d'analyse Wildfire *incluent les types de fichiers avancés que l'abonnement Wildfire prend en charge.*

- Mettez à jour l'état de la licence des pare-feux.
  1. Sélectionnez **Panorama** > **Device Deployment (Déploiement du périphérique)** > **Licenses (Licences)**.

     Chaque entrée dans la page indique si la licence est active ou non. Elle affiche également la date d'expiration des licences actives.
  2. Si vous avez préalablement activé les codes d'authentification pour l'abonnement de support directement sur les pare-feu, cliquez sur **Refresh (Actualiser)** et sélectionnez les pare-feu de la liste. Panorama récupère la ou les licences, les déploie sur les pare-feux gérés et met à jour l'état des licences sur son interface Web.
  3. (Licence Data Loss Prevention (prévention des pertes de données - DLP) uniquement) Appliquez la licence mise à jour aux pare-feux gérés pour bénéficier de Enterprise DLP.
     1. Sélectionnez **Commit (Valider)** et **Commit to Panorama (Validez sur Panorama)**.

© 2020 Palo Alto Networks, Inc.

2. Sélectionnez **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)** et **Edit Selections (Modifier les sélections)**.
3. Sélectionnez **Templates (modèles)** et sélectionnez la pile de modèles associée aux pare-feux gérés exploitant Enterprise DLP.

   Cliquez sur **OK** pour continuer.
4. **Push (Appliquez)** la configuration du modèle pour mettre à jour la licence Enterprise DLP.

© 2020 Palo Alto Networks, Inc.

Déployer des mises à niveau vers des pare-feu, des collecteurs de journaux et des appareils WildFire à l'aide de Panorama

Vous pouvez utiliser Panorama™ pour qualifier des mises à jour logicielles et de contenu en les déployant sur un sous-ensemble de pare-feu, de collecteurs de journaux dédiés ou d'appareils et et de clusters d'appareils WildFire® avant d'installer les mises à jour sur le reste de vos appareils gérés. Si vous souhaitez planifier des mises à jour de contenu régulières, Panorama nécessite une connexion directe à Internet. Pour déployer des mises à jour du logiciel ou du contenu sur demande (non programmée), la procédure diffère selon que Panorama est connecté à Internet. Panorama affiche un avertissement si vous déployez manuellement une mise à jour de contenu lorsqu'un processus de mise à jour planifiée a commencé ou commencera dans les cinq minutes.

Lors du déploiement de mises à jour, Panorama notifie les appareils gérées (pare-feu, collecteurs de journaux et appareils WildFire) que des mises à jour sont disponibles et les appareils récupèrent ensuite les packages de mise à jour depuis Panorama. Par défaut, les appareils gérés récupèrent les mises à jour via l'interface de gestion (MGT) sur Panorama. Toutefois, si vous souhaitez réduire la charge de trafic sur l'interface MGT en utilisant une autre interface pour les appareils pour récupérer les mises à jour, vous pouvez Configurer Panorama pour utiliser plusieurs interfaces.

Vous pouvez rapidement rétablir une version de contenu pour un ou plusieurs pare-feu à la version de contenu précédemment installée en utilisant Panorama. Après l'installation d'une nouvelle version de contenu sur le pare-feu, vous pouvez revenir à la version précédemment installée si la version de contenu nouvellement installée déstabilise ou perturbe autrement vos opérations réseau.

Par défaut, vous pouvez télécharger les logiciels ou les mises à jour de chaque type sur Panorama. Lorsque vous commencez n'importe quel téléchargement au-delà de ce plafond, Panorama supprime la plus ancienne mise à jour du type sélectionné. Pour modifier le maximum, consultez Gestion du stockage de Panorama pour les mises à jour logicielles et de contenu*.*

- Mises à jour prises en charge
- Planifier une mise à jour de contenu à l'aide de Panorama
- Mettre à niveau les collecteurs de journaux lorsque Panorama est connecté à Internet
- Mettre à niveau les collecteurs de journaux lorsque Panorama n'est pas connecté à Internet
- Mettre à niveau les pare-feu lorsque Panorama est connecté à Internet
- Mettre à niveau les pare-feu lorsque Panorama n'est pas connecté à Internet
- Mettre à niveau un pare-feu ZTP
- Rétablir les mises à jour du contenu depuis Panorama

Mises à jour prises en charge

Les mises à jour logicielles et de contenu que vous pouvez installer dépendent des abonnements actifs sur chaque pare-feu, collecteur de journaux et appareil et cluster d'appareils WildFire® :

© 2020 Palo Alto Networks, Inc.

Type d'appareil	Mises à jour logicielles	Mises à jour du contenu
Collecteur de journaux	Panorama™	Applications (les collecteurs de journaux n'ont pas besoin de signatures de menaces) Antivirus Filtrage d'URL BrightCloud WildFire®
Pare-feu	PAN-OS® Agent / application GlobalProtect™	Applications Applications et menaces Antivirus Filtrage d'URL BrightCloud WildFire
WildFire	PAN-OS Images VM	WildFire

Planifier une mise à jour de contenu à l'aide de Panorama

Panorama™ nécessite une connexion Internet directe pour la planification des mises à jour prises en charge sur les pare-feu, les collecteurs de journaux et les appareils et clusters d'appareils WildFire®. Sinon, vous pouvez effectuer uniquement les mises à jour sur demande. (Pour planifier des mises à jour Antivirus, WildFire ou URL BrightCloud pour les collecteurs de journaux, doivent exécuter Panorama 7.0.3 ou une version ultérieure.) Chaque pare-feu, collecteur de journaux ou appareil et cluster d'appareils WildFire recevant une mise à jour génère un journal pour indiquer que l'installation a réussi (un journal de configuration) ou échoué (un journal système). Pour planifier des mises à jour sur le serveur de gestion Panorama, consultez Installer des mises à jour pour Panorama avec une connexion Internet.

Avant de déployer des mises à jour, reportez-vous à Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire pour des détails importants sur la compatibilité des versions de contenu. Consultez les Notes de version pour la version de contenu minimale que vous devez installer pour une version de Panorama.

Panorama ne peut télécharger qu'une seule mise à jour à la fois pour les mises à jour du même type, donc si vous planifiez plusieurs mises à jour du même type à télécharger pendant le même intervalle de temps, seul le premier téléchargement réussira. Pour garantir la réussite de plusieurs mises à jour du même type, échelonnez les mises à jour.

Si vos pare-feu se connectent directement au serveur de mise à jour de Palo Alto Networks®, vous pouvez également utiliser des modèles Panorama (Device (Périphérique) > Dynamic Updates (Mises à jour dynamiques)) pour appliquer des horaires de mise à jour de contenu sur les pare-feux. Si vous souhaitez retarder l'installation des mises à jour pour une période après leur publication, vous devez déployer des calendriers à l'aide de modèles. Dans de rares cas, une mise à jour inclura des erreurs, ce qui spécifie qu'un délai augmente la probabilité que Palo Alto Networks identifie et supprime cette mise à jour du serveur de mise à jour avant que vos pare-feu ne les installent.

© 2020 Palo Alto Networks, Inc.

Procédez comme suit pour chaque type de mise à jour que vous souhaitez planifier.

STEP 1 | Sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Dynamic Updates (Mises à jour dynamiques)**, cliquez sur **Schedules (Horaires)** et **Add (Ajoutez)** un horaire.

STEP 2 | Spécifiez un **Name (Nom)** pour identifier l'horaire, le **Type** de la mise à jour et la fréquence de mise à jour (**Recurrence (Récurrence)**). Les options de fréquence disponibles dépendent du **Type** de la mise à jour.

PAN-OS® utilise le fuseau horaire de Panorama pour la planification des mises à jour.

Si vous définissez le **Type** sur **App and Threat (Applications et menaces)**, les collecteurs de journaux l'installent et n'ont besoin que du contenu des applications, pas du contenu des menaces. Les pare-feux utilisent et les applications et le contenu des menaces. Pour plus d'informations, consultez la section Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire .

STEP 3 | Sélectionnez l'une des actions de planification suivantes, puis sélectionnez les pare-feux ou les collecteurs de journaux :

- **Download And Install (Télécharger et installer)** (Recommandé) : sélectionnez **Devices (Périphériques)** (pare-feu), **Log Collectors (Collecteurs de journaux)**, ou **WildFire Appliances and Clusters (Appareils et clusters WildFire)**.
- **Download Only (Télécharger uniquement)** : Panorama télécharge la mise à jour mais ne l'installe pas.

STEP 4 | Cliquez sur **OK**.

STEP 5 | Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)**, puis **Commit (Validez)** vos changements.

Mettre à niveau les collecteurs de journaux lorsque Panorama est connecté à Internet

Pour obtenir la liste des logiciels et le contenu des mises à jour, vous pouvez installer sur collecteurs de journaux, voir Mises à jour prises en charge.

Vous devez mettre à niveau tous les collecteurs de journaux d'un groupe de collecteurs en même temps afin d'éviter de perdre des données de journal. Aucun transfert de journaux ou collecte de journaux ne se produit si les collecteurs de journaux d'un groupe de collecteurs n'utilisent pas tous la même version de PAN-OS. De plus, les données des journaux des collecteurs de journaux du groupe de collecteur ne sont pas visibles dans les onglets **ACC** ou **Monitor (Surveillance)** jusqu'à ce que tous les collecteurs de journaux exécutent la même version PAN-OS. Par exemple, si vous disposez de trois collecteurs de journaux dans un groupe de collecteurs et que vous mettez à niveau deux d'entre eux, aucun journal n'est alors transmis aux collecteurs de journaux du groupe de collecteurs.

PAN-OS® 9.0 a intégré un nouveau format de données de journaux pour les collecteurs de journaux dédiés et locaux. Lorsque vous passez à PAN-OS 10.0, les données de journaux existantes sont automatiquement converties au nouveau format lors de la mise à niveau de PAN-OS 9.0. Lors du reformatage, les données des journaux ne sont pas visibles dans les onglets **ACC** ou **Monitor (Surveillance)**. De plus, les nouvelles données des journaux ne sont pas transférées aux collecteurs de journaux avant que le reformatage a été effectué. Lors du reformatage, de nouveaux journaux sont rédigés sur le disque système du pare-feu

© 2020 Palo Alto Networks, Inc.

et après que la procédure a terminé avec succès, les nouveaux journaux sont transmis au collecteur de journaux appropriée.

Palo Alto Networks vous recommande de mettre à niveau les collecteurs de journaux lors d'une fenêtre de maintenance. En raison de la migration du format des journaux, la procédure de mise à niveau complète prend un nombre supplémentaire d'heures, selon la quantité de données de journaux sur les collecteur de journaux dédiés et locaux.

STEP 1 | Avant de mettre à niveau les collecteurs de journaux, vérifiez que vous exécutez la version du logiciel Panorama™ appropriée sur le serveur de gestion Panorama.



Palo Alto Networks® recommande vivement que Panorama et les collecteurs de journaux exécutent la même version du logiciel Panorama et que Panorama, les collecteurs de journaux et tous les pare-feu gérés exécutent la même version de contenu. Pour les détails de compatibilité de logiciels et de contenus importants, voir Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire*.*

Panorama doit exécuter la même version de logiciel (ou une version ultérieure) que le collecteur de journaux, mais doit avoir la même version ou une version antérieure :

- **Version du logiciel** : si votre serveur de gestion Panorama n'exécute pas déjà la même version de logiciel ou une version ultérieure que la version à laquelle vous souhaitez mettre à jour les collecteurs de journaux, vous devez installer la même version ou une version ultérieure sur Panorama (voir Installer les mises à jour de contenu et logicielles pour Panorama) avant de mettre à jour les collecteurs de journaux.
- **Version du contenu** : pour les versions de publication de contenu, vous devez vous assurer que tous les collecteurs de journaux exécutent la dernière version de contenu ou, au minimum, une version ultérieure à celle de Panorama. Sinon, commencez par mettre à jour les pare-feu gérés (en utilisant Panorama), puis mettez à jour les collecteurs de journaux avant de mettre à jour la version de contenu sur le serveur de gestion Panorama.

Pour vérifier les versions de logiciel et de contenu :

- **Serveur de gestion Panorama** : pour déterminer quelles versions de logiciel et de contenu sont en cours d'exécution sur le serveur de gestion Panorama, connectez-vous à l'interface Web Panorama et accédez aux paramètres informations générales (**Dashboard (Tableau de bord)**).
- **Collecteurs de journaux** : pour déterminer quelles versions de logiciel et de contenu sont en cours d'exécution sur les collecteurs de journaux, connectez-vous à la CLI de chaque collecteur de journaux et exécutez la commande **`show system info`**

STEP 2 | Installez les dernières mises à jour de contenu.



Consultez les Notes de version *pour les versions de contenu minimum requises pour une version de logiciel Panorama.*

1. **Check Now (Vérifier maintenant)** (**Panorama** > **Device Deployment (Déploiement de périphériques)** > **Dynamic Updates (Mises à jour dynamiques)**) les dernières mises à jour. Si une mise à jour est disponible, la colonne Action affiche un lien **Download (Télécharger)**.
2. Si elles ne sont pas déjà installées, **Download (Téléchargez)** les mises à jour de contenu appropriées. Une fois le téléchargement terminé, le lien se trouvant dans la colonne Action passe de **Download (Télécharger)** à **Install (Installer)**.
3. **Install (Installez)** la mise à jour de contenu (mise à jour des applications ou des applications et menaces avant tout autre) :

   Cliquez sur **Install (Installer)**, sélectionnez les collecteurs de journal et cliquez sur **OK**.

© 2020 Palo Alto Networks, Inc.

Peu importe si votre abonnement comprend le contenu Applications et Menaces, Panorama installe et n'a besoin que du contenu Applications. Pour plus d'informations, consultez la section Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire .

4. Répétez les sous-étapes 2 et 3 pour toutes les autres mises à jour (Antivirus, WildFire ou Filtrage d'URL) au besoin, une à la fois et dans n'importe quel ordre.

STEP 3 | Déterminer le chemin de mise à niveau vers PAN-OS 10.0.

Vous ne pouvez pas sauter l'installation de versions de fonctions dans le chemin de la version PAN-OS en cours vers PAN-OS 10.0. Passez en revue les problèmes connus et les modifications du comportement par défaut dans les Notes de version et les considérations de mise à niveau vers une version supérieure ou antérieure dans le Guide des nouvelles fonctionnalités de chaque version à travers laquelle vous passez dans le cadre de votre chemin de mise à niveau.

(Requis si vous faites une mise à niveau à partir de la version 7.1 ou antérieure) PAN-OS 8.0 a lancé un nouveau format de stockage des journaux. Après avoir effectué la mise à niveau vers PAN-OS 8.0, vous devez Migrer les journaux de Panorama vers le nouveau format de journal avant de continuer la mise à niveau. La migration de journaux est une tâche ponctuelle. Si vous avez déjà migré les journaux sur le collecteur de journaux pour une mise à niveau vers PAN-OS 8.0, vous n'avez pas besoin de les migrer à nouveau lorsque vous passez à PAN-OS 8.1.

Si vous mettez à niveau plusieurs collecteurs de journaux, rationalisez le processus en déterminant les chemins de mise à niveau pour tous les collecteurs de journaux que vous avez l'intention de mettre à niveau avant de commencer à télécharger des images.

STEP 4 | Pour tous les collecteurs de journaux que vous avez l'intention de mettre à jour, utilisez les chemins de mise à niveau identifiés à l'étape 3 pour mettre à niveau les collecteurs de journaux vers votre version Panorama cible.

1. Sur Panorama, **Check Now (Vérifier maintenant)** (**Panorama** > **Device Deployment (Déploiement de périphériques)** > **Software (Logiciel)**) les dernières mises à jour. Si une mise à jour est disponible, la colonne Action affiche un lien **Download (Télécharger)**.
2. Pour chaque version de votre chemin de mise à niveau, **Download (Téléchargez)** le fichier spécifique au modèle pour la version finale à laquelle vous effectuez la mise à niveau. Par exemple, pour mettre à niveau un appareil de série M vers Panorama 10, téléchargez l'image `Panorama_m-10.0.0`.

   Après un téléchargement réussi, la colonne Action passe de **Download (Télécharger)** à **Install (Installer)** pour cette image.
3. Cliquez sur **Install (Installer)** pour la première (ou prochaine) version de votre chemin de mise à niveau et sélectionnez les collecteurs de journaux appropriés.
4. Sélectionnez l'un des éléments suivants en fonction de la version que vous installez dans votre chemin de la mise à niveau (étape 3) :
   - **Upload only to device (do not install) (Charger sur le périphérique uniquement (ne pas Installer))**.
   - **Reboot device after install (Redémarrer le périphérique après l'installation)**.
5. Cliquez sur **OK** pour démarrer le chargement ou l'installation.
6. Répétez les sous-étapes 3 à 5 ci-dessus jusqu'à ce que les collecteurs de journaux exécutent la version souhaitée.

STEP 5 | Vérifiez l'état de la migration du format des journaux après la réussite d'une mise à niveau vers PAN-OS 10.0.

1. Connectez-vous à l'ILC Panorama du collecteur de journaux.
2. Exécutez la commande suivante pour vérifier l'état de la migration du formation des journaux :

© 2020 Palo Alto Networks, Inc.

```
admin> debug logdb show-es-upgrade-time
```

Réponse type lorsque la migration du format des journaux est toujours en cours :

```
Response from logger 23456212: 50.98% of indices upgraded complete.
 Approximately less than a minute remaining until migration is complete.
 Once the log migration is complete, please run the 'show log-collector-
es-cluster health' command to check the ElasticSearch cluster status to
 verify logging and reporting functionality is restored.
```

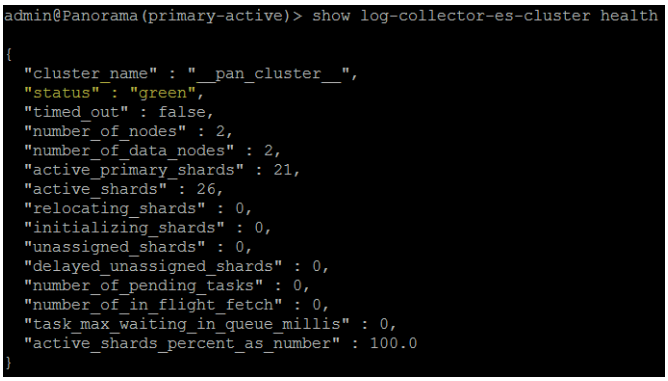
Réponse lorsque la migration du format des journaux est terminée :

```
Response from logger 23456212: 100% of indices complete, please run the
 'show log-collector-es-culster health' command to check the ElasticSearch
 cluster status to verify logging and reporting functionality is restored.
```

3. Une fois la migration du format des journaux est terminé, exécutez la commande suivante pour vérifier l'état du cluster ElasticSearch avant de passer à l'étape suivante :

```
admin> show log-collector-es-cluster health
```

Passez à l'étape suivante lorsque l'état de santé (`"status"`) du cluster ElasticSearch indique `"green"` :



STEP 6 | Vérifiez le logiciel et/ou les versions de mise à jour de contenu qui sont installées sur le collecteur de journaux.

Saisissez la commande opérationnelle **`show system info`**. Le résultat sera semblable à ci-dessous :

```
sw-version: 10.0.0
app-version: 8270-6076
app-release-date: 2020/05/08 18:21:51
```

Mettre à niveau les collecteurs de journaux lorsque Panorama n'est pas connecté à Internet

Pour obtenir la liste des logiciels et le contenu des mises à jour, vous pouvez installer sur collecteurs de journaux, voir Mises à jour prises en charge.

© 2020 Palo Alto Networks, Inc.

PAN-OS® 9.0 a intégré un nouveau format de données de journaux pour les collecteurs de journaux dédiés et locaux. Lorsque vous passez à PAN-OS 10.0, les données de journaux existantes sont automatiquement converties au nouveau format lors de la mise à niveau de PAN-OS 9.0. Lors du reformatage, les données des journaux ne sont pas visibles dans les onglets **ACC** ou **Monitor (Surveillance)**. De plus, les nouvelles données des journaux ne sont pas transférées aux collecteurs de journaux avant que le reformatage a été effectué. Lors du reformatage, de nouveaux journaux sont rédigés sur le disque système du pare-feu et après que la procédure a terminé avec succès, les nouveaux journaux sont transmis au collecteur de journaux appropriée.

Vous devez mettre à niveau tous les collecteurs de journaux d'un groupe de collecteurs en même temps afin d'éviter de perdre des données de journal. Aucun transfert de journaux ou collecte de journaux ne se produit si les collecteurs de journaux d'un groupe de collecteurs n'utilisent pas tous la même version de PAN-OS. De plus, les données des journaux des collecteurs de journaux du groupe de collecteur ne sont pas visibles dans les onglets **ACC** ou **Monitor (Surveillance)** jusqu'à ce que tous les collecteurs de journaux exécutent la même version PAN-OS. Par exemple, si vous disposez de trois collecteurs de journaux dans un groupe de collecteurs et que vous mettez à niveau deux d'entre eux, aucun journal n'est alors transmis aux collecteurs de journaux du groupe de collecteurs.

Palo Alto Networks vous recommande de mettre à niveau les collecteurs de journaux lors d'une fenêtre de maintenance. En raison de la migration du format des journaux, la procédure de mise à niveau complète prend un nombre supplémentaire d'heures, selon la quantité de données de journaux sur les collecteur de journaux dédiés et locaux.

STEP 1 | Avant de mettre à niveau les collecteurs de journaux, vérifiez que vous exécutez la version du logiciel Panorama™ appropriée sur le serveur de gestion Panorama.



Palo Alto Networks® recommande vivement que Panorama et les collecteurs de journaux exécutent la même version du logiciel Panorama et que Panorama, les collecteurs de journaux et tous les pare-feu gérés exécutent la même version de contenu. Pour les détails de compatibilité de logiciels et de contenus importants, voir Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire*.*

Panorama doit exécuter la même version de logiciel (ou une version ultérieure) que le collecteur de journaux, mais doit avoir la même version ou une version antérieure :

- **Version du logiciel** : si votre serveur de gestion Panorama n'exécute pas déjà la même version de logiciel ou une version ultérieure que la version à laquelle vous souhaitez mettre à jour les collecteurs de journaux, vous devez installer la même version ou une version ultérieure sur Panorama (voir Installer les mises à jour de contenu et logicielles pour Panorama) avant de mettre à jour les collecteurs de journaux.
- **Version du contenu** : pour les versions de publication de contenu, vous devez vous assurer que tous les collecteurs de journaux exécutent la dernière version de contenu ou, au minimum, une version plus récente que celle que vous installerez ou que vous exécutez sur Panorama. Sinon, commencez par mettre à jour les pare-feu gérés (en utilisant Panorama), puis mettez à jour les collecteurs de journaux avant de mettre à jour la version de contenu sur le serveur de gestion Panorama (voir Installer les mises à jour de contenu et logicielles pour Panorama).

Pour vérifier les versions de logiciel et de contenu :

- **Serveur de gestion Panorama** : pour déterminer quelles versions de logiciel et de contenu sont en cours d'exécution sur le serveur de gestion Panorama, connectez-vous à l'interface Web Panorama et accédez aux paramètres informations générales (**Dashboard (Tableau de bord)**).
- **Collecteurs de journaux** : pour déterminer quelles versions de logiciel et de contenu sont en cours d'exécution sur les collecteurs de journaux, connectez-vous à la CLI de chaque collecteur de journaux et exécutez la commande **`show system info`**

© 2020 Palo Alto Networks, Inc.

STEP 2 | Déterminez les mises à jour de contenu que vous devez installer sur les collecteurs de journaux. Consultez les Notes de version pour la version de contenu minimale que vous devez installer pour une version de Panorama.

Vous devez installer les mises à jour de contenu avant les mises à jour logicielles.

1. Exécutez la commande CLI **`show system info`** pour afficher les versions de mise à jour actuelles.
2. Pour chaque mise à jour de contenu, déterminez si vous avez besoin de mises à jour et notez les mises à jour de contenu que vous devez télécharger à l'étape 4.

   Assurez-vous que Panorama exécute la même version de contenu, mais pas une version ultérieure à celle exécutée sur les pare-feu gérés et les collecteurs de journaux.
3. (Au besoin) Avant de mettre à jour les versions de contenu sur les collecteurs de journaux, commencez par mettre à niveau les pare-feu gérés vers les mêmes versions de contenu ou les versions ultérieures.

STEP 3 | Déterminer le chemin de mise à niveau vers PAN-OS 9.2.

Vous ne pouvez pas sauter l'installation de versions de fonctions dans le chemin de la version PAN-OS en cours vers PAN-OS 10.0. Passez en revue les problèmes connus et les modifications du comportement par défaut dans les Notes de version et les considérations de mise à niveau vers une version supérieure ou antérieure dans le Guide des nouvelles fonctionnalités de chaque version à travers laquelle vous passez dans le cadre de votre chemin de mise à niveau.

(Requis si vous faites une mise à niveau à partir de la version 7.1 ou antérieure) PAN-OS 8.0 a lancé un nouveau format de stockage des journaux. Après avoir effectué la mise à niveau vers PAN-OS 8.0, vous devez Migrer les journaux de Panorama vers le nouveau format de journal avant de continuer la mise à niveau. La migration de journaux est une tâche ponctuelle. Si vous avez déjà migré les journaux sur le collecteur de journaux pour une mise à niveau vers PAN-OS 8.0, vous n'avez pas besoin de les migrer à nouveau lorsque vous passez à PAN-OS 8.1.

Si vous mettez à niveau plusieurs collecteurs de journaux, rationalisez le processus en déterminant les chemins de mise à niveau pour tous les collecteurs de journaux que vous avez l'intention de mettre à niveau avant de commencer à télécharger des images.

STEP 4 | Téléchargez les mises à jour de contenu et logicielles sur un hôte qui peut se connecter et charger les fichiers sur Panorama via SCP ou HTTPS.

1. Utilisez un hôte avec accès à Internet pour ouvrir une session sur le site Web d'assistance client de Palo Alto Networks.
2. Téléchargez les mises à jour de contenu :
   1. Cliquez **Dynamic Updates (Mises à jour dynamique)** dans la section Ressources.
   2. **Download (Téléchargez)** les mises à jour de contenu souhaitées et enregistrez les fichiers sur l'hôte. Effectuez cette étape pour chaque type de contenu que vous allez mettre à jour.
3. Télécharger les mises à jour logicielles :
   1. Retournez à la page principale du site d'assistance client de Palo Alto Networks et cliquez sur **Software Updates (Mises à jour logicielles)** dans la section Ressources.
   2. Consultez la colonne Télécharger pour déterminer la version à installer. Les noms de fichiers de package de mise à jour pour les appareils de série M commencent par « Panorama_m » suivi du numéro de version. Par exemple, pour mettre à niveau un appareil de série M vers Panorama 10.0.0, téléchargez l'image `Panorama_m-10.0.0`.

© 2020 Palo Alto Networks, Inc.

Vous pouvez rapidement localiser les images de Panorama en sélectionnant Panorama M Images (Images M Panorama) (pour les appareils de série M) depuis le menu déroulant Filter By (Filtrer par).

4. Cliquez sur le nom du fichier approprié et enregistrez le fichier sur l'hôte.

STEP 5 | Installez les mises à jour de contenu sur les collecteurs de journaux.

Si vous devez installer des mises à jour de contenu, vous devez le faire avant d'installer les mises à jour logicielles. En outre, installez d'abord les mises à jour de contenu sur les pare-feu, puis sur les collecteurs de journaux avant de mettre à jour la version de contenu sur Panorama.

Installez d'abord les mises à jour des applications ou des applications et menaces, puis installez toutes les autres mises à jour (Antivirus, WildFire® ou Filtrage d'URL) au besoin, une à la fois et dans n'importe quel ordre.

Peu importe si votre abonnement comprend le contenu Applications et Menaces, Panorama installe et n'a besoin que du contenu Applications. Pour plus d'informations, consultez la section Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire .

1. Dans Panorama, sélectionnez **Panorama (Panorama)** > **Device Deployment (Déploiement de périphérique)** > **Dynamic Updated (Mises à jour dynamiques)**.
2. Cliquez sur **Upload (Charger)**, sélectionnez le **Type** de mise à jour, **Browse (Rechercher)** le fichier de mise à jour de contenu approprié sur l'hôte, puis cliquez sur **OK**.
3. Cliquez sur **Install From File (Installer depuis le fichier)**, sélectionnez le **Type** de mise à jour et sélectionnez le **File Name (Nom du fichier)** de la mise à jour que vous venez de charger.
4. Sélectionnez les collecteurs de journaux.
5. Cliquez sur **OK** pour démarrer l'installation.
6. Répétez ces étapes pour chaque mise à jour de contenu.

STEP 6 | Installez les mises à jour logicielles.

1. Sélectionnez **Panorama** > **Device Deployment (Déploiement de périphérique)** > **Software (Logiciel)**.
2. Cliquez sur **Upload (Charger)**, **Browse (Rechercher)** le fichier de mise à jour logicielle approprié sur l'hôte, puis cliquez sur **OK**.
3. Cliquez sur **Install (Installer)** dans la colonne Action pour la version que vous venez de charger.
4. Sélectionnez les collecteurs de journaux sur lesquels installer la mise à jour.
5. Sélectionnez l'un des éléments suivants en fonction de la version de logiciel que vous installez dans le chemin de la mise à niveau (Étape 3) :
   - **Upload only to device (do not install) (Charger sur le périphérique uniquement (ne pas Installer))**.
   - **Reboot device after install (Redémarrer le périphérique après l'installation)**.
6. Cliquez sur **OK** pour démarrer l'installation.

STEP 7 | Vérifiez l'état de la migration du format des journaux après la réussite d'une mise à niveau vers PAN-OS 10.0.

1. Connectez-vous à l'ILC Panorama du collecteur de journaux.
2. Exécutez la commande suivante pour vérifier l'état de la migration du formation des journaux :

```
admin> debug logdb show-es-upgrade-time
```


© 2020 Palo Alto Networks, Inc.

Réponse type lorsque la migration du format des journaux est toujours en cours :

```
Response from logger 23456212: 50.98% of indices upgraded complete.
 Approximately less than a minute remaining until migration is complete.
 Once the log migration is complete, please run the 'show log-collector-
es-cluster health' command to check the ElasticSearch cluster status to
 verify logging and reporting functionality is restored.
```

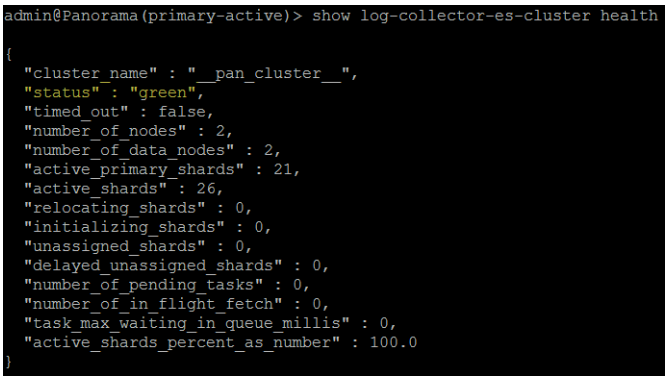
Réponse lorsque la migration du format des journaux est terminée :

```
Response from logger 23456212: 100% of indices complete, please run the
 'show log-collector-es-culster health' command to check the ElasticSearch
 cluster status to verify logging and reporting functionality is restored.
```

3. Une fois la migration du format des journaux est terminé, exécutez la commande suivante pour vérifier l'état du cluster ElasticSearch avant de passer à l'étape suivante :

```
admin> show log-collector-es-cluster health
```

Passez à l'étape suivante lorsque l'état de santé (`"status"`) du cluster ElasticSearch indique `"green"` :



STEP 8 | Vérifiez que le logiciel et/ou les versions de mise à jour de contenu sont installées sur le collecteur de journaux.

Ouvrez une session ILC du Collecteur de Journaux et rendez la commande **`montrer les informations système`** opérationnelle. Le résultat sera semblable à ci-dessous :

```
sw-version: 10.0.0
app-version: 8270-6076
app-release-date: 2020/05/08 18:21:51
```

Mettre à niveau les pare-feu lorsque Panorama est connecté à Internet

Passez en revue les notes de publication de PAN-OS 10.0 puis utilisez la procédure suivante pour mettre à niveau les pare-feux que vous gérez avec Panorama. Cette procédure s'applique aux pare-feu autonomes et aux pare-feu déployés dans une configuration à haute disponibilité (HA).

© 2020 Palo Alto Networks, Inc.

Si Panorama ne parvient pas à se connecter directement au serveur de mises à jour, suivez la procédure Mettre à niveau les pare-feu lorsque Panorama n'est pas connecté à Internet *afin de pouvoir télécharger manuellement des images dans Panorama, puis les distribuer les images sur le pare-feu.*

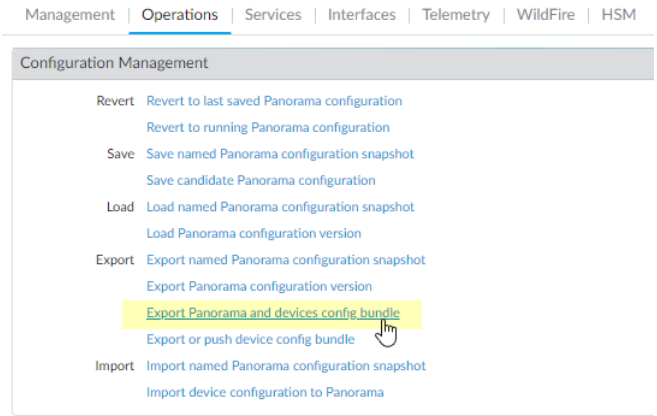
Avant de faire la mise-à-jour du pare-feu sur Panorama, vous devez :

- Assurez-vous que Panorama exécute la même version ou une version ultérieure de PAN-OS que celle utilisée pour la mise à niveau. Avant de mettre à niveau les pare-feux gérés vers PAN-OS 10.0, vous devez installer des mises à jour de contenu et de logiciel pour Panorama et déployer des mises à niveau vers les pare-feux, les collecteurs de journaux et les appareils WildFire à l'aide de Panorama pour mettre à niveau Panorama et les collecteurs de journaux vers PAN-OS 10.0
- Assurez-vous que les pare-feu sont branchés à une source d'alimentation fiable. La perte de courant au cours d'une mise à niveau peut rendre les pare-feu inutilisables.

STEP 1 | Effectuez une copie de sauvegarde du fichier de configuration actuel sur chaque pare-feu géré que vous envisagez de mettre à niveau.

Bien que le pare-feu crée automatiquement une sauvegarde de la configuration, il est recommandé de créer et de stocker une sauvegarde externe avant de procéder à la mise à niveau.

1. À partir de l'interface web de Panorama, sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)** et cliquez sur **Export Panorama and devices config bundle (Exporter le groupe de configuration des périphériques et de Panorama)** pour générer et exporter la dernière sauvegarde de configuration de Panorama et de chaque appareil géré.



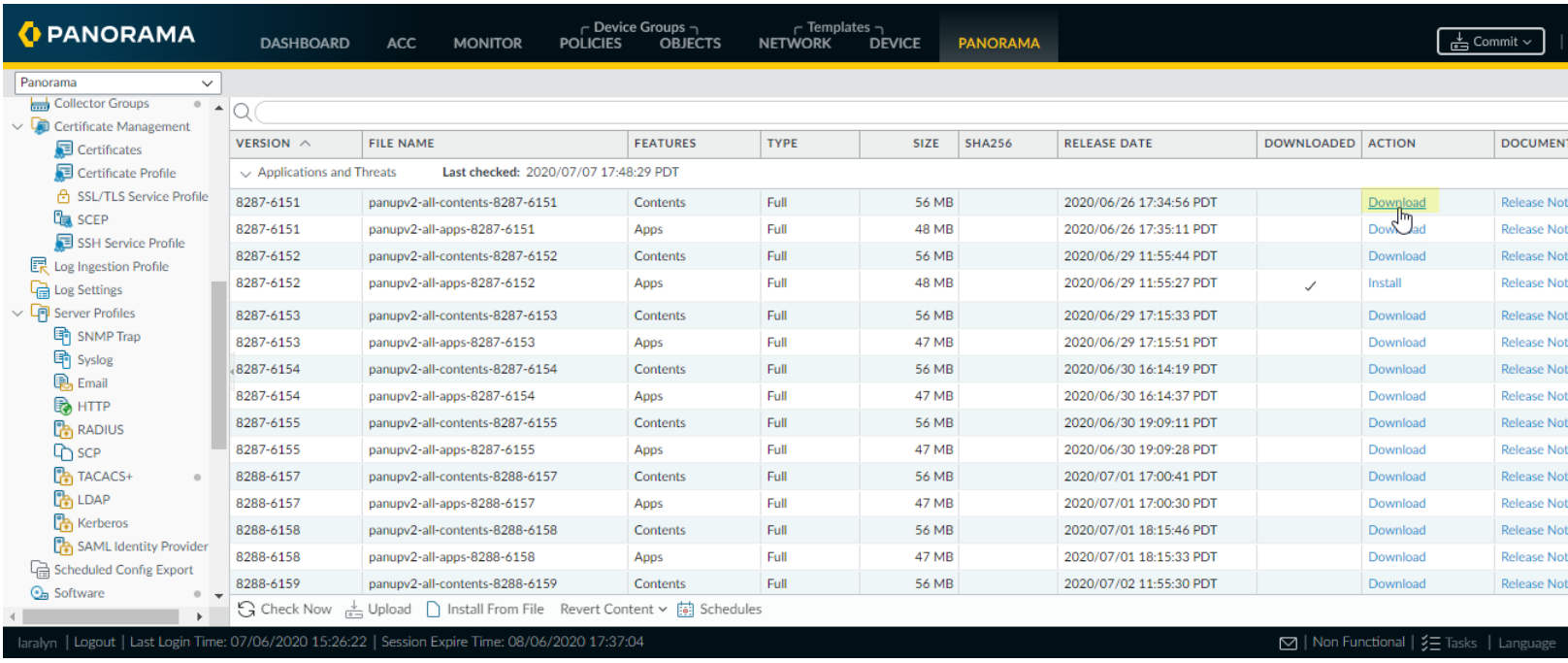
2. Enregistrez le fichier exporté dans un emplacement externe au pare-feu. Vous pouvez utiliser cette sauvegarde pour restaurer la configuration en cas de problème pendant la mise à niveau.

STEP 2 | Mettez à jour la version de contenu sur les pare-feu que vous prévoyez de mettre à niveau.

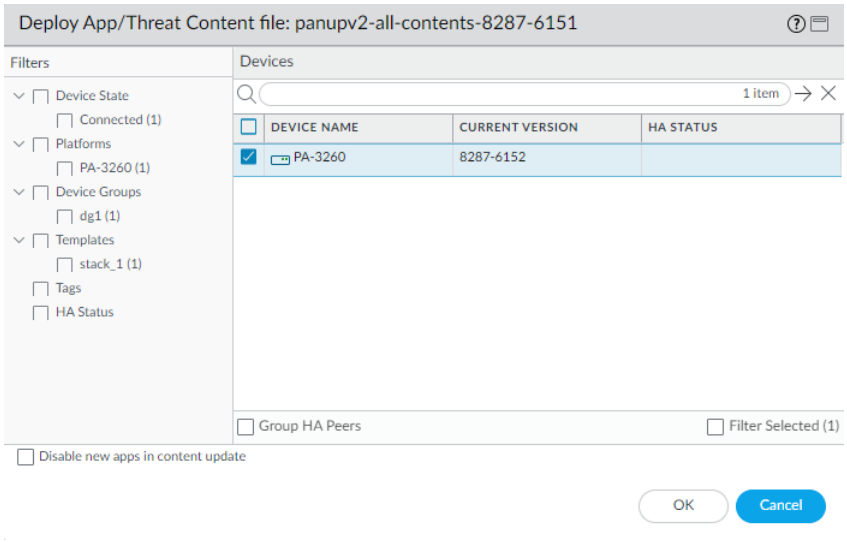
Consultez les Release Notes (Notes de publication) pour la version de contenu minimale que vous devez installer pour PAN-OS 10.0. Assurez-vous que vous utilisez les meilleures pratiques pour les mises à jour d'applications et de menaces lorsque vous déployez des mises à jour de Panorama et des pare-feu que vous gérez.

1. Sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Dynamic Updates (Mises à jour dynamiques)** et **Check Now (Vérifiez maintenant)** pour obtenir les dernières mises à jour. Si une mise à jour est disponible, la colonne Action affiche un lien **Download (Télécharger)**.

© 2020 Palo Alto Networks, Inc.



2. Si elle n'est pas déjà installée, **Download (Téléchargez)** la dernière version du contenu.
3. Cliquez sur **Install (Installer)** et sélectionnez les pare-feu sur lesquels vous voulez installer la mise à jour et cliquez sur **OK**. Si vous mettez à niveau des pare-feu HA, vous devez mettre à jour le contenu des deux homologues.

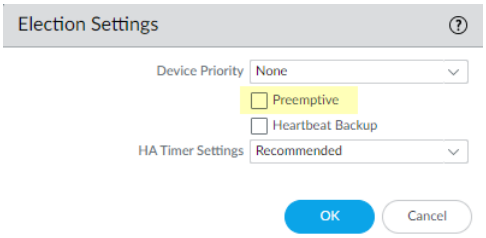


Par défaut, vous pouvez charger un maximum de deux mises à jour logicielles ou de contenu de chaque type vers un appareil Panorama. Si vous téléchargez une troisième mise à jour du même type, Panorama supprimera la mise à jour de la première version de ce type. Si vous devez télécharger plus de deux mises à jour logicielles ou mises à jour de contenu d'un seul type, utilisez la commande CLI **`setmax-num-images count <nombre>`** *pour augmenter le maximum.*

STEP 3 | (HA firewall upgrades only) Si vous mettez à niveau des pare-feu faisant partie d'une paire haute disponibilité, désactivez la préemption. Vous devez uniquement désactiver ce paramètre sur un pare-feu dans chaque paire haute disponibilité.

© 2020 Palo Alto Networks, Inc.

1. Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** et modifiez les **Election Settings (Paramètres de sélection)**.
2. si cette option est activée, désactivez (effacez) le **Preemptive (paramètre préemptif)** et cliquez sur **OK**.



3. **Commit (Validez)** la modification. Assurez que la validation est un succès avant de procéder à la mise-à-jour.

STEP 4 | Déterminer le chemin de mise à niveau vers PAN-OS 10.0.

Vous ne pouvez pas sauter l'installation de versions majeures dans le chemin de mise à jour depuis la version PAN-OS en cours vers PAN-OS 10.0.0. Passez en revue les problèmes connus et les modifications du comportement par défaut dans les Notes de version et les considérations de mise à niveau vers une version supérieure ou antérieure dans le Guide des nouvelles fonctionnalités de chaque version à travers laquelle vous passez dans le cadre de votre chemin de mise à niveau.

Si vous mettez à niveau plusieurs pare-feu, rationalisez le processus en déterminant les chemins de mise à niveau de tous les pare-feu avant de commencer à télécharger des images.

STEP 5 | Téléchargez l'image de version cible de PAN-OS 10.0.

1. Sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Software (Logiciel)** et **Check Now (Vérifiez maintenant)** pour obtenir les dernières versions.
2. **Download (Téléchargez)** le(s) fichier(s) spécifique du pare-feu pour la version finale vers laquelle vous effectuez la mise à niveau. Vous devez télécharger un fichier d'installation distinct pour chaque modèle de pare-feu (ou série de pare-feu) que vous avez l'intention de mettre à niveau.

   Par exemple, pour mettre à niveau les pare-feux PA-220 et PA-5250 vers PAN-OS 10.0.0, téléchargez les images `PanOS_220-10.0.0`, `PanOS_3000-10.0.0`, et `PanOS_5200-10.0.0`. Après avoir téléchargé avec succès une image, la colonne Action devient **Install (Installer)** pour cette image.

STEP 6 | Installez la mise à jour logicielle PAN-OS 10.0 sur les pare-feux.

Vous devez mettre à jour les pare-feux de votre plate-forme depuis PAN-OS 10.0.0 vers PAN-OS 10.0.1 ou une version ultérieure avant de pouvoir mettre à jour les pare-feux de votre branche. La mise à jour des pare-feux de branche avant les pare-feux de plate-forme peut entraîner une mauvaise surveillance des données (Panorama > SD-WAN > Monitoring) et les liens SD-WAN peuvent être affichés comme étant `en panne` de façon erronée.

1. Cliquez sur **Install (Installer)** dans la colonne Action correspondant aux modèles de pare-feu que vous souhaitez mettre à niveau. Par exemple, si vous souhaitez mettre à niveau vos pare-feux PA-220, cliquez sur**Install (installer)** dans la ligne correspondant à PanOS_220-10.0.0.
2. Dans la boîte de dialogue Déployer le fichier logiciel, sélectionnez tous les pare-feu que vous souhaitez mettre à niveau. Pour réduire les temps d'arrêt, sélectionnez uniquement un pair dans chaque paire HA. Pour les paires actives / passives, sélectionnez l'homologue passif; pour les paires actives / actives, sélectionnez l'homologue actif-secondaire.

© 2020 Palo Alto Networks, Inc.

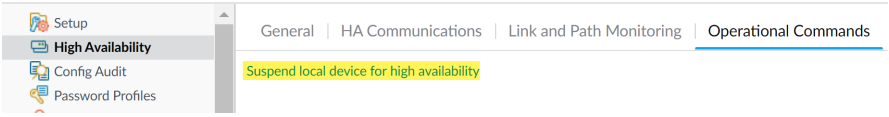
3. (Mises à niveau des pare-feu HA uniquement) Assurez-vous que le **Group HA Peers (Groupe de paire HA)** n'est pas sélectionné.
4. Sélectionnez **Reboot device after install (Redémarrer le périphérique après l'installation)**.
5. Pour débuter la mise à jour, cliquez sur **OK**.
6. Une fois l'installation terminée, redémarrez en utilisant l'une des méthodes suivantes :
   - Si vous êtes invité à redémarrer, cliquez sur **Yes (Oui)**.
   - Si vous n'êtes pas invité à redémarrer, sélectionnez **Device (Périphérique)** > **Configuration** > **Operations (Opérations)** et **Reboot Device (Redémarrez le périphérique)**.
7. Après que le pare-feu a terminé le redémarrage, sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)** et vérifiez que la version du logiciel est 10.0.0 pour les pare-feux que vous avez mis à niveau. Vérifiez également que le statut HA de tous les pare-feu passifs mis à niveau est toujours passif.

STEP 7 | (Mise à niveau des pare-feu HA uniquement) Mettez à niveau le deuxième pair HA dans chaque paire HA.

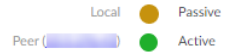
1. (Mises à niveau active/passive uniquement) Suspendez le périphérique actif dans chaque paire active / passive que vous mettez à niveau.
   1. Basculez le contexte vers le pare-feu actif.
   2. Dans le widget de haute disponibilité sur le **Dashboard (Tableau de bord)**, vérifiez que l'état du pare-feu **Local** est **Active (Actif)** et que le **Peer (Homologue)** est **Passive (Passif)**).



   3. Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **Operational Commands (Commandes opérationnelles)** > **Suspend local device (Suspendre le périphérique local)**.



   4. Revenez au widget Haute disponibilité sur le **Dashboard (Tableau de bord)** et vérifiez que **Local** est passé à **Passive (Passif)** et que **Peer (Homologue)** est passé à **Active (Actif)**.



2. Retournez sur Panorama et sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Software (Logiciel)**.
3. Cliquez sur **Install (Installer)** dans la colonne Action correspondant aux modèles de HA que vous souhaitez mettre à niveau.
4. Dans la boîte de dialogue Déployer le fichier logiciel, sélectionnez tous les pare-feu que vous souhaitez mettre à niveau. Cette fois, sélectionnez uniquement les homologues des pare-feu HA que vous venez de mettre à jour.
5. Assurez-vous que le **Group HA Peers (Groupe de paire HA)** n'est pas sélectionné.
6. Sélectionnez **Reboot device after install (Redémarrer le périphérique après l'installation)**.
7. Pour débuter la mise à jour, cliquez sur **OK**.
8. Une fois l'installation terminée, redémarrez en utilisant l'une des méthodes suivantes :
   - Si vous êtes invité à redémarrer, cliquez sur **Yes (Oui)**.
   - Si vous n'êtes pas invité à redémarrer, sélectionnez **Device (Périphérique)** > **Configuration** > **Operations (Opérations)** et **Reboot Device (Redémarrez le périphérique)**.
9. (Mises à niveau active/passive uniquement) À partir de la CLI de l'homologue que vous venez de mettre à niveau, exécutez la commande suivante pour rendre le pare-feu de nouveau fonctionnel :

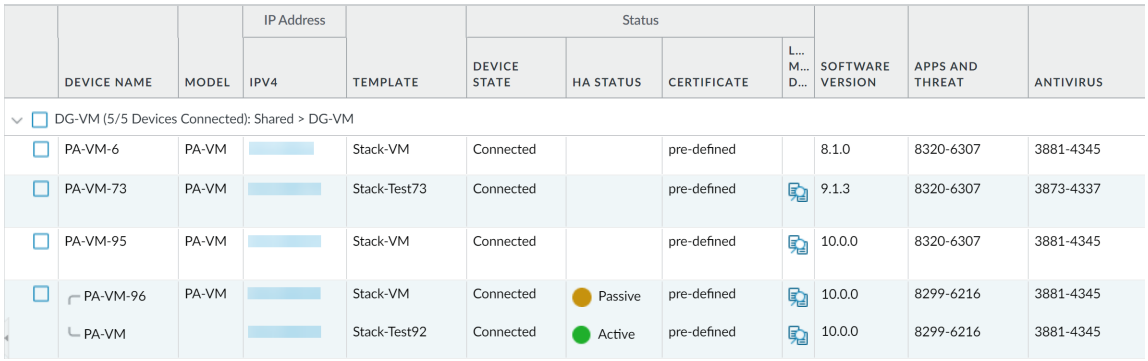
© 2020 Palo Alto Networks, Inc.

```
request high-availability state functional
```

STEP 8 | Vérifiez la version du logiciel et du contenu qui s'exécute sur chaque pare-feu géré.

1. Sur Panorama, sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)**.
2. Localisez les pare-feu et examinez les versions de contenu et logicielles dans le tableau.

   Pour les pare-feu HA, vous pouvez également vérifier que l'état HA de chaque homologue est conforme aux attentes.



	DEVICE NAME	MODEL	IP Address IPV4	TEMPLATE	Status DEVICE STATE	Status HA STATUS	Status CERTIFICATE	Status L... M... D...	SOFTWARE VERSION	APPS AND THREAT	ANTIVIRUS
	DG-VM (5/5 Devices Connected): Shared > DG-VM										
	PA-VM-6	PA-VM		Stack-VM	Connected		pre-defined		8.1.0	8320-6307	3881-4345
	PA-VM-73	PA-VM		Stack-Test73	Connected		pre-defined		9.1.3	8320-6307	3873-4337
	PA-VM-95	PA-VM		Stack-VM	Connected		pre-defined		10.0.0	8320-6307	3881-4345
	PA-VM-96	PA-VM		Stack-VM	Connected	Passive	pre-defined		10.0.0	8299-6216	3881-4345
	PA-VM			Stack-Test92	Connected	Active	pre-defined		10.0.0	8299-6216	3881-4345

STEP 9 | (Mises à niveau des pare-feu HA uniquement)Si vous avez désactivé la préemption sur l'un de vos pare-feu haute disponibilité avant de procéder à la mise à niveau, modifiez les **Election Settings (Paramètres de sélection)** (**Device (Périphérique)** > **High Availability (Haute disponibilité)**) et réactivez le paramètre **Preemptive (Préemptif)** pour ce pare-feu, puis **Commit (Validez)** le changement.

Mettre à niveau les pare-feu lorsque Panorama n'est pas connecté à Internet

Pour une liste des mises à jour de logiciels et de contenu que vous pouvez installer sur des pare-feu, voir Mises à jour prises en charge.

STEP 1 | Avant de mettre à niveau les pare-feu gérés, vérifiez que vous exécutez la version logicielle Panorama™ appropriée sur le serveur de gestion Panorama et les collecteurs de journaux.

Palo Alto Networks® recommande vivement que Panorama et les collecteurs de journaux exécutent la même version du logiciel Panorama et que Panorama, les collecteurs de journaux et tous les pare-feu gérés exécutent la même version de contenu.

Pour les détails de compatibilité de logiciels et de contenus importants, voir Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire.

Panorama doit exécuter la même version de logiciel (ou une version ultérieure) que les pare-feu, mais doit avoir la même version de contenu ou une version antérieure :

- **Version du logiciel** : si votre serveur de gestion Panorama ou les collecteurs de journaux n'exécutent pas déjà la même version de logiciel ou une version ultérieure que la version à laquelle vous souhaitez mettre à jour les pare-feu, vous devez installer la même version ou une version ultérieure sur Panorama, puis sur les collecteurs de journaux (voir Installer les mises à jour de contenu et logicielles pour Panorama) avant de mettre à jour les pare-feu.
- **Version du contenu** : pour les versions de publication de contenu, vous devez vous assurer que tous les pare-feu exécutent la dernière version de contenu ou, au minimum, qu'ils exécutent une version ultérieure de Panorama et des collecteurs de journaux ; sinon, mettez à jour les pare-feu gérés, puis

© 2020 Palo Alto Networks, Inc.

mettez à niveau les collecteurs de journaux lorsque Panorama n'est pas connecté à Internet avant de mettre à jour la version du contenu sur le serveur de gestion Panorama (voir Installer les mises à jour de contenu et logicielles pour Panorama).

Pour vérifier les versions de logiciel et de contenu :

- **Serveur de gestion Panorama** : connectez-vous à l'interface Web Panorama et accédez aux paramètres General Information (Informations générales) (**Dashboard (Tableau de bord)**).
- **Collecteurs de journaux** : connectez-vous à l'ILC de chaque collecteur de journaux et exécutez la commande **`show system info`**.

STEP 2 | Effectuez une copie de sauvegarde du fichier de configuration actuel sur chaque pare-feu géré que vous envisagez de mettre à niveau.

Bien que le pare-feu crée automatiquement une sauvegarde de la configuration, il est recommandé de créer et de stocker une sauvegarde externe avant de procéder à la mise à niveau.

1. **Export Panorama and devices config bundle (Exporter la solution de configuration des périphériques et de Panorama)** (**Panorama** > **Setup (Configuration)** > **Operations (Opérations)**) pour générer et exporter la dernière la sauvegarde de configuration de Panorama et celle de chaque appareil géré.
2. Enregistrez le fichier exporté dans un emplacement externe au pare-feu. Vous pouvez utiliser cette sauvegarde pour restaurer la configuration en cas de problème pendant la mise à niveau.

STEP 3 | Déterminez les mises à jour de contenu à installer. Consultez les Notes de version pour la version de contenu minimale que vous devez installer pour une version de PAN-OS®.

Palo Alto Networks recommande fortement que Panorama, les collecteurs de journaux et tous les pare-feu gérés exécutent la même version de contenu.

Pour chaque mise à jour de contenu, déterminez si vous avez besoin de mises à jour et notez les mises à jour de contenu que vous devez télécharger à l'étape 5.

Assurez-vous que Panorama exécute la même version de contenu, mais pas une version ultérieure à celle exécutée sur les pare-feu gérés et les collecteurs de journaux.

STEP 4 | Déterminez le chemin de mise à niveau logicielle pour les pare-feux que vous avez l'intention de mettre à jour vers Panorama 10.0. Reportez-vous au Guide des nouvelles fonctionnalités pour le chemin de mise à niveau vers PAN-OS 10.0.

Connectez-vous à Panorama, sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)**, et notez la version du logiciel actuel des pare-feu que vous souhaitez mettre à niveau.

Nous vous recommandons fortement de passer en revue les problèmes connus et les modifications du comportement par défaut dans les Notes de version et les considérations de mise à niveau vers une version supérieure ou antérieure dans le Guide des nouvelles fonctionnalités de chaque version à travers laquelle vous passez dans le cadre de votre chemin de mise à niveau.

STEP 5 | Téléchargez les mises à jour de contenu et logicielles sur un hôte qui peut se connecter et charger les fichiers sur Panorama via SCP ou HTTPS.

Par défaut, vous pouvez charger un maximum de deux mises à jour logicielles ou de contenu de chaque type vers un appareil Panorama. Si vous téléchargez une troisième mise à jour du même type, Panorama supprimera la mise à jour de la première version de ce type. Si vous devez télécharger plus de deux mises

© 2020 Palo Alto Networks, Inc.

à jour logicielles ou mises à jour de contenu d'un seul type, utilisez la commande CLI **`set max-num-images count <nombre>`** pour augmenter le nombre maximum d'images que Panorama peut stocker.

1. Utilisez un hôte avec accès à Internet pour ouvrir une session sur le site Web d'assistance client de Palo Alto Networks.
2. Téléchargez les mises à jour de contenu :
    1. Cliquez **Dynamic Updates (Mises à jour dynamique)** dans la section Ressources.
    2. **Download (Téléchargez)** la dernière version de contenu (ou, au minimum, la même version ou une version ultérieure que celle que vous installerez ou exécuterez sur le serveur de gestion Panorama) et enregistrez le fichier sur l'hôte ; répétez pour chaque type de contenu que vous devez mettre à jour.
3. Télécharger les mises à jour logicielles :
    1. Retour à la page principale du site de Support Clients de Palo Alto Networks et cliquez sur **Software Updates (Mises à jour de logiciel)** dans la section Ressources.
    2. Consultez la colonne Télécharger pour déterminer les versions à installer. Le nom des packages de mise à jour indique le modèle. Par exemple, pour mettre à niveau un pare-feu PA-220 et PA-5260 vers PAN-OS 8.0.8, téléchargez les images `PanOS_200-8.0.8`, `PanOS_3000-8.0.8`, et `PanOS_5000-8.0.8`.

        Vous pouvez rapidement localiser des images PAN-OS spécifiques en sélectionnant PAN-OS for the PA (PAN-OS pour le PA)-<série/modèle> depuis le menu déroulant Filter By (Filtrer par).
4. Cliquez sur le nom du fichier approprié et enregistrez le fichier sur l'hôte.

STEP 6 | Installez les mises à jour de contenu sur les pare-feu gérés.

Vous devez installer les mises à jour de contenu avant les mises à jour logicielles.

Installez d'abord les mises à jour des applications ou des applications et menaces, puis installez toutes les autres mises à jour (Antivirus, WildFire® ou Filtrage d'URL) au besoin, une à la fois et dans n'importe quel ordre.

1. Sélectionnez **Panorama (Panorama)** > **Device Deployment (Déploiement du périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**.
2. Cliquez sur **Upload (Charger)**, sélectionnez le **Type** de mise à jour, **Browse (Rechercher)** le fichier de mise à jour de contenu approprié, puis cliquez sur **OK**.
3. Cliquez sur **Install From File (Installer depuis le fichier)**, sélectionnez le **Type** de mise à jour et sélectionnez le **File Name (Nom du fichier)** de la mise à jour de contenu que vous venez de charger.
4. Sélectionnez les collecteurs de journaux sur lesquels installer la mise à jour.
5. Cliquez sur **OK** pour démarrer l'installation.
6. Répétez ces étapes pour chaque mise à jour de contenu.

STEP 7 | (Pare-feu servant de portails GlobalProtect™ uniquement) Chargez et activez une mise à jour du logiciel de l'agent / application GlobalProtect sur les pare-feu.

Vous activez la mise à jour sur les pare-feu, afin que les utilisateurs puissent les télécharger sur leurs points de terminaison (systèmes client).

1. Utilisez un hôte avec accès à Internet pour ouvrir une session sur le site Web d'assistance client de Palo Alto Networks.
2. Téléchargez la mise à jour du logiciel de l'agent / application GlobalProtect appropriée.

© 2020 Palo Alto Networks, Inc.

3. Sur Panorama, sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **GlobalProtect Client (Client GlobalProtect)**.
4. Cliquez sur **Upload (Charger)**, **Browse (Rechercher)** la mise à jour du logiciel de l'agent / application GlobalProtect appropriée sur l'hôte pour lequel vous avez téléchargé le fichier, puis cliquez sur **OK**.
5. Cliquez sur **Activate from File (Activer depuis le fichier)** et sélectionnez le **File Name (Nom du fichier)** de la mise à jour de l'agent / application GlobalProtect que vous venez de charger.

   Vous ne pouvez activer qu'une seule version du logiciel de l'agent / application à la fois. Si vous activez une nouvelle version mais que certains agents nécessitent une version antérieure, vous devrez réactiver à nouveau la version antérieure pour que ces agents téléchargent la mise à jour précédente.
6. Sélectionnez les pare-feu sur lesquels installer la mise à jour.
7. Cliquez sur **OK** pour l'activer.

STEP 8 | Chargez les mises à jour logicielles de PAN-OS.

1. Sélectionnez **Panorama** > **Device Deployment (Déploiement de périphérique)** > **Software (Logiciel)**.
2. Cliquez sur **Upload (Charger)**, **Browse (Rechercher)** le fichier de mise à jour logicielle approprié sur l'hôte, puis cliquez sur **OK**.

STEP 9 | Installez les mises à jour logicielles de PAN-OS.

Pour éviter les pannes lors de mise à jour du logiciel sur le pare-feu haute disponibilité (HD), mettez à jour un homologue HD à la fois.

Pour les pare-feu actifs / actifs, l'homologue que vous mettez à jour en premier n'a pas d'importance.

Pour les pare-feu actifs / passifs, vous devez d'abord mettre à jour l'homologue passif, suspendre l'homologue actif (basculement), mettre à jour l'homologue actif, puis ramener l'homologue actif à un état fonctionnel (retour arrière).

Vous devez mettre à jour les pare-feux de votre plate-forme depuis PAN-OS 10.0.0 vers PAN-OS 10.0.1 ou une version ultérieure avant de pouvoir mettre à jour les pare-feux de votre branche. La mise à jour des pare-feux de site distant (branch) avant les pare-feux de plateforme (hub) génère de mauvaises données de surveillance (Panorama > SD-WAN > Monitoring) et les liens SD-WAN peuvent être affichés comme étant `en panne` *de façon erronée.*

1. Effectuez les étapes qui s'appliquent à la configuration de votre pare-feu pour installer la mise à jour logicielle de PAN-OS que vous venez de charger.
   - **Pare-feu non-HD** : cliquez sur **Install (Installer)** dans la colonne Action, sélectionnez tous les pare-feu que vous mettez à niveau, sélectionnez **Reboot device after install (Redémarrer le périphérique après l'installation)**, puis cliquez sur **OK**.
   - **Pare-feu HD actifs / actifs :**
     1. Confirmez que le paramètre de préemption est désactivé sur le premier homologue que vous avez l'intention de mettre à niveau (**Device (Périphérique)** > **High Availability (Haute Disponibilité)** > Election Settings (Paramètres d'élection)). Si activés, modifiez les **Election Settings (Paramètres d'élection)** et désactivez le paramètre **Preemptive (Préemptif)**, puis **Commit (Validez)** votre modification. Vous devez uniquement désactiver ce paramètre sur un pare-feu dans chaque paire haute disponibilité, mais assurez-vous que la validation est réussie avant de continuer.
     2. Cliquez sur **Install (Installer)**, désactivez **Group HA Peers (Regrouper les homologues HD)**, sélectionnez un homologue HD, sélectionnez **Reboot device after install (Redémarrer le**

© 2020 Palo Alto Networks, Inc.

périphérique après l'installation), puis cliquez sur **OK**. Attendez que le pare-feu termine le redémarrage avant de poursuivre.

3. Cliquez sur **Install (Installer)**,désactivez **Group HA Peers (Regrouper les homologues HD)**, sélectionnez l'homologue HD que vous n'avez pas mis à jour à l'étape précédente, sélectionnez **Reboot device after install (Redémarrer le périphérique après l'installation)**, puis cliquez sur **OK**.

- **Pare-feu HD actifs / passifs** : dans cet exemple, le pare-feu actif est appelé fw1 et le pare-feu passif fw2 :

  1. Confirmez que le paramètre de préemption est désactivé sur le premier homologue que vous avez l'intention de mettre à niveau (**Device (Périphérique)** > **High Availability (Haute Disponibilité)** > Election Settings (Paramètres d'élection)). Si activés, modifiez les **Election Settings (Paramètres d'élection)** et désactivez le paramètre **Preemptive (Préemptif)**, puis **Commit (Validez)** votre modification. Vous devez uniquement désactiver ce paramètre sur un pare-feu dans chaque paire haute disponibilité, mais assurez-vous que la validation est réussie avant de continuer.
  2. Cliquez sur **Installer** dans la colonne Action de la mise à jour appropriée, désactivez **Group HA Peers (Regrouper les homologues HD)**, sélectionnez fw2, **Reboot device after install (Redémarrer le périphérique après l'installation)** et cliquez sur **OK**. Attendez que fw2 termine le redémarrage avant de poursuivre.
  3. Après le redémarrage de fw2, vérifiez sur fw1 (**Dashboard (Tableau de bord)** > High Availability (Haute disponibilité)) que fw2 est toujours l'homologue passif (l'état du pare-feu local est `active` et l'homologue fw2 est `passive`).
  4. Accédez à fw1 et **Suspend local device (Suspendre le périphérique local)** (**Device (Périphérique)** > **High Availability (Haute disponibilité)** > **Operational Commands (Commandes opérationnelles)**).
  5. Accédez à fw2 (**Dashboard (Tableau de bord)** > High Availability (Haute disponibilité)) et vérifiez que l'état du pare-feu local est `active` et que l'homologue est `suspended`.
  6. Accédez à Panorama, sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Software (Logiciel)**, cliquez sur **Install (Installer)** dans la colonne Action de la version appropriée, désactivez **Group HA Peers (Regrouper les homologues HD)**, sélectionnez fw1, **Reboot device after install (Redémarrer le périphérique après l'installation)**, puis cliquez sur OK. Attendez que fw1 termine le redémarrage avant de poursuivre.
  7. Accédez à fw1 (**Device (Périphérique)** > **High Availability (haute disponibilité)** > **Operational Commands (Commandes opérationnelles)**), cliquez sur **Make local device functional (Rendre l'appareil local fonctionnel)**, et attendez deux minutes avant de continuer.
  8. Sur fw1 (**Dashboard (Tableau de bord)** > High Availability (Haute disponibilité)), vérifiez que l'état du pare-feu local est `passive` et que l'homologue (fw2) est `active`.

2. Après avoir effectué les étapes ci-dessus pour une mise à jour de la version de PAN-OS, répétez l'étape 8 et l'étape 9 pour charger la version suivante de PAN-OS dans votre chemin de mise à niveau, jusqu'à ce que tous les pare-feux exécutent la version cible de PAN-OS 10.0.

STEP 10 | Vérifiez que le logiciel et/ou les versions de mise à jour de contenu sont installés sur chaque pare-feu géré.

1. Sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)**.
2. Localisez le pare-feu et examinez les valeurs dans les colonnes de la Version du logiciel, applications et menace, Antivirus, filtrage d'URL et Client GlobalProtect.

STEP 11 | Si vous avez désactivé la préemption sur l'un de vos pare-feu HD avant de procéder à la mise à niveau, modifiez les **Election Settings (Paramètres d'élection)** (**Device (Périphérique)** > **High Availability (Haute disponibilité)**) et réactivez le paramètre **Préemptif** pour ce pare-feu.

© 2020 Palo Alto Networks, Inc.

Mettre à niveau un pare-feu ZTP

Après avoir ajouté avec succès un pare-feu ZTP au serveur de gestion Panorama™, configurez la version PAN-OS cible du pare-feu ZTP. Panorama vérifie si la version du PAN-OS installée sur le pare-feu ZTP est postérieure ou égale à la version du PAN-OS cible configurée après sa première connexion réussie à Panorama. Si la version PAN-OS installée sur le pare-feu ZTP est antérieure à la version PAN-OS cible, alors le pare-feu ZTP entre dans un cycle de mise à jour jusqu'à ce que la version PAN-OS cible soit installée.

STEP 1 | Ajoutez pare-feu ZTP à Panorama.

STEP 2 | Se connecter à l'interface Web Panorama en tant qu'utilisateur admin.

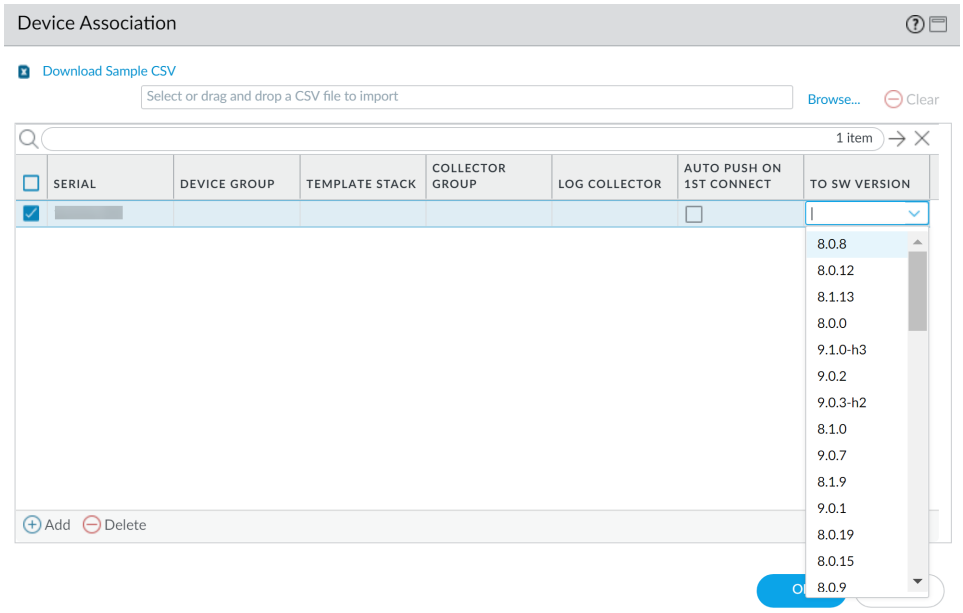
STEP 3 | Sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Updates (Mises à jour)** et **Check Now (Vérifiez maintenant)** pour obtenir les dernières mises à jour PAN-OS.

STEP 4 | Sélectionnez **Panorama** > **Managed Devices (Appareils gérés)** > **Summary (Résumé)** et sélectionnez un ou plusieurs pare-feux ZTP.

STEP 5 | **Réassocier** le(s) pare-feu(x) ZTP sélectionné(s).

STEP 6 | Dans la colonne **To SW Version (Vers la version SW)**, sélectionnez la version PAN-OS cible pour le pare-feu ZTP.

STEP 7 | Cliquez sur **OK** pour enregistrer votre configuration.



STEP 8 | Sélectionnez **Commit (Valider)** et **Commit and Push (Validez et appliquez)** vos modifications de configuration.

STEP 9 | Vérifiez la mise à jour du logiciel de pare-feu ZTP.

1. Sélectionnez **Panorama** > **Managed Devices (Appareils gérés)** > **Summary (Résumé)** et naviguez vers le(s) pare-feu(x) ZTP.
2. Vérifiez que la colonne **Software Version (Version du logiciel)** affiche la bonne version PAN-OS cible.

© 2020 Palo Alto Networks, Inc.

Rétablir les mises à jour du contenu depuis Panorama

Panorama ™ vous permet de rétablir rapidement les versions des Applications, Applications et Menaces, Antivirus, WildFire® et WildFire sur un ou plusieurs pare-feu, Collecteurs de journaux ou Applications WildFire directement à partir de Panorama. Utilisez Panorama pour rétablir les versions de contenu installées sur les périphériques gérés afin de tirer parti d'un flux de travail centralisé qui permet d'atténuer tout risque associé à l'introduction ou à la modification d'applications ou de nouvelles signatures de menaces dans une mise à jour de contenu. Panorama génère un journal système pour chaque périphérique lorsque vous inversez le contenu. Assurez-vous que vous utilisez les meilleures pratiques pour les mises à jour d'application et de menaces lorsque vous déployez des mises à jour de contenu sur vos périphériques gérés.

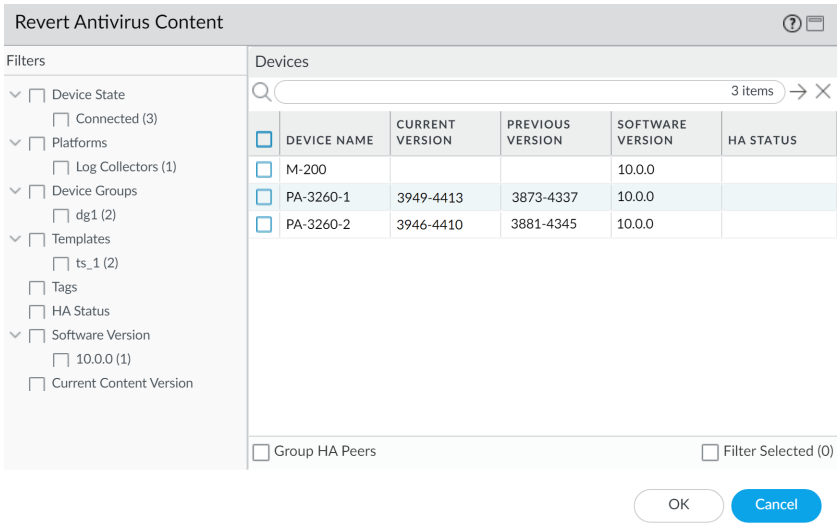
STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Sélectionnez **Panorama (Panorama)** > **Device Deployment (Déploiement de périphériques)** > **Dynamic Updates (Mises à jour dynamiques)** et **Revert Content (Rétablir le contenu)**.

STEP 3 | Sélectionnez le contenu que vous souhaitez rétablir.

Antivirus
Apps
Applications and Threats
WildFire
WildFire-Content

STEP 4 | Sélectionnz un ou plusieurs pare-feu que vous souhaitez rétablir et cliquez sur **OK**. La version de contenu que vous rétablissez doit être antérieure à celle qui est actuellement installée sur l'appareil.



© 2020 Palo Alto Networks, Inc.

Surveiller l'activité réseau

Le serveur de gestion Panorama™ offre une vue graphique complète du trafic réseau. Grâce aux outils de visibilité sur Panorama (le centre de commande de l'application (ACC), les journaux et les fonctionnalités de génération de rapport) vous pouvez centralement analyser, étudier et reporter toute l'activité réseau, identifier les domaines avec l'impact potentiel sur la sécurité et traduire en politiques les applications sécurisées.

Cette section couvre les sujets suivants :

- Utiliser Panorama pour la visibilité
- Ingérer les journaux de l'ESM Traps sur Panorama
- Cas d'utilisation : Surveiller des applications en utilisant Panorama
- Cas d'utilisation : Répondre à un incident à l'aide de Panorama

© 2020 Palo Alto Networks, Inc.

Utiliser Panorama pour la visibilité

En plus du déploiement central et des fonctions de configuration de pare-feu, Panorama vous permet de surveiller et de générer des rapports sur l'ensemble du trafic qui circule dans votre réseau. Alors que les fonctionnalités de reporting sur Panorama et le pare-feu sont très similaires, l'avantage que Panorama propose est un affichage unique des informations agrégées à travers tous vos pare-feu gérés. Cette vue agrégée fournit des informations exploitables sur les tendances de l'activité de l'utilisateur, les modèles de trafic et les menaces potentielles sur l'ensemble du réseau.

Grâce au CCA (centre de commande de l'application), l'App-Scope, la visionneuse de journaux et aux options de génération de rapports, standard et personnalisables, de Panorama, vous pouvez rapidement en apprendre davantage sur le trafic du réseau. La possibilité de voir ces informations vous permet d'évaluer l'adéquation où l'insuffisance des politiques actuelles. Vous pouvez alors utiliser ces données pour perfectionner la stratégie de sécurité de votre réseau. Par exemple, vous pouvez renforcer les règles de sécurité afin d'optimiser la conformité et la fiabilité pour tous les utilisateurs présents sur le réseau, ou gérer la capacité du réseau et réduire les risques pour les actifs tout en répondant aux besoins applicatifs des utilisateurs sur votre réseau.

Les rubriques suivantes fournissent un aperçu détaillé des possibilités de génération de rapports dans Panorama, notamment quelques cas pratiques pour illustrer la façon dont ces fonctionnalités peuvent vous aider au sein de votre infrastructure réseau. Pour une liste complète des rapports et schémas disponibles et leur description, reportez-vous à l'aide en ligne.

- Surveiller le réseau avec CCA et App-Scope
- Analyser les Données des Journaux
- Générer, planifier et envoyer des rapports par courrier électronique
- Configurez les limites de clé pour les rapports planifiés.

Surveiller le réseau avec CCA et App-Scope

CCA et App-Scope permettent tous les deux de surveiller et de créer des rapports sur les données enregistrées qui circulent sur le réseau.

Le CCA sur Panorama affiche un récapitulatif du trafic réseau. Panorama peut demander de façon dynamique des données à tous les pare-feux gérés sur le réseau et de les afficher dans le CCA. Cet affichage vous permet de surveiller le trafic par les applications, les utilisateurs et l'activité de contenu - catégories d'URL, menaces, politiques de sécurité qui bloquent efficacement les données ou les fichiers - sur l'ensemble du réseau de pare-feu de dernière génération de Palo Alto Networks.

L'App-Scope permet de détecter des comportements inattendus ou anormaux sur le réseau en un seul coup d'œil. Il inclut un ensemble de cartes et de rapports (rapports récapitulatifs, surveillance des modifications, surveillance des menaces, carte des menaces, surveillance de réseau, carte du trafic) —qui permettent d'analyser les flux de trafic par menaces ou applications, ou par la source ou la destination des flux. Vous pouvez également effectuer un tri par session ou par nombre d'octets.



*Les administrateurs du Groupe et modèles de périphériques ne peuvent afficher que les données CCA des groupes de périphériques se trouvant dans leurs*domaines d'accès*.*

Utiliser le CCA et l'App-Scope pour répondre aux questions telles que :

ACC	Surveillance > App-Scope
• Quels est le top des applications utilisées sur le réseau, et combien sont des applications	• Quelles sont les tendances d'utilisation des application ? Quelles sont les cinq principales

© 2020 Palo Alto Networks, Inc.

ACC	Surveillance > App-Scope
à haut risque ? Qui sont les plus grands utilisateurs d'applications à haut risque sur le réseau ? • Quelles sont les principales catégories d'URL consultées dans la dernière heure?	applications pour lesquelles les taux d'utilisation ont augmenté, et les cinq dont l'utilisation a diminuée ? • Comment l'activité de l'utilisateur a changé au cours de la semaine en cours par rapport à la semaine dernière ou le mois dernier ?
• Quelles sont les principales applications utilisant la bande passante ? Qui sont les utilisateurs/hôtes qui consomment le plus de bande passante ? • Quel contenu ou quels fichiers sont bloqués et ont-ils des utilisateurs spécifiques qui déclenchent cette règle de filtrage des données/blocage de fichiers ? • Quelle est la quantité de trafic échangée entre deux adresses IP spécifiques ou générée par un utilisateur spécifique ? Où est le serveur de destination ou le client est-il situé géographiquement ?	• Quels utilisateurs et applications occupent la majeure partie de la bande passante du réseau ? Et comment cette consommation a-t-elle évolué au cours des 30 derniers jours ? • Quelles sont les menaces sur le réseau, et comment ces menaces du trafic entrant et sortant sont-elles distribuées géographiquement ?

Vous pouvez alors utiliser les informations pour conserver ou appliquer des modifications aux modèles de trafic de votre réseau. Reportez-vous à la section Cas d'utilisation : Surveiller des applications en utilisant Panorama pour avoir un aperçu de la façon dont les outils de visibilité sur Panorama peuvent influencer la façon dont vous pouvez définir des politiques d'utilisation acceptables de votre réseau.

Voici quelques conseils pour vous aider à naviguer avec le CCA :

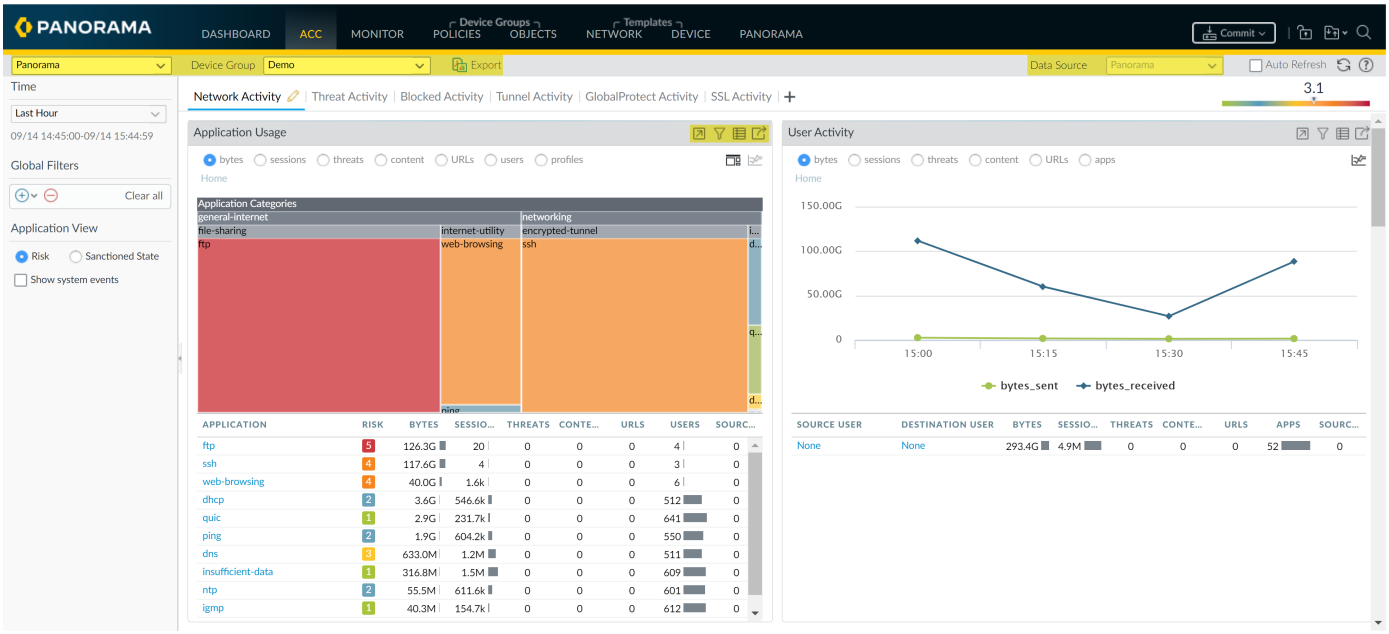


Figure 24: Conseils de navigation CCA

© 2020 Palo Alto Networks, Inc.

- **Passer d'une vue Panorama à une vue Périphérique** : utilisez le menu déroulant **Context (Contexte)** pour accéder à l'interface Web de n'importe quel pare-feu géré. Pour plus d'informations, reportez-vous à la section Changement de contexte : pare-feu ou Panorama.
- **Modifier le groupe de périphériques et la source de données** : la **Data Source (Source de données)** utilisée par défaut pour afficher les statistiques sur les cartes du CCA sont les données locales de **Panorama**, et le paramètre de **Device Group (Groupe de périphériques)** par défaut est **All (Tous)**. L'utilisation des données locales de Panorama permet de charger rapidement les tableaux. Vous pouvez cependant modifier la source de données à un **Remote Device Data (périphérique de données à distance)** si tous les périphériques gérés sont sur PAN-OS 7.0. Si les pare-feux gérés présentent un mélange de PAN-OS 7.0 et de versions antérieures, vous pouvez seulement afficher les données de Panorama. Lorsqu'il est configuré pour utiliser les données de périphériques distants, Panorama interroge tous les pare-feux gérés et présente une vue agrégée des données. L'affichage à l'écran indique le nombre total de pare-feux sondés et le nombre de pare-feux qui ont répondu à la demande d'informations.
- **Sélectionnez les onglets et les widgets à afficher** : l'ACC comprend trois onglets et un ensemble de widgets qui vous permettent de trouver les informations qui vous intéressent. À l'exception du widget d'utilisation d'applications et du widget d'informations hôte, tous les autres widgets affichent des données uniquement si la fonction correspondante a été autorisée sur le pare-feu quand vous avez activé la journalisation.
- **Ajuster le cadre du temps et affiner les données** - la période de temps considérée dans le CCA varie depuis les 15 dernières minutes à la dernière heure, journée, semaine, mois ou n'importe quel moment personnalisé. Par défaut, chaque widget affiche les 10 meilleurs articles et regroupe tous les éléments restants comme **others (autres)**. Vous pouvez trier les données dans chaque widget en utilisant divers attributs — par exemple, sessions, octets, menaces, contenu et URLs. Vous pouvez également définir les filtres pour filtrer l'affichage dans le tableau et le graphique dans un widget et puis promouvoir le filtre widget comme un filtre global pour faire pivoter la vue dans l'ensemble de tous les widgets dans la CCA.

Analyser les Données des Journaux

L'onglet **Monitor (Surveillance)** sur Panorama donne un accès pour enregistrer les données ; ces journaux sont une liste archivée des sessions qui ont été traitées par les pare-feu gérés et transmis au Panorama.

Les données du journal peuvent être largement regroupées en deux catégories : celles qui détaillent les informations sur les flux de votre réseau telles que les applications, menaces, profils d'information hôte, catégories d'URL, types de contenu/fichiers et celles qui enregistrent les événements système, les modifications de configuration et les les informations de mappage User-ID™.

Basé sur le journal de transfert de configuration sur les pare-feu gérés, l'onglet **Monitor (Surveillance)** > **Logs (Journaux)** peut inclure des journaux sur les flux de trafic, menaces, filtrage des URL, filtrage de données, informations profil hôte (IPH) des correspondances et des soumissions WildFire™. Vous pouvez consulter les journaux afin de vérifier une multitude d'informations relatives à une session ou à une transaction spécifique. Ces informations incluent, entre autres, l'utilisateur à l'origine de la session, l'action (autoriser ou refuser) exécutée par le pare-feu pendant la session, ainsi que les ports, zones et adresses de la source et de la destination. Les journaux Système et Configuration peuvent indiquer un changement de configuration ou une alarme que le pare-feu a déclenché lorsqu'un seuil configuré est dépassé.

Si Panorama va gérer les pare-feux exécutant des versions de logiciels plus récentes que PAN-OS 7.0, spécifiez un serveur WildFire à partir duquel Panorama puisse recueillir des informations d'analyse pour les échantillons WildFire que ces pare-feux soumettent. Panorama utilise les informations pour remplir les journaux WildFire qui manquent de valeurs de champ introduites dans PAN-OS 7.0. Les pare-feu exécutant les versions antérieures ne remplissent pas ces champs. Pour spécifier le serveur, sélectionnez Panorama > Setup (Configuration) > WildFire, modifiez les paramètres généraux, puis entrez le nom du WildFire Private Cloud (Cloud Privé WildFire). La valeur par défaut est wildfire-public-cloud (cloud public WildFire), où le cloud WildFire est hébergé aux États-Unis.

© 2020 Palo Alto Networks, Inc.

Générer, planifier et envoyer des rapports par courrier électronique

Vous pouvez configurer les rapports pour qu'ils s'exécutent immédiatement ou planifier leur exécution à des intervalles spécifiques. Vous pouvez enregistrer et exporter les rapports, ou les envoyer par e-mail à des destinataires spécifiques. L'envoi par e-mail s'avère particulièrement utile si vous souhaitez partager des rapports avec des administrateurs qui n'ont pas accès à Panorama. Panorama prend en charge les mêmes types de rapports que le pare-feu de Palo Alto Networks.

A partir de Panorama 10.0.2 et de la version du plug-in Cloud Services 1.8.0, vous pouvez générer des rapports programmés des données de Cortex Data Lake.

Dans PAN-OS 10.0.3 et versions ultérieures, cette option est activée par défaut.

Pour faire cela, vous devez d'abord activer la fonctionnalité depuis le CLI de Panorama en saisissant

```
admin@Panorama> request plugins cloud_services logging-service sched-report-enable
```

Une validation régulière n'activera pas ce changement. Au contraire, vous devez basculer en mode de configuration :

```
admin@Panorama> configure
```

et saisir

```
admin@Panorama# commit force
```

Puis, suivez les étapes ci-dessous afin de générer des rapports programmés.

Nous vous recommandons d'installer des versions logicielles correspondantes sur Panorama et les pare-feu pour lesquels vous générerez des rapports. Par exemple, si le serveur de gestion Panorama exécute Panorama 10.0, installez PAN-OS 10.0 sur ses pare-feux gérés avant de générer les rapports. Ceci permet d'éviter des problèmes lors de la génération de rapports comprenant des champs pris en charge par la version de Panorama mais qui ne le sont pas dans une version antérieure de PAN-OS installée sur les pare-feu.

STEP 1 | Configurez les rapports prédéfinis de Panorama.

1. Sélectionnez **Panorama (Panorama)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez **Logging and Reporting (journalisation et de rapports.)**
2. (En option) Sélectionnez**Log Export and Reporting (Exportation des journaux et rapports)**et activez (cochez) **Use Data for Pre-Defined Reports (Utiliser les données pour des rapports prédéfinis)** pour décharger le cumul de rapports horaires vers les Collecteurs de journaux (Log Collectors).

   Il est conseillé d'activer ce paramètre pour les pare-feux VM-50, VM-50 Lite et PA-200.
3. Sélectionnez **Pre-Defined Reports (Rapports prédéfinis)** et activez (cochez) rapports prédéfinis pour appliquer depuis Panorama.

© 2020 Palo Alto Networks, Inc.

4. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements de configuration.
5. (Pare-feux VM-50, VM-50 Lite, et PA-200 uniquement) Accédez au CLI des pare-feux pour activer les rapports prédéfinis.

   Cette commande doit être lancée sur chaque pare-feu VM-50, VM-50 Lite et PA-200.

   ```
   admin> debug run-panorama-predefined-report yes
   ```

STEP 2 | Configurez Panorama pour qu'il reçoive et stocke les informations sur les utilisateurs et les groupes d'utilisateurs qu'il reçoit des pare-feu.

Requis pour générer des rapports basés sur les noms d'utilisateur et les groupes au lieu des adresses IP uniquement.

1. Si vous souhaitez que Panorama inclut des informations sur les groupes d'utilisateurs dans les rapports, mettez à niveau les pare-feux gérés vers PAN-OS 8.1 ou une version ultérieure. Panorama ne peut pas synchroniser les informations de groupe à partir de pare-feu exécutant des versions antérieures.
2. Sélectionnez **Panorama** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les paramètres de Panorama et **Enable reporting and filtering on groups (Activer les rapports et le filtrage sur les groupes)**.
3. Configurez les groupes de périphériques si vous ne l'avez pas déjà fait. Pour chaque groupe de périphériques :
   - Sélectionnez un **Master Device (Périphérique principal)**, qui est le pare-feu qui fournit des informations sur les utilisateurs et les groupes d'utilisateurs à Panorama.
   - Autorisez Panorama à **Store users and groups from Master Device (Stocker les utilisateurs et les groupes à partir du périphérique principal)**.

STEP 3 | Générez des rapports.

Les étapes pour générer un rapport dépendent du type.

- Rapport personnalisé :
  1. Sélectionnez **Monitor (Surveillance)** > **Manage Custom Reports (Gérer les rapports personnalisés)** et **Add (Ajoutez)** le rapport.
  2. Saisissez un **Name (Nom)** pour identifier le rapport.
  3. Sélectionnez une **Datebase (base de données)** pour le rapport.

     Vous pouvez baser le rapport sur des **Summary Databases (Bases de données récapitulatives)** ou des bases de données de **Detailed Logs (Journaux détaillés)**.

     Pour baser le rapport sur les journaux stockés sur le serveur de gestion Panorama et les collecteurs de journaux, sélectionnez **Panorama Data (Données de Panorama)** (recommandé pour des performances plus rapides).

     Pour baser les rapports sur les journaux stockés sur les pare-feu gérés, sélectionnez **Remote Device Data (Données de périphérique distant)**. Cette option est destinée aux cas dans lesquels les pare-feu peuvent avoir des journaux qui n'ont pas encore été transmis à Panorama. Cependant, comme Panorama doit directement interroger les pare-feu, cette option est plus lente.
  4. Sélectionnez **Scheduled (Planifié)**.
  5. Définissez vos critères de filtrage de journaux en sélectionnant le **Time Frame (Délai)**, l'ordre **Sort By (Trier par)**, la préférence **Group By (Regrouper par)**, et les colonnes (attributs de journal) que le rapport affichera.

© 2020 Palo Alto Networks, Inc.

Il faut sélectionner l'ordre Sort By (Regrouper par) pour générer un rapport précis. Si vous ne sélectionnez pas un ordre Sort By (Regrouper par), le rapport personnalisé généré contient les correspondance des journaux les plus récentes de la base de données sélectionnée.

6. (Facultatif) Utilisez le **Query Builder (Générateur de requêtes)** pour continuer d'affiner les critères de filtrage des journaux en fonction des attributs du journal.
7. Pour tester les paramètres de rapport, sélectionnez **Run Now (Lancer l'exécution)**. Si nécessaire, modifiez les paramètres pour modifier les informations que le rapport affiche.
8. Cliquez sur **OK** pour enregistrer le rapport personnalisé.

- **Rapport récapitulatif au format PDF** :

1. Sélectionnez **Monitor (Surveillance)** > **PDF Reports (Rapports PDF)** > **Manage PDF Summary (Gérer le résumé PDF)** et ajoutez le rapport.
2. Saisissez un **Name (Nom)** pour identifier le rapport.
3. Utilisez la liste déroulante pour chaque groupe de rapports et sélectionnez un ou plusieurs éléments pour concevoir le rapport récapitulatif au format PDF. Vous pouvez inclure jusqu'à 18 éléments.
4. Cliquez sur **OK** pour enregistrer les paramètres.

STEP 4 | Configurer un **Report Group (groupe de rapports)**.

Il peut inclure des rapports prédéfinis, des rapports récapitulatifs au format PDF, et des rapports personnalisés. Panorama compile tous les rapports inclus dans un seul fichier PDF.

1. Sélectionnez **Monitor (Surveillance)** > **PDF Reports (Rapports PDF)** > **Groupes de rapports** et **Add (Ajoutez)** un groupe de rapports.
2. Saisissez un **Name (Nom)** pour identifier le groupe de rapports.
3. (Facultatif) Sélectionnez **Title Page (Titre de la page)** et ajoutez un **Title (Titre)** pour la sortie PDF.
4. Sélectionnez les rapports dans les listes Rapport prédéfini, Rapport personnalisé et Rapport récapitulatif au format PDF.
5. **Add (Ajoutez)** les rapports sélectionnés au groupe de rapports.
6. Cliquez sur **OK** pour enregistrer les paramètres.

STEP 5 | Configurez un profil de serveur de messagerie.

Le profil définit comment le pare-feu se connecte au serveur et envoie l'e-mail.

1. Sélectionnez **Device (périphérique)** > **Server Profiles (Profils de serveur)** > **Email (E-mail)** et **Add (Ajoutez)** un profil de serveur.
2. Saisissez un **Name (Nom)** pour identifier le profil.
3. **Add (Ajoutez)** jusqu'à quatre serveurs SMTP et **Add (Ajoutez)** les informations suivantes pour chacun :

   - **Name (Nom)** : un nom permettant d'identifier le serveur SMTP (de 1 à 31 caractères). Ce champ n'est qu'une étiquette et ne doit pas forcément être le nom d'hôte d'un serveur de messagerie existant.
   - **Email Display Name (Nom complet de messagerie)** : nom apparaissant dans le champ "De" du courrier électronique.
   - **From (De)** : adresse de messagerie à partir de laquelle les messages de notification seront envoyés.
   - **To (À)** : adresse de messagerie vers laquelle les messages électroniques de notification seront envoyés.
   - **Additional Recipient (Destinataire supplémentaire)** : pour envoyer des notifications à un second compte, saisissez l'adresse supplémentaire ici.

© 2020 Palo Alto Networks, Inc.

- **Email Gateway (Passerelle de courriel)**, l'adresse IP ou nom d'hôte de la passerelle SMTP à utiliser pour envoyer les emails.

4. Cliquez sur **OK** pour enregistrer le profil.

STEP 6 | Planifiez le rapport pour la livraison par courrier électronique.

1. Sélectionnez **Monitor (Surveillance)** > **PDF Reports (Rapports PDF)** > **Planificateur de e-mail** et **Add (Ajouter)** un profil de planificateur d'e-mail.
2. Saisissez un **Name (Nom)** pour identifier le profil.
3. Sélectionnez le **Report Group (Groupe de rapports)**, le profil de serveur de messagerie que vous venez de créer (**Email Profile (Profil d'e-mail)**) et la **Recurrence (Récurrence)** du rapport (la valeur par défaut est **Disable (Désactiver)**).
4. **Send test email (Envoyez un e-mail de test)** pour vérifier que les paramètres de messagerie sont exacts.
5. Cliquez sur **OK** pour enregistrer vos modifications.
6. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

Configurez les limites de clé pour les rapports planifiés.

Les rapports du serveur de gestion Panorama™ et le pare-feu série PA-7000 utilisent des clés (des valeurs uniques que vous pouvez cumuler) d'un ou plusieurs Collecteurs de journaux afin d'élaborer et générer des rapports. Afin d'améliorer la précision des rapports planifiés, vous pouvez maintenant configurer les limites maximales et minimales de clés. En augmentant le nombre de clés compatibles, les rapports planifiés peuvent maintenant inclure plus de données qui peuvent être cumulées, triées et regroupées.

La limite minimale de clés se base sur les valeurs **Sort By (trier par)** et **Group By (regrouper par)**configurées pour le rapport planifié en utilisant le calcul suivant :

<Sort By value> x 100 x <Group By value>(<Trier par valeur> x 100 x <Regrouper par valeur>

Par exemple, si **Sort By (trier par)** est configuré sur **Top 25 (25 premiers)** et **Group By (regrouper par)** est configuré sur **5 Groups (5 groupes)**, la limite de clés minimale par défaut est de 12 500 clés. La valeur **Group By (Regrouper par)** n'est pas prise en compte dans le calcul lorsque le réglage est sur **None (aucune)**. La limite de clés minimale par défaut est limitée à et ne peut dépasser la limite de clés maximale.

Vous ne pouvez configurer les limites de clés que pour les appareils de la série M et les appareils virtuels de Panorama. Les limites de clés de la série PA-7000 ne peuvent pas être configurées.

Les clés minimales et maximales possibles sont augmentées pour les modèles Panorama suivants :

Modèle Panorama	Limite de clés minimale	Limite de clés maximale
PA-7000 Series	1 000 - Par défaut, non configurable	25 000 - Par défaut, non configurable
M-200	15 000	50 000
M-500	15 000	50 000
M-600	15 000	50 000

© 2020 Palo Alto Networks, Inc.

Modèle Panorama	Limite de clés minimale	Limite de clés maximale
Appareil virtuel Panorama en mode Legacy (historique)	5 000	25 000
Appareil virtuel Panorama (tous les modèles compatibles)	15 000	50 000

STEP 1 | Connectez-vous à la CLI de Panorama.

STEP 2 | Configurez la limite de clés maximale à l'aide de la commande suivante :

Vous pouvez réglez la limite de clés maximale entre 0 et 50, où 50 est égal à 50 000 clés. Dans cet exemple, nous fixons la limite de clés maximale pour l'appareil virtuel Panorama à 30 000 clés.

```
admin@Panorama> request max-report-keys set limit <Key Limit>
```

```
admin@Panorama> request max-report-keys set limit 30

cfg.report.max-keys-limit: 30
```

STEP 3 | Configurez la limite de clés minimale à l'aide de la commande suivante :

Vous pouvez réglez la limite de clés maximale entre 0 et 15, où 15 est égal à 15 000 clés. Dans cet exemple, nous fixons la limite de clés minimale pour l'appareil virtuel Panorama à 15 000 clés.

```
admin@Panorama> request min-report-keys set limit <Key Limit>
```

```
admin@Panorama> request min-report-keys set limit 15

cfg.report.min-keys-limit: 15
```

STEP 4 | (En option) Réglez la limite de clés minimale sur le paramètre par défaut.

```
admin@Panorama> request min-report-keys set limit 0
```

STEP 5 | Validez les nouvelles limites de clés maximale et minimale de Panorama à l'aide de la commande suivante :

```
admin@Panorama> commit-all
```


© 2020 Palo Alto Networks, Inc.

Ingérer les journaux de l'ESM Traps sur Panorama

La visibilité est une première étape critique dans la prévention et la réduction de l'impact d'une attaque. Pour vous aider à relever ce défi, Panorama propose une vue intégrée des journaux de pare-feu (événements sur le réseau) et des journaux de Traps™ ESM Server (événements de sécurité sur les points de terminaison) afin de détecter toute activité suspecte ou malveillante.

Pour connaître les événements observés sur le réseau et sur vos points de terminaison, ainsi que leur contexte, transférez les événements de sécurité que les agents Traps signalent au serveur ESM vers Panorama. Panorama peut servir de récepteur Syslog qui ingère ces journaux à partir des composants Traps ESM à l'aide de Syslog via TCP, UDP ou SSL. Ensuite, Panorama peut corréler des événements de sécurité discrets qui se produisent sur les points de terminaison avec ce qui se passe sur le réseau et générer des preuves de correspondance. Ces preuves vous donnent plus de contexte sur la chronologie et le flux des événements pour vous permettre d'étudier les problèmes et de corriger les failles de sécurité dans votre réseau.

STEP 1 | Définissez le profil d'ingestion du journal sur Panorama et associez-le à un groupe de collecteurs.



L'appareil virtuel Panorama en mode hérité ne peut pas ingérer les journaux Traps.

1. Sélectionnez **Panorama** > **Log Ingestion Profile (Profils d'ingestion de journaux)**, puis cliquez sur **Add (Ajouter)**.
2. Saisissez un **Name (Nom)** pour le profil.
3. Cliquez sur **Add (Ajouter)** et saisissez les détails pour le serveur ESM. Vous pouvez ajouter jusqu'à quatre serveurs ESM à un profil.
    1. Saisissez un **Source Name (Nom de source)**.
    2. Indiquez le **Port** sur lequel Panorama écoutera les messages Syslog. La portée est de 23 000 à 23 999.
    3. Sélectionnez le protocole de la couche **Transport** : TCP, UDP ou SSL.
    4. Sélectionnez Traps_ESM pour **External Log type (Type de journal externe)** et vos Traps ESM **version**. Par exemple, pour Traps ESM 4.0 ou 4.1, sélectionnez **3.4.1+**.

        Comme les formats de journaux Traps sont mis à jour, les définitions des journaux mis à jour seront disponibles grâce à des mises à jour de contenu sur Panorama.
4. Sélectionnez **Panorama** > **Collector Groups (Groupes de collecteurs)** > **Log Ingestion (Ingestion des journaux)** et **ajoutez (Add)** le profil d'ingestion des journaux afin que le groupe de collecteurs puisse recevoir les journaux du ou des ESM Server(s) listé(s) dans le profil.

    Si vous activez le protocole SSL pour une communication Syslog sécurisée entre Panorama et le(s) serveur(s) ESM, vous devez associer un certificat aux collecteurs gérés appartenant au groupe de collecteurs (**Panorama** > **Managed Collectors (Collecteurs gérés)** > **Général** et sélectionnez le certificat à utiliser pour **Inbound Certificate for Secure Syslog (Certificat entrant pour Syslog sécurisé)**).
5. **Validez** les modifications à Panorama et au groupe de collecteurs.

STEP 2 | Configurez Panorama en tant que récepteur Syslog sur le serveur ESM.

© 2020 Palo Alto Networks, Inc.

Les Traps ESM 4.0 et les versions ultérieures prennent en charge la redirection des journaux vers un récepteur Syslog externe et vers Panorama. Étant donné que les versions précédentes de Traps ESM ne prennent pas en charge le transfert de journaux vers plusieurs récepteurs syslog, vous devez configurer Panorama en tant que récepteur syslog dans les configurations du **Syslog** (pour Traps ESM 3.4, voir Activer le transfert de journaux vers une plateforme de journalisation externe).

Pour Traps ESM 4.0 et versions ultérieures :

1. Depuis la console ESM, sélectionnez **Settings (Paramètres)** > **ESM** > **Panorama**, puis **Enable log forwarding to Panorama (Activez la redirection de journaux vers Panorama)**.
2. Entrez le nom d'hôte Panorama ou l'adresse IP en tant que **Panorama-server (Serveur Panorama)** et le **Panorama Server Port (Serveur port de Panorama)** sur lequel Panorama écoute. Répétez cette étape pour un **Panorama Failover Server (Serveur de basculement Panorama)** facultatif.
3. Sélectionnez le **Communication Protocol (Protocole de communication)** de la couche Transport : TCP, TCP avec SSL ou UDP. Si vous sélectionnez TCP avec SSL, le serveur ESM nécessite un certificat de serveur pour activer l'authentification du client.

   Depuis Panorama, vous devez exporter le certificat de l'autorité de certification racine pour le certificat entrant pour Syslog sécurisé et importer le certificat dans le magasin de certificats racines approuvés de l'hôte sur lequel vous avez installé le serveur ESM.

STEP 3 | Consultez les journaux ESM et les événements corrélés.

1. Sélectionnez **Monitor (Surveillance)** > **External Logs (Journaux externes)** > **Traps ESM** pour afficher les journaux ingérés sur Panorama.
2. Sélectionnez **Monitor (Surveillance)** > **Automated Correlation Engine (Moteur de corrélation automatique)** > **Correlated Events (Événements corrélés)**, et filtrez le nom de l'objet de corrélation **Wildfire and Traps ESM Correlated C2** pour trouver les événements corrélés. Panorama génère des événements corrélés lorsqu'un hôte sur votre réseau présente une activité de commande et de contrôle qui correspond au comportement observé pour un fichier malveillant dans l'environnement virtuel WildFire. Cet événement corrélé vous alerte d'une activité suspecte qu'un agent Traps et le pare-feu ont observée depuis un ou plusieurs hôtes infectés sur votre réseau.

© 2020 Palo Alto Networks, Inc.

Cas d’utilisation : Surveiller des applications en utilisant Panorama

Cet exemple vous explique le processus d'évaluation d'efficacité de vos stratégies actuelles et vous aide à détecter les endroits où vous devriez affiner les réglages pour renforcer les politiques d'utilisation acceptables pour votre réseau.

Lorsque vous ouvrez une session Panorama, le widget **Top Applications (Principales applications)** sur le **Dashboard (tableau de bord)** donne un aperçu des applications les plus utilisées au cours de la dernière heure. Pour afficher le widget, sélectionnez **Widgets** > **Application** > **Top applications (Principales applications)** dans la barre d'outils. Vous pouvez soit jeter un coup d'œil sur la liste des principales applications et promener votre souris sur chaque blocage d'application dont vous souhaitez voir le détail, ou vous pouvez accéder à l'onglet **ACC (CCA)** pour afficher les mêmes informations qu'une liste ordonnée. L’image suivante est une vue du widget **Top Applications (Principales applications)** sur le **Dashboard (Tableau de bord)**.

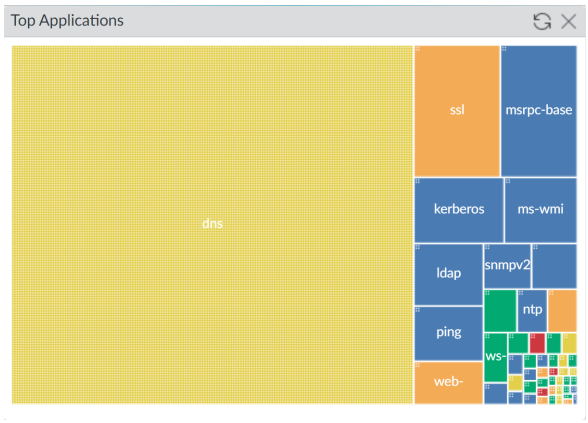


Figure 26: Widget Top Applications

La source des données de cet écran est une base de données sur les statistiques d'application. Elle n'utilise pas les journaux de trafic et est générée, que vous ayez ou non activé la journalisation des règles de sécurité. Cette vue sur le trafic de votre réseau décrit tout ce qui est autorisé sur votre réseau et qui circule parce qu'il n'est pas bloqué par les règles que vous avez définies.

Dans l'onglet **ACC (CCA)**, vous pouvez sélectionner et activer/désactiver la **Data Source (Source de données)** pour être locale sur **Panorama (Panorama)** ou vous pouvez interroger les pare-feux gérés (**Remote Device Data (périphérique de données à distance)**) pour les données ; Panorama agrège et affiche automatiquement les informations. Pour un flux plus rapide, envisagez d'utiliser Panorama comme source de données (avec le transfert des journaux vers Panorama activé) car le délai nécessaire au chargement de données depuis des périphériques distants varie en fonction de la période pour laquelle vous choisissez d'afficher les données et du volume de trafic généré sur votre réseau. Si votre pare-feu gérés ont une combinaison de PAN-OS 7.0 et des versions antérieures, les **Remote Device Data (données du périphérique distant)** ne sont pas disponibles.

L’exemple du **Dashboard (Tableau de bord)** dans Figure 26: Widget Top Applications montre DNS comme une application courante. Si vous cliquez sur le bloc d'application DNS, Panorama ouvre l'onglet **ACC (CCA)** > **Network Activity (Activité réseau)** avec DNS appliqué comme filtre global et affiche des informations sur l'application, les utilisateurs qui ont accédé à l'application et les détails sur le niveau de risque et les caractéristiques de l'application.

© 2020 Palo Alto Networks, Inc.

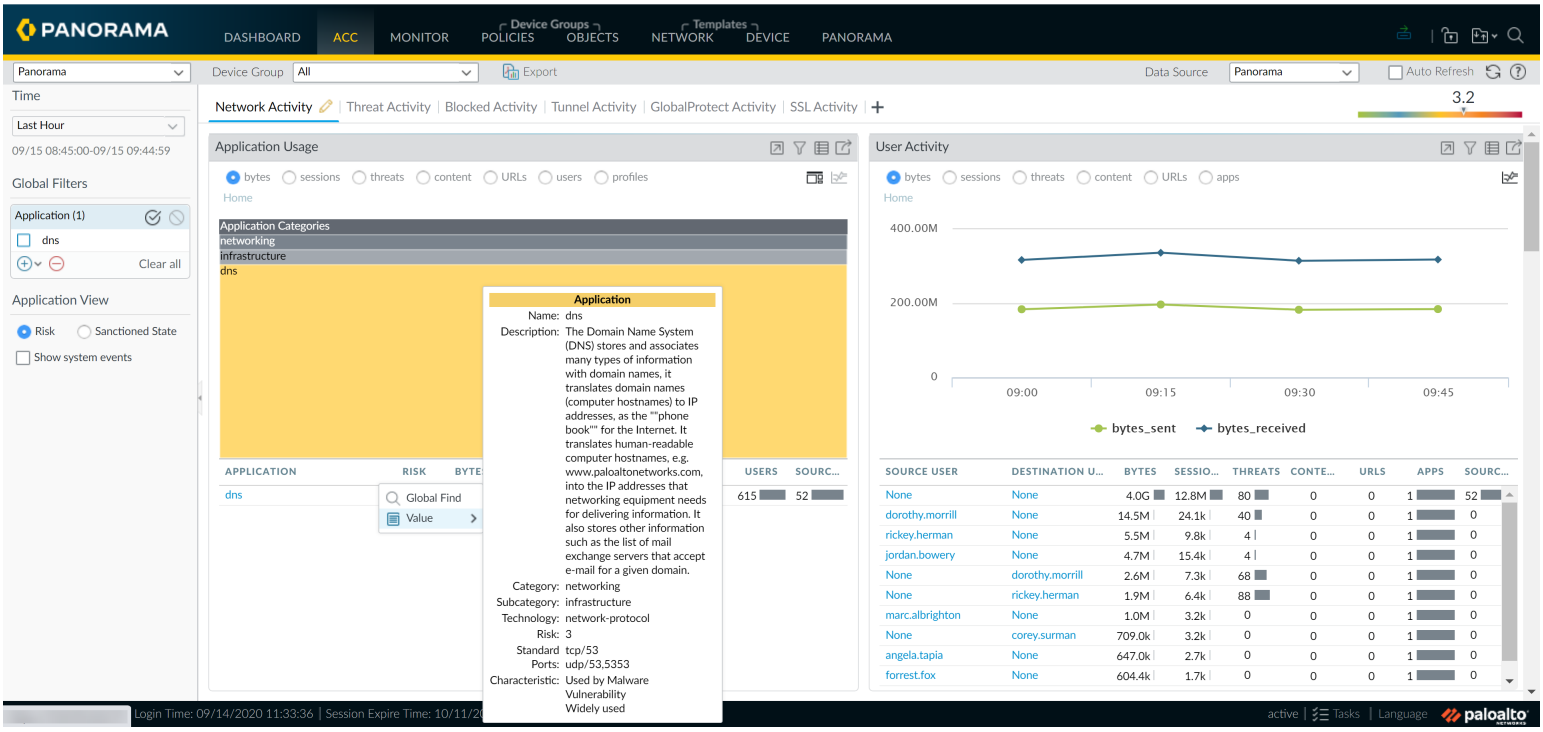


Figure 27: Onglet Network Activity (Activité réseau)

Dans le widget **User Activity (activité de l'utilisateur)**, vous pouvez aussi voir combien d'utilisateurs utilisent DNS et le volume de trafic généré. Si vous avez activé l'ID-utilisateur, vous serez en mesure d'afficher les noms des utilisateurs qui sont générateurs de ce trafic et permet de passer en revue toutes les sessions, contenus ou menaces associées à chaque utilisateur.

Dans l'onglet **Threat Activity (activité de menace)**, affichez le widget **Compromised Hosts (hôtes compromis)** pour voir quels objets de corrélation ont été appariés et affichez la preuve de correspondance associée à l'utilisateur et à l'application. Vous pouvez également afficher le nom de la menace, la catégorie et l'ID dans le widget de **Threat Activity (l'activité de la menace)**.

Avec DNS, défini comme un filtre global, utilisez **Destination IP Activity (l'IP de Destination d'activité)** et les widgets de **Destination Regions (régions de destination)** pour vérifier vers qui le trafic était destiné. Vous pouvez également visualiser les zones d'entrée et de sortie et la règle de sécurité qui est de laisser passer ce sujet.

Pour plus d'informations, recherchez dans les journaux de trafic pour une vue filtrée et examinez chaque entrée de journal pour connaître les ports utilisés, les paquets envoyés, les octets envoyés et reçus. Ajustez les colonnes pour voir plus ou moins d'informations, en fonction de vos besoins.

L'onglet **Monitor (Surveillance** > **App-Scope (App-Scope) Traffic Map (Carte du trafic)** affiche une carte géographique du flux de trafic et fournit une vue du trafic entrant par rapport au trafic sortant. Vous pouvez également utiliser l'onglet **Monitor (Moniteur)** > **App-Scope** > **Change Monitor (Changer la Surveillance)** pour afficher les modifications des profils de trafic. Par exemple, comparez les applications principales utilisées pendant cette heure par rapport à la semaine ou au mois précédent afin de déterminer si un modèle ou une tendance se dégage.

Avec toutes les informations que vous avez découvertes, vous pouvez évaluer les modifications à apporter à vos configurations de stratégie. Voici quelques suggestions à examiner :

- Soyez restrictif et créez une règle préalable sur Panorama afin de bloquer ou autoriser tout trafic DNS. Utilisez ensuite les groupes de périphériques Panorama pour créer et transférer cette règle de politique vers un ou plusieurs pare-feux.

© 2020 Palo Alto Networks, Inc.

- Faire respecter les limites d'utilisation de bande passante et créer une règle de profil et de la politique de QoS qui priorise le trafic non commercial. Utilisez les groupes de périphériques et de modèles de Panorama pour configurer QoS et insérer les règles à un ou plusieurs pare-feux.
- Planifiez un groupe de rapports personnalisés réunissant l'activité spécifique à l'utilisateur et celle des principales applications utilisées sur votre réseau pour observer ce modèle pendant une semaine supplémentaire ou deux avant de passer à l'action.

En plus de contrôler une application spécifique, vous pouvez vérifier les applications inconnues dans la liste des applications principales. Ce sont des applications qui ne correspondent pas à une signature ID-App™ définie et s'affichent sous le nom de unknown-udp et unknown-tcp. Pour examiner de près ces applications inconnues, cliquez sur le nom pour afficher les détails du trafic non classifié.

Utilisez la même procédure pour rechercher les adresses IP des source principales des hôtes à l'origine du trafic inconnu, ainsi que l'adresse IP de l'hôte de destination avec lequel la session a été établie. Concernant le trafic inconnu, par défaut, les journaux de trafic exécutent une capture de paquet (pcap) lorsqu'une application inconnue est détectée. La flèche verte de la colonne de gauche représente les bribes de capture de paquet des données d'applications. Un clic sur la flèche verte affiche la pcap dans le navigateur.

Ayant les adresses IP des serveurs (IP de destination), le port de destination et la capture de paquets, vous serez mieux placé pour identifier l'application et pour prendre une décision sur la façon dont vous souhaitez agir sur votre réseau. Par exemple, vous pouvez créer une application personnalisée qui identifie le trafic au lieu de l'étiqueter comme TCP inconnu ou trafic UDP. Reportez-vous à l'article Identification des applications inconnues pour plus d'informations sur l'identification d'une application inconnue et à Signatures d'applications personnalisées pour des informations sur le développement des signatures personnalisées afin de distinguer une application.

© 2020 Palo Alto Networks, Inc.

Cas d’utilisation : Répondre à un incident à l'aide de Panorama

Les menaces réseau peuvent avoir plusieurs origines, notamment des infections par logiciel malveillant et espion suite à des téléchargements, des attaques d'hameçonnage, des serveurs sans correctif et des attaques DoS aléatoires ou ciblées, pour n'en citer que quelques-unes. Pour pouvoir réagir aux attaques ou aux infections réseau, il faut disposer de processus et de systèmes qui alertent l'administrateur de l'attaque et fournissent les données nécessaires à la détection de la source de l'attaque et des méthodes utilisées.

L’avantage qu’offre Panorama est une vue centralisée et consolidée des modèles et des journaux prélevés dans les pare-feux gérés sur votre réseau. Vous pouvez utiliser les informations provenant du moteur de corrélation automatique seul ou en combinaison avec les rapports et les journaux générés depuis une "Security Information Event Manager" (SIEM), pour étudier comment une attaque a été déclenchée et la façon de prévenir les crises futures et la perte de dommages à votre réseau.

Les questions posées par ce cas pratique sont les suivantes :

- Comment êtes vous informé d’un incident ?
- Comment confirmez-vous que l’incident n’est pas un faux positif ?
- Quel est votre programme d’action immédiate ?
- Comment utilisez-vous les informations disponibles pour reconstituer la séquence des événements qui ont précédé ou suivi l’événement déclencheur ?
- Quels sont les changements à prendre en compte pour la sécurisation de votre réseau ?

Ce cas pratique suit un incident spécifique et montre comment les outils de visibilité de Panorama peuvent vous aider à répondre au rapport.

- Notification d'un incident
- Revoir les Widgets du CCA
- Consultation des journaux des menaces
- Consultation des journaux WildFire
- Consultation des journaux de filtrage des données
- Mise à jour des règles de sécurité

Notification d'un incident

Plusieurs méthodes d'alerte sur incident sont possibles en fonction de la configuration des pare-feux Palo Alto Networks et des outils de tiers disponibles pour une analyse approfondie. Vous pouvez recevoir une notification par message électronique déclenchée par une entrée de journal enregistrée dans Panorama ou sur votre serveur Syslog, vous pouvez être informé via un rapport spécialisé généré par votre solution SIEM, ou qu'un service ou une solution tierce payante peuvent vous avertir. Pour cet exemple, disons que vous recevez une notification par message électronique de la part de Panorama. Cet e-mail vous informe qu’un événement a été déclenché par une alerte pour Zero Access gent.Gen Command And Control Traffic et qu’il correspond à une signature de logiciel espion. Le message électronique mentionne également l'adresse IP de la source et de la destination de la session, une ID de menace et l'horodatage de la journalisation de l'événement.

Revoir les Widgets du CCA

Dans l'onglet **ACC (CCA)** > **Threat Activity (menace d'activité)** , cochez le widget **Compromised Hosts (hôtes compromis)** et le widget **Threat Activity (activité de menace)** pour toute menace critique ou de haute gravité. Dans le widget **Compromised Hosts (Hôtes compromis)**, examinez les objets correspondants et

© 2020 Palo Alto Networks, Inc.

cliquez sur une valeur de comptage de correspondance pour afficher la preuve de correspondance pour l'incident associé.

Consultation des journaux des menaces

Pour commencer à enquêter sur l'alerte, utilisez l'ID de la menace pour rechercher les journaux de menace sur Panorama (**Monitor (surveillance)** > **Logs (Journaux)** > **Threat (Menaces)**). Depuis les journaux de menaces, vous pouvez trouver l'adresse IP de la victime, exporter la capture des paquets (PCAP, en cliquant sur l'icône icône de à l'entrée du journal) et utiliser un analyseur de réseau tels que WireShark pour examiner les détails de paquet. Dans le cas de HTTP, recherchez le REFERER HTTP mal formé ou défectueux dans le protocole, l'hôte suspect, les chaînes d'URL, l'agent utilisateur, l'adresse IP et le port afin de valider l'incident. Les données de ces pcap sont également utiles en cas de recherche des modèles de données similaires et de création de signatures personnalisées, ou pour modifier la politique de sécurité pour mieux affronter la menace dans l'avenir.

À la suite de cette évaluation manuelle, si vous vous sentez confiant sur la signature, envisagez de passer de la signature d'une action d'alerte à une action de bloc pour une approche plus agressive. Dans certains cas, vous pouvez choisir d'ajouter l'IP du pirate à une liste d'interdiction pour éviter qu'un trafic quelconque émanant de cette adresse IP n'atteigne le réseau interne.

Si vous détectez une signature de logiciel espion basée sur DNS, l'adresse IP de votre serveur DNS local peut s'afficher comme adresse Victim IP (IP victime). Souvent, c'est parce que le pare-feu se trouve en amont du serveur local DNS, et donc, les demandes DNS désignent le serveur DNS local comme source IP , et ne montrent pas l'adresse IP du client à l'origine de la demande.

Si vous voyez ce problème, activez l'action d'engouffrer un DNS dans le profil Anti-Spyware dans les règles de sécurité pour identifier les hôtes infectés sur votre réseau. Engouffrer un DNS vous permet de contrôler les connexions sortantes vers des domaines malveillants et de rediriger les requêtes DNS vers une adresse IP interne qui n'est pas utilisée ; le gouffre qui n'apporte pas de réponse. Lorsqu'un hôte compromis initie une connexion à un domaine malveillant, au lieu d'aller sur Internet, le pare-feu redirige la demande vers l'adresse IP, que vous avez défini, et il est engouffré. La consultation des journaux du trafic de tous les hôtes connectés au gouffre vous permet désormais de localiser tous les hôtes compromis et de prendre une action corrective afin d'éviter la propagation des logiciels malveillants.

Pour poursuivre l'enquête sur l'incident, utilisez les informations sur l'agresseur et l'adresse IP de la victime pour trouver des renseignements additionnels, tels que :

- Où l'attaquant se trouve-t-il géographiquement ? L'adresse IP est-elle une adresse IP individuelle ou une adresse IP de réseau ?
- L'événement causé par un utilisateur ayant été dupé en allant sur un site Web, un téléchargement, ou était il envoyé via une pièce jointe ?
- Le malware est-il propagé ? Il y a-t-il d'autres hôtes compromis/points de terminaison sur le réseau ?
- Est-ce une vulnérabilité zero-day ?

Les détails du journal pour chaque entrée de journal indiquent les journaux associés à l'événement. Ces informations désignent le trafic, la menace, le filtrage des URL ou d'autres journaux que vous pouvez consulter et font des associations entre les événements ayant mené à l'incident. Par exemple, filtrez le journal du trafic ((**Monitor (Surveillance)** > **Logs (Journaux)** > **Traffic (Trafic)**) en utilisant l'adresse IP à la fois comme source et destination IP pour avoir une image complète des hôtes/clients internes avec lesquels l'adresse IP de la victime a établi une connexion.

© 2020 Palo Alto Networks, Inc.

Consultation des journaux WildFire

Outre les journaux de la menace, utilisez l'adresse IP de la victime pour filtrer si les journaux de présentation WildFire. Les journaux de présentations WildFire contiennent des informations sur les fichiers téléchargés vers le service WildFire pour analyse. Parce qu'un spyware embarque généralement lui-même clandestinement, examiner les journaux de présentations WildFire pour vous indique si la victime a récemment téléchargé un fichier suspect. Le rapport de recherche WildFire affiche des informations sur l'URL sur laquelle le fichier ou l'exe a été obtenu, et le comportement de son contenu. Il vous dit si le fichier est malveillant, s'il a modifié des clés de registre, lu/écrit dans des fichiers, créé de nouveaux fichiers, ouvert des canaux de communication, provoqué des pannes d'applications, s'est intégré à des processus, a téléchargé des fichiers ou présenté d'autres comportements malveillants. Utilisez ces informations pour déterminer s'il faut bloquer l'application qui a provoqué l'infection (navigation web, SMTP, FTP), établir des règles de filtrage d'URL plus strictes ou limiter certaines applications/actions (par exemple, les téléchargements de fichiers à des groupes d'utilisateurs spécifiques).

L'accès aux journaux WildFire de Panorama nécessite les éléments suivants : un abonnement WildFire, un profil de fichier de blocage qui est attaché à une règle de sécurité et le transfert du journal de menace à Panorama.

Si Panorama va gérer les pare-feux exécutant des versions de logiciels plus récentes que PAN-OS 7.0, spécifiez un serveur WildFire à partir duquel Panorama puisse recueillir des informations d'analyse pour les échantillons WildFire que ces pare-feux soumettent. Panorama utilise les informations pour remplir les journaux WildFire qui manquent de valeurs de champ introduites dans PAN-OS 7.0. Les pare-feu exécutant les versions antérieures ne remplissent pas ces champs. Pour spécifier le serveur, sélectionnez Panorama > Setup (Configuration) > WildFire, modifiez les paramètres généraux, puis entrez le nom du WildFire Private Cloud (Cloud Privé WildFire). La valeur par défaut est wildfire-public-cloud (cloud public WildFire), où le cloud WildFire est hébergé aux États-Unis.

Si WildFire détermine que le fichier est malveillant, une nouvelle signature antivirus est créée dans les 24 à 48 heures et mise à votre disposition. Si vous avez un abonnement WildFire, la signature est rendue disponible en 30-60 minutes dans le cadre de la prochaine mise à jour de signature WildFire. Aussitôt que le pare-feu de prochaine génération Palo Alto Networks a reçu la signature obtenue, votre configuration est adaptée pour bloquer le fichier malveillant, le fichier est bloqué et les informations sur le fichier bloqué apparaissent sur votre journal de menaces. Ce processus est étroitement intégré pour vous protéger contre cette menace et résulte de la propagation de logiciels malveillants sur votre réseau.

Consultation des journaux de filtrage des données

Le journal de filtrage des données (**Monitor (Surveillance)** > **Logs (Journaux)** > **Data Filtering (filtrage des données)**) est une autre source précieuse pour enquêter sur l'activité malveillante du réseau. Vous pouvez régulièrement consulter les journaux de tous les fichiers pour lesquels vous avez été alerté, et vous pouvez également utiliser les journaux pour suivre les transferts de fichier et de données depuis ou vers l'adresse IP de la victime ou de l'utilisateur, et vérifier la direction et le flux du trafic serveur vers client ou client vers serveur. Pour recréer les événements qui ont précédé et suivi un événement, filtrez les journaux de l'adresse IP de la victime comme destination, et consultez les journaux d'activité réseau.

Étant donné que Panorama agrège les informations de tous les pare-feux gérés, il présente un bon aperçu de toutes les activités sur votre réseau. Certains des autres outils visuels que vous pouvez utiliser pour étudier le trafic sur votre réseau sont la **Threat Map (Carte des menaces)**, **Traffic Map (Carte du trafic)** et la **Threat Monitor (Surveillance de la menace)**. La carte des menaces et la carte de circulation (**Monitor (Surveillance)** > **AppScope** > **Threat Map (Carte de menace)** ou **Traffic Map (Carte de circulation)**) vous permettent de visualiser les régions géographiques pour le trafic entrant et sortant. Elle peut s'avérer particulièrement utile pour afficher une activité inhabituelle qui pourrait indiquer une attaque possible depuis l'extérieur, par exemple, une attaque DDoS. Si, par exemple, vous n'avez pas beaucoup de

© 2020 Palo Alto Networks, Inc.

transactions avec l'Europe de l'Est et que la carte révèle un niveau anormal de trafic dans cette région, cliquez dans la zone correspondante de la carte pour lancer et afficher les informations CCA des principales applications, les détails du trafic sur le compte de session, les octets reçus et envoyés, les sources et les destinations principales, les utilisateurs ou les adresses IP, et la gravité des menaces détectées, le cas échéant. L'écran de menaces (**Monitor (Surveillance)** > **AppScope** > **Threat Monitor (Surveillance des menaces)**) affiche les dix principales menaces présentes sur votre réseau, ou la liste des principaux pirates ou des principales victimes sur le réseau.

Mise à jour des règles de sécurité

Avec toutes les informations que vous avez découvertes, vous pouvez maintenant voir l'impact des menaces sur le réseau (le niveau de l'attaque, sa source, les hôtes compromis, le facteur de risque) et évaluer les modifications et, le cas échéant, le suivi. Voici quelques suggestions à examiner :

- Les attaques DDSS de Forestall en améliorant votre profil de Protection DoS pour configurer la suppression anticipée aléatoire ou pour supprimer les cookies SYN pour les inondations TCP. Envisagez de limiter le trafic ICMP ou UDP. Évaluez les options que vous avez en fonction des tendances et des modèles que vous avez remarqués dans vos journaux, et mettez en œuvre les modifications à l'aide des modèles Panorama.

  Créer une liste de blocage dynamique (**Objects (objets)** > **Dynamic Block Lists (listes de Block dynamiques)**), bloquer des adresses IP spécifiques que vous avez découvertes provenant de plusieurs sources de renseignement : l'analyse de votre propre menace ouvre une session, des attaques de DDoS d'adresses IP spécifiques, ou d'une liste rouge d'IP tiers.

  La liste doit se présenter sous forme de fichier texte localisé sur un serveur Web. À l'aide des groupes de périphériques sur Panorama, transmettez l'objet aux pare-feux gérés afin qu'ils puissent accéder au serveur Web et importer la liste à une fréquence définie. Après avoir créé un objet de liste du bloc dynamique, définir une règle de sécurité qui utilise l'objet adresse dans les champs de la source et de destination pour bloquer le trafic en provenance ou à l'adresse IP, plage ou sous-réseau défini. Cette approche vous permet de bloquer les intrus jusqu'à ce que vous résolviez le problème ou apportiez des changements de politique à un niveau plus large pour sécuriser votre réseau.
- Utilisez ces informations pour déterminer s'il faut bloquer l'application qui a provoqué l'infection (navigation web, SMTP, FTP), établir des règles de filtrage d'URL plus strictes ou limiter certaines applications/actions (par exemple, les téléchargements de fichiers à des groupes d'utilisateurs spécifiques).
- Sur Panorama, vous pouvez également changer de contexte de périphérique et configurer le pare-feu pour les rapports de Botnet qui identifient des hôtes infectés par des robots sur le réseau.

© 2020 Palo Alto Networks, Inc.

Panorama Haute Disponibilité

Pour assurer la redondance en cas de défaillance du système ou du réseau, vous pouvez déployer deux serveurs de gestion Panorama™ dans une configuration haute disponibilité (HD). Panorama prend en charge une configuration HD dans laquelle un homologue est l'actif-principal et l'autre est le passif-secondaire. Si une défaillance se produit sur l'homologue principal, il se déconnecte automatiquement et l'homologue secondaire devient actif.

- Configuration requise pour Panorama HD
- Priorité et basculement sur Panorama en HD
- Déclencheurs de basculement
- Remarques sur la journalisation de Panorama en HD
- Synchronisation entre les homologues HD Panorama
- Gérer une paire HD Panorama

© 2020 Palo Alto Networks, Inc.

Configuration requise pour Panorama HD

Pour configurer Panorama en HD, vous avez besoin d'une paire de serveurs Panorama identiques aux exigences suivantes sur chacun :

- **Même facteur de forme** : les homologues doivent être du même modèle et du même mode : appareils M-600, appareils M-500, appareils M-200, appareils virtuels Panorama sur AWS, Azure, GCP, et ESXi en mode Panorama, en mode gestion uniquement ou en mode hérité (ESXi et vCloud Air uniquement). Les appareils Panorama en mode Collecteur de journaux ne prennent pas en charge la haute disponibilité.
- **La même version de système d'exploitation Panorama** : ils doivent exécuter la même version de Panorama pour synchroniser les informations de configuration et maintenir la parité pour un basculement transparent.
- **Le même ensemble de licences** : ils doivent avoir la même licence de capacité de gestion de périphériques.
- (Appareil virtuel Panorama uniquement) **Numéro de série unique** : ils doivent avoir des numéros de série uniques ; si le numéro de série est le même pour les deux instances de Panorama, elles seront en mode suspendu jusqu'à ce que vous résolviez le problème.

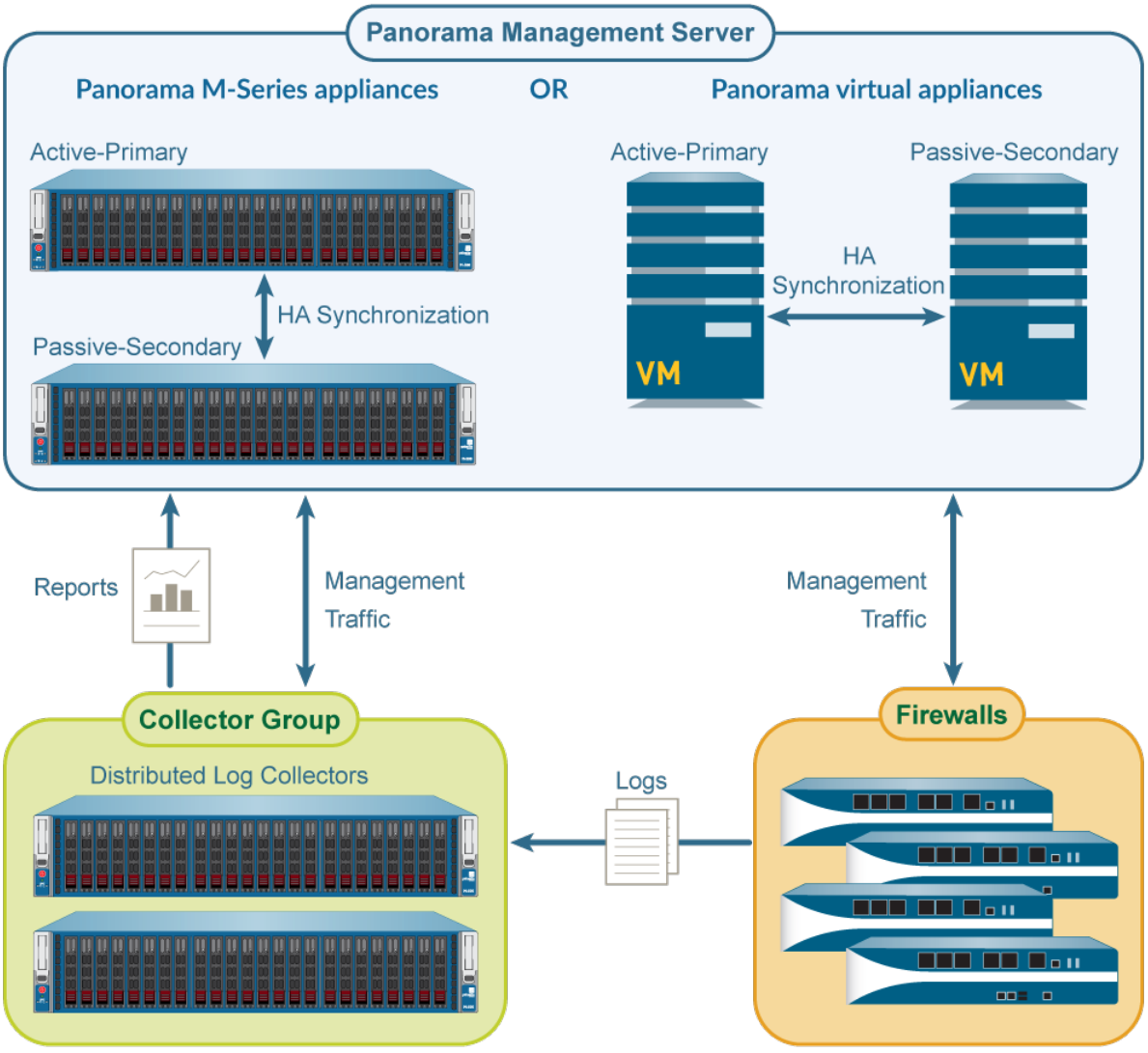


Figure 28: Organisation de la HD de Panorama

© 2020 Palo Alto Networks, Inc.

Les serveurs Panorama en configuration HD sont des homologues et vous pouvez utiliser l'un ou l'autre (actif ou passif) pour gérer de manière centralisée les pare-feu, les collecteurs de journaux et les appareils et clusters d'appareils WildFire, à de rares exceptions près (voir Synchronisation entre les homologues HA de Panorama). Les homologues HD utilisent l'interface de gestion (MGT) pour synchroniser les éléments de configuration appliqués aux pare-feu gérés, aux collecteurs de journaux et aux appareils et clusters d'appareils WildFire pour conserver les informations d'état. En général, les homologues HD sont situés sur des sites différents d'un point de vue géographique, et vous devez donc vous assurer que l'adresse IP de l'interface MGT affectée à chaque homologue peut être routée via votre réseau. La connectivité HD utilise le port TCP 28 avec cryptage activé. Si le cryptage n'est pas activé, les ports 28769 et 28260 sont utilisés pour la connectivité HD et pour synchroniser la configuration entre les paires HD. Nous recommandons moins de 500 ms de latence entre les paires. Pour déterminer la latence, faites un Ping lors d'une période de trafic normal.

© 2020 Palo Alto Networks, Inc.

Priorité et basculement sur Panorama en HD

Chaque homologue Panorama dans la paire HD est affecté à une valeur *prioritaire* . La valeur prioritaire de l'homologue principal ou secondaire détermine quel homologue sera utilisé comme point principal d'administration et de gestion de journal. L'homologue défini en tant que principal assume l'état actif, et le secondaire devient passif. L'homologue actif gère tous les changements de configuration et les transmet aux pare-feux gérés. L'homologue passif ne peut pas exécuter de changement de configuration ou transmettre la configuration aux pare-feu gérés. Cependant, l'un ou l'autre des homologues peut être utilisé pour exécuter des rapports ou lancer des requêtes sur les journaux.

L'homologue passif est synchronisé et prêt à passer à l'état actif si une défaillance du chemin, du lien, du système ou du réseau se produit sur le Panorama actif.

Lorsqu'un basculement se produit, seul l'état actif ou passif des modifications de périphérique change. La priorité (principal et secondaire) ne change pas. Par exemple, lorsque l'homologue principal échoue, son état passe de principal actif à principal passif.

Un homologue dans l'état d'actif-secondaire peut exécuter toutes les fonctions à deux exceptions près :

- Il ne peut pas gérer les fonctions de déploiement de pare-feu ou de Collecteur de journaux telles que les mises à jour de licences ou les mises à niveau logicielles.
- Il ne peut pas se connecter à un NFS jusqu'à ce que vous ayez manuellement fait passer sa priorité sur principal. Seul l'appareil virtuel Panorama en mode hérité prend en charge NFS.

Le tableau qui suit répertorie les fonctionnalités de Panorama en fonction de ses paramètres d'état et de priorité :

Capability	active-primary	passive-primary passive-secondary	active-secondary
Switch device context	■	■	■
Perform distributed reporting	■	■	■
Manage shared policy	■	■	■
Log to local disk	■	■ (Optional on the Panorama virtual appliance only)	■ (Optional on the Panorama virtual appliance only)
Log to an NFS partition (Panorama virtual appliance only)	■	■	■
Deploy software and licenses	■	■	■
Export Panorama configuration	■	■	■

Figure 29: Capacités de la HD de Panorama

Pour plus d'informations, reportez-vous à la section Configuration requise pour Panorama HD ou Définir la HD (haute disponibilité) sur Panorama.

© 2020 Palo Alto Networks, Inc.

Déclencheurs de basculement

Lorsqu'une panne survient sur le périphérique actif et si le périphérique passif assume la tâche consistant à gérer les pare-feux, l'événement est appelé basculement. Un basculement est déclenché lorsqu'une des mesures surveillées du périphérique actif échoue. Cet échec change l'état du Panorama primaire de primaire actif à primaire passif et le Panorama secondaire devient actif secondaire.

Les conditions déclenchant un basculement sont :

- Les homologues Panorama ne peuvent pas communiquer entre eux et l'homologue actif ne répond pas aux sondages d'état et de statut ; la mesure utilisée est Sondage de pulsation (heartbeat) Haute Disponibilité / HD (High Availability / HA) et messages Hello.

  Lorsque les homologues Panorama ne peuvent pas communiquer entre eux, l'homologue actif surveille si les périphériques sont toujours connectés avant de déclencher un basculement. Ce contrôle permet d'éviter un basculement et de causer un scénario de division, où les deux homologues Panorama se trouvent à l'état actif.
- Une ou plusieurs destinations (adresses IP) spécifiées sur l'homologue actif n'ont pas pu être jointes. La mesure utilisée est Surveillance des chemins de Haute Disponibilité / HD (High Availability / HA).

Outre les déclenchements de basculement répertoriés ci-dessus, un basculement se produit également lorsque l'administrateur met le pare-feu à l'état suspendu ou en cas de préemption. La préemption précise qu'à une reprise après défaillance (ou une suspension initiée par l'utilisateur), l'appareil Panorama principal doit être privilégié pour reprendre le rôle actif . Par défaut, la préemption est activée et lorsque l'appareil Panorama principal reprend après une défaillance et devient disponible. L'appareil Panorama secondaire perd le contrôle et revient à l'état passif. En cas de préemption, l'événement est consigné dans le journal système.

Si vous vous connectez à un magasin de données NFS, ne désactivez pas la préemption, car elle permet à l'homologue principal (monté sur le NFS) de reprendre le rôle actif et d'écrire sur le magasin de données NFS. Pour tous les autres déploiements, la préemption n'est requise que si vous voulez vous assurer qu'un périphérique spécifique soit le périphérique actif privilégié.

Sondage de pulsation (heartbeat) Haute Disponibilité / HD (High Availability / HA) et messages Hello

Les homologues haute disponiblité utilisent les messages Hello et les pulsations pour vérifier que l'homologue est réactif et opérationnel. Les messages Hello sont envoyés d'un homologue vers un autre pendant l'intervalle Hello configuré pour vérifier l'état de l'autre. La pulsation est une requête ping ICMP envoyée à l'homologue, qui répond au ping pour vérifier que les périphériques sont connectés et répondent. Par défaut, l'intervalle est de 1 000 millisecondes pour la pulsation et de 8 000 ms pour les messages Hello.

Surveillance des chemins de Haute Disponibilité / HD (High Availability / HA)

Le suivi de chemin vérifie l'état de connectivité et le lien réseau pour une adresse IP ou un groupe d'adresses IP (groupe de sentier). L'homologue actif utilise des requêtes ping ICMP pour vérifier qu'une ou plusieurs adresses IP de destination peuvent être jointes. Par exemple, vous pouvez contrôler la disponibilité des périphériques réseau interconnectés comme un routeur ou un commutateur, la connectivité à un serveur ou autre dispositif vital qui est dans le flux du trafic. Assurez-vous que le nœud/périphérique que vous surveillez n'a pas tendance à être non réactif, surtout lors de son chargement, car ceci pourrait entraîner un échec de surveillance du chemin et déclencher un basculement.

© 2020 Palo Alto Networks, Inc.

L’intervalle du ping est 5 000 ms. L'adresse IP est considérée comme inaccessible lorsque trois requêtes ping à la suite (la valeur par défaut) échouent, et qu'un échec de périphérique est déclenché lorsqu'une ou toutes les adresses IP surveillées deviennent inaccessibles. Par défaut, si l'une des adresses IP devient inaccessible, l'état HD passe à l'état non fonctionnel.

© 2020 Palo Alto Networks, Inc.

Remarques sur la journalisation de Panorama en HD

La configuration de Panorama dans une configuration HD fournit la redondance pour la collecte de journaux. Comme les services gérés sont connectés aux deux homologues Panorama sur SSL, lorsqu'un changement d'état survient, chaque Panorama envoie un message aux périphériques connectés. Les périphériques sont informés de l'état HD de Panorama et peuvent transmettre les journaux en conséquence.

Par défaut, lorsque les pare-feu gérés ne peuvent pas se connecter à Panorama, ils mettent les journaux en mémoire tampon ; lorsque la connexion est rétablie, ils reprennent l'envoi de journaux d'où il était laissé en dernier.

Les options de journalisation du Panorama matériel et de l'appareil virtuel Panorama diffèrent :

- Basculement de journalisation sur un appareil virtuel Panorama en mode hérité
- Basculement de journalisation sur un appareil de série M ou un appareil virtuel Panorama en mode Panorama

Basculement de journalisation sur un appareil virtuel Panorama en mode hérité

L'appareil virtuel Panorama en mode hérité présente les options de basculement de journalisation suivantes :

Type de stockage de journaux	Description
Disque virtuel	Par défaut, les périphériques gérés envoient les journaux à chacun des homologues HD Panorama, sous forme de flux de journaux distincts. Lorsqu'un homologue devient inaccessible, par défaut, les périphériques gérés mettent les journaux en mémoire tampon et lorsque l'homologue se reconnecte, ils reprennent l'envoi des journaux là où ils se sont arrêtés (en fonction de la capacité de stockage disque et de la durée de la déconnexion). La capacité maximale de stockage des journaux dépend de la plate-forme virtuelle (VMware ESXi ou vCloud Air) ; voir Modèles Panorama pour plus de détails. *Vous pouvez choisir de transférer les journaux uniquement vers l'homologue actif (voir Modifier le journal de transfert et la mise en mémoire tampon par défaut). Cependant, l'agrégation de journaux n'est pas prise en charge sur la paire HD. Ainsi, si vous vous connectez à un disque virtuel, pour la surveillance et les rapports, vous devez interroger l'homologue Panorama qui collecte les journaux auprès des pare-feu gérés.*
Système de fichiers réseau (NFS)	Vous pouvez monter le stockage NFS uniquement sur un appareil virtuel Panorama qui s'exécute sur un serveur VMware ESXi. Seul le Panorama principal actif est monté sur la partition de journaux basée sur NFS et peut

© 2020 Palo Alto Networks, Inc.

Type de stockage de journaux	Description
	recevoir les journaux. Au basculement, le périphérique principal passe à l'état primaire passif. Dans ce scénario, avant la préemption, l'appareil Panorama secondaire actif gère les périphériques, mais il ne reçoit pas les journaux et ne peut pas les écrire sur le NFS. Pour permettre à l'homologue secondaire actif de se connecter au NFS, vous devez le faire passer manuellement en principal pour qu'il puisse être monté sur la partition NFS. Pour obtenir des instructions, reportez-vous à la section Commuter la priorité pour reprendre la journalisation NFS après un basculement sur Panorama.

Basculement de journalisation sur un appareil de série M ou un appareil virtuel Panorama en mode Panorama

Si vous transférez des journaux de pare-feu aux collecteurs de journaux locaux sur une paire haute disponibilité d'appareils M-600, d'appareils M-500, d'appareils M-200 ou d'appareils virtuels Panorama en mode Panorama, vous spécifiez les pare-feux qui envoient des journaux aux collecteurs de journaux lorsque vous configurez un groupe de collecteurs. Vous pouvez configurer un groupe de collecteurs distinct pour le collecteur de journaux de chaque homologue Panorama ou configurer un seul groupe de collecteurs pour contenir les collecteurs de journal des deux homologues. Dans un groupe de collecteurs qui contient les deux collecteurs de journaux locaux, la liste de préférence de transfert de journaux détermine quel collecteur de journaux reçoit les journaux des pare-feu. Pour les pare-feu des séries PA-7000 et PA-5200, vous avez la possibilité d'envoyer des journaux à tous les collecteurs de journaux du groupe de collecteurs, auquel cas Panorama utilise l'équilibrage de charge circulaire pour sélectionner le collecteur de journaux recevant les journaux à un moment donné.

Dans un groupe de collecteurs contenant les deux collecteurs de journaux, vous pouvez également activer la redondance afin que chaque journal comporte deux copies et que chaque copie réside sur un collecteur de journaux différent. Cette redondance garantit qu'aucun journal n'est perdu en cas d'indisponibilité d'un collecteur de journaux : vous pouvez voir tous les journaux transférés au groupe de collecteurs et générer des rapports sur toutes les informations de journal. La redondance du journal n'est disponible que si chaque collecteur de journaux du groupe de collecteurs a le même nombre de disques.



Tous les collecteurs de journaux d'un groupe de collecteurs particulier doivent être du même modèle: uniquement des appareils M-200, uniquement des appareils M-500, uniquement des appareils M-600 ou uniquement des appareils virtuels Panorama en mode Panorama.

L'activation de la redondance générant un plus grand nombre de journaux, cette configuration nécessite une capacité de stockage supérieure. L'activation de la redondance multiplie par deux le trafic de traitement des journaux dans un groupe de collecteurs, réduisant ainsi de moitié son débit de journalisation maximum car chaque collecteur de journaux doit distribuer une copie de chaque journal qu'il reçoit. (Lorsque l'espace vient à manquer sur un groupe de collecteurs, il supprime les journaux antérieurs.)

© 2020 Palo Alto Networks, Inc.

Synchronisation entre les homologues HD Panorama

Les homologues HD Panorama synchronisent la configuration en cours chaque fois que vous validez les modifications sur l'homologue Panorama actif. La configuration candidate est synchronisée entre les homologues chaque fois que vous enregistrez la configuration sur l'homologue actif ou juste avant que le basculement ait lieu.

Les paramètres qui sont communs aux deux, comme les objets partagés et les règles de politique, les objets et règles de groupe de périphériques, la configuration des modèles, les profils de certificat et les profils de service SSL/TLS et la configuration de l'accès administratif sont synchronisés entre les paires Panorama HA.

Lorsque vous Activation de la récupération automatique de la validation, la synchronisation HA se produit seulement après que le pare-feu ait testé avec succès la connexion entre lui-même et Panorama après une transmission de Panorama.

Les paramètres qui ne sont pas synchronisés sont ceux qui sont propres à chaque homologue, tels les suivants :

- La configuration Panorama HD : paramètre de priorité, adresse IP de l'homologue, chemin de groupes de surveillance et adresses IP
- Configuration de Panorama : adresse IP de l'interface de gestion, paramètres FQDN, bannière de connexion, serveur NTP, fuseau horaire, emplacement géographique, serveur DNS, adresses IP autorisées pour accéder à Panorama, paramètres système SNMP et horaires de mise à jour de contenu dynamique
- Exportations programmées de configuration
- Configuration de la partition NFS et toutes les affectations de quota de disque pour la journalisation. Cela s'applique uniquement à un appareil virtuel Panorama en mode hérité qui s'exécute sur un serveur VMware ESXi.
- Affectation de quota de disque pour les différents types de journaux et bases de données sur l'espace de stockage local de Panorama (SSD)

> *Si vous utilisez une clé principale pour crypter les clés privées et les certificats utilisés sur Panorama, la même clé principale doit être utilisée pour crypter les clés privées et les certificats sur les deux homologues HD. Si les clés principales sont différentes, Panorama ne peut pas synchroniser les homologues HD.*

Pour plus d'informations, reportez-vous à la section Configuration requise pour Panorama HD ou Définir la HD (haute disponibilité) sur Panorama.

© 2020 Palo Alto Networks, Inc.

Gérer une paire HD Panorama

- Définir la HD (haute disponibilité) sur Panorama
- Configurer l'authentification à l'aide de certificats personnalisés entre homologues HD
- Tester le basculement HD de Panorama
- Commuter la priorité pour reprendre la journalisation NFS après un basculement sur Panorama
- Rétablir le Panorama primaire à l'état actif



Pour installer des logiciels ou des mises à jour de contenu, voir Installer les mises à jour pour Panorama dans une configuration HD*.*

Définir la HD (haute disponibilité) sur Panorama

Consultez la Configuration requise pour Panorama HD avant d'effectuer les étapes suivantes :

STEP 1 | Définissez la connectivité entre les ports MGT et les homologues HD.

Les homologues Panorama communiquent entre eux par le biais du port MGT. Assurez-vous que les adresses IP que vous affectez au port MGT sur les serveurs de Panorama dans la paire HD peuvent être acheminées et que les homologues peuvent communiquer entre eux via votre réseau. Pour configurer le port MGT, voir Effectuer la configuration initiale de l'appareil virtuel Panorama ou Effectuer la configuration initiale de l'appareil de série M.

Sélectionnez un périphérique dans la paire et exécutez les tâches restantes.

STEP 2 | Activez la HD et (éventuellement) le cryptage de la connexion HD.

1. Sélectionnez **Panorama (Panorama)** > **High Availability (Haute Disponibilité)** et modifiez la section **Setup (Configuration)**.
2. Sélectionnez **Enable HD (Activer la HD)**.
3. Dans le champ **Peer HA IP Address (Adresse IP de l'homologue HD)**, saisissez l'adresse IP attribuée à l'homologue Panorama.
4. Dans le champ **Peer HA Serial (Numéro de série HA de l'homologue)**, saisissez le numéro de série de l'homologue Panorama.

   Saisissez le numéro de série de l'homologue HA de Panorama pour réduire votre surface d'attaque face aux attaques de force brute sur l'IP de Panorama.
5. Dans le champ **Monitor Hold Time (Temps d'attente pour la surveillance)**, saisissez la durée (en millisecondes) d'attente du système avant d'intervenir suite à un échec de la liaison de contrôle (de 1 000 à 60 000 ms, 3 000 ms par défaut).
6. Si vous ne voulez pas le cryptage, décochez la case **Encryption Enabled (Cryptage activé)** et cliquez sur **OK**. Aucune autre étape n'est requise. Si vous voulez le cryptage, cochez **Encryption Enabled (Cryptage activé)** et cliquez sur **OK**, puis exécutez les tâches suivantes :
   1. Sélectionnez **Panorama (Panorama)** > **Certificate Management (Gestion de Certificat)** > **Certificates (Certificats)**.
   2. Sélectionnez **Export HD key (Exporter la clé HD)**. Enregistrez la clé HD sur un emplacement réseau auquel le périphérique homologue peut accéder.
   3. Sur le Panorama homologue, accédez à **Panorama (Panorama)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)**, sélectionnez **Import HA key (Importer la clé HD)**, accédez à l'emplacement où vous avez sauvegardé la clé et importez-la.

STEP 3 | Définissez la priorité HD.

© 2020 Palo Alto Networks, Inc.

1. Sous **Panorama (Panorama)** > **High Availability (Haute Disponibilité)**, modifiez la section **Election Settings (Paramètres de sélection)**.
2. Définir la **Device Priority (priorité du périphérique)** comme **Primary (Primaire)** ou **Secondary (Secondaire)**. Assurez-vous de mettre un homologue comme primaire et l'autre comme secondaire.

   Si les deux homologues ont le même paramètre de priorité, l'homologue portant le numéro de série le plus élevé sera placé à l'état suspendu.
3. Définissez le comportement **Preemptive (préemptif)**. Par défaut, la préemption est activée. La sélection de préemption (activée ou désactivée) doit être la même sur les deux homologues.

   Si vous utilisez un NFS pour l'enregistrement et avez désactivé la préemption, pour reprendre la connexion au NFS voir Commuter la priorité pour reprendre la journalisation NFS après un basculement sur Panorama.

STEP 4 | Pour configurer la surveillance de chemin, définissez un ou plusieurs groupes de chemins.

Le groupe de chemin d'accès répertorie les adresses IP de destination (nœuds) que Panorama doit pinger pour vérifier la connectivité réseau.

Effectuez les étapes suivantes pour chaque groupe de chemins incluant les nœuds que vous souhaitez surveiller.

1. Sélectionnez **Panorama (Panorama)** > **High Availability (Haute Disponibilité)** et, dans la section Groupe de chemins, cliquez sur **Add (Ajouter)**.
2. Saisissez un **Name (Nom)** pour le groupe de chemins.
3. Sélectionnez la **Failure Condition (Condition d'échec)** pour ce groupe :
   - **any (tout)** déclenche un échec de surveillance des chemins si l'une des adresses IP devient inaccessible.
   - **all (tout)** déclenche un échec de surveillance des chemins uniquement si aucune des adresses IP n'est accessible.
4. **Add (Ajouter)** chaque adresse IP de destination que vous souhaitez surveiller.
5. Cliquez sur **OK**. La section Path Group (Groupe de chemins) affiche le nouveau groupe.

STEP 5 | (Facultatif) Sélectionnez la condition d'échec pour la surveillance de chemins sur Panorama.

1. Sélectionnez **Panorama (Panorama)** > **High Availability (Haute Disponibilité)** et modifiez la section Surveillance des chemins.
2. Sélectionnez une **Failure Condition (Condition de panne)** :
   - **all (Tout)** : cette condition déclenche un basculement uniquement lorsque tous les groupes de chemins surveillés échouent.
   - **any (Chaque)** déclenche un basculement quand un seul groupe de chemin contrôlé échoue.
3. Cliquez sur **OK**.

STEP 6 | Validez vos modifications de configuration.

Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

STEP 7 | Configurez l'autre homologue Panorama.

Répétez de l'étape 2 à l'étape 6 pour l'autre homologue de la paire HD.

STEP 8 | Synchronisez les homologues Panorama.

1. Accédez au **Dashboard (Tableau de bord)** sur le Panorama actif et sélectionnez **Widgets** > **System (Système)** > **High Availability (Haute disponibilité)** pour afficher le widget HD.

© 2020 Palo Alto Networks, Inc.

2. **Sync to peer (Synchroniser avec l'homologue)**, cliquez sur **Yes (Oui)** et attendez que **Running config (Configuration actuelle)** affiche **Synchronized (Synchronisé)**.
3. Accédez au **Dashboard (Tableau de bord)** sur le Panorama passif et sélectionnez **Widgets** > **System (Système)** > **High Availability (Haute disponibilité)** pour afficher le widget HD.
4. Vérifiez que **Running config (Configuration actuelle)** affiche **Synchronized (Synchronisé)**.

Configurer l'authentification à l'aide de certificats personnalisés entre homologues HD

Vous pouvez configurer l'authentification à l'aide de certificats personnalisés pour sécuriser la connexion haute disponibilité entre les homologues HA Panorama.

STEP 1 | Générer un certificat autorité de certification (CA) sur Panorama.

1. Sélectionnez **Panorama (Panorama)** > **Certificate Management (Gestion de Certificat)** > **Certificates (Certificats)**.
2. Créez un certificat racine CA auto-signé ou importez un certificat de votre CA d'entreprise.

STEP 2 | Configurez un profil de certificat incluant l'autorité de certification racine et l'autorité de certification intermédiaire.

1. Sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificats)**.
2. Configurez un profil de certificat.

STEP 3 | Configurez un profil de service SSL/TLS.

1. Sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **SSL/TLS Service Profile (Profil de service SSL/TLS)**.
2. Configurez un profil SSL/TLS pour définir le certificat et le protocole que Panorama et ses périphériques de gestion utilisent pour les services SSL/TLS.

STEP 4 | Configurez la communication sécurisée avec le serveur sur Panorama.

1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Management (Gestion)** et **Edit (Modifiez)** les paramètres de Panorama.
2. Vérifiez que la case **Custom Certificate Only (Certificat personnalisé uniquement)** n'est pas cochée. Cela vous permet de continuer à gérer tous les périphériques lors de la migration vers des certificats personnalisés.

   Lorsque la case Custom Certificate Only (Certificat personnalisé uniquement) est cochée, Panorama ne s'authentifie pas et ne peut pas gérer les périphériques à l'aide de certificats prédéfinis.
3. Sélectionnez le profil de service SSL/TLS depuis le menu déroulant **SSL/TLS Service Profile (Profil de service SSL/TLS)**. Ce profil de service SSL/TLS s'applique à toutes les connexions SSL entre Panorama, les pare-feu, les collecteurs de journaux et les homologues HD de Panorama.
4. Sélectionnez le profil du certificat depuis la liste déroulante **Certificate Profile (Profil du certificat)**.
5. (Facultatif) Configurez une liste d'autorisation.
   1. Cliquez sur **Add (Ajouter)** sous Authorization List (Liste d'autorisation).
   2. Sélectionnez **Subject (Objet)** ou **Subject Alt Name (Autre nom de l'objet)** comme type d'identifiant.
   3. Saisissez le Common Name (Nom commun).
6. Dans **Disconnect Wait Time (min) (Délai d'attente de déconnexion (min))**, saisissez le nombre de minutes que Panorama doit attendre avant de mettre fin et de rétablir la connexion avec ses périphériques gérés. Ce champ est vide par défaut et la plage est comprise entre 0 et 44 640 minutes.

© 2020 Palo Alto Networks, Inc.

Le délai d'attente de déconnexion de déconnexion ne commence pas à décompter tant que vous n'avez pas validé la nouvelle configuration.

1. Cliquez sur **OK**.
2. **Commit (Validez)** vos modifications.

STEP 5 | Mettez à niveau le Panorama côté client vers la version 8.1.

Mettre à niveau Panorama.

STEP 6 | Configurez la communication sécurisée avec le client.

1. Sélectionnez **Panorama** > **High Availability (Haute disponibilité)** et **Edit (Modifiez)** la section HD.
2. Sélectionnez **Certificate (Certificat)** et **Certificate Profile (Profil de certificat)**.
3. Cliquez sur **OK**.
4. **Commit (Validez)** vos modifications.

Tester le basculement HD de Panorama

Pour vérifier que votre configuration HD fonctionne correctement, déclenchez un basculement manuel et vérifiez que l'homologue passe facilement d'un état à l'autre.

STEP 1 | Connectez-vous à l'homologue Panorama actif.

Vous pouvez vérifier l'état du serveur Panorama dans l'angle inférieur droit de l'interface Web.

STEP 2 | Suspendez l'homologue Panorama actif.

Sélectionnez **Panorama** > **High Availability (Haute Disponibilité)** et cliquez sur le lien **Suspend local Panorama (suspendre le Panorama local)** dans la section Commandes opérationnelles.

STEP 3 | Vérifiez que l'homologue Panorama passif est passé à l'état actif.

Sur le **Dashboard (Tableau de bord)** Panorama, dans le widget **High Availability (Haute disponibilité)**, vérifiez que l'état du serveur passif **local (local)** passe à **active (actif)** et que l'état de l'**Peer (homologue)** est **suspended (suspendu)**.

STEP 4 | Restaurez l'homologue suspendu à l'état fonctionnel. Patientez quelques minutes, puis vérifiez que la préemption s'est produite, si le mode préemptif a été activé.

Sur le Panorama que vous précédemment suspendu :

1. Sélectionnez **Panorama** > **High Availability (Haute Disponibilité)** et, dans la section des commandes opérationnelles, cliquez sur **Make local Panorama functional (Rendre le Panorama local fonctionnel)**.
2. Dans le widget **High Availability (Haute Disponibilité)** sur le **Dashboard (Tableau de bord)**, confirmez que le Panorama (Local) est devenu l'homologue actif et que l'autre homologue est maintenant à l'état passif.

Commuter la priorité pour reprendre la journalisation NFS après un basculement sur Panorama

L'appareil virtuel Panorama en mode hérité exécuté sur un serveur ESXi peut utiliser un magasin de donnée NFS pour la journalisation. Dans une configuration HD, seul le l'homologue Panorama principal est monté sur la partition de journaux basée sur NFS et peut écrire sur NFS. Lorsqu'un basculement se produit, et lorsque le Panorama passif devient actif, son état devient actif-secondaire. Bien que l'homologue Panorama secondaire puisse activement gérer les périphériques, il ne peut pas recevoir de journaux ou écrire sur

© 2020 Palo Alto Networks, Inc.

NFS, car il ne possède pas de partition NFS. Lorsque les pare-feu ne peuvent pas transférer de journaux vers l'homologue principal de Panorama, chaque pare-feu écrit les journaux sur son disque local. Les périphériques gardent un pointeur sur le dernier ensemble d'entrées de journaux transféré vers Panorama, de sorte que lorsque le Panorama actif principal redevient disponible, ils peuvent reprendre le transfert des journaux vers ce dernier.

Utilisez les instructions de cette section pour passer manuellement à la priorité sur l'homologue Panorama secondaire actif pour qu'il puisse commencer la journalisation vers la partition NFS. Les scénarios typiques dans lesquels vous pourriez avoir besoin déclencher ce changement sont les suivants :

- La préemption est désactivée. Par défaut, la préemption est activée sur Panorama et l'homologue principal reprend en tant qu'actif lorsqu'il redevient disponible. Lorsque la préemption est désactivée, vous devez faire passer la priorité de l'homologue secondaire sur principal pour qu'il puisse monter la partition NFS, recevoir des journaux depuis les périphériques gérés, et écrire sur la partition NFS.
- Le Panorama actif échoue et ne peut pas récupérer de son échec à court terme. Si vous ne modifiez pas la priorité, lorsque la capacité de stockage maximale du pare-feu est atteinte, les journaux les plus anciens sont écrasés pour lui permettre de poursuivre la journalisation sur son disque local. Cette situation peut entraîner la perte de journaux.

STEP 1 | Connectez-vous au panorama principal actuellement passif, sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)** et, dans la section Opérations de périphérique, cliquez sur **Shutdown Panorama (Arrêter Panorama)**.

STEP 2 | Connectez-vous au Panorama secondaire actif, sélectionnez **Panorama** > **High Availability (Haute Disponibilité)** , modifiez les paramètres de sélection, et définissez la **Priority (Priorité)** comme **Primary (Principale)**.

STEP 3 | Cliquez sur **OK** pour enregistrer vos modifications.

STEP 4 | Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

Ne pas redémarrer lorsque vous y êtes invité.

STEP 5 | Connectez-vous à la CLI Panorama et saisissez la commande suivante pour modifier la propriété de la partition NFS à cet homologue : **`request high-availability convert-to-primary`**

STEP 6 | Sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)** et, dans la section opérations du périphérique, cliquez sur **Reboot Panorama (redémarrer Panorama)**.

STEP 7 | Mettez sous tension l'homologue Panorama que vous avez arrêté à l'étape 1. Cet homologue devrait maintenant être à l'état secondaire-passif.

Rétablir le Panorama primaire à l'état actif

Par défaut, la fonctionnalité de préemption sur Panorama permet au Panorama principal de reprendre son fonctionnement d'homologue actif aussitôt qu'il devienne disponible. Cependant, si la préemption est désactivée, le seul moyen de forcer l'appareil Panorama principal à devenir actif à la reprise après un échec, un état non fonctionnel ou suspendu, consiste à suspendre l'homologue Panorama secondaire.

Avant que le Panorama actif secondaire ne passe à l'état suspendu, il transfère la configuration candidate au périphérique passif, de sorte que les modifications de configuration non validées sont enregistrées et accessibles sur l'autre homologue.

© 2020 Palo Alto Networks, Inc.

STEP 1 | Suspendre Panorama.

1. Connectez-vous à l'homologue Panorama que vous souhaitez mettre en mode suspendu.
2. Sélectionnez **Panorama** > **High Availability (Haute Disponibilité)** et cliquez sur le lien **Suspend local Panorama (suspendre le Panorama local)** dans la section Commandes opérationnelles.

STEP 2 | Vérifiez que l'état s'affiche et que le périphérique a été suspendu à la demande de l'utilisateur.

Sur le **Dashboard (Tableau de bord)**, sur le widget **High Availability (Haute disponibilité)**, vérifiez que l'état **local (local)** est **suspended (suspendu)**.

Un basculement est déclenché lorsque vous suspendez un homologue et que l'autre Panorama endosse le rôle d'homologue actif.

STEP 3 | Restaurer l'homologue Panorama suspendu à l'état fonctionnel.

1. Dans l'onglet **Panorama** > **High Availability (Haute Disponibilité)**, section Commandes opérationnelles, cliquez sur le lien **Make local Panorama functional (rendre fonctionnel le Panorama local)**.
2. Sur le **Dashboard (Tableau de bord)**, dans le widget **High Availability (Haute Disponibilité)**, confirmez que le périphérique est passé à l'état actif ou passif.

Gérer Panorama

Cette section explique comment administrer et gérer le serveur de gestion Panorama™. Elle comprend les rubriques suivantes :

- Prévisualisation, validation ou confirmation des modifications de configuration
- Activation de la récupération automatique de la validation
- Gérer Panorama et les sauvegardes de configuration du pare-feu
- Comparer les modifications dans les configurations de Panorama
- Gérez les Verrous pour Restreindre les Modifications de Configuration
- Ajouter des logos personnalisés à Panorama
- Utilisez le Gestionnaire de Tâches Panorama
- Gérer les Quotas de Stockage et les Périodes d'Expiration pour les Journaux et Rapports
- Contrôler Panorama
- Redémarrer ou arrêter Panorama
- Configurer les profils et la complexité de mot de passe Panorama

Pour avoir des instructions sur la configuration initiale, notamment les paramètres d'accès réseau, les licences, la mise à niveau de la version du logiciel Panorama et la définition d'un accès administratif à Panorama, reportez-vous à la section Configurer Panorama.

© 2020 Palo Alto Networks, Inc.

Prévisualisation, validation ou confirmation des modifications de configuration

Vous pouvez effectuer des Opérations de prévisualisation, validation ou confirmation de Panorama sur les modifications en attente de la configuration de Panorama, puis appliquer ces modifications aux périphériques gérés par Panorama, y compris les pare-feu, les collecteurs de journaux, les appareils WildFire et les clusters d'appareils. Vous pouvez filtrer les modifications en attente par administrateur ou *emplacement*, puis vous pouvez confirmer, appliquer, valider ou prévisualiser uniquement ces modifications. Ces emplacements peuvent être des groupes de périphériques spécifiques, des modèles, des groupes de collecteurs, des collecteurs de journaux, des appareils et des clusters WildFire, des paramètres partagés ou le serveur de gestion Panorama.

Étant donné que Panorama applique sa configuration actuelle, vous ne pouvez pas appliquer les modifications aux périphériques tant que vous ne les avez pas d'abord validées dans Panorama. Si les modifications ne sont pas prêtes à être activées sur les périphériques, vous pouvez sélectionner **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** pour valider les modifications apportées à la configuration de Panorama sans les appliquer aux périphériques. Plus tard, lorsque les modifications sont prêtes à être activées sur les périphériques, vous pouvez sélectionner **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)**. Si les modifications sont prêtes à être activées sur Panorama et les périphériques, sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** comme décrit dans la procédure suivante.

STEP 1 | Configurez l'étendue des modifications apportées à la configuration que vous allez valider, confirmer ou prévisualiser.

1. Cliquez sur **Commit (Valider)** en haut de l'interface Web.
2. Sélectionnez l'une des options suivantes :
   - **Commit All Changes (Valider tous les changements)** (par défaut) : applique la validation à tous les changements pour lesquels vous détenez des privilèges d'administrateur. Vous ne pouvez filtrer manuellement l'étendue de validation lorsque vous sélectionnez cette option. Au lieu de cela, le rôle d'administrateur affecté au compte que vous avez utilisé pour vous connecter détermine l'étendue de validation.
   - **Commit Changes Made By (Valider les changements apportés par)** : vous permet de filtrer l'étendue de validation par administrateur ou emplacement. Le rôle administrateur affecté au compte que vous avez utilisé pour vous connecter détermine les changements que vous pouvez filtrer.

   Pour valider les changements d'autres administrateurs, le compte que vous utilisez pour vous connecter doit s'être vu affecté le rôle de super-utilisateur ou un profil de rôle administrateur pour lequel le privilège de Commit For Other Admins (Valider pour le compte d'autres administrateurs) doit être activé.
3. (Facultatif) Pour filtrer l'étendue de validation par administrateur, sélectionnez **Commit Changes Made By (Valider les changements apportés par)**, cliquez sur le lien adjacent, sélectionnez les administrateurs, puis cliquez sur **OK**.
4. (Facultatif) Pour filtrer par emplacement, sélectionnez **Commit Changes Made By (Valider les changements apportés par)** et supprimez les changements que vous souhaitez exclure de l'étendue de validation.

   Si des dépendances entre les changements de configuration que vous avez inclus et ceux que vous avez exclus entraînent une erreur de validation, effectuez une

© 2020 Palo Alto Networks, Inc.

validation qui comprend tous les changements. Par exemple, lorsque vous validez des modifications apportées à un groupe de périphériques, vous devez inclure les modifications de tous les administrateurs qui ont ajouté, supprimé ou repositionné des règles pour la même base de règles dans ce groupe de périphériques.

STEP 2 | Prévisualisez les modifications que la validation activera.

Lorsque vous prévisualisez les modifications après avoir supprimé et rajouté le même périphérique à une règle de politique, Panorama affiche ce même périphérique comme ayant été supprimé de la configuration active et ajouté à la configuration candidate. De plus, l'ordre des périphériques dans la liste des périphériques cible de la configuration active peut alors différer de la configuration candidate et est présenté comme une modification lorsque vous prévisualisez les changements lorsqu'il n'y a pas de changements de configuration.

Cela peut être utile si, par exemple, vous ne vous souvenez pas de tous vos changements et vous n'êtes pas sûr de vouloir tous les activer.

Panorama compare les configurations que vous avez sélectionnées dans la Commit Scope (Étendue de validation) de la configuration en cours d'exécution. La fenêtre de prévisualisation affiche les configurations côte à côte et utilise un code couleur pour indiquer quelles modifications sont des ajouts (en vert), des modifications (en jaune) ou des suppressions (en rouge).

Preview Changes (Prévisualiser les modifications) et sélectionnez les **Lines of Context (Lignes du contexte)**, soit le nombre de lignes (des fichiers de configuration comparés) à afficher avant et après les différences mises en surbrillance. Ces lignes vous aident à corréler la sortie de prévisualisation dans les paramètres de l'interface Web. Fermez la fenêtre d'aperçu lorsque vous avez terminé l'examen des modifications.

Etant donné que les résultats de la prévisualisation s'affichent dans une nouvelle fenêtre, votre navigateur doit autoriser les fenêtres contextuelles. Si la fenêtre de prévisualisation ne s'ouvre pas, reportez-vous à la documentation de votre navigateur pour connaître les étapes permettant de débloquer l'ouverture des fenêtres contextuelles.

STEP 3 | Prévisualisez les paramètres individuels pour lesquels vous effectuez des modifications,

ce qui peut s'avérer utile si vous souhaitez connaître les détails des changements, comme les types de paramètres et la personne qui les a modifiés.

1. Cliquez sur **Change Summary (Récapitulatif des modifications)**.
2. (Facultatif) **Group By (Regrouper par)** nom de colonne (comme le **Type** de paramètre).
3. **Close (Fermez)** la boîte de dialogue Change Summary (Récapitulatif des modifications) lorsque vous avez terminé l'examen des modifications.

STEP 4 | Confirmez les modifications avant de procéder à la validation afin d'en garantir la réussite.

1. **Validate Changes (Validez les modifications)**.

   Les résultats présentent toutes les erreurs et tous les avertissements qu'une validation afficherait.
2. Résolvez les erreurs que les résultats de validation identifient.

STEP 5 | (Facultatif) Modifiez la portée d'application.

Par défaut, la portée d'application comprend tous les emplacements avec des modifications nécessitant une validation de la part de Panorama.

© 2020 Palo Alto Networks, Inc.



Si vous sélectionnez Commit (Valider) > Push to Devices (Appliquer aux périphériques), la portée d'application inclut tous les emplacements associés aux périphériques qui ne sont pas synchronisés avec la configuration actuelle de Panorama.

1. **Remove Selections (Supprimez les sélections)** pour supprimer les pare-feu indiqués dans la portée d'application.
2. **Edit Selections (Modifiez les sélections)** et sélectionnez :
   - **Device Groups (Groupes de périphériques)** : sélectionnez des groupes de périphériques ou des pare-feu ou systèmes virtuels individuels.
   - **Templates (Modèles)** : sélectionnez des modèles, des piles de modèles ou des pare-feu individuels.
   - **Collector Groups (Groupes de collecteurs)** : sélectionnez les groupes de collecteurs.
3. Cliquez sur **OK** pour enregistrer les modifications dans la portée d'application.

STEP 6 | Validez les modifications que vous apportez aux groupes de périphériques ou aux modèles.

1. **Validate Device Group Push (Valider l'application au groupe de périphériques)** ou **Validate Template Push (Valider l'application au modèle)**.

   Les résultats présentent toutes les erreurs et tous les avertissements qu'une opération d'application afficherait.
2. Résolvez les erreurs que les résultats de validation identifient.

STEP 7 | Validez vos modifications sur Panorama et appliquez-les aux périphériques.

Commit and Push (Valider et appliquer) les modifications de configuration.



Utilisez le Gestionnaire de Tâches Panorama *pour voir les détails sur les validations qui sont en attente (éventuellement, vous pouvez les annuler), en cours, terminées ou échouées.*

© 2020 Palo Alto Networks, Inc.

Activation de la récupération automatique de la validation

Pour s'assurer que les configurations brisées causées par des changements de configuration ont été appliquées par le serveur de gestion Panorama™ aux pare-feux gérés, ou validées localement sur le pare-feu, activez **Automated Commit Recovery (Récupération automatique des validations)** pour permettre aux pare-feux gérés de tester les changements de configuration pour chaque validation et pour vérifier que les changements n'ont pas interrompu la connexion entre Panorama et le pare-feu géré. Vous pouvez configurer le nombre de tests que chaque pare-feu géré effectue et l'intervalle auquel chaque test intervient avant que le pare-feu géré ne revienne automatiquement à la configuration d'exécution précédente. Lorsque vous activez la récupération automatique de la validation, la configuration du pare-feu géré est rétablie et non la configuration Panorama. Par ailleurs, le pare-feu géré teste sa connexion à Panorama toutes les 60 minutes afin de garantir la continuité de la communication au cas où une configuration réseau sans rapport aurait modifié la connectivité interrompue entre le pare-feu et Panorama ou si les impacts d'une configuration validée dans le passé affectaient la connectivité. Pour les configurations High Availability (haute disponibilité - HA), la synchronisation HA entre les homologues HA suite à une application de Panorama n'a lieu qu'après un test de connectivité.

La récupération automatisée de la validation est activée par défaut. Cependant, si vous avez désactivé la récupération automatique de la validation et que vous souhaitez ensuite réactiver cette fonctionnalité dans un environnement de production existant, vérifiez d'abord qu'il n'existe aucune règle de politique qui puisse interrompre la connexion entre Panorama et le pare-feu géré. Par exemple, dans le cas où le trafic de gestion traverse le plan de données, il se peut qu'une règle de politique restreigne le trafic du pare-feu vers Panorama.

Le pare-feu génère un journal de configuration après que la configuration du pare-feu soit revenue avec succès à la dernière configuration en cours. Qui plus est, le pare-feu génère un journal système lorsque l'administrateur désactive cette fonctionnalité, lorsqu'un événement de retour à la configuration commence en raison d'un test de connectivité qui échoue après une poussée de configuration, et lorsque le test de connectivité Panorama qui est effectué toutes les 60 minutes échoue et provoque le retour à la configuration du pare-feu.

Activez Automated Commit Recovery (Récupération automatisée de la validation) indépendamment de tout autre changement de configuration. Si cette fonctionnalité est activée en même temps que d'autres changements de configuration qui entraînent une rupture de connexion entre Panorama et les pare-feu gérés, la configuration du pare-feu ne peut pas être rétablie automatiquement.

STEP 1 | Se connecter à l'interface Web Panorama.

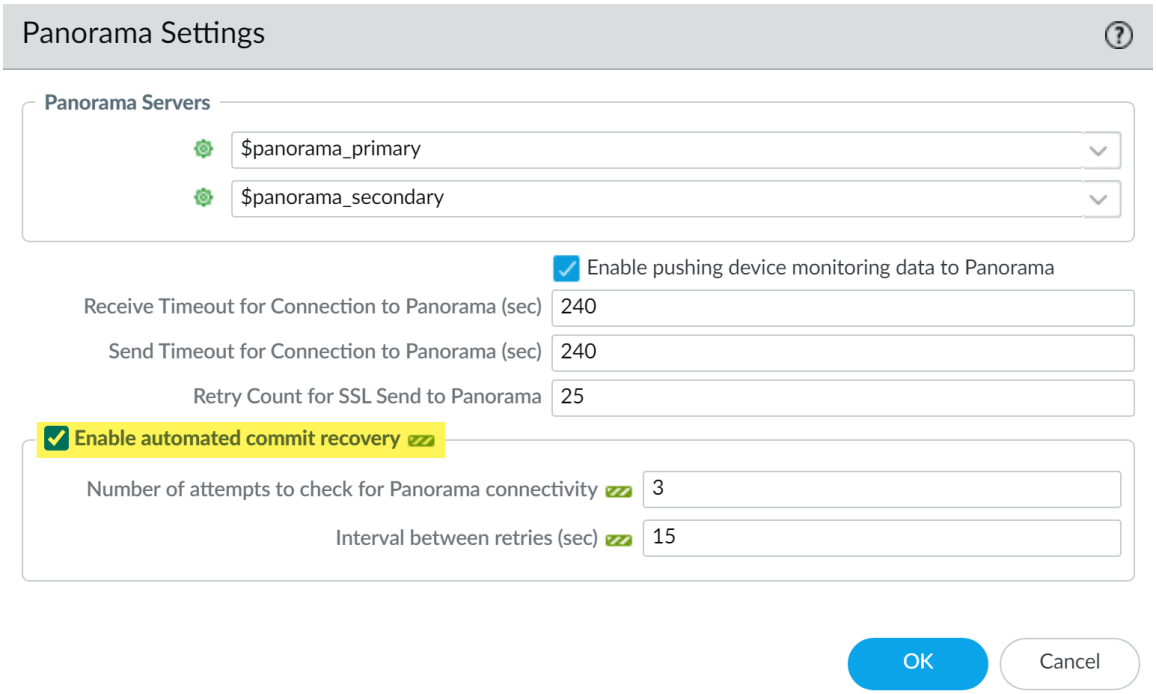
STEP 2 | Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)**et sélectionnez le modèle ou la pile de modèles souhaité(e) dans la liste déroulante de contexte **Template (Modèle)**.

STEP 3 | Activation de la récupération automatique de la validation.

1. **Edit** (Modifiez) les paramètres de Panorama.
2. **Activation de la récupération automatique de la validation**.
3. Configurez le **Nombre de tentatives de vérification de la connectivité Panorama** (par défaut, 1 tentative).

© 2020 Palo Alto Networks, Inc.

4. Configurez **Interval between retries (Intervalle entre les tentatives)** (par défaut, 10 secondes).
5. Cliquez sur **OK** pour enregistrer vos modifications.



STEP 4 | **Commit (Valider)** > **Commit and Push (Valider et appliquer)** et **Commit and Push (Validez et appliquez)** vos changements.

STEP 5 | Vérifiez que la fonction de récupération automatique de la validation est activée sur vos pare-feux gérés.

1. Accédez à l'interface Web du pare-feu.
2. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et, dans les Paramètres de Panorama, vérifiez que l'option **Enable automated commit recovery (Activer la récupération automatique de la validation)** est activée (cochée).

© 2020 Palo Alto Networks, Inc.

Gérer Panorama et les sauvegardes de configuration du pare-feu

La configuration en cours d'exécution sur Panorama comprend tous les paramètres que vous avez validés et qui sont donc actifs. La configuration candidate est une copie de la configuration en cours d'exécution ainsi que de toutes les modifications apportées depuis la dernière validation. La sauvegarde des versions de la configuration en cours d'exécution ou candidate vous permet de restaurer ultérieurement ces versions. Par exemple, si une validation montre que la configuration candidate actuelle a plus d'erreurs que vous ne souhaitez réparer, vous pouvez restaurer une configuration candidate précédente. Vous pouvez également revenir à la configuration en cours sans enregistrer d'abord une sauvegarde.



Consultez Opérations de prévisualisation, validation ou confirmation de Panorama *pour plus d'informations sur la validation des modifications de configuration apportées à Panorama et sur les modifications apportées aux périphériques gérés.*

Après une validation sur un pare-feu local qui exécute Pan-OS 5.0 ou ultérieur, une sauvegarde de sa configuration actuelle est envoyée à Panorama. Toutes les validations effectuées sur le pare-feu local déclenchent la sauvegarde, y compris les validations qu'un administrateur effectue localement sur le pare-feu ou les validations automatiques lancées par PAN-OS (telles qu'un rafraîchissement du nom de domaine complet). Par défaut, panorama stocke jusqu'à 100 sauvegardes pour chaque pare-feu, bien que cela soit configurable. Pour stocker des sauvegardes de configuration de Panorama et de pare-feu sur un hôte externe, vous pouvez planifier des exportations de panorama ou d'exportation sur demande. Vous pouvez également importer des configurations depuis les pare-feu dans des groupes et des modèles de périphériques Panorama pour Transition d'un pare-feu à une gestion Panorama.

(VMware ESXi et vCloud Air uniquement) la fonctionnalité de sauvegarde (snapshot) VMware n'est pas compatible avec un appareil virtuel Panorama déployé sur VMware ESXi et vCloud Air. Prendre des sauvegardes (snapshots) d'un appareil virtuel Panorama peut avoir un impact sur la performance, avoir pour conséquence une perte de paquets intermittente et incohérente et Panorama peut ne plus répondre. De plus, vous pouvez perdre l'accès au CLI de Panorama et à l'interface web et le basculement vers le mode Panorama n'est pas possible. Au contraire, save and export (sauvegardez et exportez) la sauvegarde (snapshot) nommée de votre configuration vers n'importe quel emplacement du réseau.

- Planifier l'exportation des fichiers de configuration
- Sauvegarde et exportation de configurations de pare-feu et de Panorama
- Annulation des modifications apportées à la configuration de Panorama
- Configurer le nombre maximal de sauvegardes de configuration stockées sur Panorama
- Charger une sauvegarde de configuration sur un pare-feu géré

Planifier l'exportation des fichiers de configuration

Panorama enregistre une sauvegarde de la configuration en cours d'exécution ainsi que les configurations en cours d'exécution de tous les pare-feu gérés. Les sauvegardes sont au format XML avec les noms de fichiers qui sont basés sur des numéros de série (de Panorama ou des pare-feux). Utilisez ces instructions pour programmer les exportations quotidiennes des sauvegardes vers un hôte distant. Panorama exporte les sauvegardes dans un seul fichier au format gzip. Vous avez besoin des privilèges de super-utilisateur pour planifier l'exportation.



Si Panorama est dans une configuration haute disponibilité (HD), vous devez suivre ces instructions sur chaque homologue pour vous assurer que les exportations planifiées

© 2020 Palo Alto Networks, Inc.

continuent après un basculement. Panorama ne synchronise pas les exportations de configuration planifiées entre les homologues HD.

Pour exporter des sauvegardes à la demande, consultez Sauvegarde et exportation de configurations de pare-feu et de Panorama.

STEP 1 | Sélectionnez **Panorama** > **Scheduled Config Export (Exportation planifiée de la configuration)** et cliquez sur **Add (Ajouter)**.

STEP 2 | Entrez un **Name (Nom)** et une **Description** pour l'exportation planifiée du fichier et cliquez sur **Enable (Activer)**.

STEP 3 | En utilisant le format 24-heures, entrez une quotidienne **Scheduled Export Start Time (heure planifiée du début de l'exportation)** ou sélectionnez-en une dans la liste déroulante.



Si vous configurez une exportation programmée vers deux ou plusieurs serveurs, échelonnez l'heure de début des exportations programmées. La planification du lancement de plusieurs exportations en même temps entraîne des divergences entre les configurations exportées.

STEP 4 | Réglez l'exportation**Protocol** (Protocole) sur Copie sécurisée (**SCP** (SCP)) ou Protocole de Transfert de Fichiers (**FTP** (FTP)).

STEP 5 | Entrez les détails pour accéder au serveur, y compris : **Hostname (Nom d'hôte)** ou adresse IP, **Port**, **Path (Chemin)** pour charger le fichier, **Username (Nom d'utilisateur)** et **Password (Mot de passe)**.

Le **chemin d'accès** prend en charge les caractères suivants : **.**(période), **+**, **{** et **}**, **/**, **-**, **_**, **0-9**, **a-z**, et **A-Z**. Les espaces ne sont pas pris en charge dans le fichier **Chemin d'accès**.



Si vous exportez vers un serveur FTP en utilisant une adresse IPv6 comme nom d'hôte, vous devez saisir l'adresse entre crochets ([ ]). Par exemple, ***[2001:0db8:0000:0000:0000:8a2e:0370:7334]****.*

Si vous exportez vers un serveur BSD, vous devrez modifier l'invite de mot de passe SSHD comme suit : ***<nom d'utilisateur>@<nom d'hôte> <mot de passe>:***

STEP 6 | (SCP uniquement) Cliquez sur **Test SCP server connection (Tester la connexion au serveur SCP)**. Pour permettre le transfert sécurisé des données, vous devez vérifier et accepter la clé d'hôte du serveur SCP. Panorama n'établira pas la connexion jusqu'à ce que vous n'acceptiez la clé de l'hôte. Si Panorama dispose d'une configuration HD, effectuez cette étape sur chaque homologue HD afin que chacun accepte la clé d'hôte du serveur SCP. Si Panorama peut réussir sa connexion au serveur SCP, il crée et télécharge le fichier de test nommé ssh-export-tes.ttx.

STEP 7 | Cliquez sur **OK** pour enregistrer vos modifications.

STEP 8 | Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

© 2020 Palo Alto Networks, Inc.

Sauvegarde et exportation de configurations de pare-feu et de Panorama

Sauvegarder une copie de la configuration candidate au stockage permanent sur Panorama vous donne la possibilité de rétablir plus tard à cette sauvegarde (voir Annulation des modifications apportées à la configuration de Panorama). De plus, Panorama vous permet d'enregistrer et d'exporter les configurations des groupes de périphériques, des modèles et des piles de modèle que vous spécifiez. Cela s'avère utile pour conserver des modifications qui risqueraient autrement d'être perdues en cas d'événement système ou d'action administrateur entraînant le redémarrage de Panorama. Après redémarrage, Panorama revient à la version actuelle de la configuration active, que Panorama sauvegarde dans un fichier nommé `running-config.xml`. Sauvegarder une copie s'avère également utile lorsque vous souhaitez rétablir les paramètres d'une configuration de Panorama antérieure à la version actuelle de la configuration active. Panorama n'enregistre pas automatiquement la configuration candidate au stockage permanent. Vous devez enregistrer manuellement la configuration du candidat comme un fichier instantané par défaut (`.snapshot.xml`) ou comme un fichier instantané personnalisé. Panorama sauvegarde le fichier instantané en local, mais vous pouvez l'exporter vers un hôte externe.



Vous n'avez pas à sauvegarder une copie de configuration pour annuler les modifications apportées depuis la dernière validation ou le dernier redémarrage ; il suffit de sélectionner Config (Configuration) > Revert Changes (Annulez les modifications) (voir Annulation des modifications apportées à la configuration de Panorama).

Palo Alto Networks vous conseille d'effectuer une sauvegarde de toutes les configurations importantes sur un hôte externe.

STEP 1 | Enregistrez les modifications sur la configuration candidate.

- Pour remplacer l'instantané par défaut (`.snapshot.xml`) avec toutes les modifications apportées par tous les administrateurs, effectuez l'une des tâches suivantes :
  - Sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)** et **Save candidate Panorama configuration (Enregistrer la configuration candidate de Panorama)**.
  - Connectez-vous à Panorama avec un compte administrateur disposant du rôle de super-utilisateur ou d'un profil de rôle administrateur avec le privilège **Save For Other Admins (Enregistrer pour le compte d'autres administrateurs)** activé. Sélectionnez ensuite **Config (Configuration)** > **Save Changes (Sauvegardez les modifications)** dans la partie supérieure de l'interface web, sélectionnez **Save All Changes (Sauvegardez toutes les modifications)** et **Save (Sauvegardez)**.
- Pour remplacer l'instantané par défaut (`.snapshot.xml`) en intégrant les changements apportées par les administrateurs aux configurations de groupes de périphériques, de modèles ou de piles de modèles donnés :
  1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)**, **Save candidate Panorama configuration (Enregistrer la configuration candidate de Panorama)** et **Select Device Group & Templates (Sélectionner le groupe de périphériques et les modèles)**.
  2. Sélectionnez les groupes de périphériques, les modèles ou les piles de modèles devant faire l'objet de l'annulation.
  3. Cliquez sur **OK** pour confirmer l'opération.
  4. (Facultatif) Pour écraser la configuration en cours d'exécution avec l'instantané, cliquez sur **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos modifications.
- Pour créer un instantané qui inclut toutes les modifications apportées par tous les administrateurs, mais sans écraser le fichier instantané par défaut :

© 2020 Palo Alto Networks, Inc.

1. Sélectionnez **Panorama (Panorama)** > **Setup (Configuration)** > **Operations (Opérations)** et **Save named Panorama configuration snapshot (enregistrez l'instantané de configuration nommé Panorama)**.
2. Saisissez le **Name (Nom)** du nouveau fichier de configuration ou celui existant.
3. Cliquez sur **OK** et **Close (Fermez)**.

- Pour sauvegarder uniquement certaines modifications apportées à la configuration candidate sans écraser des parties du fichier instantané par défaut :

  1. Connectez-vous à Panorama avec un compte administrateur disposant de privilèges d'accès requis pour sauvegarder les modifications souhaitées.
  2. Sélectionnez **Config (Configuration)** > **Save Changes (Sauvegardez les modifications)** dans la partie supérieure de l'interface web.
  3. Sélectionnez **Save Changes Made By (Sauvegardez les modifications apportées par)**.
  4. Pour filtrer le champ de Sauvegardes par administrateur, cliquez sur <*administrator-name*>, choisissez les administrateurs, et cliquez sur **OK**.
  5. Pour filtrer le champ de sauvegardes par emplacement, effacer tout emplacement à exclure. Ces emplacements peuvent être des groupes de périphériques spécifiques, des modèles, des groupes de collecteurs, des collecteurs de journaux, des appareils et des clusters WildFire, des paramètres partagés ou le serveur de gestion Panorama.
  6. Cliquez sur **Save (Enregistrer)**, spécifiez le **Name (Nom)** d'un nouveau fichier de configuration ou d'un fichier de configuration existant et cliquez sur **OK**.

- Pour enregistrer la configuration d'un groupe de périphériques, d'un modèle ou d'une pile de modèles devant faire l'objet :

  1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)**, **Save named Panorama configuration snapshot (Enregistrer l'instantané de configuration candidate de Panorama)** et **Select Device Group & Templates (Sélectionner le groupe de périphériques et les modèles)**.
  2. Sélectionnez les groupes de périphériques, les modèles ou les piles de modèles devant être enregistrés.
  3. Cliquez sur **OK** pour confirmer l'opération.

STEP 2 | Exportez un candidat ou une configuration en cours d'exécution vers un hôte externe à Panorama ou à un pare-feu.

Vous pouvez planifier les exportations quotidiennes vers un serveur SCP ou FTP (voir Planifier l'exportation des fichiers de configuration) ou exporter des configurations à la demande. Pour l'exportation à la demande, sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)** et sélectionnez l'une des options suivantes :

- **Export named Panorama configuration snapshot (Exporter l'image instantanée de configuration nommée Panorama)** : -exporte la configuration en cours d'exécution, un instantané de configuration de candidat nommé ou une configuration précédemment importée (candidat ou en cours d'exécution). Panorama exporte la configuration en tant que fichier XML avec le **Name (Nom)** que vous spécifiez. **Select Device Group & Templates (Sélectionnez le groupe de périphériques et les modèles)** pour spécifier les configurations de groupes de périphériques, de modèles ou de piles de modèles à exporter.
- **Export Panorama configuration version (Exporter la version de configuration de Panorama)** : sélectionnez une **Version** de la configuration en cours d'exécution pour l'exporter en tant que fichier XML. **Select Device Groups & Templates (Sélectionnez le groupe de périphériques et les modèles)** pour spécifier les configurations de groupes de périphériques, de modèles ou de piles de modèles à exporter en tant que fichier XML.
- **Export Panorama and devices config bundle (Exporter Panorama et le module de configuration des périphériques)** : -génère et exporte la dernière version de la sauvegarde de configuration en cours

© 2020 Palo Alto Networks, Inc.

d'exécution de Panorama et de chaque pare-feu géré. Pour automatiser le processus de création et l'exportation de l'ensemble de la configuration quotidiennement vers un serveur Secure Copy (SCP) ou FTP, voir Planifier l'exportation des fichiers de configuration.

- **Export or push device config bundle (Exportation ou push du package de dispositif de configuration)**-Après avoir importé une configuration de pare-feu dans Panorama, Panorama crée un ensemble de configurations de pare-feux nommé <firewall_name> _import.tgz, dans laquelle toutes les politiques locales et les objets sont supprimés. Vous pouvez alors cliquer **Export or push device config bundle (Exporter ou transférer le module de dispositif de configuration des périphériques)** pour effectuer une des actions suivantes :
  - **Push & Commit (Transférer et Valider)** le module de configuration au pare-feu pour enlever toute configuration locale, vous permettant de gérer le pare-feu à partir de Panorama.
  - **Export (Exportez)** la configuration vers le pare-feu sans la charger. Lorsque vous êtes prêt à charger la configuration, connectez-vous à l'ILC du pare-feu et exécutez la commande de mode de configuration **`Charger l'état de l'appareil`**. Cette commande nettoie le pare-feu comme l'option **Push & Commit (Appliquer & valider)**.

La procédure complète de Transition d'un pare-feu à une gestion Panorama nécessite des étapes supplémentaires.

Annulation des modifications apportées à la configuration de Panorama

Lorsque vous annulez des modifications, vous remplacez les paramètres de la configuration candidate actuelle par les paramètres d'une autre configuration. Annuler des modifications s'avère utile lorsque vous voulez revenir sur des modifications apportées à tous les paramètres en une seule opération plutôt que de reconfigurer manuellement chaque paramètre.

Vous pouvez annuler des modifications en cours apportées à Panorama depuis la dernière validation. Vous pouvez annuler toutes les modifications en attente sur Panorama ou sélectionner des groupes de périphériques, des modèles ou des piles de modèles spécifiques. Panorama fournit l'option de filtrer les modifications en cours en fonction des administrateurs ou des emplacements. Ces emplacements peuvent être des groupes de périphériques spécifiques, des modèles, des groupes de collecteurs, des collecteurs de journaux, des appareils et des clusters WildFire, des paramètres partagés ou le serveur de gestion Panorama. Si vous avez créé un instantané pour une configuration candidate qui est antérieure à la configuration active (reportez-vous à Sauvegarde et exportation de configurations de pare-feu et de Panorama), vous pouvez aussi revenir à cet instantané de configuration candidate. Revenir à un instantané vous permet de restaurer une configuration candidate existant avant la dernière validation. Panorama enregistre automatiquement une nouvelle version de la configuration en cours d'exécution chaque fois que vous validez des modifications, et vous pouvez restaurer l'une de ces versions.

Le rétablissement de la configuration d'un serveur de gestion Panorama nécessite une validation complète et doit être effectuée par un super utilisateur. Des validations complètes sont nécessaires pour effectuer certaines opérations de Panorama, telles que le rétablissement et le chargement d'une configuration de Panorama, et ne sont pas prises en charge pour les profils de rôle d'administrateur personnalisés.

- Revenir à la configuration actuelle de Panorama (fichier nommé **`running-config.xml`**).

  Cette opération annule les modifications apportées à la configuration candidate depuis la dernière validation.

  - Pour annuler toutes les modifications apportées par tous les administrateurs, effectuez l'une des tâches suivantes :

© 2020 Palo Alto Networks, Inc.

- Sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)**, **Revert to running configuration (Revenir à la dernière configuration actuelle de Panorama)** et cliquez sur **Yes (Oui)** pour confirmer l'opération.
- Connectez-vous à Panorama avec un compte administrateur disposant du rôle de super-utilisateur ou d'un profil de rôle administrateur avec le privilège **Commit For Other Admins (Valider pour le compte d'autres administrateurs)** activé. Sélectionnez ensuite **Config (Configuration)** > **Revert Changes (Annuler les modifications)**, sélectionnez **Revert All Changes (Annulez toutes les modifications)** et **Revert (Annulez)**.

- Pour annuler uniquement des changements spécifiques à la configuration candidate :
  1. Connectez-vous à Panorama avec un compte administrateur disposant de privilèges d'accès requis pour annuler les modifications souhaitées.

     Les privilèges contrôlant les opérations de validation contrôlent également les opérations d'annulation.
  2. Sélectionnez **Config (Configuration)** > **Revert Changes (Annuler les modifications)**.
  3. Sélectionnez **Revert Changes Made By (Annulez les modifications apportées par)**.
  4. Pour filtrer le champ d'annulations par administrateur, cliquez sur *<administrator-name> (nom de l'administrateur)*, choisissez les administrateurs, et cliquez sur **OK**.
  5. Pour filtrer le champ d'annulations par emplacement, effacez tout emplacement à exclure.
  6. **Revert (Annulez)** les modifications.
- Pour annuler des modifications apportées à un groupe de périphériques, un modèle ou une piles de modèles donnés sur la configuration active :
  1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)**, **Revert to running Panorama configuration (Revenir à la configuration active de Panorama)** et **Select Device Group & Templates (Sélectionner le groupe de périphériques et les modèles)**.
  2. Sélectionnez les groupes de périphériques, les modèles ou les piles de modèles devant faire l'objet de l'annulation.
  3. Cliquez sur **OK** pour confirmer l'opération.
  4. (Facultatif) Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos modifications pour remplacer la configuration active.

- Revenir à l'instantané par défaut (`.snapshots.xml`) de la configuration candidate de Panorama.
  - Pour annuler toutes les modifications apportées par les administrateurs :
    1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)** et **Revert to last saved Panorama configuration (Rétablir la dernière configuration de Panorama sauvegardée)**.
    2. Cliquez sur **Yes (Oui)** pour confirmer l'opération.
    3. (Facultatif) Pour écraser la configuration en cours d'exécution avec l'instantané, cliquez sur **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos modifications.
  - Pour annuler des modifications apportées à un groupe de périphériques, un modèle ou une piles de modèles donnés sur la configuration active :
    1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)**, **Revert to last saved Panorama configuration (Revenir à la dernière configuration de Panorama qui a été enregistrée)** et **Select Device Group & Templates (Sélectionner le groupe de périphériques et les modèles)**.
    2. Sélectionnez les groupes de périphériques, les modèles ou les piles de modèles devant faire l'objet de l'annulation.
    3. Cliquez sur **OK** pour confirmer l'opération.

© 2020 Palo Alto Networks, Inc.

4. (Facultatif) Pour écraser la configuration en cours d'exécution, sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos modifications à l'aide de l'instantané.

- Revenir à une version précédente de la configuration active qui est stockée sur Panorama.
  - Pour annuler les modifications apportées par les administrateurs :
    1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)**, **Load Panorama configuration version (Charger la version de la configuration de Panorama)** et **Select Device Group & Templates (Sélectionner le groupe de périphériques et les modèles)**.
    2. Sélectionnez une **Version** de configuration et cliquez sur **OK**.
    3. (Facultatif) Pour écraser la configuration en cours d'exécution avec la version que vous venez de rétablir, cliquez sur **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos modifications.
  - Pour annuler des modifications apportées à un groupe de périphériques, un modèle ou une piles de modèles donnés sur la configuration active :
    1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)**, **Load Panorama configuration version (Charger la version de la configuration de Panorama)** et sélectionnez le **Name (Nom)** d'une version de configuration.
    2. **Select Device Groups & Templates (Sélectionnez les groupes de périphériques et les modèles)** pour sélectionner les groupes de périphériques, les modèles ou les piles de modèles spécifiques devant faire l'objet de l'annulation.
    3. Cliquez sur **OK** pour confirmer l'opération.
    4. (Facultatif) Pour écraser la configuration en cours d'exécution avec l'instantané, cliquez sur **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos modifications.

- Revenir à l'un des états suivants :
  - Version personnalisée de la configuration d'exécution de panorama que vous avez précédemment importée.
  - Instantané au nom personnalisé de la configuration candidate (plutôt que l'instantané par défaut).

  1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)**, **Load named Panorama configuration snapshot (Charger l'instantané de configuration de Panorama nommé)**, puis sélectionnez le **Name (Nom)** du fichier de configuration que vous venez d'importer.
  2. (Facultatif) **Load Shared Objects (Charger les objets partagés)** ou **Load Shared Policies (Charger les politiques partagées)** pour charger tous les objets ou politiques partagés. Vous pouvez charger tous les objets et politiques partagés ainsi que tous les objets et politiques configurés dans les groupes de périphériques et les modèles que vous spécifiez à l'étape suivante.
  3. (Facultatif) **Select Device Groups & Templates (Sélectionnez les groupes de périphériques et les modèles)** pour sélectionner les configurations des groupes de périphériques, des modèles ou des piles de modèles spécifiques à charger. Sautez cette étape si vous souhaiter annuler la configuration de Panorama au complet.
  4. Cliquez sur **OK** pour confirmer l'opération.
  5. (Facultatif) Pour écraser la configuration en cours d'exécution avec l'instantané, cliquez sur **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos modifications.

- Restaurez un Panorama en cours d'exécution ou une configuration candidate que vous avez précédemment exportée vers un hôte externe.

© 2020 Palo Alto Networks, Inc.

1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)**, **Import named Panorama configuration snapshot (importez l'instantané de configuration nommé Panorama)**, **Browse (accédez)** au fichier de configuration sur l'hôte externe, puis cliquez sur **OK**.
2. **Load named Panorama configuration snapshot (Chargez un instantané de la configuration nommé Panorama)**, puis sélectionnez le **Name (Nom)** de la configuration que vous venez d'importer.
3. (Facultatif) **Load Shared Objects (Charger les objets partagés)** ou **Load Shared Policies (Charger les politiques partagées)** pour charger tous les objets ou politiques partagés. Vous pouvez charger tous les objets et politiques partagés ainsi que tous les objets et/ou politiques configurés dans les groupes de périphériques et les modèles que vous spécifiez à l'étape suivante.
4. (Facultatif) **Select Device Groups & Templates (Sélectionnez les groupes de périphériques et les modèles)** pour sélectionner les configurations des groupes de périphériques, des modèles ou des piles de modèles spécifiques à charger. Sautez cette étape si vous souhaiter annuler la configuration de Panorama au complet.
5. Cliquez sur **OK** pour confirmer l'opération.
6. (Facultatif) Pour écraser la configuration en cours d'exécution avec l'instantané que vous venez d'importer, cliquez sur **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos modifications.

Configurer le nombre maximal de sauvegardes de configuration stockées sur Panorama

STEP 1 | Sélectionnez **Panorama (Panorama)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les Paramètres de journalisation et de rapports.

STEP 2 | Sélectionnez **Log Export and Reporting (Exportation et génération de rapports de journaux)** et entrez le **NNumber of Versions for Config Backups (Nombre de versions pour les sauvegardes de configuration)** (la valeur par défaut est 100, la plage est comprise entre 1 et 1 048 576).

STEP 3 | Cliquez sur **OK** pour enregistrer vos modifications.

STEP 4 | Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

Charger une sauvegarde de configuration sur un pare-feu géré

Utilisez Panorama pour charger une sauvegarde de configuration sur un pare-feu géré. Vous pouvez choisir de revenir à une configuration enregistrée ou validée au préalable sur le pare-feu. Panorama transmet la version sélectionnée au pare-feu géré et la configuration candidate actuelle sur le pare-feu est écrasée.

STEP 1 | Sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)** > **Summary (Récapitulatif)**.

STEP 2 | Sélectionnez **Manage (Gestion)** dans la colonne Sauvegardes.

STEP 3 | Faites un choix entre Configurations sauvegardées et Configurations validées.

- Cliquez sur un numéro de version pour visualiser le contenu de cette version.
- **Load (Charger)** une version de configuration

STEP 4 | Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

© 2020 Palo Alto Networks, Inc.

Comparer les modifications dans les configurations de Panorama

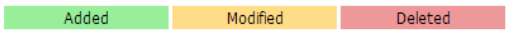
Pour comparer les changements de configuration sur Panorama, vous pouvez sélectionner deux ensembles de fichiers de configuration : la configuration candidate, la configuration en cours d'exécution ou toute autre version de configuration précédemment enregistrée ou enregistrée sur Panorama. La comparaison côte à côte vous permet de :

- Prévisualiser les modifications de configuration avant de les valider dans Panorama. Vous pouvez, par exemple, prévisualiser les modifications intervenues entre la configuration candidate et la configuration en cours. L'idéal est de sélectionner la version la plus ancienne dans le volet de gauche, et la version la plus récente dans le volet de droite, pour comparer et identifier facilement les modifications.
- Effectuer un *audit de configuration* pour consulter et comparer les modifications intervenues entre les deux ensembles de fichiers de configuration.

*Les administrateurs du groupe et modèles de périphériques ne peuvent comparer que les configurations des groupes et modèles de périphériques se trouvant dans leurs*domaines d'accès*.*

- Comparez les modifications dans les configurations de Panorama.
  1. Sélectionnez **Panorama** > **Config Audit (Vérification de configuration)**.
  2. Dans chaque menu déroulant, sélectionnez une configuration pour la comparaison.
  3. Sélectionnez le nombre de lignes que vous souhaitez inclure pour **Context (Contexte)**, et cliquez sur **Go (Aller)**.

     Panorama utilise l'ombrage de couleur pour mettre en surbrillance les éléments que vous avez ajoutés (vert), modifiés (jaunes) ou supprimés (rouge).



- Configurez le nombre de versions stockées sur Panorama pour des audits de configuration.
  1. Sélectionnez **Panorama (Panorama)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les Paramètres de journalisation et de rapports.
  2. Saisissez le **Number of Versions for Config Audit (Nombre de versions pour la vérification de configuration)** (la plage est 1 – 1048576 ; la valeur par défaut est 100).
  3. Cliquez sur **OK** pour enregistrer vos modifications.
  4. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

- Affichez et comparez les fichiers de configuration Panorama avant de valider.
  1. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Preview Changes (Prévisualiser les modifications)**.
  2. Sélectionnez le nombre de **Lines of Context (Lignes de contexte)** que vous voulez voir, puis cliquez sur **OK**.

© 2020 Palo Alto Networks, Inc.

Gérez les Verrous pour Restreindre les Modifications de Configuration

Verrouiller le candidat ou la configuration en cours d'exécution empêche les autres administrateurs de modifier la configuration jusqu'à ce que vous supprimiez manuellement le verrou ou que Panorama le supprime automatiquement (après une validation). Les verrous garantissent que les administrateurs ne rendent pas les modifications contradictoires aux mêmes paramètres ou paramètres interdépendants pendant les sessions de connexion simultanées.

Si vous modifiez des paramètres qui ne sont pas liés aux paramètres d'autres administrateurs qui changent dans les sessions simultanées, vous n'avez pas besoin de verrous de configuration pour empêcher les conflits de validation. Panorama met en files d'attente de validation des opérations et les exécute dans l'ordre où les administrateurs lancent les validations. Pour plus d'informations, reportez-vous à la section Opérations de prévisualisation, validation ou confirmation de Panorama.

Une validation de la configuration de modèle ou de groupe de périphérique échouera si un pare-feu affecté au modèle ou au groupe de périphériques comporte un verrou de configuration ou de configuration qu'un administrateur définit localement sur ce pare-feu.

- Voir les détails sur les verrous actuels.

  Par exemple, vous pouvez vérifier si d'autres administrateurs ont défini des verrous et lire les commentaires qu'ils ont entrés pour expliquer les verrous.

  Cliquez sur le cadenas verrouillé ( ) en haut de l'interface Web. Le nombre adjacent indique le nombre de verrous actuels.

- Verrouillez une configuration.

  Les administrateurs en lecture seule qui ne peuvent pas modifier les configurations de pare-feu ou de panorama ne peuvent pas définir des verrous.

  1. Cliquez sur l'icône de cadenas en haut de l'interface Web.

     L'icône varie selon que les verrous existants sont définis ( ) ou ne sont pas définis ( ).
  2. **Take a Lock (Prenez un verrou)** et sélectionnez le **Type** de verrou :
     - **Config (Configuration)**: empêche d'autres administrateurs de modifier la configuration candidate.

       Un administrateur de rôle personnalisé qui ne peut pas commettre des modifications peut définir un verrou de Config (configuration) et enregistrer les modifications apportées à la configuration candidate. Toutefois, parce que cet administrateur ne peut pas valider les modifications, Panorama ne libère pas automatiquement le verrou après une validation ; l'administrateur doit supprimer manuellement le verrou de Config (configuration) après avoir apporté les modifications nécessaires.

     - **Commit (Verrou de validation)** : empêche d'autres administrateurs de modifier la configuration active.
  3. Sélectionnez **Location (emplacement)** pour déterminer l'étendue du verrou :
     - **Shared (Partagé)** : restreint les modifications apportées à l'intégralité de la configuration de Panorama, y compris tous les groupes de périphériques et modèles .

© 2020 Palo Alto Networks, Inc.

- **Template (Modèle)** -limite les modifications aux pare-feu inclus dans le modèle sélectionné. (vous ne pouvez pas mettre un verrou pour une pile de modèles, uniquement pour les modèles individuels dans la pile.)
- **Device group (Groupe d'appareils)** -Limite des changements pour le groupe de périphériques sélectionnés, mais pas ses groupes de périphériques descendants.

4. (Facultatif) L'idéal est de saisir un **Comment (Commentaire)** pour décrire la raison pour laquelle vous placez un verrou.
5. Cliquez sur **OK** et **Close (Fermez)**.

- Déverrouiller une configuration.

  Seul un super-utilisateur ou l'administrateur qui a verrouillé la configuration peut la déverrouiller manuellement. Toutefois, panorama supprime automatiquement un verrou après l'achèvement de l'opération de validation que l'administrateur qui a défini le verrou a initié.

  1. Cliquez sur le cadenas verrouillé ( ) en haut de l'interface Web.
  2. Sélectionnez l'entrée de verrou dans la liste.
  3. Cliquez sur **Remove Lock (supprimer le verrou)**, **OK**, et **Close (fermer)**.

- Configurez panorama pour verrouiller automatiquement la configuration en cours d'exécution lorsque vous modifiez la configuration candidate. Ce paramètre s'applique à tous les administrateurs Panorama.
  1. Sélectionnez **Panorama (Panorama)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les Paramètres Généraux.
  2. Sélectionnez **Automatically Acquire Commit Lock (Acquérir automatiquement un verrou de validation)**, puis cliquez sur **OK**.
  3. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

© 2020 Palo Alto Networks, Inc.

Ajouter des logos personnalisés à Panorama

Vous pouvez télécharger des fichiers image pour personnaliser les domaines suivants sur Panorama :

- Image d'arrière-plan sur l'écran de connexion
- En-tête sur le coin supérieur gauche de l'interface web ; vous pouvez également cacher l'arrière-plan par défaut de Panorama
- Page de titre et pied de page dans les rapports PDF

Les types d'image pris en charge sont .jpg, .gif, et .png. Les fichiers image à utiliser dans les rapports PDF ne peuvent pas contenir de canal alpha. La taille de l'image doit être inférieure à 128 Kb (131 072 octets) ; les dimensions recommandées sont affichées à l'écran. Si ses dimensions sont supérieures à la taille recommandée, l'image est automatiquement recadrée.

STEP 1 | Sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)**.

STEP 2 | Dans la section Divers, cliquez sur **Custom Logos (Logos personnalisés)**.

STEP 3 | Cliquez sur l'icône de téléchargement de logo et sélectionnez une image pour l'une des options suivantes : l'écran de connexion, le coin gauche de l'interface utilisateur principale, la page de titre du rapport PDF et le pied de page du rapport PDF.

STEP 4 | Cliquez sur **Open (Ouvrir)** pour ajouter l'image. Pour afficher l'aperçu de l'image, cliquez sur l'icône de prévisualisation du logo.

STEP 5 | (Facultatif) Pour effacer l'en-tête d'arrière-plan vert sur l'interface Web Panorama, cochez la case correspondant à **Remove Panorama background header (Supprimer l'en-tête dans l'arrière-plan de Panorama)**.

STEP 6 | Cliquez sur **Close (Fermer)** pour enregistrer vos modifications.

STEP 7 | Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

© 2020 Palo Alto Networks, Inc.

Utilisez le Gestionnaire de Tâches Panorama

Cliquez sur **Tasks (tâches)** () en bas de l'interface Web pour ouvrir le gestionnaire des tâches, qui affiche des détails sur toutes les opérations effectuées par les administrateurs (par exemple, validations manuelles) ou ce panorama ou un pare-feu géré initié (par exemple, génération de rapports planifié) depuis le dernier Panorama ou redémarrage du pare-feu. Vous pouvez utiliser le gestionnaire des tâches pour dépanner les opérations en échec, enquêter sur les avertissements associés aux validations terminées ou annuler les validations en attente.

*Les administrateurs du Groupe et modèles de périphériques ne peuvent afficher que les tâches se trouvant dans leurs*domaines d'accès*.*

STEP 1 | Cliquez sur **Tasks (tâches)**.

STEP 2 | **Show (Afficher)** les tâches **Running (en cours d'exécution)** (en cours) ou **All (toutes)** les tâches (par défaut), éventuellement filtrer par type (**Reports (rapports)**; **Log Requests (Journaux de Requêtes)** ; (ou **Jobs (Tâches de)**validation, téléchargement et installation), puis sélectionnez **Panorama (Panorama)** (par défaut) ou le pare-feu pour lequel vous souhaitez visualiser les tâches.

STEP 3 | Effectuez l'une des actions suivantes :

- **Affichez ou masquez les détails de la tâche** (par défaut, le gestionnaire des tâches affiche le type, l'État, l'heure de début et les messages pour chaque tâche. Pour visualiser l'heure de fin et l'ID de travail d'une tâche, vous devez afficher manuellement ces colonnes. Pour afficher ou masquer une colonne, ouvrez le menu déroulant dans n'importe quel en-tête de colonne, sélectionnez **Columns (colonnes)**, puis sélectionnez ou désactivez les colonnes à votre guise.
- **Examinez les avertissements ou les échecs** — Lisez les écritures de la colonne messages pour les détails de la tâche. Si la colonne indique **trop de messages**, cliquez sur l'entrée dans la colonne Type pour afficher plus d'informations.
- **Affichez une description de validation** — si un administrateur a entré une description pour une validation, cliquez sur **Commit Description (valider la description)** dans la colonne messages pour l'afficher.
- Vérifiez la position d'une validation dans la file d'attente : la colonne messages indique la position dans la file d'attente des validations en cours.
- **Annuler la validation en attente** : **Clear Commit Queue (Effacer la file d'attente de validation)** pour annuler toutes les validations en attente (disponible uniquement pour les rôles administratifs prédéfinis). Pour annuler une validation individuelle, cliquez sur **x** dans la colonne action (la validation reste dans la file d'attente jusqu'à ce que Panorama la retire). Vous ne pouvez pas annuler les validations qui sont en cours.

© 2020 Palo Alto Networks, Inc.

Gérer les Quotas de Stockage et les Périodes d'Expiration pour les Journaux et Rapports

- Stockage de journaux et rapports
- Périodes d'expiration des journaux et des rapports
- Configurer les quotas de stockage et les périodes d'expiration pour les journaux et les rapports
- Configurer l'heure d'exécution pour les rapports Panorama

Stockage de journaux et rapports

Vous pouvez modifier les quotas de stockage par défaut pour chaque type de journal. Lorsqu'un quota de journal atteint la taille maximale, Panorama commence à écraser les entrées de journal les plus anciennes avec les nouvelles entrées du journal. La capacité de stockage pour les rapports n'est pas configurable. Les emplacements de stockage des journaux et les capacités de stockage des rapports varient selon le modèle Panorama :

- **Appareil virtuel Panorama en mode Panorama** : l'espace de stockage pour les rapports est de 200 Mo. L'appareil utilise son disque système virtuel pour stocker les journaux système et de configuration générés par Panorama et les collecteurs de journaux. Le disque système virtuel stocke également les journaux de statistiques d'application (App Stats) que Panorama reçoit automatiquement à des intervalles de 15 minutes depuis tous les pare-feu gérés. Panorama stocke tous les autres types de journaux sur ses disques de journalisation virtuels (1 à 12).
- **Appareil virtuel Panorama en mode de Gestion uniquement.** : l'espace de stockage pour les rapports est de 500 Mo. L'appareil utilise son disque système virtuel pour stocker les journaux système et de configuration générés par Panorama et les collecteurs de journaux. Le disque système virtuel stocke également les journaux de statistiques d'application (App Stats) que Panorama reçoit automatiquement à des intervalles de 15 minutes depuis tous les pare-feu gérés. Vous devez Collecteurs gérés pour transférer des journaux à partir de pare-feu gérés comme Panorama en mode Gestion uniquement ne peut pas stocker tout autre type de journal.
- **Appareil virtuel Panorama en mode hérité** : l'espace de stockage pour les rapports est de 200 Mo pour Panorama 8.0 ou versions antérieures, et de 500 Mo pour Panorama 8.0.1 et versions ultérieures. Panorama écrit tous les journaux dans son espace de stockage attribué ; il peut s'agir de l'un des espaces suivants :
  - **Disque du système virtuel** : par défaut, environ 11 Go sont alloués au stockage de journaux sur le disque du système virtuel que vous avez créé lors de l'installation de Panorama. Si vous ajoutez un disque de journalisation virtuel ou une partition NFS, Panorama utilise toujours le disque système pour stocker les journaux système et de configuration générés par Panorama et les collecteurs de journaux, et pour stocker les journaux de statistiques d'application collectés des les pare-feu.
  - **Disque de journalisation virtuel dédié** : stocke tous les types de journaux, sauf ceux qui résident sur le disque système.
  - **Partition NFS** : cette option est disponible uniquement pour Panorama exécuté sur un serveur VMware ESXi. La partition NFS stocke tous les types de journaux à l'exception de ceux qui résident sur le disque système.
- **Appareil M-600, M-500 ou M200** : l'espace de stockage pour les rapports est de 500 Mo pour Panorama 6.1 ou versions ultérieures, et de 200 Mo pour les versions antérieures. Les appareils de série M utilisent leurs SSD internes pour stocker les journaux de configuration et les journaux système que génèrent Panorama et les collecteurs de journaux, et pour stocker les journaux de statistiques d'application collectés des pare-feu. Panorama enregistre tous les autres types de journaux sur ses disques compatibles RAID. Les disques RAID sont soit localement dans l'appareil de série M en mode Panorama ou dans un collecteur de journaux dédié (appareil de série M en mode collecteur de journaux).

© 2020 Palo Alto Networks, Inc.

Vous modifiez les quotas de stockage de journal sur les disques RAID lorsque vous Configurez un groupe de collecteurs.

Pour plus de détails sur les options et les capacités de stockage des journaux, voir Modèles Panorama. Vous pouvez accroître la capacité de stockage des journaux sur l'appareil virtuel Panorama en ajoutant des disques de journalisation virtuels ou du stockage NFS. Vous pouvez augmenter le stockage sur un appareil de la série M en ajoutant des disques RAID ou en passant d'un lecteur de 1 To à un disque de 2 To.

Périodes d'expiration des journaux et des rapports

Vous pouvez configurer la suppression automatique basée sur le temps pour les journaux que le serveur de gestion Panorama et le journal des collectionneurs recueillent auprès des pare-feux, ainsi que les journaux et rapports que Panorama et les collecteurs du journal produisent localement. Ceci est utile dans les déploiements où la suppression périodique des informations surveillées est souhaitée ou nécessaire. Par exemple, la suppression des informations de l'utilisateur après une certaine période peut être obligatoire dans votre organisation pour des raisons juridiques. Vous configurez des périodes d'expiration distinctes pour :

- **Rapports** : Panorama supprime les rapports expirés en même temps qu'il génère de nouveaux rapports (voir Configurer l'heure d'exécution pour les rapports Panorama).
- **Chaque type de journal** : Panorama évalue les journaux lorsqu'il les reçoit et supprime les journaux qui dépassent le délai d'expiration configuré.
- *Panorama effectue une synchronisation des périodes d'expiration entre paires de haute disponibilité (HD). Parce que seul l'homologue HD actif génère des journaux, l'homologue passif n'a aucun journal ou rapport à supprimer, à moins que le basculement se produise et qu'il commence à générer des journaux.*

  Lorsqu'un quota de journal atteint la taille maximale, Panorama commence à écraser les entrées de journal les plus anciennes par les nouvelles entrées du nouveau journal.

Configurer les quotas de stockage et les périodes d'expiration pour les journaux et les rapports

STEP 1 | Configurer les quotas de stockage et les délais d'expiration pour :

- Les journaux de tous les types qu'un appareil virtuel Panorama en mode hérité reçoit des pare-feu.
- Les journaux de statistiques de l'application que Panorama reçoit des pare-feu.
- Les journaux système et de configuration que Panorama et les collecteurs de journaux génèrent localement.

Le serveur de gestion Panorama stocke ces fichiers journaux localement.

Si vous réduisez un quota de stockage tel que les journaux actuels le dépassent, après avoir validé le changement, Panorama supprime les journaux les plus anciens pour s'adapter au quota.

1. Sélectionnez **Panorama (Panorama)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les Paramètres de journalisation et de rapports.
2. Dans les paramètres de **Log Storage (Stockage de journaux)**, entrez le stockage **Quota (%)** pour chaque type de journal.

   Lorsque vous modifiez la valeur du pourcentage, l'écran est actualisé pour afficher la valeur absolue correspondante (colonne Quota Go/Mo), en fonction de la capacité de stockage totale allouée à Panorama.

© 2020 Palo Alto Networks, Inc.

3. Entrez les **Max Days (Jours maximum)** pour chaque type de journal (plage de 1 à 2 000).

   Par défaut, les champs sont vides, ce qui signifie que les journaux n'expirent jamais.

   Sélectionnez Restore Defaults (Rétablir les valeurs par défaut) si vous souhaitez réinitialiser les quotas et les délais d'expiration aux valeurs par défaut.

STEP 2 | Configurez la période d'expiration pour les rapports générés par Panorama.

1. Sélectionnez **Log Export and Reporting (Exportation et génération de rapports de journaux)** et entrez la **Report Expiration Period (Période d'expiration du rapport)** en jours (plage de 1 à 2 000).

   Par défaut, les champs sont vides, ce qui signifie que les journaux n'expirent jamais.
2. Cliquez sur **OK** pour enregistrer vos modifications.

STEP 3 | Configurez les quotas de stockage et les périodes d'expiration des journaux de tous types (à l'exception des journaux AppStats) que les appliances M-600, M-500, M-200 ou Panorama en mode Panorama reçoivent des pare-feux.

Les collecteurs de journaux locaux ou dédiés stockent ces journaux.

Vous configurez ces quotas de stockage au niveau du groupe de collecteurs, pas pour les collecteurs de journaux individuels.

1. Sélectionnez **Panorama** > **Collector Groups (Groupes de collecteurs)** et modifiez le groupe de collecteurs.
2. Dans l'onglet **General (Général)**, cliquez sur la valeur de **Log Storage (Stockage des journaux)**.

   Aucune valeur ne s'affiche, sauf si vous avez affecté des collecteurs de journaux au groupe de collecteurs. Si le champ affiche 0 Mo après avoir attribué des collecteurs de journaux, vérifiez que vous avez activé les paires de disques lors de la configuration d'un collecteur géré *et que vous avez validé les modifications (Panorama > Managed Collectors (Collecteurs gérés) > Disks (Disques)).*
3. Entrez le **Quota (%)** du stockage pour chaque type de journal.

   Lorsque vous modifiez la valeur de pourcentage, l'écran est actualisé pour afficher la valeur absolue correspondante (colonne Quota Go/Mo), en fonction de la capacité de stockage totale allouée au groupe de collecteurs.
4. Entrez les **Max Days (Jours maximum)** pour chaque type de journal (plage de 1 à 2 000).

   Par défaut, les champs sont vides, ce qui signifie que les journaux n'expirent jamais.

   Sélectionnez Restore Defaults (Rétablir les valeurs par défaut) si vous souhaitez réinitialiser les quotas et les délais d'expiration aux valeurs par défaut.
5. Cliquez sur **OK** pour enregistrer vos modifications.

STEP 4 | Validez les modifications apportées dans Panorama et appliquez-les au groupe de collecteurs.

1. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** et **Edit Selections (Modifier les sélections)** dans la portée d'application.
2. Sélectionnez **Collector Groups (Groupes de collecteurs)**, sélectionnez le groupe de collecteurs que vous avez modifié, puis cliquez sur **OK**.
3. **Commit and Push (Validez et appliquez)** vos modifications.

STEP 5 | Vérifier que Panorama ait appliqué les changements de quota de stockage.

© 2020 Palo Alto Networks, Inc.

1. Sélectionner **Panorama (Panorama)** > **Setup (Paramétrage)** > **Management (Gestion)** et, dans les paramètres de journalisation et de rapports, vérifier que les valeurs de **Log Storage (Stockage de journaux)** sont correctes pour les journaux que les de serveur de gestion Panorama stockent.
2. Sélectionner **Panorama (Panorama)** > **Collector Groups(Groupes Collecteurs)**, Sélectionnez le groupe de collecteur que vous avez modifié, puis vérifiez si les valeurs de **Log Storage (Stockage des journaux)** dans l'onglet **General (Général)** sont correctes pour les journaux que les collecteurs de journaux stockent.



Vous pouvez également vérifier les quotas de stockage du Groupe Collecteur en vous connectant à une ILC de Collecteur de journaux et en entrant la commande opérationnelle ***show log-diskquota-pct****.*

Configurer l'heure d'exécution pour les rapports Panorama

Panorama génère des rapports quotidiennement à l'heure que vous spécifiez. Panorama supprime tous les rapports expirés après avoir généré les nouveaux rapports.

STEP 1 | Sélectionnez **Panorama (Panorama)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les Paramètres de journalisation et de rapports.

STEP 2 | Sélectionnez **Log Export and Reporting (Exportation et génération de rapports de journaux)** et définissez le **Report Runtime (Heure d'exécution du rapport)** sur une heure en utilisant le format d'horloge 24 heures (02:00 par défaut ; plage comprise entre 00:00 [minuit] et 23:00).

STEP 3 | Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

© 2020 Palo Alto Networks, Inc.

Contrôler Panorama

Pour surveiller Panorama et ses collecteurs gérés, vous pouvez périodiquement afficher leurs journaux système et de configuration (filtrer les journaux par type), configurer un gestionnaire SNMP pour collecter (GET) régulièrement des statistiques Panorama ou configurer des interruptions SNMP ou des alertes par courrier électronique qui vous informent lorsqu'une métrique surveillée change d'état ou atteint un seuil sur Panorama. Les alertes email et interruptions SNMP sont utiles pour la notification immédiate des événements système critiques nécessitant votre attention. Pour configurer les alertes emails ou des interruptions SNMP, voir Configurer le transfert des journaux de Panorama vers des destinations extérieures.

- Journaux système et de configuration de Panorama
- Surveiller Panorama et les Statistiques de Collecteur de journaux en utilisant SNMP

Journaux système et de configuration de Panorama

Vous pouvez configurer Panorama pour envoyer des notifications lorsqu'un événement système ou un changement de configuration se produit. Par défaut, Panorama enregistre chaque changement de configuration dans les journaux de configuration. Dans les journaux système, chaque événement a un niveau de gravité pour indiquer son urgence et son impact. Lorsque vous Configurer le transfert des journaux de Panorama vers des destinations extérieures, vous pouvez transférer tous les journaux système et de configuration ou filtrer les journaux en fonction d'attributs tels que l'heure de réception ou le niveau de gravité (journaux système uniquement). Le tableau suivant résume les niveaux de gravité pour les journaux système :

Sévérité	Description
Critique	Indique un échec et la nécessité d'une attention immédiate, comme une défaillance matérielle, y compris le basculement à haute disponibilité (HD) et les pannes de liens.
Élevée	Problèmes sérieux qui vont empêcher le fonctionnement du système, notamment en cas de déconnexion d'un collecteur de journaux ou un échec de validation.
Moyenne	Notifications de niveau intermédiaire, comme les mises à niveau de paquet d'antivirus, ou une application de la configuration d'un groupe de collecteurs.
Faible	Notifications de gravité mineure telles que les changements de mot de passe utilisateur.
Informations	Les événements de notification tels que Connection ou déconnection, tout changement de configuration, la réussite d'authentification et les notifications d'échec, valider un succès et tous les autres événements que les autres niveaux de gravité ne couvrent pas.

Panorama stocke les journaux système et de configuration localement ; l'emplacement exact et la capacité de stockage varient selon le modèle Panorama (voir Stockage de journaux et rapports). Lorsque la limite de capacité est atteinte, Panorama supprime les journaux les plus anciens pour créer de l'espace pour les nouveaux journaux. Si vous avez besoin de stocker les journaux pendant des périodes plus longues que ce que permet le stockage local, consultez Configurer le transfert des journaux de Panorama vers des destinations extérieures.

© 2020 Palo Alto Networks, Inc.

Pour plus d'informations sur l'utilisation de Panorama pour surveiller les journaux de pare-feu, voir Surveiller l'activité réseau.

Surveiller Panorama et les Statistiques de Collecteur de journaux en utilisant SNMP

Vous pouvez configurer un gestionnaire SNMP pour demander des statistiques d'un serveur de gestion de Panorama et configurer Panorama pour répondre. Par exemple, le gestionnaire SNMP peut demander le mode haute disponibilité (HD), l'état de Panorama et la version Panorama. Si le serveur de gestion Panorama dispose d'un collecteur de journaux local, Panorama peut également fournir des statistiques de journalisation : journaux moyens par seconde, durée de stockage, périodes de conservation, utilisation du disque de journalisation, statut de transfert de journaux depuis des pare-feu individuels vers Panorama et les serveurs externes et état des connexions entre le pare-feu et le collecteur de journaux. Panorama ne synchronise pas les configurations de SNMP entre homologues HD ; vous devez activer les requêtes et réponses SNMP sur chaque homologue.

Vous pouvez également configurer un collecteur de journaux dédié pour répondre aux requêtes des mêmes statistiques de journalisation que le serveur de gestion Panorama. Cette information est utile lors de l'évaluation quand vous avez besoin d'étendre la capacité de stockage de journal.

Vous ne pouvez configurer le gestionnaire SNMP pour contrôler Panorama ou collecteur de journaux (à l'aide de SET messages) ; un gestionnaire SNMP ne peut recueillir que des statistiques (à l'aide de GET messages).

Pour plus d'informations sur la façon dont panorama implémente SNMP, consultez le support SNMP.

STEP 1 | Configurer le gestionnaire SNMP pour obtenir des statistiques de Panorama et des collecteurs de journaux.

Les étapes suivantes sont une vue d'ensemble des tâches effectuées sur le gestionnaire SNMP. Pour les étapes spécifiques, reportez-vous à la documentation de votre gestionnaire SNMP.

1. Pour permettre au gestionnaire SNMP d'interpréter les statistiques, chargez les MIBs prises en charge et, si nécessaire, compilez-les.
2. Pour chaque appareil Panorama que le gestionnaire SNMP surveillera, définissez ses paramètres de connexion (adresse IP et port) et les paramètres d'authentification (chaîne de communauté SNMPv2c ou nom d'utilisateur SNMPv3 et mot de passe). Tous les appareils Panorama utilisent le port 161.

   Le gestionnaire SNMP peut utiliser les mêmes ou différents paramètres de connexion et d'authentification pour plusieurs serveurs de gestion Panorama et collecteurs de journaux. Les paramètres doivent correspondre à ceux que vous définissez lorsque vous configurez SNMP sur Panorama (voir étape Configurez le serveur de gestion Panorama pour répondre aux requêtes de statistiques d'un gestionnaire SNMP et étape Configurez les collecteurs de journaux dédiés (le cas échéant) afin de répondre aux requêtes SNMP). Par exemple, si vous utilisez SNMPv2c, la chaîne de communauté que vous définissez lors de la configuration du périphérique doit correspondre à la chaîne de communauté que vous définissez sur le gestionnaire SNMP de ce périphérique.
3. Déterminer les identificateurs d'objet (OIDs) des statistiques que vous suivrez. Par exemple, pour surveiller la fréquence d'enregistrement, un navigateur MIB montre que cette statistique correspond à OID 1.3.6.1.4.1.25461.2.3.30.1.1 dans PAN-PRODUCT-MIB.my. Pour plus d'informations, consultez Utilisation d'un gestionnaire SNMP pour explorer les MIBs et les objets.
4. Configurez le gestionnaire SNMP de manière à surveiller les OIDs souhaitées.

STEP 2 | Activer le trafic SNMP sur l'interface de gestion (MGMT) du serveur de gestion Panorama.

© 2020 Palo Alto Networks, Inc.

1. Sélectionnez **Panorama (Panorama)** > **Setup (Configuration)** > **Management (Gestion)**, puis modifiez les paramètres d'interface de gestion.
2. Dans la section Services, cochez la case **SNMP** et cliquez sur **OK**.

STEP 3 | Autoriser le trafic SNMP sur l'interface de gestion (MGT) de n'importe quel appareil de série M en mode collecteur de journaux :

1. Sélectionnez **Panorama (Panorama)** > **Managed Collectors (Collecteurs gérés)** et sélectionnez le collecteur de journaux.
2. Sélectionnez l'onglet **Management (Gestion)**, cochez la case **SNMP** et cliquez sur **OK**.

STEP 4 | Configurer le serveur de gestion Panorama pour répondre aux demandes de statistiques à partir d'un gestionnaire SNMP.

1. Sélectionnez **Panorama (Panorama)** > **Setup (Configuration)** > **Operations (Opérations)** et, dans la section Divers, cliquez sur **SNMP Setup (Configuration SNMP)**.
2. Sélectionnez la **Version** de SNMP et configurez les valeurs d'authentification de la manière suivante. Pour les détails de version, consultez SNMP Support (support SNMP).

   - **V2c**-Entrer la **SNMP Community String (Chaîne de communauté SNMP)**, qui identifie une communauté de gestionnaires SNMP et de périphériques surveillés (Panorama, dans ce cas), et sert de mot de passe pour authentifier les membres de la communauté de l'un à l'autre.

     N'utilisez pas la chaîne de communauté ***`public`*** *définie par défaut ; elle est connue et, par conséquent, n'est pas sécurisée.*

   - **V3**— créer au moins un groupe d'affichage SNMP et un utilisateur. Les vues et les comptes d'utilisateurs fournissent l'authentification, la confidentialité et le contrôle d'accès lorsque les gestionnaires SNMP obtiennent des statistiques de l'appareil.

     Vues)-Chaque vue est un OID appairé et un masque de bits : l'OID, une MIB et le masque (au format hexadécimal) spécifient que les objets sont accessibles à l'intérieur (notamment les correspondances) ou à l'extérieur (correspondants à exclure) de cette MIB. Cliquez sur **Add (Ajouter)** dans la première liste et entrez un **Name (nom)** pour le groupe de vues. Pour chaque vue dans le groupe, cliquez sur **Add (Ajouter)** et configurer la vue **Name (nom)**, **OID (OID)**, correspondant à **Option (Option)** (**include (inclure)** ou **exclude (exclure)**) et **Mask (masque)**.

     Utilisateurs, cliquez sur Ajouter dans la seconde liste, entrez un nom d'utilisateur dans la colonne utilisateurs, sélectionnez le groupe **d'affichage** dans le menu déroulant, entrez le mot de passe d'authentification (**Auth Password**) utilisé pour s'authentifier auprès du gestionnaire SNMP et entrez le mot de passe privé (**mot de passe Priv**) utilisé pour chiffrer les messages SNMP au gestionnaire SNMP.
3. Cliquez sur **OK** pour enregistrer les paramètres.

STEP 5 | Configurer les collecteurs de journaux dédiés (le cas échéant) afin de répondre aux requêtes SNMP.

Pour chaque groupe de Collecteur :

1. Sélectionner **Panorama (Panorama)** > **Collector Groups (Groupes de Collecteurs)** et sélectionnez le groupe de collecteurs.
2. Sélectionnez l'onglet **Monitoring (Surveillance)**, configurez les mêmes paramètres que dans l'étape Configurer le serveur de gestion Panorama pour répondre aux demandes de statistiques d'un gestionnaire SNMP, et cliquez sur **OK**.

STEP 6 | Validez les modifications apportées dans Panorama et appliquez-les aux groupes de collecteurs.

1. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** et **Edit Selections (Modifier les sélections)** dans la portée d'application.

© 2020 Palo Alto Networks, Inc.

2. Sélectionnez **Collector Groups (Groupes de collecteurs)**, sélectionnez les groupes de collecteurs que vous avez modifiés, puis cliquez sur **OK**.
3. **Commit and Push (Validez et appliquez)** vos modifications.

STEP 7 | Surveiller les statistiques Panorama et Collecteur de journaux dans un gestionnaire SNMP.

Reportez-vous à la documentation de votre gestionnaire SNMP.

© 2020 Palo Alto Networks, Inc.

Redémarrer ou arrêter Panorama

L'option de redémarrage initie un redémarrage en douceur de Panorama. Un arrêt stoppe le système et le met hors tension. Pour redémarrer Panorama après un arrêt, déconnectez manuellement le cordon d'alimentation puis rebranchez-le sur le système.

STEP 1 | Sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)**.

STEP 2 | Dans la section Opérations du périphérique, sélectionnez **Reboot Panorama (Redémarrer Panorama)** ou **Shutdown Panorama (Arrêter Panorama)**.

© 2020 Palo Alto Networks, Inc.

Configurer les profils et la complexité de mot de passe Panorama

Pour sécuriser le compte administrateur local, vous pouvez définir des exigences en matière de complexité de mot de passe, à appliquer au moment où les administrateurs modifient ou créent de nouveaux mots de passe. Contrairement aux profils de mot de passe, qui peuvent être appliqués aux comptes individuels, les règles de complexité de mot de passe sont au niveau du pare-feu et s'appliquent à tous les mots de passe.

Pour mettre en place les mises à jour périodiques de mot de passe, créez un profil de mot de passe qui définit le délai de validité de ces derniers.

STEP 1 | Configurez les paramètres minimum de complexité de mot de passe.

1. Sélectionnez **Panorama** > **Setup (Paramétrage)** > **Management (Gestion)** et modifiez la section de complexité minimale de mot de passe.
2. Sélectionnez **Enabled (Activé)**.
3. Définissez les **Password Format Requirements (Critères de format pour le mot de passe)**. Vous pouvez mettre en place des critères de majuscules, minuscules, numériques et les caractères spéciaux qu'un mot de passe doit contenir.
4. Pour éviter que le nom d'utilisateur de compte (ou la version inversée du nom) soit utilisée dans le mot de passe, sélectionnez **Block Username Inclusion (including reversed) (Bloquer l'intégration du nom d'utilisateur (inversé inclus))**.
5. Définissez les **Functionality Requirements (Exigences relatives aux fonctionnalités)**.

   Si vous avez configuré un profil de mot de passe pour un administrateur, les valeurs définies dans le profil de mot de passe remplaceront celles que vous aviez définies dans la section.

STEP 2 | Créez des profils de mot de passe.

Vous pouvez créer plusieurs profils de mot de passe et les appliquer aux comptes administrateurs selon les besoins pour mettre en œuvre la sécurité.

1. Sélectionnez **Panorama** > **Password Profiles (Profils de Mot de Passe)** et cliquez sur **Add (Ajouter)**.
2. Saisissez le **Name (Nom)** du profil de mot de passe, et définissez ce qui suit :
   1. **Required Password Change Period (Période de modification du mot de passe)** : fréquence, en jours, à laquelle les mots de passe doivent être modifiés.
   2. **Expiration Warning Period (Avertissement avant la date d'expiration)** : nombre de jours avant l'expiration où l'administrateur recevra un rappel de mot de passe.
   3. **Post Expiration Grace Period (Période de grâce après expiration)** : nombre de jours pendant lesquels l'administrateur peut toujours se connecter au système après expiration du mot de passe.
   4. **Post Expiration Admin Login Count (Nombre d'ouvertures de session administrateur après expiration)** : nombre de fois où l'administrateur peut se connecter au système après expiration du mot de passe.

Les plug-ins Panorama

L'architecture de plug-in extensible Panorama permet la prise en charge de plug-ins d'intégration tiers, tels que VMware NSX, et d'autres produits Palo Alto Networks, comme le service de cloud GlobalProtect. Avec cette architecture modulaire, vous pouvez profiter des nouvelles fonctionnalités sans attendre une nouvelle version de PAN-OS.

Vous pouvez également configurer le plug-in VM-Series de Panorama. Le plug-in VM-Series est un plug-in unique qui permet l'intégration avec des environnements de cloud publics, comme Google Cloud Platform (GCP), Azure, AWS et les hyperviseurs de cloud privés, comme KVM, ESXi, etc. Le plug-in VM-Series vous permet de publier des mesures à partir des pare-feu VM-Series déployés dans des clouds publics. Vous pouvez utiliser Panorama pour configurer les paramètres du plug-in VM-Series pour les clouds publics et transmettre votre configuration à vos pare-feu gérés.

> A propos de Panorama Plugins (Plug-ins).
> Plug-in VM-Series et plug-ins Panorama

© 2020 Palo Alto Networks, Inc.

A propos de Panorama Plugins (Plug-ins).

Panorama prend en charge une architecture de plug-in élargie qui permet l'intégration et la configuration des capacités suivantes :

- **AWS** : Le plugiciel AWS vous permet de surveiller vos charges de travail sur AWS. Avec ce plugin, vous pouvez activer la communication entre Panorama (exécutant la version PAN-OS 8.1.3 et toute version ultérieure) et vos VPC AWS pour que Panorama puisse collecter un ensemble d'attributs (ou d'éléments de métadonnées) prédéfinis en tant qu'étiquettes pour vos instances EC2 et enregistrer les informations sur votre pare-feu Palo Alto Networks. Lorsque vous faites référence à ces étiquettes dans les groupes d'adresses dynamiques et que vous les faites correspondre à des règles de politique de sécurité, vous pouvez continuellement appliquer la politique sur l'ensemble des ressources déployées au sein de vos VPC.
- **Azure** : Le plugin vous permet de surveiller vos machines virtuelles sur le cloud Azure public. Avec ce plugin, vous pouvez activer la communication entre Panorama (exécutant la version PAN-OS 8.1.6 et toute version ultérieure) et vos abonnements Azure pour que Panorama puisse collecter un ensemble d'attributs (ou d'éléments de métadonnées) prédéfinis en tant qu'étiquettes pour vos machines virtuelles Azure et enregistrer les informations sur votre pare-feu Palo Alto Networks. Lorsque vous faites référence à ces étiquettes dans les groupes d'adresses dynamiques et que vous les faites correspondre à des règles de politique de sécurité, vous pouvez continuellement appliquer la politique sur l'ensemble des ressources déployées au sein de vos Vnets de vos abonnements.
- **Cisco ACI :** Le plug-in ACI de Cisco vous permet de surveiller vos points de terminaison dans votre trame Cisco ACI. Avec ce plugin, vous activez la communication entre Panorama (exécutant la version 8.1.6 et toute version ultérieure) et vos votre Cisco APIC pour que Panorama puisse collecter des informations du terminal en tant qu'étiquettes pour vos groupes de terminaux et enregistrer les informations sur votre pare-feu Palo Alto Networks. Lorsque vous faites référence à ces étiquettes dans les groupes d'adresses dynamiques et que vous les faites correspondre à des règles de politique de sécurité, vous pouvez continuellement appliquer la politique sur l'ensemble des ressources déployées au sein de vos VPC.
- **Cisco TrustSec** : Le plug-in Cisco TrustSec permet de surveiller les terminaux dans votre environnement Cisco TrustSec. Avec ce plugin, vous activez la communication entre Panorama et votre serveur Cisco pxGrid pour que Panorama puisse collecter des informations du terminal en tant qu'étiquettes pour vos terminaux et enregistrer les informations sur vos pare-feu Palo Alto Networks®. Lorsque vous faites référence à ces étiquettes dans les groupes d'adresses dynamiques et que vous les faites correspondre à des règles de politique de sécurité, vous pouvez continuellement appliquer la politique sur l'ensemble des ressources déployées au sein de votre environnement Cisco TrustSec.
- **Cloud Services** : Le plug-in Cloud Services permet d'utiliser Cortex Data Lake et Prisma Access. Cortex Data Lake résout les problèmes de journalisation opérationnelle et le service de cloud Prisma Access déploie votre infrastructure de sécurité à vos sites réseau distants et à votre personnel nomade.
- **Enterprise Data Loss Prevention (prévention des pertes de données - DLP)** : Enterprise Data Loss Prevention (prévention des pertes de données - DLP) est un ensemble d'outils et de processus qui vous permettent de protéger les informations sensibles de tout accès, mauvaise utilisation, extraction ou partage non autorisé. Enterprise DLP est activé par un service cloud pour vous aider à inspecter le contenu et à analyser les données dans le contexte approprié afin d'identifier avec précision les données sensibles et de les sécuriser pour éviter les incidents. Enterprise DLP est compatible avec Panorama et les pare-feux gérés exploitant PAN-OS 10.0.2 et versions ultérieures.
- **GCP** : vous permet de sécuriser les services Kubernetes dans un cluster Google Kubernetes Engine. Configurez le plug-in Panorama pour que Google Cloud Platform (GCP) se connecte à votre cluster GKE et prenne connaissance des services qui sont exposés à Internet.
- **Interconnect** : le plug-in Interconnect vous permet de Gérer les déploiements de pare-feu à grande échelle. Utilisez le plugin Interconnect pour configurer un déploiement Panorama à deux niveaux (sur la version PAN-OS 8.1.3 de Panorama ou toute version ultérieure) pour une architecture horizontale évolutive. Avec le plugin Interconnect, vous pouvez déployer un contrôleur Panorama avec un maximum

© 2020 Palo Alto Networks, Inc.

de 64 nœuds Panorama ou de 32 paires HA Panorama pour gérer centralement un grand nombre de pare-feux.

- **Nutanix** : Le plug-in Panorama pour Nutanix permet de surveiller les VM dans votre environnement Nutanix. Il vous permet de suivre l'inventaire des machines virtuelles dans votre Nutanix Prism Central afin que vous puissiez appliquer de manière cohérente une politique de sécurité qui s'adapte automatiquement aux changements dans votre environnement Nutanix. Lorsque les machines virtuelles sont approvisionnées, désapprovisionnées ou déplacées, cette solution vous permet de collecter les adresses IP et les ensembles d'attributs (ou éléments de métadonnées) associés sous forme d'étiquettes. Vous pouvez ensuite utiliser les étiquette pour définir des Dynamic Address Group (groupe d'adresses dynamiques) et les utiliser dans la politique de sécurité. Le plug-in Panorama pour Nutanix nécessite Panorama 9.0.4 ou une version ultérieure.
- **SD-WAN** : Le plug-in Software-Defined Wide Area Network (SD-WAN) vous permet d'utiliser des services internet divers et privés pour créer un WAN intelligent et dynamique qui aide à réduire les coûts et à maximiser la qualité et l'utilisation des applications. Au lieu d'utiliser des MPLS onéreux et chronophages avec des composants comme des routeurs, des pare-feux, des contrôleurs de chemin WAN et des optimisateurs de WAN pour connecter votre WAN à internet, le SD-WAN sur un pare-feu Palo Alto Networks vous permet d'utiliser des services internet moins chers et moins de pièces d'équipement.
- **VMware NSX** : Le plug-in VMware NSX permet l'intégration entre le pare-feu VM-Series sur VMware NSX et VMware NSX Manager. Cette intégration vous permet de déployer le pare-feu VM-Series en tant que service sur un cluster de serveurs ESXi.
- **VMware vCenter** : Le plug-in Panorama pour VMware vCenter vous permet de surveiller les machines virtuelles dans votre environnement vCenter. Le plug-in récupère les adresses IP des machines virtuelles dans votre environnement vCenter et les convertit en étiquettes que vous pouvez utiliser pour élaborer des politiques à l'aide de groupes d'adresses dynamiques.
- **Zero Touch Provisioning** : Le Zero Touch Provisioning (ZTP) est conçu pour simplifier et automatiser l'intégration de nouveaux pare-feux à Panorama. ZTP rationalise le processus de déploiement initial du pare-feu en permettant aux administrateurs réseau d'envoyer les pare-feu gérés directement à leurs succursales et d'ajouter automatiquement le pare-feu au serveur de gestion Panorama, permettant aux entreprises d'économiser du temps et des ressources lors du déploiement de nouveaux pare-feux. Le ZTP est pris en charge par la version PAN-OS 9.1.3 et toute version ultérieure.
- **IPS Signature Converter (Convertisseur de signature IPS)**—le IPS Signature Converter plugin (plug in de convertisseur de signature IPS) pour Panorama offre une solution automatique de conversion des règles des systèmes de prévention d'intrusion tiers (Snort et Suricata) en des signatures de menace au format personnalisé de Palo Alto Networks. Vous pouvez ensuite enregistrer ces signatures sur les pare-feux qui appartiennent à des groupes de périphériques que vous indiquez et les utiliser pour appliquer la politique dans les profils de Protection des vulnérabilités et de Sécurité antispyware.

Vous pouvez installer plusieurs plug-ins et récupérer des mises à jour d'adresse IP de plusieurs sources sur une seule instance de Panorama. Cela vous permet de créer et d'appliquer une politique de sécurité cohérente pour sécuriser les applications et les services sur plusieurs environnements cloud. Les adresses IP récupérées sont utilisées dans la politique de sécurité via les Dynamic Address Group (groupe d'adresses dynamiques) ; lorsqu'un service est ajouté ou supprimé de votre environnement, Panorama enregistre la modification et valide la mise à jour vers les pare-feux. Lors du déploiement de plusieurs plug-ins sur Panorama, vous devez planifier avec soin votre device group hierarchy (hiérarchie de groupe de périphériques) afin de vous assurer que les mises à jour soient correctement transmises à vos pare-feux.

Reportez-vous à la Matrice de compatibilité de Palo Alto Networks pour obtenir des détails sur les différentes versions plugins et des informations sur la comptabilité.

Installer les plug-ins Panorama

Vous pouvez installer un ou plusieurs plugins disponibles sur Panorama pour activer l'intégration du service de cloud GlobalProtect et Cortex Data Lake, de VMware NSXou pour surveiller vos machines virtuelles sur AWS ou sur le cloud public Azure.

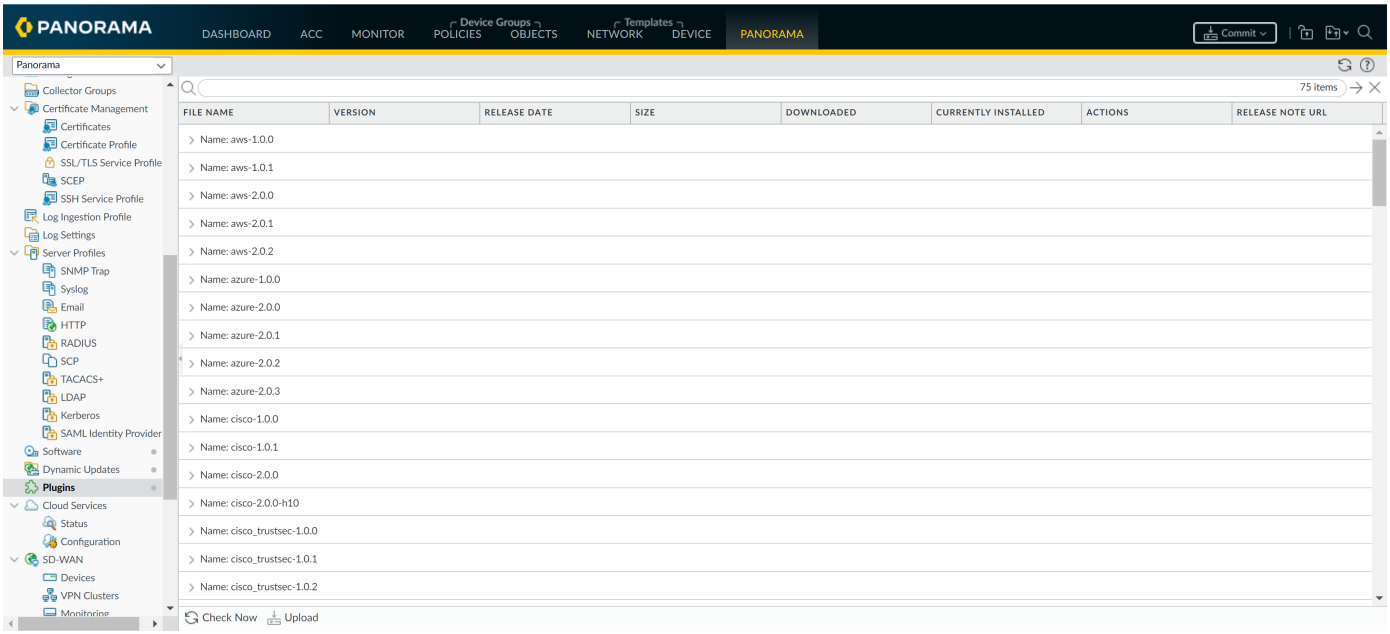
© 2020 Palo Alto Networks, Inc.

Pour le plug-in de services cloud, vous devez activer un code d'autorisation valide sur le portail de support client et sélectionner la région (Amérique ou Europe) vers laquelle envoyer les journaux.

Si vous avez une version d'un plugin actuellement installée et que vous installezune nouvelle version du plugin, Panorama remplace la version actuellement installée.

STEP 1 | Télécharger le plugin (module d'extension)

1. Sélectionnez **Panorama** > **Plugins**.



2. Sélectionnez **Check Now (Vérifiez maintenant)**pour récupérer la liste des mises à jour disponibles.
3. Sélectionnez **Download (Télécharger)** dans la colonne Action pour installer le plug-in (module d'extension).

   Reportez-vous à la Compatibility Matrix (Matrice de compatibilité) pour connaître la version PAN-OS minimale compatible pour chaque plug-in Panorama.

STEP 2 | Installez le plug-in.

Sélectionnez la version du plug-in et cliquez sur **Install (Installer)** dans la colonne Action pour installer le plug-in. Panorama vous alertera lorsque l'installation est terminée. Pour plus de détails, référez-vous à l'installation du plug-in VMware NSX. Ou le plug-in Could Services.

Lorsque vous installez le plug-in pour la première fois sur une paire Panorama HA, installez le plug-in sur l'homologue passif avant l'homologue actif. Lors de l'installation du plug-in sur l'homologue passif, il passe à un état non fonctionnel. Ensuite, après l'installation réussie du plug-in sur l'homologue actif, celui-ci retourne à un état fonctionnel.

© 2020 Palo Alto Networks, Inc.

Plug-in VM-Series et plug-ins Panorama

Quelle est la différence entre le plug-in VM-Series et les différents plug-ins pour Panorama ?

Le plug-in VM-Series est destiné aux pare-feu VM-Series. C'est un plug-in unique qui permet l'intégration avec des environnements de cloud publics, comme Google Cloud Platform (GCP), Azure et AWS, ainsi que les hyperviseurs de cloud privés, comme KVM, ESXi, etc. Lorsque vous déployez le pare-feu, le plug-in intégré détecte automatiquement l'environnement virtuel sur lequel le pare-feu est déployé et charge les composants du plug-in qui vous permettent de gérer les interactions avec cet environnement cloud. Par exemple, lorsque vous déployez le pare-feu VM-Series sur GCP, le pare-feu VM-Series charge les composants du plug-in qui permettent l'intégration avec GCP. Vous pouvez ensuite utiliser le plug-in VM-Series pour configurer le pare-feu VM-Series sur GCP afin de publier des métriques dans Google Stackdriver Monitoring. De même, le plug-in VM-Series sur le pare-feu VM-Series sur Azure vous permet de configurer le pare-feu pour publier des métriques Azure Application Insights ou de configurer les détails dont les pare-feu ont besoin pour fonctionner en tant que paire HA. Le plug-in VM-Series est préinstallé sur le pare-feu VM-Series. Vous pouvez le mettre à niveau ou le rétrograder, mais pas le supprimer. Sur Panorama, le plug-in VM-Series est disponible, mais il n'est pas préinstallé. Si vous choisissez d'utiliser Panorama pour gérer les intégrations sur vos pare-feu, installez le plug-in VM-Series sur Panorama pour établir la communication avec le plug-in VM-Series sur vos pare-feu.

Les plug-ins Panorama sont destinés aux pare-feu matériels et aux pare-feu VM-Series. Étant donné que les plug-ins Panorama sont facultatifs, vous pouvez les ajouter, les supprimer, les réinstaller ou les mettre à niveau sur Panorama. Le plug-in Panorama n'est pas intégré. Vous devez l'installer pour permettre la communication avec l'environnement de gestion dont vous avez besoin. Par exemple, vous utilisez le plug-in Services cloud sur Panorama pour permettre la configuration entre Panorama/les pare-feu et Cortex Data Lake. Le plug-in GCP sur Panorama permet la communication entre Panorama et votre déploiement GCP afin que vous puissiez sécuriser le trafic entrant ou sortant d'un service déployé dans un cluster Google Kubernetes Engine (GKE).

Installation du plug-in VM-Series sur Panorama

Pour afficher et configurer les intégrations Cloud qui sont déployées sur vos pare-feu VM-Series, le plug-in VM-Series doit être installé sur Panorama et sur le pare-feu VM-Series. Le plug-in est automatiquement installé sur le pare-feu, mais vous devez manuellement installer le plug-in sur Panorama avant de pouvoir transférer les configurations à vos groupes de périphériques.

Le plug-in VM-Series prend en charge tous les clouds, une mise à jour pourrait ne pas s'appliquer à vos pare-feu VM-Series. Avant de mettre le plug-in à jour, consultez les notes de version. Ne mettez à jour le plug-in que lorsque des changements sont pertinents pour votre cloud.

STEP 1 | Téléchargez le plug-in VM-Series.

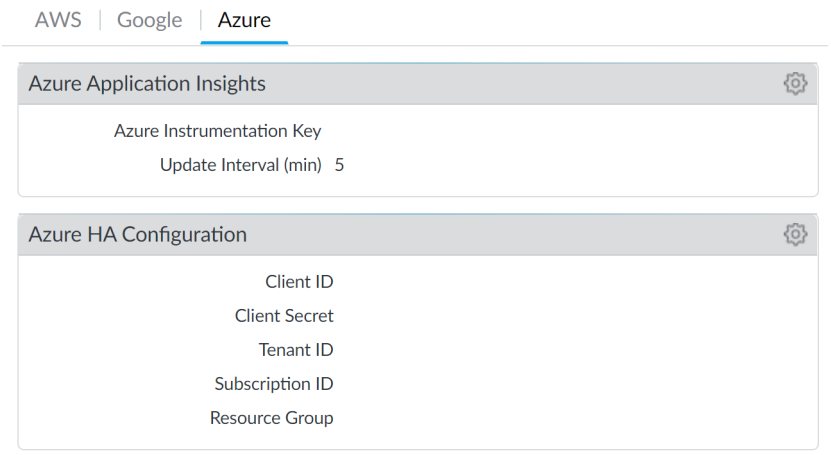
1. Sélectionnez **Panorama** > **Plugins (Plug-ins)** et utilisez **Check Now (Vérifier maintenant)** pour chercher de nouveaux paquets de plug-ins. Le nom du plug-in VM-Series est `vm_series`.
2. Consultez les notes de version du plug-in pour déterminer la version qui vous procure des mises à niveaux qui vous sont utiles.
3. Sélectionnez une version du plug-in et cliquez sur **Download (Télécharge)** dans la colonne Action.

STEP 2 | Installez le plug-in VM-Series.

1. Dans la colonne Action, cliquez sur **Install (Installer)**. Panorama vous alerte lorsque l'installation est terminée.
2. Pour afficher le plug-in, sélectionnez **Device (Périphérique)** > **VM-Series**.

© 2020 Palo Alto Networks, Inc.

- Si votre pare-feu est installé sur un cloud privé et que l'hyperviseur ou le service ne dispose pas d'une intégration, vous voyez un onglet nommé VM-Series et le message par défaut suivant : `VM Series plugin infrastructure support is installed to allow the firewall's functionality to be enhanced in response to new features launched by hypervisor, or to meet new security needs.`
- Si votre pare-feu est déployé dans un cloud public, Panorama affiche les onglets pour les clouds pris en charge.



STEP 3 | (Facultatif) Enregistrez votre configuration et transmettez-la à vos pare-feu gérés.

STEP 4 | (Facultatif) Sur la pare-feu VM-Series, sélectionnez **Device (Périphérique)** > **VM-Series**. Si vous avez configuré l'intégration de votre plateforme, vous voyez un seul onglet correspondant au cloud dans lequel le pare-feu est déployé. Si vous n'avez pas configuré d'intégration, vous voyez le message par défaut qui s'affiche au-dessus de l'infrastructure du plug-in VM-Series.

© 2020 Palo Alto Networks, Inc.

Dépannage

Les rubriques suivantes traitent des problèmes relatifs au serveur de gestion Panorama™ et aux collecteurs de journaux dédiés :

- Dépannage des problèmes système Panorama
- Dépannage des problèmes de stockage et de connexion
- Remplacement d'un pare-feu RMA
- Dépanner des échecs de validation
- Résoudre les problèmes d'enregistrement ou erreurs de numéro de série
- Dépannage des erreurs de déclaration
- Résoudre les erreurs de licence de gestion des périphériques
- Dépannage des configurations de pare-feu automatiquement inversées
- Effectuer la mises à jour du contenu lorsque la paire HA de Panorama est en panne
- Affichage de l'état de réussite ou d'échec d'une tâche
- Tester la correspondance aux politiques et la connectivité des périphériques gérés
- Downgrader vers Panorama 10.0

© 2020 Palo Alto Networks, Inc.

Dépannage des problèmes système Panorama

- Générer des fichiers de diagnostic pour Panorama
- Diagnostic de l'état de suspension de Panorama
- Surveiller la vérification d'intégrité des fichiers système
- Gestion du stockage de Panorama pour les mises à jour logicielles et de contenu
- Récupération suite à un Split Brain dans les déploiements HD de Panorama

Générer des fichiers de diagnostic pour Panorama

Les fichiers de diagnostic aident à la surveillance de l'activité système et à détecter les causes potentielles des problèmes Panorama. Pour aider le Support technique de Palo Alto Networks à résoudre un problème, le représentant du support technique pourrait demander un dossier de prise en charge technique. La procédure suivante décrit comment télécharger un fichier de support technique et à le transférer sur votre dossier de prise en charge.

STEP 1 | Sélectionnez **Panorama** > **Support** et cliquez sur **Generate Tech Support File (Générer un fichier de Support Technique)**.

STEP 2 | Téléchargez et enregistrez le fichier sur votre ordinateur.

STEP 3 | Téléchargez le fichier dans votre dossier sur le site Web de soutien à la clientèle de Palo Alto Networks.

Diagnostic de l'état de suspension de Panorama

Si Panorama se trouve dans un état suspendu, vérifiez les conditions suivantes :

- **Numéros de série** : vérifiez que le numéro de série de chaque appareil virtuel Panorama est unique. Si le même numéro de série est utilisé pour créer deux, voire plusieurs instances de Panorama, toutes les instances utilisant le même numéro de série sont suspendues.
- **Mode** : si vous déployez l'appareil virtuel Panorama dans une configuration haute disponibilité (HD), vérifiez que les deux homologues HD sont dans le même mode : mode Panorama ou mode hérité.
- **Priorité HD** : vérifiez que vous avez défini le paramètre de priorité HD sur un homologue comme *Primaire* et l'autre comme *Secondaire*. Si le paramètre de priorité est identique sur les deux homologues, l'homologue Panorama ayant la valeur numérique de numéro de série la plus élevée passe en mode suspendu.
- **Version du logiciel Panorama** : vérifiez que les deux homologues HD Panorama exécutent la même version de Panorama (numéro de version majeure et mineure).

Surveiller la vérification d'intégrité des fichiers système

Panorama contrôle régulièrement l'intégrité du système de fichiers (FSCK) afin d'éviter une corruption des fichiers système de Panorama. Cette vérification se produit après huit remises à zéro ou après un redémarrage qui se produit 90 jours après que la dernière FSCK ait été exécutée. Si Panorama est en cours d'exécution d'une FSCK, l'interface web et les écrans de connexion SSH (Secure Shell) affichent un avertissement indiquant qu'une FSCK est en cours. Vous ne pouvez pas vous connecter avant la fin de ce processus. Le temps nécessaire à l'accomplissement de cette procédure varie en fonction de la taille, du système de stockage. Selon la taille, l'opération peut prendre plusieurs heures avant que vous puissiez vous reconnecter à Panorama.

© 2020 Palo Alto Networks, Inc.

Après avoir téléchargé et installé avec succès une mise à jour du logiciel PAN-OS sur Panorama ou un pare-feu géré, la mise à jour de logiciel est validée après le redémarrage de Panorama ou du pare-feu géré dans le cadre de la procédure d'installation du logiciel afin de garantir l'intégrité du logiciel PAN-OS. Cela garantit que la mise à jour du logiciel en fonctionnement est connue pour être bonne et que le Panorama ou le pare-feu géré n'est pas compromis à cause d'une exploitation distante ou physique.

Pour afficher la progression du FSCK, configurez l'accès à la console Panorama et regarder l'état.

Gestion du stockage de Panorama pour les mises à jour logicielles et de contenu

Vous pouvez installer des mises à jour du contenu et des logiciels pour Panorama et déployer des mises à jour sur les pare-feu, les collecteurs de journaux et les appareils WildFire à l'aide de Panorama. Vous ne pouvez pas configurer la quantité d'espace disponible sur le Panorama pour stocker les mises à jour. Lorsque la capacité de stockage allouée atteint 90 %, Panorama vous prévient de libérer l'espace (supprimer les mises à jour stockées) les pour nouveaux téléchargements ou les mises à jour. Le nombre maximum de mises à jour est un paramètre global qui s'applique à toutes les mises à jour que stocke Panorama. Vous devez accéder à la CLI pour configurer ce paramètre. La valeur par défaut est deux mises à jour de chaque type.

- Modifier le nombre maximum de mises à jour de chaque type.

  Accéder à l'ILC de Panorama et entrez les informations suivantes, où <*nombre*>peut être compris entre 2 et 64 :

  ```
  > set max-num-images count <number>
  ```

- Afficher le nombre de mises à jour que Panorama stocke actuellement.

  Entrez :

  ```
  > show max-num-images
  ```

- L'interface web permet de supprimer des mises à jour pour libérer de l'espace sur Panorama.
  1. Sélectionnez le type de mise à jour à supprimer :
     - Mises à jour de Pare-feu ou de Collecteur de Journaux :

       Images du logiciel PAN-OS / Panorama : sélectionnez **Panorama** > **Device Deployment (Déploiement d'appareils)** > **Software (Logiciel)**.

       Mise à jour du logiciel de l'agent / application Global Protect™ : sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **GlobalProtect Client (Client GlobalProtect)**.

       Mises à jour de contenu : sélectionnez **Panorama** > **Device Deployment (Déploiement du périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**.
     - Panorama Software images — sélectionnez **Panorama** > **Software (Logiciel)**.
     - Mises à jour de contenu de Panorama : sélectionnez **Panorama** > **Dynamic Updates (mises à jour dynamiques)**.
  2. Cliquez sur l'icône **X** dans la colonne à droite de l'image ou la mise à jour.

- L'ILC permet de supprimer des mises à jour pour libérer de l'espace sur Panorama.

  Supprimer les images logicielles par version :

© 2020 Palo Alto Networks, Inc.

```
> delete software version <version_number>
```

Supprimer les mises à jour :

```
> delete content update <filename>
```

Récupération suite à un Split Brain dans les déploiements HD de Panorama

Lorsque Panorama est configuré en haute disponibilité (HD), les pare-feux gérés sont connectés aux homologues HD Panorama actif et passif. Lorsque la connexion entre les homologues Panorama actif et passif échoue, avant que l'homologue Panorama passif prenne le rôle de l'homologue actif, il vérifie si un pare-feu est connecté aux homologues actif et passif. Si même un pare-feu est connecté aux deux homologues, le basculement n'est pas déclenché.

Dans les rares cas où un basculement est déclenché quand un jeu de pare-feux est connecté à l'homologue actif et un jeu de pare-feux connecté à l'homologue passif, mais qu'aucun des pare-feu ne soit connecté aux deux homologues, c'est appelé un demi-cerveau. Lorsque surgit un demi-cerveau, les conditions suivantes se produisent :

- Aucun des homologues de Panorama n'est au courant de l'état ni du rôle HD de l'autre homologue.
- Les deux homologues Panorama deviennent actifs et gèrent un ensemble unique de pare-feux.

Pour résoudre un demi-cerveau, déboguer vos problèmes de réseau et restaurer la connectivité entre les homologues Panorama HD.

Cependant, si vous devez modifier la configuration de votre pare-feu sans restaurer la connexion entre les homologues, voici quelques options :

- Ajoutez manuellement les mêmes modifications de configuration aux deux homologues Panorama. Cela permet de garantir la synchronisation de la configuration lorsque le lien est rétabli.
- Si vous devez ajouter/modifier la configuration à un seul emplacement de Panorama, effectuez les modifications et synchronisez la configuration (assurez-vous d'initier la synchronisation à partir de l'homologue sur lequel vous avez effectué les modifications), lorsque le lien entre les homologues Panorama est rétabli. Pour synchroniser les homologues, sélectionnez l'onglet **Dashboard (Tableau de bord)** et cliquez sur le lien **Sync to peer (Synchroniser les homologues)** dans le widget Haute Disponibilité.
- Si vous devez ajouter/modifier la configuration uniquement pour les pare-feux connectés à cet emplacement, vous pouvez effectuer les modifications de configuration, indépendamment, sur chaque homologue Panorama. Comme les homologues sont déconnectés, aucune réplication ne se produit et chaque homologue dispose désormais d'un fichier de configuration totalement différent (ils sont désynchronisés). Par conséquent, afin de s'assurer que les modifications de configuration sur chaque homologue ne soient perdues lorsque la connexion est rétablie, vous ne pouvez pas autoriser la resynchronisation de la configuration. Pour résoudre ce problème, exportez la configuration de chaque homologue Panorama et fusionnez manuellement les modifications à l'aide d'un outil de comparaison et de fusion externe. Après que les modifications sont intégrées, vous pouvez importer le fichier de configuration unifié sur le Panorama primaire et ensuite synchroniser le fichier de configuration importé avec l'homologue.

© 2020 Palo Alto Networks, Inc.

Dépannage des problèmes de stockage et de connexion

La migration des journaux est possible uniquement pour un appareil M-Series. Reportez-vous à Migrer un appareil virtuel Panorama vers un autre hyperviseur *pour faire migrer un appareil virtuel Panorama.*

- Vérifier l'utilisation du Port de Panorama
- Résolution du stockage zéro de journaux pour un groupe de collecteurs
- Remplacer un disque défaillant sur un appareil de la série M
- Remplacez le disque virtuel sur un serveur ESXi
- Remplacez le disque virtuel sur vCloud air
- Migrer les journaux vers un nouvel appareil de la série M en Mode Collecteur de Journaux
- Migrer les journaux vers un nouvel appareil de la série M en Mode Panorama
- Migrer les journaux vers un nouvel appareil de la série M en Mode Panorama en haute disponibilité.
- Migrer les journaux vers le même modèle d'appareil de la série M en Mode Panorama en haute disponibilité
- Migrer les collecteurs de journaux après défaillance/RMA de Panorama non-HD
- Régénérer les métadonnées pour les appareils de la série M en paires RAID
- Afficher les tâches de requête de journaux

Vérifier l'utilisation du Port de Panorama

Pour vous assurer que Panorama peut communiquer avec les pare-feu gérés, les collecteurs de journaux et les appareils et clusters d'appareils WildFire, ainsi que leur homologue haute disponibilité (HD), utilisez le tableau suivant pour vérifier les ports que vous devez ouvrir sur votre réseau. Panorama utilise le protocole TCP pour les communications de port.

Par défaut, Panorama utilise l'interface de gestion (MGT) pour gérer les périphériques (pare-feu, collecteurs de journaux et appareils et clusters d'appareils WildFire), collecter des journaux, communiquer avec des groupes de collecteurs et déployer des mises à jour logicielles et matérielles. Toutefois, vous pouvez éventuellement affecter les fonctions de collecte de journaux et de communication du groupe de collecteurs aux interfaces Eth1 ou Eth2 sur un appareil M-600, M-500 ou M-200 exécutant Panorama 6.1 à 7.1. Si l'appareil exécute Panorama 8.0 ou une version ultérieure, vous pouvez affecter n'importe quelle fonction aux interfaces Eth1, Eth2, Eth3, Eth4 ou Eth5, sur l'appareil M-600, M-500 ou M-200. Les ports répertoriés dans le tableau ci-dessous s'appliquent quelle que soit la fonction que vous associez à une interface. Par exemple, si vous associez la collecte de journaux à l'interface MGT et la communication du groupe de collecteurs à l'interface Eth2, MGT utilisera le port 3978 et Eth2 le port 28270. (L'appareil virtuel Panorama ne peut utiliser que l'interface MGT pour toutes ces fonctions.)

© 2020 Palo Alto Networks, Inc.

Communication des périphériques et sens d'établissement de la connexion	Ports utilisés dans Panorama 5.x	Ports utilisés dans Panorama 6.x à 7.x	Ports utilisés dans Panorama 8.x et versions ultérieures	Description
Panorama et Panorama (HD) Sens : Chaque homologue initie sa propre connexion à l'autre	28	28	28	Pour la connectivité HD et la synchronisation si le cryptage est activé. Utilisé pour la communication entre les collecteurs de journaux d'un groupe de collecteurs pour la distribution des journaux.
Panorama et Panorama (HD) Sens : Chaque homologue initie sa propre connexion à l'autre	28769 et 28260 (5.1) 28769 et 49160 (5.0)	28260 et 28769	28260 et 28769	Pour la connectivité HD et la synchronisation si le cryptage n'est pas activé.
Panorama et pare-feu gérés Sens : initié par le pare-feu	3978	3978	3978	Une connexion bidirectionnelle, dans laquelle les journaux sont transférés du pare-feu vers Panorama ; et les modifications de configuration sont transmises de Panorama aux pare-feu gérés. Les commandes de commutation de contexte sont envoyées via la même connexion.
Panorama et collecteur de journaux Sens : Initié par le Collecteur de Journaux	3978	3978	3978	Pour la gestion et la collecte des journaux/création de rapports. Utilisé pour la communication entre le collecteur de journaux local sur un Panorama en mode Panorama et pour communiquer avec les collecteurs de journaux dans un déploiement de collecte de journaux distribuée.
Panorama et périphériques gérés (pare-feu, collecteurs de journaux et appareils et clusters d'appareils WildFire)	3978	3978	28443	Les périphériques exécutant PAN-OS 8.x ou des versions ultérieures utilisent le port 28443 pour récupérer

© 2020 Palo Alto Networks, Inc.

Communication des périphériques et sens d'établissement de la connexion	Ports utilisés dans Panorama 5.x	Ports utilisés dans Panorama 6.x à 7.x	Ports utilisés dans Panorama 8.x et versions ultérieures	Description
Sens : • Initié par les périphériques gérés exécutant PAN-OS 8.x ou versions ultérieures. • Initié par Panorama pour les périphériques exécutant PAN-OS 7.x ou versions antérieures.				les fichiers de mise à jour logicielle et de contenu de Panorama. Les périphériques exécutant des versions 7.x ou antérieures ne récupèrent pas les fichiers de mise à jour de Panorama ; Panorama envoie les fichiers de mise à jour aux périphériques via le port 3978. La prise en charge de la gestion de Panorama des appareils et des clusters d'appareils WildFire nécessite PAN-OS 8.0.1 ou une version ultérieure installée sur les appareils WildFire gérés. Nous recommandons que Panorama exécute la version 8.0.1 ou ultérieure pour gérer les appareils et les clusters d'appareils WildFire.
Collecteur de journaux à collecteur de journaux Sens : Chaque Collecteur de Journaux établit une connexion avec les autres collecteurs de journaux dans le groupe collecteur	49190	28270	28270	Pour la distribution de blocs et toutes les données binaires entre collecteurs de journaux.
Panorama vers Cortex Data Lake	ND	ND	444 *Version C8.0.5 et ultérieure.*	Pour configurer un canal de communication sécurisé avec Cortex Data Lake. Les pare-feu gérés utilisent le port 3978 pour communiquer avec Cortex Data Lake.

© 2020 Palo Alto Networks, Inc.

Résolution du stockage zéro de journaux pour un groupe de collecteurs

La capacité de stockage de journaux du groupe de collecteurs peut afficher 0 Mo si les paires de disques ne sont pas activées pour la journalisation. Pour activer les paires de disques, procédez comme suit pour chaque collecteur de journaux du groupe de collecteurs.

STEP 1 | Ajoutez les paires de disques RAID.

1. Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** et cliquez sur le nom du collecteur.
2. Sélectionnez **Disks (Disques)** et **Add (Ajoutez)** chaque paire de disques RAID, puis cliquez sur **OK**.

STEP 2 | Validez les modifications apportées dans Panorama et appliquez-les au groupe de collecteurs.

1. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** et **Edit Selections (Modifier les sélections)** dans la portée d'application.
2. Sélectionnez **Collector Groups (Groupes de collecteurs)**, sélectionnez le groupe de collecteurs que vous avez modifié, puis cliquez sur **OK**.
3. **Commit and Push (Validez et appliquez)** vos modifications.

STEP 3 | Vérifiez l'état des collecteurs de journaux et des paires de disques.

1. Sélectionnez **Panorama** > **Managed Collectors (collecteurs gérés)** et vérifiez que la configuration de chaque collecteur de journaux est synchronisée avec Panorama.

   La colonne État de configuration doit afficher **In Sync (synchronisation)** et la colonne État d'exécution doit afficher **connected (connectée)**.
2. Cliquez sur **Statistics (statistiques)** dans la dernière colonne pour chaque collecteur de journaux et vérifiez que les paires de disques sont **Enabled (activées)** et **Available (disponibles)**.

Remplacer un disque défaillant sur un appareil de la série M

Si un disque tombe en panne sur l'appareil de la série M, vous devez remplacer le disque et le reconfigurer dans une paire RAID. Pour plus d'informations, reportez-vous au Guide de référence des appareils matériels de la série M.

Remplacez le disque virtuel sur un serveur ESXi

Vous ne pouvez redimensionner un disque virtuel après son ajout à l'appareil virtuel Panorama sur un serveur ESXi. Étant donné que l'appareil virtuel Panorama en mode hérité ne permet qu'un emplacement de stockage de journaux, vous devez remplacer le disque virtuel comme suit pour modifier la capacité de stockage de journaux. En mode Panorama, vous pouvez simplement ajouter un autre disque (jusqu'à un maximum de 12) pour Augmenter la capacité de stockage de journaux sur l'appareil virtuel Panorama.

Sur l'appareil virtuel Panorama en mode hérité, vous perdez les journaux sur le disque existant lorsque vous le remplacez. Pour les options de conservation des journaux existants, voir Conserver les journaux existants lors de l'ajout de stockage sur l'appareil virtuel Panorama en mode hérité.

STEP 1 | Retirez l'ancien disque virtuel.

1. Accéder au client VMware vSphere et sélectionnez l' **Virtual Machines (Machines virtuelles)** onglet.
2. Faites un clic droit sur l'appareil virtuel Panorama et sélectionnez **Power (Alimentation)** > **Power Off (Mettre hors tension)**.

© 2020 Palo Alto Networks, Inc.

3. Cliquez droit sur l'application virtuelle Panorama et sélectionnez **Edit Settings (Modifier les paramètres)**.
4. Sélectionnez le disque virtuel dans l'onglet **Hardware (matériel)** et cliquez sur **Remove (supprimer)**.
5. Sélectionnez l'une des options de suppression et cliquez sur **OK**.

STEP 2 | Ajoutez le nouveau disque virtuel.

1. Ajouter un disque virtuel à Panorama sur un serveur ESXi.

   Panorama fonctionnant sur ESXi 5.5 et versions ultérieures prend en charge un disque virtuel de jusqu'à 8 To. Les versions antérieures d'ESXi prennent en charge un disque virtuel d'un maximum de 2 To.
2. Dans le vSphere Client, cliquez droit sur l'appareil virtuel Panorama et sélectionnez **Power (Alimentation)** > **Power On (Allumer)**.

   Le processus de redémarrage peut prendre plusieurs minutes et le message `cache de données indisponible` s'affiche.

STEP 3 | Assurez-vous que la capacité de stockage mise à jour du journal soit correcte.

1. Connectez-vous à l'appareil virtuel Panorama.
2. Sélectionnez **Panorama (Panorama)** > **Setup (Configuration)** > **Management (Gestion)** et vérifiez que la section paramètres de journalisation et de reporting, champ stockage du journal, affiche correctement la capacité de stockage du journal modifiée .

Remplacez le disque virtuel sur vCloud air

Vous ne pouvez redimensionner un disque virtuel après son ajout à un appareil virtuel Panorama sur VMware vCloud Air. Étant donné que l'appareil virtuel Panorama en mode hérité ne permet qu'un emplacement de stockage de journaux, vous devez remplacer le disque virtuel comme suit pour modifier la capacité de stockage de journaux. En mode Panorama, vous pouvez simplement Ajouter un disque virtuel à Panorama sur vCloud Air (jusqu'à un maximum de 12).

Sur l'appareil virtuel Panorama en mode hérité, vous perdez les journaux sur le disque existant lorsque vous le remplacez. Pour les options de conservation des journaux existants, voir Conserver les journaux existants lors de l'ajout de stockage sur l'appareil virtuel Panorama en mode hérité.

STEP 1 | Retirez l'ancien disque virtuel.

1. Accéder à la console Web vCloud Air et sélectionner votre **Virtual Private Cloud OnDemand (Cloud Virtuel Privé sur Demande)** région.
2. Sélectionnez l'application virtuelle Panorama dans la **Virtual Machines (Machines virtuelles)** onglet.
3. Sélectionnez **Actions (Actions)** > **Edit Resources (Modifier les ressources)**.
4. Cliquez sur **x** pour le disque virtuel que vous supprimez.

STEP 2 | Ajoutez le nouveau disque virtuel.

1. **Add another disk (Ajouter un autre disque)**.
2. Défnissez le **Storage (Stockage)** sur 8 To et spécifiez le niveau de stockage sur **Standard** ou **SSD-Accelerated (Accéléré par SSD)**.
3. Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.

STEP 3 | Redémarrez Panorama.

1. Connectez-vous à l'appareil virtuel Panorama.

© 2020 Palo Alto Networks, Inc.

2. Sélectionnez **Panorama (Panorama)** > **Setup (Configurationn)** > **Operations (Opérations)** et **Reboot Panorama (redémarrez Panorama)**.

STEP 4 | Assurez-vous que la capacité de stockage mise à jour du journal soit correcte.

1. Connectez-vous à l'appareil virtuel Panorama après son redémarrage.
2. Sélectionnez **Panorama (Panorama)** > **Setup (Configuration)** > **Management (Gestion)** et vérifiez que la section paramètres de journalisation et de reporting, champ stockage du journal, affiche correctement la capacité de stockage du journal modifiée .

Migrer les journaux vers un nouvel appareil de la série M en Mode Collecteur de Journaux

Si vous avez besoin de remplacer un appareil M-500 ou M-100 en mode collecteur de journaux (collecteur de journaux dédié), vous pouvez migrer les journaux qu'il réunit depuis les pare-feu en déplaçant ses disques RAID vers un nouvel appareil de série M. Cette procédure vous permet de récupérer les journaux après une panne système sur l'appareil de la série M ou de migrer des journaux dans le cadre d'une mise à niveau de matériel (d'un appareil M-100 à un appareil M-500).

La migration des journaux en retirant les disques de journalisation des appareils M-Series et en les chargeant dans un serveur de gestion M-600 Panorama n'est pas prise en charge. Pour migrer d'un appareil M-600, paramétrez l'appareil M-600, configurez le transfert des journaux vers le nouvel appareil M-600 et configurez l'appareil M-Series comme un collecteur de journaux géré jusqu'à ce que vous n'ayez plus besoin d'accéder aux journaux stockés sur l'appareil M-Series.

STEP 1 | Effectuez la configuration initiale du nouvel appareil de Série M qui sera un collecteur de journaux dédié.

1. Montez l'appareil de série M dans une baie. Se référer au Guide de référence du matériel de la série-M pour obtenir des instructions.
2. Effectuez la configuration initiale de l'appareil de série M.

   Lors de la configuration des interfaces, configurez uniquement l'interface de gestion (Management). Le passage au mode collecteur de journaux (plus loin dans cette procédure) supprime toutes les configurations d'interface. Si le collecteur de journaux utilisera des interfaces autre que des interfaces de gestion, ajoutez-les lors de la configuration du collecteur de journaux (voir l'étape 2).
3. Enregistrez Panorama.
4. Achetez et activez la licence d'assistance Panorama ou transférez des licences comme suit uniquement si le nouvel appareil de la série M est du même modèle de matériel que l'ancien appareil de série M. Si le nouvel appareil de série M est un modèle différent de l'ancien appareil de série M, vous devez acheter de nouvelles licences.
   1. Connectez-vous au site web de support de Palo Alto Networks.
   2. puis cliquez Sélectionnez l'**Assets (Actif)** onglet puis cliquez **Spares (pièces de rechange)** lien.
   3. Cliquez sur le numéro de série du nouvel appareil de la série M.
   4. Cliquer**Transfer Licenses (Transférer les Licences)**.
   5. **Select (Sélectionnez)**le vieil appareil de la série M et cliquez sur **Submit (Soumettre)**.
5. Activer une licence de gestion de périphérique. Si vous effectuez la migration d'un appareil de M-100 à un appareil M-500, entrez le code d'identification associé à la licence de migration.

© 2020 Palo Alto Networks, Inc.

6. Installer les mises à jour de contenu et logicielles pour Panorama. Pour des informations importantes sur les versions logicielles, voir Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire.
7. Passez du mode Panorama au mode collecteur de journaux.
   1. Accédez à l'ILC du Collecteur de journaux et basculez en mode collecteur de journaux :

      ```
      > request system system-mode logger
      ```

   2. Entrez **Y** pour confirmer le changement de mode. L'appareil de série M redémarre. Si le processus de redémarrage termine votre session du logiciel d'émulation de terminal, reconnectez à l'appareil de Série M pour afficher l'invite de connexion Panorama.

      *Si une invite **CMS Login** s'affiche, appuyez sur Entrée sans saisir de nom d'utilisateur ou de mot de passe.*
8. Utilisez l'ILC du collecteur de journaux pour activer la connectivité entre le collecteur de journaux et le serveur de gestion de panorama. <IPaddress1> est pour l'interface de gestion Panorama active et <IPaddress2> est pour l'interface de gestion Panorama passive.

```
> configure
# set deviceconfig system panorama-server <IPaddress1> panorama-server-2
 <IPaddress2>
# commit
# exit
```

STEP 2 | Sur le serveur d'administration de Panorama, ajouter le nouveau Collecteur de Journaux comme un collecteur géré.

Pour toutes les étapes avec des commandes nécessitant un numéro de série du dispositif, vous devez taper le numéro de série entier ; appuyer sur la touche TAB ne complétera pas un numéro partiel.

1. Configurez le collecteur de journaux comme un collecteur géré à l'aide de l'interface Web de Panorama en utilisant les commandes suivantes de CLI :

```
> configure
# set log-collector <LC_serial_number> deviceconfig system hostname <nom
 d'hôte du collecteur de journaux>
# exit
```

   Si l'ancien collecteur de journaux utilisait des interfaces autres que l'interface MGT pour la collecte de journaux et la communication du groupe de collecteurs, vous devez définir les interfaces sur le nouveau collecteur de journaux lorsque vous le configurez comme un collecteur géré (Panorama > Managed Collectors (Collecteurs gérés) > Interfaces).
2. Vérifiez que le Collecteur de Journaux est connecté au Panorama et que le statut de ses paires de disques est présent/disponible.

```
> show log-collector serial-number <log-collector_SN>
```

   Les paires de disques s'affichent comme étant désactivées à ce stade du processus de restauration.
3. Validez vos modifications sur Panorama. Ne pas valider tout de suite les modifications sur le groupe collecteur .

© 2020 Palo Alto Networks, Inc.

```
> configure
# commit
# exit
```

STEP 3 | Supprimer les disques RAID de l'ancien collecteur de journaux .

1. Mise hors tension de l'ancien Collecteur de Journaux en appuyant sur le bouton d'alimentation jusqu'à ce que le système s'arrête.
2. Retirez les paires de disques. Pour plus d'informations, reportez-vous à la procédure de remplacement dans le Guide de Référence des appareils de la série-M.

STEP 4 | Préparez les disques pour la migration.

La génération des métadonnées de chaque paire de disques recrée les index. Par conséquent, selon le volume de données, ce processus peut prendre beaucoup de temps. Afin d'accélérer le processus, vous pouvez lancer plusieurs sessions ILC et exécuter la commande de régénération des métadonnées dans chaque session pour terminer le processus simultanément pour chaque paire. Pour plus d'informations, consultez régénération des métadonnées pour les paires RAID des unités de Série M.

1. Insérez les disques dans le nouveau collecteur de journal. Pour plus d'informations, reportez-vous à la procédure de remplacement dans le Guide de Référence des appareils de la série-M.

   Les supports de disques de l'appareil M-100 sont incompatibles avec ceux de l'appareil M-500. Par conséquent, lors de la migration entre ces modèles de matériel, vous devez dévisser chaque disque de son ancien support et insérez le disque dans le nouveau support avant d'insérer le disque dans le nouvel appareil.

   Vous devez maintenir la liaison de paire de disques. Bien que vous puissiez placer une paire de disques de l'emplacement A1/A2 de l'ancien appareil dans l'emplacement B1/B2 du nouvel appareil, vous devez conserver les disques ensemble dans le même emplacement ; dans le cas contraire, Panorama ne restaurera peut-être pas les données avec succès.
2. Activez les paires de disques en exécutant la commande ILC suivante pour chaque paire :

```
> request system raid add <slot> force no-format
```

Par exemple :

```
> request system raid add A1 force no-format
> request system raid add A2 force no-format
```

Les arguments **forçage**et **non-formatage** sont requis. L'argument **forçage**associe la paire de disques avec le nouveau Collecteur de Journaux. L'argument **non-formatage** empêche le reformatage des disques et conserve les journaux stockés sur les disques.

3. Générez les métadonnées pour chaque paire de disques.

```
> request metadata-regenerate slot <slot_number>
```

Par exemple :

```
> request metadata-regenerate slot 1
```


© 2020 Palo Alto Networks, Inc.

STEP 5 | Ajoutez un collecteur de journaux sans disque à un groupe de collecteurs.

À partir de ce moment, seules les validations requises pour terminer le processus de migration sur Panorama et les collecteurs de journaux sont requises. Attendez avant de faire d'autres changements.

1. Accédez à la CLI de Panorama.
2. Remplacez la restriction de Panorama pour permettre à un collecteur de journaux sans disque d'être ajouté à un groupe de collecteurs : **request log-migration-set-start**

STEP 6 | Migrez les journaux.

Vous devez utiliser l'ILC de Panorama pour cette étape, pas l'interface web.

Vous devez attribuer le nouveau Collecteur de Journaux au groupe Collecteur qui contient l'ancien Collecteur de Journaux.

1. Assignez le nouveau Collecteur de Journaux au groupe collecteur et validez vos modifications sur Panorama.

```
> configure
# set log-collector-group <collector_group_name> logfwd-setting collectors
 <numéro de série du nouveau collecteur de journaux>
# commit
# exit
```

2. Pour chaque paire de disques, migrer les journaux de l'ancien Collecteur de Journaux vers le nouveau Collecteur de Journaux et rattachez la paire de disques au nouveau Collecteur de Journaux.

```
> request log-migration from <old_LC_serial_number> old-disk-pair <paire
 de vieux disques> to <numéro de série du nouveau collecteur de journaux>
 new-disk-pair <paire de disques de journaux>
```

Par exemple :

```
> request log-migration from 003001000010 old-disk-pair A to 00300100038
 new-disk-pair A
```

STEP 7 | Reconfigurez le groupe de collecteurs

1. Utilisez l'interface Web pour attribuer le nouveau Collecteur de journaux aux pare-feux qui transmettent les journaux (**Panorama (Panorama)** > **Collector Groups (Groupes de Collecteurs)** > **Device Log Forwarding (Transfert du journal des périphériques)**). Donner au nouveau Collecteur de Journaux la même priorité dans les listes de préférence de pare-feu de l'ancien Collecteur de Journaux.

Vous ne pouvez pas utiliser la CLI pour modifier les affectations de priorité des listes de préférences du pare-feu.

2. Supprimer l'ancien Collecteur de Journaux du groupe collecteur.

```
> configure
# delete log-collector-group <group_name> logfwd-setting collectors
 <numéro de série de l'ancien collecteur de journaux>
```


© 2020 Palo Alto Networks, Inc.

Par exemple :

```
# delete log-collector-group DC-Collector-Group logfwd-setting collectors
 003001000010
```

3. Supprimer l'ancien Collecteur de Journaux de la configuration de Panorama et valider vos modifications sur Panorama.

```
# delete log-collector <old_LC_serial_number>
# commit
# exit
```

4. Validez les modifications apportées au groupe de collecteurs pour que les pare-feu gérés puissent envoyer les journaux au nouveau collecteur de journaux.

```
> commit-all log-collector-config log-collector-
group <collector_group_name>
```

Par exemple :

```
> commit-all log-collector-config log-collector-group DC-Collector-Group
```

STEP 8 | Générez de nouvelles clés sur le nouveau collecteur de journaux dédié.

Cette commande est requise pour ajouter le nouveau collecteur de journaux au groupe de collecteurs et ne doit être exécutée que pour le groupe de collecteurs du collecteur de journaux en cours de remplacement. Cette étape supprime les clés RSA existantes et permet à Panorama de créer de nouvelles clés RSA.

1. Accédez à la CLI de Panorama.
2. Supprimez toutes les clés RSA sur le nouveau collecteur de journaux :

   request logdb update-collector-group-after-replace collector-group *<nom du groupe de collecteurs>*

   Le processus peut prendre jusqu'à 10 minutes.

STEP 9 | Confirmez que le statut de SearchEngine est Active (Actif) pour tous les collecteurs de journaux du groupe de collecteurs.

Ne continuez pas tant que le statut de SearchEngine n'est pas Active (Actif) pour tous les collecteurs de journaux du groupe de collecteurs. Cela entraînera la purge des journaux du collecteur de journaux en cours de remplacement.

1. Accédez à la CLI de Panorama.
2. Affichez les détails du collecteur de journaux en exécutant les commandes suivantes :
   - Sur Panorama pour tous les collecteurs de journaux :

     show log-collector all

© 2020 Palo Alto Networks, Inc.

Vous pouvez également exécuter la commande suivante sur chaque collecteur de journaux dédié :

```
show log-collector detail
```

3. Confirmez que l'état de SearchEngine est Active (Actif).

```
Redistribution status:       none
```

```
Last commit-all: commit succeeded, current ring version 1
```

```
SearchEngine status:     Active
```

```
md5sum 4e5055a359f7662fab8f8c4f57e24525 updated at 2017/06/14 09:58:19
```

STEP 10 | Sur le nouveau collecteur de journaux, remplacez le numéro de série du collecteur de journaux précédent par le numéro de série du nouveau collecteur de journaux.

Vous devez remplacer le numéro de série de l'ancien collecteur de journaux par le numéro de série du nouveau collecteur de journaux afin que le nouveau collecteur de journaux ne s'exécute pas avec des problèmes de purge, ce qui empêcherait le collecteur de journaux de purger les anciennes données des journaux migrés.

1. Accédez à la CLI du collecteur de journaux.
2. Remplacez le numéro de série de l'ancien collecteur de journaux par le numéro de série du nouveau collecteur de journaux :

   request log-migration-update-logger from *<numéro de série de l'ancien collecteur de journaux>* to *<numéro de série du nouveau collecteur de journaux>*

Migrer les journaux vers un nouvel appareil de la série M en Mode Panorama

Si vous devez remplacer un appareil M-500 ou M-100 en mode Panorama (serveur de gestion Panorama), vous pouvez migrer les journaux qu'il collecte depuis les pare-feu en déplaçant ses disques RAID vers un nouvel appareil de série M. Cela vous permet de récupérer les journaux après une panne système sur l'appareil de la série M ou de migrer des journaux dans le cadre d'une mise à niveau matérielle (d'un appareil M-100 à un appareil M-500).

La migration des journaux en retirant les disques de journalisation des appareils M-Series et en les chargeant dans un serveur de gestion M-600 Panorama n'est pas prise en charge. Pour migrer d'un appareil M-600, paramétrez l'appareil M-600, configurez le transfert des journaux vers le nouvel appareil M-600 et configurez l'appareil M-Series comme un collecteur de journaux géré jusqu'à ce que vous n'ayez plus besoin d'accéder aux journaux stockés sur l'appareil M-Series.

Cette procédure de migration couvre les scénarios suivants dans le cadre desquels vous remplacez un seul appareil de série M, n'appartenant pas à une configuration HA, par un collecteur géré (collecteur de journaux) dans un groupe de collecteurs.

© 2020 Palo Alto Networks, Inc.

STEP 1 | Transmettre les journaux sur le SSD de l'ancien appareil de série M vers une destination externe si vous souhaitez les conserver.

Le SSD stocke les journaux système et de configuration que génèrent Panorama et les collecteurs de journaux. Vous ne pouvez pas déplacer le SSD entre les appareils de la série M.

Configurez le transfert des journaux de Panorama vers des destinations extérieures.

STEP 2 | Exportez la configuration Panorama de l'appareil de série M mis hors service en mode Panorama.

1. Connectez-vous à l'appareil Panorama et sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)**.
2. Cliquez sur **Save named Panorama configuration snapshot (Enregistrer un instantané de configuration nommé Panorama)**, entrez un **Name (Nom)** pour identifier la configuration et cliquez **sur OK**.
3. Cliquez sur **Export named Panorama configuration snapshot (Exporter l'instantané de configuration nommé Panorama),** sélectionnez le **Name (Nom)** de la configuration que vous venez d'enregistrer et cliquez sur **OK** . Panorama exporte la configuration de votre système client sous forme de fichier XML.

STEP 3 | Supprimez les disques RAID de l'appareil de la série M.

1. Mettez hors tension l'ancien appareil de la série M en appuyant sur le bouton d'alimentation jusqu'à ce que le système s'arrête.
2. Retirez les paires de disques. Pour plus d'informations, reportez-vous à la procédure de remplacement dans le Guide de Référence des appareils de la série-M.

STEP 4 | Effectuer la configuration initiale du nouvel appareil de série M.

1. Montez l'appareil de série M dans une baie. Se référer au Guide de référence du matériel de la série-M pour obtenir des instructions.
2. Effectuez la configuration initiale de l'appareil de série M.
3. Enregistrez Panorama.
4. Achetez et activez une licence d'assistance Panorama ou transférez des licences comme suit uniquement si le nouvel appareil de la série M est du même modèle de matériel que l'ancien appareil de série M. Si le nouvel appareil de série M est un modèle différent de l'ancien appareil de série M, vous devez acheter de nouvelles licences.
    1. Connectez-vous au site web de support de Palo Alto Networks.
    2. puis cliquez Sélectionnez l'**Assets (Actif)** onglet puis cliquez **Spares (pièces de rechange)** lien.
    3. Cliquez sur le numéro de série du nouvel appareil de la série M.
    4. Cliquer**Transfer Licenses (Transférer les Licences)**.
    5. **Select (Sélectionnez)**le vieil appareil de la série M et cliquez sur **Submit (Soumettre)**.
5. Activer une licence de gestion de périphérique. Si vous effectuez la migration d'un appareil de M-100 à un appareil M-500, entrez le code d'identification associé à la licence de migration.
6. Installer les mises à jour de contenu et logicielles pour Panorama. Pour des informations importantes sur les versions logicielles, voir Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire.

STEP 5 | Chargez l'instantané de configuration Panorama que vous avez exporté depuis l'appareil de série M mis hors service vers le nouvel appareil de série M en mode Panorama.

1. Se connecter à l'interface Web Panorama du nouvel appareil M-Series, sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)**.

© 2020 Palo Alto Networks, Inc.

2. Cliquez sur **Import named Panorama configuration snapshot (Importer un instantané de configuration nommé Panorama)**, **Browse (Rechercher)** le fichier de configuration que vous avez exporté depuis l'appareil de série M mis hors service, et cliquez sur **OK**.
3. Cliquez sur **Load named Panorama configuration snapshot (Charger un instantané de configuration nommé Panorama)**, sélectionnez le **Name (Nom)** de la configuration que vous venez d'importer, sélectionnez une **Decryption Key (Clé de décryptage)** (la clé maître pour Panorama), et cliquez sur **OK**. Panorama écrase sa configuration candidate actuelle avec la configuration chargée. Panorama affiche toutes les erreurs qui se produisent lors du chargement du fichier de configuration. Si des erreurs se produisent, enregistrez-les dans un fichier local. Résolvez chaque erreur pour vous assurer que la configuration migrée est valide.

   Pour remplacer une RMA Panorama, assurez-vous de Retain Rule UUIDs (Conserver les UUID des règles) lorsque vous chargez l'instantané de configuration Panorama. Si vous ne sélectionnez pas cette option, Panorama supprime tous les UUID des règles précédents de l'instantané de configure et affecte de nouveaux UUID aux règles sur Panorama, ce qui signifie qu'il ne conserve pas les informations associées aux UUID antérieurs, comme le nombre de correspondance à la règle de politique.
4. Effectuez les changements de configuration supplémentaires qui s'avèrent nécessaires.

   Si l'ancien appareil M-Series utilisait des interfaces autres que l'interface de gestion pour les services Panorama (tels que la collecte de journaux), vous devez définir ces interfaces sur le nouvel appareil M-Series (Panorama > Setup (Configuration) > Interfaces)).
5. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Validate Commit (Confirmer la validation)**. Résolvez les erreurs avant de poursuivre.
6. **Commit (Validez)** vos modifications dans la configuration de Panorama.

STEP 6 | Insérez les disques dans le nouvel appareil de la série M. Pour plus d'informations, reportez-vous à la procédure de remplacement dans le Guide de Référence des appareils de la série-M.

Les supports de disques de l'appareil M-100 sont incompatibles avec ceux de l'appareil M-500. Par conséquent, lors de la migration entre ces modèles de matériel, vous devez dévisser chaque disque de son ancien support et insérez le disque dans le nouveau support avant d'insérer le disque dans le nouvel appareil.

Vous devez maintenir la liaison de paire de disques. Bien que vous puissiez placer une paire de disques de l'emplacement A1/A2 de l'ancien appareil dans l'emplacement B1/B2 du nouvel appareil, vous devez conserver les disques ensemble dans le même emplacement ; dans le cas contraire, Panorama ne restaurera peut-être pas les données avec succès.

STEP 7 | Contactez le Support Client Palo Alto Networks pour copier les métadonnées du groupe de collecteurs depuis l'appareil de série M mis hors service vers le nouvel appareil de série M, puis relancez le processus mgmtsrvr.

STEP 8 | Si l'appareil de série M faisait partie d'un groupe de collecteurs, vérifiez que le numéro de série de l'appareil de série M désaffecté fait toujours partie du bon groupe de collecteurs :

```
debug log-collector-group show name <nom du groupe de collecteurs de journaux>
```

Si le numéro de série de l'appareil de série M mis hors service ne fait plus partie du bon groupe de collecteurs, les dossiers d'assistance technique ont mal été copiés à l'étape précédente. Contactez à nouveau l'assistance client de Palo Alto Networks pour copier les dossiers d'assistance technique à l'emplacement correct.

© 2020 Palo Alto Networks, Inc.

STEP 9 | Préparez les disques pour la migration.

La génération des métadonnées de chaque paire de disques recrée les index. Par conséquent, selon le volume de données, ce processus peut prendre beaucoup de temps. Afin d'accélérer le processus, vous pouvez lancer plusieurs sessions ILC et exécuter la commande de régénération des métadonnées dans chaque session pour terminer le processus simultanément pour chaque paire. Pour plus d'informations, consultez régénération des métadonnées pour les paires RAID des unités de Série M.

1. Insérez les disques dans le nouvel appareil de la série M. Pour plus d'informations, reportez-vous à la procédure de remplacement dans le Guide de Référence des appareils de la série-M.

   Les supports de disques de l'appareil M-100 sont incompatibles avec ceux de l'appareil M-500. Par conséquent, lors de la migration entre ces modèles de matériel, vous devez dévisser chaque disque de son ancien support et insérez le disque dans le nouveau support avant d'insérer le disque dans le nouvel appareil.

   Vous devez maintenir la liaison de paire de disques. Bien que vous puissiez placer une paire de disques de l'emplacement A1/A2 de l'ancien appareil dans l'emplacement B1/B2 du nouvel appareil, vous devez conserver les disques ensemble dans le même emplacement ; dans le cas contraire, Panorama ne restaurera peut-être pas les données avec succès.
2. Activez les paires de disques en exécutant la commande ILC suivante pour chaque paire :

```
admin> request system raid add <slot> force no-format
```

   Par exemple :

```
admin> request system raid add A1 force no-format
admin> request system raid add A2 force no-format
```

   Les arguments **forçage**et **non-formatage** sont requis. L'argument **forçage** associe la paire de disques au nouvel appareil. L'argument **non-formatage** empêche le reformatage des disques et conserve les journaux stockés sur les disques.
3. Générez les métadonnées pour chaque paire de disques.

   Cette étape peut prendre un maximum de six heures, selon le volume des données des journaux qui sont contenues sur les disques.

```
admin> request metadata-regenerate slot <slot_number>
```

   Par exemple :

```
admin> request metadata-regenerate slot 1
```

STEP 10 | Configurez le collecteur de journaux local sur le nouvel appareil de la série M.

Pour toutes les étapes avec des commandes nécessitant un numéro de série du dispositif, vous devez taper le numéro de série entier ; appuyer sur la touche TAB ne complétera pas un numéro partiel.

N'activez pas les disques sur le nouvel appareil de la série M à ce stade. Lorsque vous migrez les journaux avec succès, Panorama active automatiquement les disques.

© 2020 Palo Alto Networks, Inc.

1. Configurez le collecteur de journaux en tant que collecteur géré à l'aide de l'interface web de Panorama ou en utilisant les commandes ILC suivantes :

```
admin> configure
admin# set log-collector <log-collector_SN> deviceconfig system hostname
 <nnom d'hôte du collecteur de journaux>
admin# exit
```

2. Vérifiez que le Collecteur de Journaux est connecté à Panorama et que le statut de ses paires de disques est présent/disponible.

```
admin> show log-collector serial-number <log-collector_SN>
```

   Les paires de disques s'affichent comme étant désactivées à ce stade du processus de restauration.
3. Validez vos modifications sur Panorama. Ne pas valider tout de suite les modifications sur le groupe collecteur .

```
admin> configure
admin# commit
```

STEP 11 | Ajoutez un collecteur de journaux sans disque à un groupe de collecteurs.

À partir de ce moment, seules les validations requises pour terminer le processus de migration sur Panorama et les collecteurs de journaux sont requises. Attendez avant de faire d'autres changements.

1. Accédez à l'ILC du nouvel appareil de série M.
2. Remplacez la restriction de Panorama pour permettre à un collecteur de journaux sans disque d'être ajouté à un groupe de collecteurs : **request log-migration-set-start**
3. Validez la restriction remplacée :

```
admin> configure
admin# commit force
```

STEP 12 | Migrez les journaux.

1. Accédez à l'ILC du nouvel appareil de série M.
2. Assignez le nouveau Collecteur de Journaux au groupe collecteur et validez vos modifications sur Panorama.

```
admin# set log-collector-group <collector_group_name> logfwd-setting
 collectors <collecteur_géré_SN>
admin# commit
admin# exit
```

   L'ancien collecteur de journal local apparaît encore dans la liste des membres, car vous ne l'avez pas supprimé de la configuration.
3. Pour chaque paire de disques, migrer les journaux vers le nouvel appareil.

© 2020 Palo Alto Networks, Inc.

```
admin> request log-migration from <old_LC_serial_number> old-disk-pair
 <paire de vieux disques> to <numéro de série du nouveau collecteur de
 journaux> new-disk-pair <paire de disques de journaux>
```

Par exemple :

```
admin> request log-migration from 003001000010 old-disk-pair A to
 00300100038 new-disk-pair A
```

4. Validez les modifications sur Panorama.

```
admin> configure
admin# commit
```

STEP 13 | Reconfigurez le groupe de collecteurs

1. Se connecter à l'interface Web Panorama du nouvel appareil M-Series pour attribuer le nouveau Collecteur de journaux aux pare-feu qui transmettent les journaux (**Panorama** > **Collector Groups (Groupes de Collecteurs)** > **Device Log Forwarding (Transfert du journal des périphériques)**). Donner au nouveau Collecteur de Journaux la même priorité dans les listes de préférence de pare-feu de l'ancien Collecteur de Journaux.

   Vous ne pouvez pas utiliser la CLI pour modifier les affectations de priorité des listes de préférences du pare-feu.

2. Accédez à l'ILC du nouvel appareil de série M.
3. Supprimer l'ancien Collecteur de Journaux du groupe collecteur.

```
admin# delete log-collector-group <group_name> logfwd-setting collectors
 <numéro de série de l'ancien collecteur de journaux>
```

Par exemple :

```
admin# delete log-collector-group DC-Collector-Group logfwd-setting
 collectors 003001000010
```

4. Supprimer l'ancien Collecteur de Journaux de la configuration de Panorama et valider vos modifications sur Panorama.

```
admin# delete log-collector <old_LC_serial_number>
admin# commit
admin# exit
```

5. Validez les modifications apportées au groupe de collecteurs pour que les pare-feu gérés puissent envoyer les journaux au nouveau collecteur de journaux.

```
admin> commit-all log-collector-config log-collector-
group <collector_group_name>
```

Par exemple :

© 2020 Palo Alto Networks, Inc.

```
admin> commit-all log-collector-config log-collector-group DC-Collector-Group
```

STEP 14 | Générez de nouvelles clés sur le nouveau collecteur de journaux.

Cette commande est requise pour ajouter le nouveau collecteur de journaux au groupe de collecteurs et ne doit être exécutée que pour le groupe de collecteurs du collecteur de journaux en cours de remplacement. Cette étape supprime les clés RSA existantes et permet à Panorama de créer de nouvelles clés RSA.

1. Accédez à l'ILC du nouvel appareil de série M.
2. Supprimez toutes les clés RSA du nouveau collecteur de journaux :

   request logdb update-collector-group-after-replace collector-group *<nom du groupe de collecteurs>*

   Le processus peut prendre jusqu'à 10 minutes.

STEP 15 | Confirmez que le statut de SearchEngine est Active (Actif) pour tous les collecteurs de journaux du groupe de collecteurs.

Ne continuez pas tant que le statut de SearchEngine n'est pas Active (Actif) pour tous les collecteurs de journaux du groupe de collecteurs. Cela entraînera la purge des journaux du collecteur de journaux en cours de remplacement.

1. Accédez à l'ILC du nouvel appareil de série M.
2. Affichez les détails du collecteur de journaux en exécutant les commandes suivantes :
   - Sur Panorama pour tous les collecteurs de journaux :

     show log-collector all

     Vous pouvez également exécuter la commande suivante sur chaque collecteur de journaux dédié :

     ```
     show log-collector detail
     ```
3. Confirmez que l'état de SearchEngine est Active (Actif).

```
Redistribution status:       none
```

```
Last commit-all: commit succeeded, current ring version 1
```

```
SearchEngine status:     Active
```

```
md5sum 4e5055a359f7662fab8f8c4f57e24525 updated at 2017/06/14 09:58:19
```

STEP 16 | Sur le nouveau collecteur de journaux, remplacez le numéro de série du collecteur de journaux précédent par le numéro de série du nouveau collecteur de journaux.

Vous devez remplacer le numéro de série de l'ancien collecteur de journaux par le numéro de série du nouveau collecteur de journaux afin que le nouveau collecteur de journaux ne s'exécute pas avec des

© 2020 Palo Alto Networks, Inc.

problèmes de purge, ce qui empêcherait le collecteur de journaux de purger les anciennes données des journaux migrés.

1. Accédez à la CLI du collecteur de journaux.
2. Remplacez le numéro de série de l'ancien collecteur de journaux par le numéro de série du nouveau collecteur de journaux :

   request log-migration-update-logger from *<numéro de série de l'ancien collecteur de journaux>* to *<numéro de série du nouveau collecteur de journaux>*

Migrer les journaux vers un nouvel appareil de la série M en Mode Panorama en haute disponibilité.

Si vous devez remplacer un appareil M-500 ou M-100 en mode Panorama (serveur de gestion Panorama) par un appareil de série M d'un autre modèle, vous pouvez migrer les journaux qu'il collecte depuis les pare-feu en déplaçant ses disques RAID vers le nouvel appareil de série M. Cela vous permet de migrer des journaux dans le cadre d'une mise à niveau matérielle (d'un appareil M-100 à un appareil M-500). Vous pouvez migrer d'un appareil M-100 vers et depuis un appareil M-500. Les migrations entre les appareils M-100 et M-500 vers des appareils M-200 et M-600, et depuis ces derniers, ne sont pas possibles.

La migration des journaux en retirant les disques de journalisation des appareils M-Series et en les chargeant dans un serveur de gestion M-600 Panorama n'est pas prise en charge. Pour migrer d'un appareil M-600, paramétrez l'appareil M-600, configurez le transfert des journaux vers le nouvel appareil M-600 et configurez l'appareil M-Series comme un collecteur de journaux géré jusqu'à ce que vous n'ayez plus besoin d'accéder aux journaux stockés sur l'appareil M-Series.

Cette procédure de migration couvre les scénarios suivants :

- Un homologue HA Panorama a un collecteur géré (Collecteur de Journaux) dans un groupe de collecteurs.

© 2020 Palo Alto Networks, Inc.

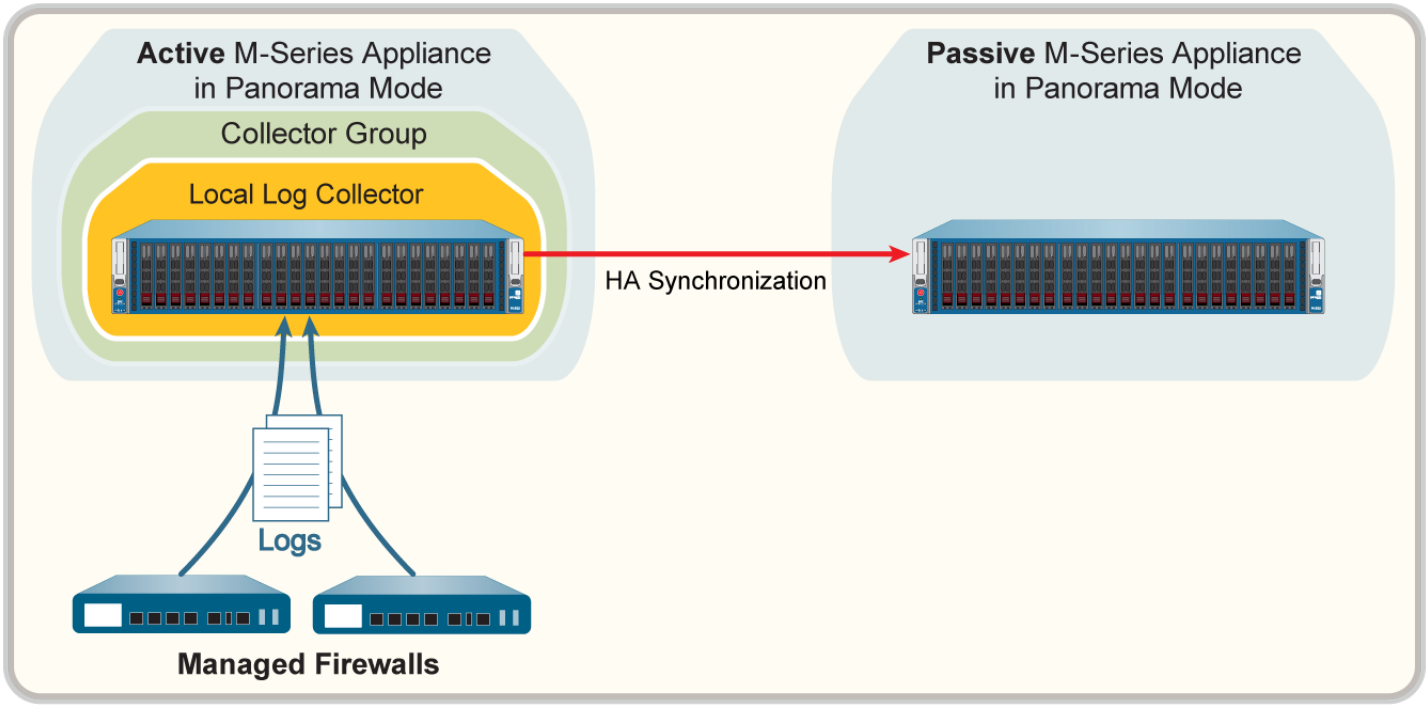


Figure 30: Homologue HD Panorama avec groupe de collecteurs

- Les deux homologues Panorama HD ont des collecteurs gérés qui appartiennent à un seul groupe de collecteurs. Pour plus de détails, consultez Plusieurs collecteurs de journaux locaux par groupe de collecteurs.
- Les deux homologues HD Panorama ont un collecteur géré et chacun est assigné à un groupe distinct de collecteurs. Pour plus de détails, consultez Collecteur de journaux local unique par groupe de collecteurs.

STEP 1 | Transmettre les journaux sur le SSD de l'ancien appareil de série M vers une destination externe si vous souhaitez les conserver.

Le SSD stocke les journaux système et de configuration que génèrent Panorama et les collecteurs de journaux. Vous ne pouvez pas déplacer le SSD entre les appareils de la série M.

Configurez le transfert des journaux de Panorama vers des destinations extérieures.

STEP 2 | Exportez la configuration Panorama de l'appareil de série M principal mis hors service en mode Panorama.

1. Se connecter à l'interface Web Panorama de l'appareil M-Series que vous remplacez et sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)**.
2. Cliquez sur **Save named Panorama configuration snapshot (Enregistrer un instantané de configuration nommé Panorama)**, entrez un **Name (Nom)** pour identifier la configuration et cliquez **sur OK**.
3. Cliquez sur **Export named Panorama configuration snapshot (Exporter l'instantané de configuration nommé Panorama),** sélectionnez le **Name (Nom)** de la configuration que vous venez d'enregistrer et cliquez sur **OK** . Panorama exporte la configuration de votre système client sous forme de fichier XML.

STEP 3 | Supprimez les disques RAID de l'appareil de la série M.

1. Mettez hors tension l'ancien appareil de la série M en appuyant sur le bouton d'alimentation jusqu'à ce que le système s'arrête.

© 2020 Palo Alto Networks, Inc.

2. Retirez les paires de disques. Pour plus d'informations, reportez-vous à la procédure de remplacement dans le Guide de Référence des appareils de la série-M.

STEP 4 | Effectuer la configuration initiale du nouvel appareil de série M.

Répétez cette étape pour chaque nouvel appareil de série M de la configuration HA.

1. Montez l'appareil de série M dans une baie. Se référer au Guide de référence du matériel de la série-M pour obtenir des instructions.
2. Effectuez la configuration initiale de l'appareil de série M.
3. Enregistrez Panorama.
4. Achetez et activez une licence d'assistance Panorama ou transférez des licences comme suit uniquement si le nouvel appareil de la série M est du même modèle de matériel que l'ancien appareil de série M. Si le nouvel appareil de série M est un modèle différent de l'ancien appareil de série M, vous devez acheter de nouvelles licences.
    1. Connectez-vous au site web de support de Palo Alto Networks.
    2. puis cliquez Sélectionnez l'**Assets (Actif)** onglet puis cliquez **Spares (pièces de rechange)** lien.
    3. Cliquez sur le numéro de série du nouvel appareil de la série M.
    4. Cliquer**Transfer Licenses (Transférer les Licences)**.
    5. **Select (Sélectionnez)**le vieil appareil de la série M et cliquez sur **Submit (Soumettre)**.
5. Activer une licence de gestion de périphérique. Si vous effectuez la migration d'un appareil de M-100 à un appareil M-500, entrez le code d'identification associé à la licence de migration.
6. Installer les mises à jour de contenu et logicielles pour Panorama. Pour des informations importantes sur les versions logicielles, voir Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire.
7. Définir la HD (haute disponibilité) sur Panorama. Le nouvel appareil de la série M doit avoir la même priorité que l'homologue HD que vous remplacez.

STEP 5 | Chargez l'instantané de configuration Panorama que vous avez exporté depuis l'appareil de série M principal mis hors service vers le nouvel appareil de série M principal en mode Panorama.

1. Se connecter à l'interface Web Panorama du nouvel appareil M-Series, sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)**.
2. Cliquez sur **Import named Panorama configuration snapshot (Importer un instantané de configuration nommé Panorama)**, **Browse (Rechercher)** le fichier de configuration que vous avez exporté depuis l'appareil de série M mis hors service, et cliquez sur **OK**.
3. Cliquez sur **Load named Panorama configuration snapshot (Charger un instantané de configuration nommé Panorama)**, sélectionnez le **Name (Nom)** de la configuration que vous venez d'importer, sélectionnez une **Decryption Key (Clé de décryptage)** (la clé maître pour Panorama), et cliquez sur **OK**. Panorama écrase sa configuration candidate actuelle avec la configuration chargée. Panorama affiche toutes les erreurs qui se produisent lors du chargement du fichier de configuration. Si des erreurs se produisent, enregistrez-les dans un fichier local. Résolvez chaque erreur pour vous assurer que la configuration migrée est valide.

    Pour remplacer une RMA Panorama, assurez-vous de Retain Rule UUIDs (Conserver les UUID des règles) lorsque vous chargez l'instantané de configuration Panorama. Si vous ne sélectionnez pas cette option, Panorama supprime tous les UUID des règles précédents de l'instantané de configure et affecte de nouveaux UUID aux règles sur Panorama, ce qui signifie qu'il ne conserve pas les informations associées aux UUID antérieurs, comme le nombre de correspondance à la règle de politique.
4. Effectuez les changements de configuration supplémentaires qui s'avèrent nécessaires.

© 2020 Palo Alto Networks, Inc.

Si l'ancien appareil M-Series utilisait des interfaces autres que l'interface de gestion pour les services Panorama (tels que la collecte de journaux), vous devez définir ces interfaces sur le nouvel appareil M-Series (Panorama > Setup (Configuration) > Interfaces)).

5. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Validate Commit (Confirmer la validation)**. Résolvez les erreurs avant de poursuivre.
6. **Commit (Validez)** vos modifications dans la configuration de Panorama. Une fois validée, la configuration Panorama est synchronisée sur les homologues HA.

STEP 6 | Insérez les disques dans le nouvel appareil de la série M. Pour plus d'informations, reportez-vous à la procédure de remplacement dans le Guide de Référence des appareils de la série-M.

Répétez cette étape pour chaque nouvel appareil de série M de la configuration HA.

Les supports de disques de l'appareil M-100 sont incompatibles avec ceux de l'appareil M-500. Par conséquent, lors de la migration entre ces modèles de matériel, vous devez dévisser chaque disque de son ancien support et insérez le disque dans le nouveau support avant d'insérer le disque dans le nouvel appareil.

Vous devez maintenir la liaison de paire de disques. Bien que vous puissiez placer une paire de disques de l'emplacement A1/A2 de l'ancien appareil dans l'emplacement B1/B2 du nouvel appareil, vous devez conserver les disques ensemble dans le même emplacement ; dans le cas contraire, Panorama ne restaurera peut-être pas les données avec succès.

STEP 7 | Contactez le Support Client Palo Alto Networks pour copier les métadonnées du groupe de collecteurs depuis l'appareil de série M mis hors service vers le nouvel appareil de série M, puis relancez le processus mgmtsrvr.

STEP 8 | Si l'appareil de série M faisait partie d'un groupe de collecteurs, vérifiez que le numéro de série de l'appareil de série M désaffecté fait toujours partie du bon groupe de collecteurs :

`debug log-collector-group show name <nom du groupe de collecteurs de journaux>`

Si le numéro de série de l'appareil de série M mis hors service ne fait plus partie du bon groupe de collecteurs, les dossiers d'assistance technique ont mal été copiés à l'étape précédente. Contactez à nouveau l'assistance client de Palo Alto Networks pour copier les dossiers d'assistance technique à l'emplacement correct.

STEP 9 | Préparez les disques pour la migration.

La génération des métadonnées de chaque paire de disques recrée les index. Par conséquent, selon le volume de données, ce processus peut prendre beaucoup de temps. Afin d'accélérer le processus, vous pouvez lancer plusieurs sessions ILC et exécuter la commande de régénération des métadonnées dans chaque session pour terminer le processus simultanément pour chaque paire. Pour plus d'informations, consultez régénération des métadonnées pour les paires RAID des unités de Série M.

1. Activez les paires de disques en exécutant la commande ILC suivante pour chaque paire :

```
admin> request system raid add <slot> force no-format
```

Par exemple :

© 2020 Palo Alto Networks, Inc.

```
admin> request system raid add A1 force no-format
admin> request system raid add A2 force no-format
```

Les arguments **forçage**et **non-formatage** sont requis. L'argument **forçage** associe la paire de disques au nouvel appareil. L'argument **non-formatage** empêche le reformatage des disques et conserve les journaux stockés sur les disques.

2. Générez les métadonnées pour chaque paire de disques.

   Cette étape peut prendre un maximum de six heures, selon le volume des données des journaux qui sont contenues sur les disques.

```
admin> request metadata-regenerate slot <slot_number>
```

Par exemple :

```
admin> request metadata-regenerate slot 1
```

STEP 10 | Configurez le collecteur de journaux local sur le nouvel appareil de la série M.

Pour toutes les étapes avec des commandes nécessitant un numéro de série du dispositif, vous devez taper le numéro de série entier ; appuyer sur la touche TAB ne complétera pas un numéro partiel.

N'activez pas les disques sur le nouvel appareil de la série M à ce stade. Lorsque vous migrez les journaux avec succès, Panorama active automatiquement les disques.

1. Configurez le collecteur de journaux en tant que collecteur géré à l'aide de l'interface web de Panorama ou en utilisant les commandes ILC suivantes :

```
admin> configure
admin# set log-collector <log-collector_SN> deviceconfig system hostname
 <nnom d'hôte du collecteur de journaux>
admin# exit
```

2. Validez vos modifications sur Panorama. Ne pas valider tout de suite les modifications sur le groupe collecteur .

```
admin> configure
admin# commit
```

3. Vérifiez que le Collecteur de Journaux est connecté à Panorama et que le statut de ses paires de disques est présent/disponible.

```
admin> show log-collector serial-number <log-collector_SN>
```

Les paires de disques s'affichent comme étant désactivées à ce stade du processus de restauration.

STEP 11 | Ajoutez un collecteur de journaux sans disque à un groupe de collecteurs.

À partir de ce moment, seules les validations requises pour terminer le processus de migration sur Panorama et les collecteurs de journaux sont requises. Attendez avant de faire d'autres changements.

© 2020 Palo Alto Networks, Inc.

1. Accédez à l'ILC du nouvel appareil de série M.
2. Remplacez la restriction de Panorama pour permettre à un collecteur de journaux sans disque d'être ajouté à un groupe de collecteurs : **requestlog-migration-set-start**
3. Validez les modifications sur Panorama.

```
admin> configure
admin# commit force
```

STEP 12 | Migrez les journaux.

1. Accédez à l'ILC du nouvel appareil de série M.
2. Assignez le nouveau Collecteur de Journaux au groupe collecteur et validez vos modifications sur Panorama.

```
admin# set log-collector-group <collector_group_name> logfwd-setting
 collectors <collecteur_géré_SN>
admin# commit
admin# exit
```

   L'ancien collecteur de journal local apparaît encore dans la liste des membres, car vous ne l'avez pas supprimé de la configuration.
3. Pour chaque paire de disques, migrer les journaux vers le nouvel appareil.

```
admin> request log-migration from <old_LC_serial_number> old-disk-pair
 <paire de vieux disques> to <numéro de série du nouveau collecteur de
 journaux> new-disk-pair <paire de disques de journaux>
```

   Par exemple :

```
admin> request log-migration from 003001000010 old-disk-pair A to
 00300100038 new-disk-pair A
```

4. Validez les modifications sur Panorama.

```
admin> configure
admin# commit
```

STEP 13 | Reconfigurez le groupe de collecteurs

1. Se connecter à l'interface Web Panorama du nouvel appareil M-Series pour attribuer le nouveau Collecteur de journaux aux pare-feu qui transmettent les journaux (**Panorama** > **Collector Groups (Groupes de collecteurs)** > **Device Log Forwarding (Transfert du journal des périphériques)**). Donner au nouveau Collecteur de Journaux la même priorité dans les listes de préférence de pare-feu de l'ancien Collecteur de Journaux.

   Vous ne pouvez pas utiliser la CLI pour modifier les affectations de priorité des listes de préférences du pare-feu.
2. Accédez à l'ILC du nouvel appareil de série M.
3. Supprimer l'ancien Collecteur de Journaux du groupe collecteur.

© 2020 Palo Alto Networks, Inc.

```
admin# delete log-collector-group <group_name> logfwd-setting collectors
 <numéro de série de l'ancien collecteur de journaux>
```

Par exemple :

```
admin# delete log-collector-group DC-Collector-Group logfwd-setting
 collectors 003001000010
```

4. Supprimer l'ancien Collecteur de Journaux de la configuration de Panorama et valider vos modifications sur Panorama.

```
admin# delete log-collector <old_LC_serial_number>
admin# commit
admin# exit
```

5. Validez les modifications apportées au groupe de collecteurs pour que les pare-feu gérés puissent envoyer les journaux au nouveau collecteur de journaux.

```
admin> commit-all log-collector-config log-collector-
group <collector_group_name>
```

Par exemple :

```
admin> commit-all log-collector-config log-collector-group DC-Collector-
Group
```

STEP 14 | Générez de nouvelles clés sur le nouveau collecteur de journaux.

Cette commande est requise pour ajouter le nouveau collecteur de journaux au groupe de collecteurs et ne doit être exécutée que pour le groupe de collecteurs du collecteur de journaux en cours de remplacement. Cette étape supprime les clés RSA existantes et permet à Panorama de créer de nouvelles clés RSA.

1. Accédez à l'ILC du nouvel appareil de série M.
2. Supprimez toutes les clés RSA du nouveau collecteur de journaux :

   request logdb update-collector-group-after-replacecollector-group *<nom du groupe de collecteurs>*

   Le processus peut prendre jusqu'à 10 minutes.

STEP 15 | Confirmez que le statut de SearchEngine est Active (Actif) pour tous les collecteurs de journaux du groupe de collecteurs.

Ne continuez pas tant que le statut de SearchEngine n'est pas Active (Actif) pour tous les collecteurs de journaux du groupe de collecteurs. Cela entraînera la purge des journaux du collecteur de journaux en cours de remplacement.

1. Accédez à l'ILC du nouvel appareil de série M.
2. Affichez les détails du collecteur de journaux en exécutant les commandes suivantes :
   - Sur Panorama pour tous les collecteurs de journaux :

     show log-collector all

© 2020 Palo Alto Networks, Inc.

Vous pouvez également exécuter la commande suivante sur chaque collecteur de journaux dédié :

```
show log-collector detail
```

3. Confirmez que l'état de SearchEngine est Active (Actif).

```
Redistribution status:       none
```

```
Last commit-all: commit succeeded, current ring version 1
```

```
SearchEngine status:     Active
```

```
md5sum 4e5055a359f7662fab8f8c4f57e24525 updated at 2017/06/14 09:58:19
```

STEP 16 | Sur le nouveau collecteur de journaux, remplacez le numéro de série du collecteur de journaux précédent par le numéro de série du nouveau collecteur de journaux.

Vous devez remplacer le numéro de série de l'ancien collecteur de journaux par le numéro de série du nouveau collecteur de journaux afin que le nouveau collecteur de journaux ne s'exécute pas avec des problèmes de purge, ce qui empêcherait le collecteur de journaux de purger les anciennes données des journaux migrés.

1. Accédez à la CLI du collecteur de journaux.
2. Remplacez le numéro de série de l'ancien collecteur de journaux par le numéro de série du nouveau collecteur de journaux :

   request log-migration-update-logger from *<numéro de série de l'ancien collecteur de journaux>* to *<numéro de série du nouveau collecteur de journaux>*

STEP 17 | Configurez le nouvel homologue haute disponibilité Panorama secondaire.

1. Transmettre les journaux sur le SSD de l'ancien appareil de série M vers une destination externe si vous souhaitez les conserver.
2. Supprimer les disques RAID de l'appareil de la série M.
3. Effectuer la configuration initiale du nouvel appareil de série M.
4. Insérer les disques dans le nouvel appareil de la série M.
5. Répétez les étapes 7 à 16 pour migrer les journaux des anciens appareils de série M vers le nouvel appareil de série M.
6. Définir la HD (haute disponibilité) sur Panorama. Le nouvel appareil de la série M doit avoir la même priorité que l'homologue HD que vous remplacez.
7. Se connecter à l'interface Web Panorama de l'homologue HA principal et cliquez sur **Dashboard (Tableau de bord)** > **High Availability (Haute disponibilité)** > **Sync to peer (Synchroniser avec l'homologue)** pour synchroniser la configuration des homologues HD de l'appareil M-Series.

Migrer les journaux vers le même modèle d'appareil de la série M en Mode Panorama en haute disponibilité

Si vous devez remplacer un appareil M-600, M-500, M-200 ou M-100 déployé dans une configuration haute disponibilité en mode Panorama (serveur de gestion Panorama) par un appareil de série M du même

© 2020 Palo Alto Networks, Inc.

modèle, vous pouvez migrer les journaux qu'il collecte depuis les pare-feu en déplaçant ses disques RAID vers le nouvel appareil de série M. En déplaçant les disques, vous pouvez récupérer les journaux après l'échec d'un système sur l'appareil de série M.

Cette procédure de migration couvre les scénarios suivants :

- Un homologue HA Panorama a un collecteur géré (Collecteur de Journaux) dans un groupe de collecteurs.

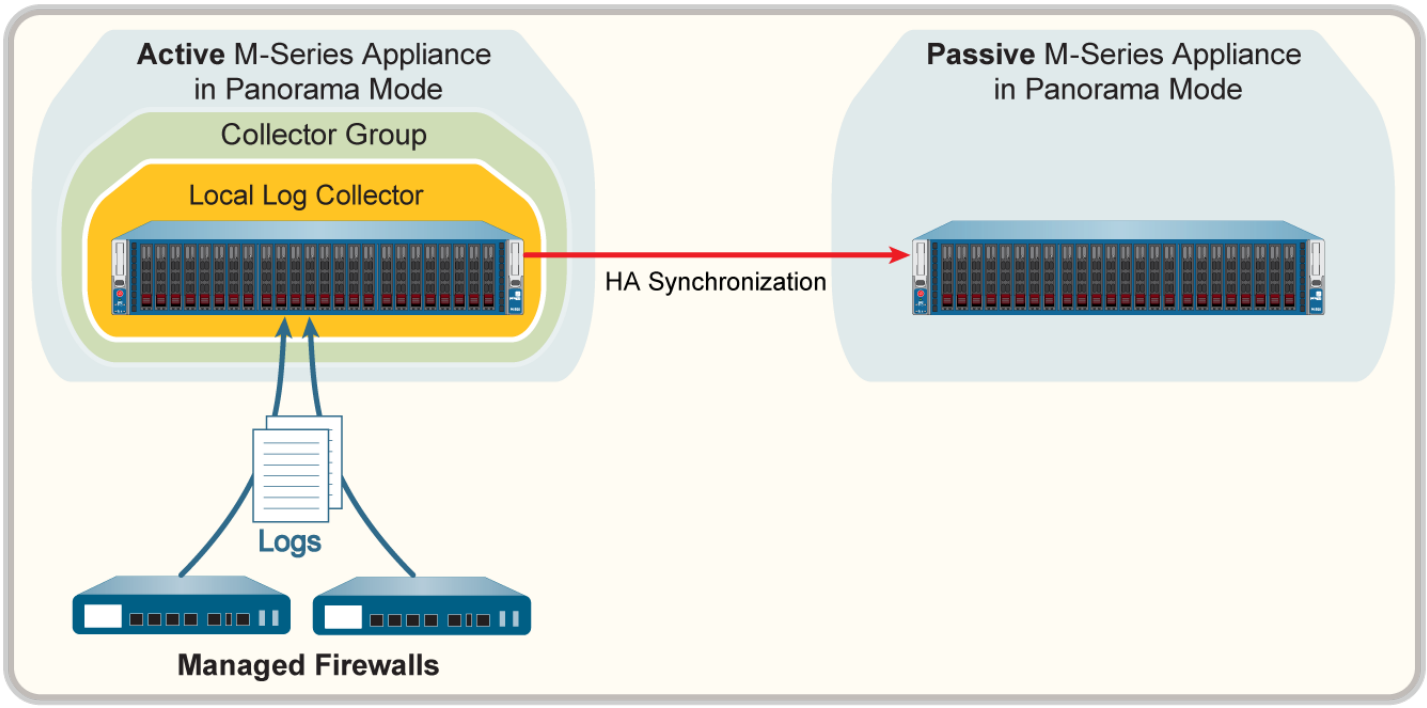


Figure 31: Homologue HD Panorama avec groupe de collecteurs

- Les deux homologues Panorama HD ont des collecteurs gérés qui appartiennent à un seul groupe de collecteurs. Pour plus de détails, consultez Plusieurs collecteurs de journaux locaux par groupe de collecteurs.
- Les deux homologues HD Panorama ont un collecteur géré et chacun est assigné à un groupe distinct de collecteurs. Pour plus de détails, consultez Collecteur de journaux local unique par groupe de collecteurs.

STEP 1 | Transmettre les journaux sur le SSD de l'ancien appareil de série M vers une destination externe si vous souhaitez les conserver.

Le SSD stocke les journaux système et de configuration que génèrent Panorama et les collecteurs de journaux. Vous ne pouvez pas déplacer le SSD entre les appareils de la série M.

Configurez le transfert des journaux de Panorama vers des destinations extérieures.

STEP 2 | Supprimez les disques RAID de l'appareil de la série M.

1. Mettez hors tension l'ancien appareil de la série M en appuyant sur le bouton d'alimentation jusqu'à ce que le système s'arrête.
2. Retirez les paires de disques. Pour plus d'informations, reportez-vous à la procédure de remplacement dans le Guide de Référence des appareils de la série-M.

STEP 3 | Effectuer la configuration initiale du nouvel appareil de série M.

© 2020 Palo Alto Networks, Inc.

1. Montez l'appareil de série M dans une baie. Se référer au Guide de référence du matériel de la série-M pour obtenir des instructions.
2. Effectuez la configuration initiale de l'appareil de série M.

   Si l'ancien appareil M-Series utilisait des interfaces autres que l'interface de gestion pour les services Panorama (tels que la collecte de journaux), vous devez définir ces interfaces lors de la configuration initiale du nouvel appareil M-Series (Panorama > Setup (Configuration) > Interfaces).
3. Enregistrez Panorama.
4. Achetez et activez une licence d'assistance Panorama ou transférez des licences comme suit uniquement si le nouvel appareil de la série M est du même modèle de matériel que l'ancien appareil de série M. Si le nouvel appareil de série M est un modèle différent de l'ancien appareil de série M, vous devez acheter de nouvelles licences.
   1. Connectez-vous au site web de support de Palo Alto Networks.
   2. puis cliquez Sélectionnez l'**Assets (Actif)** onglet puis cliquez **Spares (pièces de rechange)** lien.
   3. Cliquez sur le numéro de série du nouvel appareil de la série M.
   4. Cliquer**Transfer Licenses (Transférer les Licences)**.
   5. **Select (Sélectionnez)**le vieil appareil de la série M et cliquez sur **Submit (Soumettre)**.
5. Activer une licence de gestion de périphérique. Si vous effectuez la migration d'un appareil de M-100 à un appareil M-500, entrez le code d'identification associé à la licence de migration.
6. Installer les mises à jour de contenu et logicielles pour Panorama. Pour des informations importantes sur les versions logicielles, voir Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire.
7. Effectuez les changements de configuration supplémentaires qui s'avèrent nécessaires.

   Si l'ancien appareil M-Series utilisait des interfaces autres que l'interface de gestion pour les services Panorama (tels que la collecte de journaux), vous devez définir ces interfaces sur le nouvel appareil M-Series (Panorama > Setup (Configuration) > Interfaces)).
8. Définir la HD (haute disponibilité) sur Panorama. Le nouvel appareil de la série M doit avoir la même priorité que l'homologue HD que vous remplacez.

STEP 4 | Insérez les disques dans le nouvel appareil de la série M. Pour plus d'informations, reportez-vous à la procédure de remplacement dans le Guide de Référence des appareils de la série-M.

Les supports de disques de l'appareil M-100 sont incompatibles avec ceux de l'appareil M-500. Par conséquent, lors de la migration entre ces modèles de matériel, vous devez dévisser chaque disque de son ancien support et insérez le disque dans le nouveau support avant d'insérer le disque dans le nouvel appareil.

Vous devez maintenir la liaison de paire de disques. Bien que vous puissiez placer une paire de disques de l'emplacement A1/A2 de l'ancien appareil dans l'emplacement B1/B2 du nouvel appareil, vous devez conserver les disques ensemble dans le même emplacement ; dans le cas contraire, Panorama ne restaurera peut-être pas les données avec succès.

STEP 5 | Si l'appareil de série M faisait partie d'un groupe de collecteurs, vérifiez que le numéro de série de l'appareil de série M désaffecté fait toujours partie du bon groupe de collecteurs :

```
debug log-collector-group show name <nom du groupe de collecteurs de journaux>
```

STEP 6 | Préparez les disques pour la migration.

© 2020 Palo Alto Networks, Inc.

La génération des métadonnées de chaque paire de disques recrée les index. Par conséquent, selon le volume de données, ce processus peut prendre beaucoup de temps. Afin d'accélérer le processus, vous pouvez lancer plusieurs sessions ILC et exécuter la commande de régénération des métadonnées dans chaque session pour terminer le processus simultanément pour chaque paire. Pour plus d'informations, consultez régénération des métadonnées pour les paires RAID des unités de Série M.

1. Activez les paires de disques en exécutant la commande ILC suivante pour chaque paire :

```
admin> request system raid add <slot> force no-format
```

Par exemple :

```
admin> request system raid add A1 force no-format
admin> request system raid add A2 force no-format
```

Les arguments **forçage**et **non-formatage** sont requis. L'argument **forçage** associe la paire de disques au nouvel appareil. L'argument **non-formatage** empêche le reformatage des disques et conserve les journaux stockés sur les disques.

2. Générez les métadonnées pour chaque paire de disques.

```
admin> request metadata-regenerate slot <slot_number>
```

Par exemple :

```
admin> request metadata-regenerate slot 1
```

STEP 7 | Configurez le collecteur de journaux local sur le nouvel appareil de la série M.

Pour toutes les étapes avec des commandes nécessitant un numéro de série du dispositif, vous devez taper le numéro de série entier ; appuyer sur la touche TAB ne complétera pas un numéro partiel.

N'activez pas les disques sur le nouvel appareil de la série M à ce stade. Lorsque vous migrez les journaux avec succès, Panorama active automatiquement les disques.

1. Configurez le collecteur de journaux en tant que collecteur géré à l'aide de l'interface web de Panorama ou en utilisant les commandes ILC suivantes :

```
admin> configure
admin# set log-collector <log-collector_SN> deviceconfig system hostname
 <nnom d'hôte du collecteur de journaux>
admin# exit
```

2. Validez vos modifications sur Panorama. Ne pas valider tout de suite les modifications sur le groupe collecteur .

```
admin> configure
admin# commit
```

3. Vérifiez que le Collecteur de Journaux est connecté à Panorama et que le statut de ses paires de disques est présent/disponible.

© 2020 Palo Alto Networks, Inc.

```
admin> show log-collector serial-number <log-collector_SN>
```

Les paires de disques s'affichent comme étant désactivées à ce stade du processus de restauration.

STEP 8 | Ajoutez un collecteur de journaux sans disque à un groupe de collecteurs.

À partir de ce moment, seules les validations requises pour terminer le processus de migration sur Panorama et les collecteurs de journaux sont requises. Attendez avant de faire d'autres changements.

1. Accédez à la CLI de Panorama.
2. Remplacez la restriction de Panorama pour permettre à un collecteur de journaux sans disque d'être ajouté à un groupe de collecteurs : **request log-migration-set-start**
3. Validez la restriction remplacée :

```
admin> configure
admin# commit force
```

STEP 9 | Migrez les journaux.

1. Accédez à la CLI de Panorama.
2. Assignez le nouveau Collecteur de Journaux au groupe collecteur et validez vos modifications sur Panorama.

```
admin# set log-collector-group <collector_group_name> logfwd-setting
 collectors <collecteur_géré_SN>
admin# commit
admin# exit
```

L'ancien collecteur de journal local apparaît encore dans la liste des membres, car vous ne l'avez pas supprimé de la configuration.

3. Pour chaque paire de disques, migrer les journaux vers le nouvel appareil.

```
admin> request log-migration from <old_LC_serial_number> old-disk-pair
 <paire de vieux disques> to <numéro de série du nouveau collecteur de
 journaux> new-disk-pair <paire de disques de journaux>
```

Par exemple :

```
admin> request log-migration from 003001000010 old-disk-pair A to
 00300100038 new-disk-pair A
```

4. Validez les modifications sur Panorama.

```
admin> configure
admin# commit
```

STEP 10 | Reconfigurez le groupe de collecteurs

1. Utilisez l'interface Web pour attribuer le nouveau Collecteur de journaux aux pare-feu qui transmettent les journaux (**Panorama (Panorama)** > **Collector Groups (Groupes de Collecteurs)** > **Device Log Forwarding (Transfert du journal des périphériques)**). Donner au nouveau Collecteur

© 2020 Palo Alto Networks, Inc.

de Journaux la même priorité dans les listes de préférence de pare-feu de l'ancien Collecteur de Journaux.

Vous ne pouvez pas utiliser la CLI pour modifier les affectations de priorité des listes de préférences du pare-feu.

2. Supprimer l'ancien Collecteur de Journaux du groupe collecteur.

```
admin# delete log-collector-group <group_name> logfwd-setting collectors
 <numéro de série de l'ancien collecteur de journaux>
```

Par exemple :

```
admin# delete log-collector-group DC-Collector-Group logfwd-setting
 collectors 003001000010
```

3. Supprimer l'ancien Collecteur de Journaux de la configuration de Panorama et valider vos modifications sur Panorama.

```
admin# delete log-collector <old_LC_serial_number>
admin# commit
admin# exit
```

4. Synchroniser la configuration des paires HD de l'appareil de la série M.

```
admin> request high-availability sync-to-remote running-config
```

5. Validez les modifications apportées au groupe de collecteurs pour que les pare-feu gérés puissent envoyer les journaux au nouveau collecteur de journaux.

```
admin> commit-all log-collector-config log-collector-
group <collector_group_name>
```

Par exemple :

```
admin> commit-all log-collector-config log-collector-group DC-Collector-
Group
```

STEP 11 | Générez de nouvelles clés sur le nouveau collecteur de journaux.

Cette commande est requise pour ajouter le nouveau collecteur de journaux au groupe de collecteurs et ne doit être exécutée que pour le groupe de collecteurs du collecteur de journaux en cours de remplacement. Cette étape supprime les clés RSA existantes et permet à Panorama de créer de nouvelles clés RSA.

1. Accédez à la CLI de Panorama.
2. Supprimez toutes les clés RSA du nouveau collecteur de journaux :

   request logdb update-collector-group-after-replacecollector-group <nom du groupe de collecteurs>

   Le processus peut prendre jusqu'à 10 minutes.

STEP 12 | Confirmez que le statut de SearchEngine est Active (Actif) pour tous les collecteurs de journaux du groupe de collecteurs.

© 2020 Palo Alto Networks, Inc.

Ne continuez pas tant que le statut de SearchEngine n'est pas Active (Actif) pour tous les collecteurs de journaux du groupe de collecteurs. Cela entraînera la purge des journaux du collecteur de journaux en cours de remplacement.

1. Accédez à la CLI de Panorama.
2. Affichez les détails du collecteur de journaux en exécutant les commandes suivantes :
   - Sur Panorama pour tous les collecteurs de journaux :

     show log-collector all

     Vous pouvez également exécuter la commande suivante sur chaque collecteur de journaux dédié :

     ```
     show log-collector detail
     ```
3. Confirmez que l'état de SearchEngine est Active (Actif).

```
Redistribution status:       none
```

```
Last commit-all: commit succeeded, current ring version 1
```

```
SearchEngine status:     Active
```

```
md5sum 4e5055a359f7662fab8f8c4f57e24525 updated at 2017/06/14 09:58:19
```

STEP 13 | Sur le nouveau collecteur de journaux, remplacez le numéro de série du collecteur de journaux précédent par le numéro de série du nouveau collecteur de journaux.

Vous devez remplacer le numéro de série de l'ancien collecteur de journaux par le numéro de série du nouveau collecteur de journaux afin que le nouveau collecteur de journaux ne s'exécute pas avec des problèmes de purge, ce qui empêcherait le collecteur de journaux de purger les anciennes données des journaux migrés.

1. Accédez à la CLI du collecteur de journaux.
2. Remplacez le numéro de série de l'ancien collecteur de journaux par le numéro de série du nouveau collecteur de journaux :

   request log-migration-update-logger from *<numéro de série de l'ancien collecteur de journaux>* to *<numéro de série du nouveau collecteur de journaux>*

Migrer les collecteurs de journaux après défaillance/RMA de Panorama non-HD

En cas de défaillance du système sur un serveur de gestion de Panorama qui n'est pas déployé dans une configuration de haute disponibilité (HD), utilisez cette procédure pour restaurer la configuration sur le Panorama de remplacement et rétablissez l'accès aux journaux sur les collecteurs de journaux dédiés qu'il gère. Les scénarios de migration autorisés varient selon le modèle du serveur de gestion Panorama :

© 2020 Palo Alto Networks, Inc.

Panorama ancien/échoué	Nouveau/panorama de remplacement
Appareil virtuel Panorama	• Appareil virtuel Panorama • Appareil M-200 • Appareil M-500 • Appareil M-600
Appareil M-100	• Appareil virtuel Panorama • Appareil M-200 • Appareil M-500 • Appareil M-600
Appareil M-500	• Appareil virtuel Panorama • Appareil M-200 • Appareil M-500 • Appareil M-600

Panorama gère un fichier porte-clés qui mappe les segments et les partitions des collecteurs de journaux dédiés utilisés pour stocker les journaux. Un appareil de la série M en mode Panorama stocke le fichier porte-clés sur son disque flash SSD interne ; un appareil virtuel Panorama stocke le fichier porte-clés sur son disque interne. Lorsqu'une panne se produit, un Panorama non-HD ne peut pas récupérer automatiquement le fichier porte-clés. Par conséquent, lorsque vous remplacez Panorama, vous devez restaurer le fichier porte-clés pour accéder aux journaux sur les collecteurs de journaux dédiés.

Cette procédure requiert que vous ayez sauvegardé et exporté votre configuration de Panorama *avant que la défaillance du système ne se soit produite.*

Palo Alto Networks recommande le déploiement Panorama dans une configuration HD. L'homologue actif Panorama synchronise automatiquement le fichier porte-clés à l'homologue passif dans une configuration HD, ce qui maintient l'accès aux journaux sur les collecteurs de journaux dédiés, même si vous devez remplacer l'un des homologues.

STEP 1 | Effectuez la configuration initiale du nouvel appareil Panorama.

1. Configuration de l'appareil de série M ou Configurez l'appareil virtuel Panorama selon vos besoins. Si vous faites la configuration d'une nouvelle configuration de la série M, référez-vous à Se référer au Guide de référence du matériel de la série-M pour obtenir des instructions pour savoir comment monter en rack le nouvel appareil M-Series.
2. Effectuez la configuration initiale de l'appareil de Série M ou effectuez une configuration initiale de l'appareil virtuel Panorama virtuel.

   Si l'ancien appareil M-Series utilisait des interfaces autres que l'interface de gestion pour les services Panorama (tels que la collecte de journaux), vous devez définir ces interfaces lors de la configuration initiale *du nouvel appareil M-Series (Panorama > Setup (Configuration) > Interfaces). L'appareil virtuel Panorama ne prend pas en charge les interfaces autres que MGT.*
3. Enregistrez Panorama.
4. Transférez les licences comme suit uniquement si le nouvel appareil Panorama est du même modèle que l'ancien appareil. Dans le cas contraire, vous devez acheter de nouvelles licences.
   1. Connectez-vous au site web de support de Palo Alto Networks.

© 2020 Palo Alto Networks, Inc.

2. puis cliquez Sélectionnez l'**Assets (Actif)** onglet puis cliquez **Spares (pièces de rechange)** lien.
3. Cliquez sur le numéro de série du nouvel appareil de la série M.
4. Cliquer**Transfer Licenses (Transférer les Licences)**.
5. **Select (Sélectionnez)** l'ancien appareil, puis cliquez sur **Submit (Soumettre)**.

5. Activer une licence d'assistance Panorama.
6. Activer une licence de gestion de périphérique.
7. Installer les mises à jour de contenu et logicielles pour Panorama.

L'appareil de M-500 nécessite Panorama 7.0 ou une version ultérieure. Les appareils M-200 et M-600 nécessitent Panorama 8.1. Pour des informations importantes sur les versions logicielles, voir Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire.

STEP 2 | Restaurez la configuration de l'ancien Panorama sur le Panorama de remplacement.

1. Connectez-vous au nouveau Panorama et sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)**.
2. Cliquez sur **Import named Panorama configuration snapshot (Importer un snapshot de configuration nommé Panorama)**, **Browse (Rechercher)** le fichier enregistré, puis cliquez sur **OK (OK)**.
3. Cliquez sur **Load named Panorama configuration snapshot (Charger un instantané de configuration nommé Panorama)**, sélectionnez le **Name (Nom)** du fichier que vous venez d'importer et cliquez sur **OK**.

   Pour remplacer une RMA Panorama, assurez-vous de Retain Rule UUIDs (Conserver les UUID des règles) lorsque vous chargez l'instantané de configuration Panorama. Si vous ne sélectionnez pas cette option, Panorama supprime tous les UUID des règles précédents de l'instantané de configure et affecte de nouveaux UUID aux règles sur Panorama, ce qui signifie qu'il ne conserve pas les informations associées aux UUID antérieurs, comme le nombre de correspondance à la règle de politique.
4. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.
5. Sélectionnez **Panorama (Panorama)** > **Managed Collectors (collecteurs gérés)** et vérifiez que la colonne connectée affiche une case à cocher pour le collecteur de journaux dédié.

   Si le collecteur de journaux dédié n'apparaît pas, vous devez le reconfigurer, lui et son groupe de collecteurs comme décrit à l'étape suivante. Sinon, passez à l'étape Extraire le fichier porte-clé pour restaurer l'accès aux journaux stockés sur le collecteur de journaux dédié.

STEP 3 | Configurez le collecteur de journaux dédié et le groupe collecteur s'ils manquent sur Panorama.

1. Accédez à l'ILC du collecteur de journaux dédié et entrez les commandes suivantes pour afficher le nom de son groupe de collecteurs.
   1. Saisissez la commande suivante :

      ```
      > request fetch ring from log-collector <serial_number>
      ```

      Le message d'erreur suivant s'affiche :

      ```
      Server error: Failed to fetch ring info from <serial_number>
      ```
   2. Saisissez la commande suivante :

      ```
      > less mp-log ms.log
      ```


© 2020 Palo Alto Networks, Inc.

Le message d'erreur suivant s'affiche :

```
Dec04 11:07:08 Error:
 pan_cms_convert_resp_ring_to_file(pan_ops_cms.c:3719): Current
 configuration does not contain group CA-Collector-Group
```

Dans cet exemple, le message d'erreur indique que le groupe Collector manquant porte le nom de "groupe collecteur CA".

2. Configurer le groupe de collecteur et affectez-lui le Collecteur de Journaux dédié.

```
> configure
# set log-collector-group <collector-group-name>
# set log-collector-group <collector-group-name> logfwd-setting
collector <numéro-de-série>
```

3. Valider les modifications apportées dans Panorama, mais pas dans le groupe collecteur.

```
# commit
# exit
```

STEP 4 | Extraire le fichier porte-clé pour restaurer l'accès aux journaux stockés sur le collecteur de journaux dédié.

1. Accéder à l'ILC du nouveau Panorama.
2. Extraire le fichier porte-clés :

```
> request fetch ring from log-collector <serial-number>
```

Par exemple :

```
> request fetch ring from log-collector 009201000343
```

Si vous ne connaissez pas le numéro de série du collecteur de journaux dédié, connectez-vous à son ILC et entrez la commande opérationnelle ***montrer les informations système***

3. Validez vos modifications sur le groupe de collecteurs

```
> commit-all log-collector-config log-collector-group <collector-group-
name>
```

Régénérer les métadonnées pour les appareils de la série M en paires RAID

Lorsqu'une défaillance du système se produit sur l'appareil M-600, M-500 ou M-200 et que vous devez déplacer physiquement les disques d'un appareil à un autre, il est nécessaire de régénérer les métadonnées. Les métadonnées sont nécessaires pour localiser les journaux sur le disque ; Lorsqu'un utilisateur émet une requête de journal, la requête consulte ces métadonnées pour accéder aux données demandées.

Pour chaque paire de disques configurée en RAID dans l'appareil de la série M, vous devez accéder à l'application ILC et exécuter la commande suivante pour régénérer les métadonnées :

© 2020 Palo Alto Networks, Inc.

```
> request metadata-regenerate slot <slot_number>
```

Par exemple :

```
> request metadata-regenerate slot 1
```

La taille des disques RAID détermine combien de temps la régénération des métadonnées prend. En moyenne, il faut une heure par 100 Go. Lorsque vous exécutez la commande, la session ILC est verrouillée jusqu'à ce que la commande soit entièrement exécutée . Vous pouvez utiliser plusieurs sessions ILC pour gagner du temps. Par exemple, pour remplacer quatre paires RAID de disques de 1 To avec un total de 4 To de données de journaux, lancez quatre sessions ILC et exécutez la commande dans chaque session pour régénérer simultanément les métadonnées pour toutes les paires / emplacements en environ 10 heures.

Pendant la régénération de métadonnées, le collecteur de groupe auquel appartiennent ces disques n'est pas disponible, et la paire de disque n'est pas disponible pour n'importe quel enregistrement ou déclaration d'opérations (écrit/requêtes). Toutefois, vous pouvez effectuer d'autres tâches telles que la manutention de nouvelles connexions de pare-feu ou de gestion des modifications de configuration sur les pare-feu gérés. Tous les autres groupes de collecteurs que Panorama gère et qui ne font pas partie de ce processus RMA peuvent effectuer normalement la fonctionnalité de journalisation et de création de rapports assignée.

Afficher les tâches de requête de journaux

Vous pouvez afficher les tâches de vos requêtes de journaux pour les examiner et mieux comprendre pourquoi l'interrogation des données des journaux demande plus de temps que prévu. Pour commencer, vous devez afficher toutes les tâches de requête de journaux sur Panorama. Après avoir identifié la tâche de requête de journaux que vous devez examiner, utilisez l'ID de la tâche pour afficher des informations détaillées sur la requête afin de mieux comprendre pourquoi la requête de journaux pose problème. Lorsque l'on interroge les donnés des journaux sur Panorama, les informations d'ID de la tâche détaillées sont effacées lorsque les nouvelles tâches de requête de journaux sont exécutées.

STEP 1 | Connectez-vous à l'ILC Panorama.

STEP 2 | Affichez les tâches de requête de journaux exécutées dans Panorama.

Le résultat CLI comprend les informations générales de chaque requête de journaux exécutée comme l'ID de la tâche lorsque la requête a été lancée, l'état de la requête, le base de données de journaux qui a été interrogée, le nombre de journaux interrogés, la durée (en ms) nécessaire pour que la requête renvoie les résultats, l'administrateur qui a exécuté la requête et les filtres appliqués à la requête.

```
admin@Panorama> show query jobs
```


© 2020 Palo Alto Networks, Inc.

```
admin@bingdot34> show query jobs

ID        Enqueue Time         State       Database  nlogs     Runtime(ms)    Us
er            Filter
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
42        2020/01/02 14:35:46  COMPLETE    threat    110       166.27         ad
min           ((((receive_time leq 'now')) and (((subtype eq 'file')) or ((subty
pe eq 'data')))) and ((receive_time in 'last-hour')))


41        2020/01/02 14:35:46  COMPLETE    system    110       163.84         ad
min           (((receive_time leq now)) and (receive_time in last-hour))

40        2020/01/02 14:35:46  COMPLETE    config    110       158.23         ad
min           (((receive_time leq now)) and (receive_time in last-hour))

39        2020/01/02 14:35:36  COMPLETE    config    110       162.58         ad
min           (((receive_time leq now)) and (receive_time in last-hour))

38        2020/01/02 14:35:36  COMPLETE    system    110       172.68         ad
min           (((receive_time leq now)) and (receive_time in last-hour))

37        2020/01/02 14:35:36  COMPLETE    threat    110       188.80         ad
min           ((((receive_time leq 'now')) and (((subtype eq 'file')) or ((subty
pe eq 'data')))) and ((receive_time in 'last-hour')))
```

STEP 3 | Affichez les détails des informations de la requête des journaux au sujet d'une tâche spécifique en utilisant l'ID de la tâche.

```
admin@Panorama> show query jobid <Job ID>
```

```
admin@bingdot34> show query jobid 42

Serial          ID        State     Num Req   Num Proc  RTT(Max)      Avg Recs/R
TTSoftware Ver    CG                                Last Update Time
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
LOGDB           42        DONE      110       0         0.00      0.00
9.2.0           LOCAL                             2020/01/02 14:35:46

PODABCD12       42        FAILED    110       0         0.00      0.00
9.2.0           PODABCD12                         2020/01/02 14:35:46
```


© 2020 Palo Alto Networks, Inc.

Remplacement d'un pare-feu RMA

Pour réduire les efforts nécessaires à la restauration de la configuration sur un pare-feu géré impliquant une RMA (Authorisation de Retour de Marchandise), vous pouvez remplacer le numéro de série de l'ancien pare-feu par celui du nouveau pare-feu ou du pare-feu de remplacement sur Panorama. Pour restaurer ensuite la configuration sur le pare-feu de remplacement, vous pouvez soit importer l'état de pare-feu que vous avez préalablement généré et exporté depuis le pare-feu, soit utiliser Panorama pour générer un *un état partiel de périphérique* pour les pare-feux gérés exécutant PAN-OS 5.0 et versions ultérieures. En remplaçant le numéro de série et en important l'état de périphérique, vous pouvez reprendre la gestion du pare-feu à l'aide de Panorama.

- Génération d'état de périphérique partiel pour les pare-feux
- Avant de commencer le remplacement d'un pare-feu RMA
- Restauration de la configuration du pare-feu après un remplacement

Génération d'état de périphérique partiel pour les pare-feux

Lorsque vous utilisez Panorama pour générer un état de périphérique partiel, il réplique la configuration des pare-feu gérés avec quelques exceptions pour les configurations VPN à grande échelle (LSVPN). Vous créez l'État partiel de périphérique en combinant deux facettes de la configuration du pare-feu :

- La configuration centralisée gérée par Panorama — Panorama maintient un instantané des règles de stratégie partagées et des modèles qu'il déplace aux pare-feux.
- Configuration locale sur le pare-feu — lorsque vous validez un changement de configuration sur un pare-feu, il envoie une copie de son fichier de configuration local à Panorama. Panorama stocke ce fichier et l'utilise pour compiler l'ensemble d'état partiel de périphérique.



Dans une configuration LSVPN, l'ensemble d'état de périphérique partiel que vous générez sur Panorama n'est pas le même que sur la version que vous pouvez exporter d'un pare-feu (en sélectionnant Device (Périphérique) > Setup(Configuration) > Operations (Opérations) et en cliquant sur Export device state (Exporter l'état du périphérique)). Si vous avez exécuté manuellement l'exportation d'état de périphérique ou si vous avez programmé un script d'API XML pour exporter le fichier vers un serveur distant, vous pouvez utiliser l'état de périphérique exporté dans le flux de travail de remplacement de votre pare-feu.

Si vous n'avez pas exporté l'état de l'appareil, l'état de l'appareil que vous générez dans le flux de travail de remplacement n'inclut pas les informations de configuration dynamique, telles que les détails du certificat et les pare-feux enregistrés, nécessaires pour restaurer la configuration complète d'un pare-feu en tant que Portail LSVPN. Pour plus d'informations, reportez-vous à la section Avant de commencer le remplacement d'un pare-feu RMA*.*

Panorama ne stocke pas l'état de périphérique ; vous le générez sur demande à l'aide des commandes de la CLI répertoriées dans Restauration de la configuration du pare-feu après un remplacement.

Avant de commencer le remplacement d'un pare-feu RMA

- ❑ Le pare-feu que vous remplacez doit avoir Pan-OS 5.0.4 ou une version ultérieure. Panorama ne peut pas générer l'*état du périphérique* pour des pare-feux exécutant des versions antérieures de PAN-OS .
- ❑ Enregistrez les détails suivants sur le pare-feu que vous remplacez :
  - **Numéro de série** : vous devez entrer le numéro de série sur le site web du Support Client de Palo Alto Networks pour transférer les licences de l'ancien pare-feu au pare-feu de remplacement. Vous

© 2020 Palo Alto Networks, Inc.

saisirez également cette information sur Panorama, pour remplacer toutes les références à l'ancien numéro de série par le numéro de série du pare-feu de remplacement.

- (Recommandé) **Version de PAN-OS et version de la base de données de contenu** : l'installation des mêmes versions du logiciel et de la base de données de contenu, notamment l'URL du fournisseur de la base de données, vous permet de créer le même état sur le pare-feu de remplacement. Si vous décidez d'installer la dernière version de la base de données de contenu, il se peut que vous remarquiez les différences en raison des mises à jour et des ajouts à la base de données. Pour vérifier les versions installées sur le pare-feu, accédez aux journaux système du pare-feu, stockés sur Panorama.

- Préparez le pare-feu de remplacement pour le déploiement. Avant d'importer le bundle d'état de périphérique et de restaurer la configuration, vous devez :
  - Vérifier que le pare-feu de remplacement est du même modèle et est activé pour des fonctionnalités opérationnelles similaires. Considérez les fonctions opérationnelles suivantes : faut-il que le pare-feu de remplacement ait plusieurs systèmes virtuels, supporte les cadres Jumbo, ou fonctionne en mode CC ou FIPS ?
  - Configurez un accès réseau, transférez les licences et installez la version PAN-OS appropriée et la version de base de données du contenu .
- Vous devez utiliser l'ILC de Panorama pour compléter ce processus de remplacement du pare-feu, et votre compte administrateur doit donc avoir le rôle de super-utilisateur ou d'administrateur Panorama.
- Si vous disposez d'une configuration LSVPN et remplacez un pare-feu Palo Alto Networks déployé en tant que périphérique satellite ou en tant que portail LSVPN, les informations de configuration dynamique requises pour restaurer la connectivité LSVPN ne seront pas disponibles lorsque vous restaurerez l'état de périphérique partiel généré sur Panorama. Si vous avez suivi la recommandation selon laquelle il faut fréquemment générer et exporter l'état de périphérique pour les pare-feux dans une configuration LSVPN, utilisez l'état de périphérique que vous avez déjà exporté depuis le pare-feu lui-même au lieu d'en générer un sur Panorama.

  Si vous n'avez pas exporté manuellement l'état du périphérique depuis le pare-feu et que vous deviez générer un état partiel de périphérique sur Panorama, la configuration dynamique manquante a un impact sur le processus de remplacement de pare-feu comme suit :

  - **Si le pare-feu que vous remplacez est un portail GlobalProtect** qui est explicitement configuré avec le numéro de série des satellites (**Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > **Satellite Configuration (Configuration Satellite)**), lors de la restauration de la configuration du pare-feu, bien que la configuration dynamique soit perdue, le pare-feu du portail pourra authentifier les satellites avec succès. Une authentification réussie renseignera les informations de configuration dynamique et la connectivité LSVPN sera rétablie.
  - **Si vous remplacez un pare-feu satellite**, il ne sera pas en mesure de se connecter et de s'authentifier auprès du portail. Cet échec de connexion se produit parce que le numéro de série n'a pas été explicitement configuré sur le pare-feu (**Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > **Satellite Configuration (Configuration satellite)**) ou parce que, bien que le numéro de série ait été configuré de façon explicite, le numéro de série du pare-feu remplacé ne correspond pas à celui de l'ancien pare-feu. Pour restaurer la connectivité, après avoir importé l'ensemble d'état de périphérique, l'administrateur du satellite doit se connecter au pare-feu et saisir les informations d'authentification (nom d'utilisateur et mot de passe) pour s'authentifier sur le portail. Lorsque l'authentification a lieu, la configuration dynamique requise pour la connectivité LSVPN est générée sur le portail.

  Cependant, si le pare-feu a été configuré en haute disponibilité, après la restauration de la configuration, le pare-feu synchronise automatiquement la configuration en cours avec son homologue et obtient la dernière configuration dynamique requise pour fonctionner sans problème.

© 2020 Palo Alto Networks, Inc.

Restauration de la configuration du pare-feu après un remplacement

Pour restaurer la configuration du pare-feu sur le nouveau pare-feu, vous devez d'abord effectuer la configuration initiale sur le nouveau pare-feu, y compris la définition du mode opérationnel, la mise à niveau du logiciel Pan-OS et la version du contenu pour correspondre à ce qui était installé sur l'ancien pare-feu. Vous exportez ensuite l'état du périphérique de l'ancien pare-feu depuis Panorama et l'importez sur le nouveau pare-feu. Enfin, vous allez revenir à Panorama pour valider que le nouveau pare-feu est connecté, puis le synchroniser avec panorama.

STEP 1 | Effectuez la configuration initiale sur le nouveau pare-feu et vérifiez la connectivité réseau.

Utilisez un port série ou une connexion Secure Shell (SSH) pour ajouter une adresse IP, une adresse IP de serveur DNS, et pour vérifier que le pare-feu peut accéder au serveur de mises à jour de Palo Alto Networks.

STEP 2 | (Facultatif) Définissez le mode opérationnel sur le nouveau pare-feu pour qu'il corresponde à celui de l'ancien pare-feu.

Une connexion de port série est nécessaire pour cette tâche.

1. Saisissez l'interface de ligne de commande pour accéder au mode de maintenance sur le pare-feu :

```
> debug system maintenance-mode
```

2. Pour le mode opérationnel, sélectionnez **définir le mode FIPS** ou **réglez le mode CCEAL 4** à partir du menu principal.

STEP 3 | Récupérez la ou les licences sur le nouveau pare-feu.

Saisissez la commande suivante pour extraire les licences :

```
> request license fetch
```

STEP 4 | (Facultatif) Faites correspondre l'état opérationnel du nouveau pare-feu à celui de l'ancien pare-feu. Par exemple, activez la fonction de systèmes virtuels multiples (multi-vsys) pour un pare-feu compatible avec la fonction de systèmes virtuels multiples.

Saisissez les commandes correspondant à vos paramètres de pare-feu :

```
> set system setting multi-vsys on
> set system setting jumbo-frame on
```

STEP 5 | Mettez à jour la version de PAN-OS sur le nouveau pare-feu.

Vous devez mettre à niveau vers les mêmes versions de PAN-OS installées sur l'ancien pare-feu. Vous devez mettre à niveau vers les mêmes versions de contenu qui étaient installées sur l'ancien pare-feu.

Entrez les commandes suivantes :

1. Pour mettre à niveau la version de base de données de contenu :

```
> request content upgrade download latest
> request content upgrade install version latest
```

2. Pour mettre à niveau la version de l'anti-virus de contenu :

© 2020 Palo Alto Networks, Inc.

```
> request anti-virus upgrade download latest
> request anti-virus upgrade install version latest
```

3. Pour mettre à niveau la version du logiciel PAN-OS :

```
> request system software download version <version>
> request system software install version <version>
```

STEP 6 | Accédez à l'ILC de Panorama et exportez le module d'état de périphérique depuis l'ancien pare-feu vers un ordinateur à l'aide de la copie sécurisée (SCP) ou TFTP (vous ne pouvez pas le faire à partir de l'interface Web).

Si vous avez exporté manuellement l'état du périphérique à partir du pare-feu, vous pouvez ignorer cette étape.

La commande d'exportation génère un ensemble d'état de périphérique en tant que fichier compressé et l'exporte vers l'emplacement spécifié. Cet état de périphérique n'inclut pas la configuration dynamique LSVPN (information satellite et détails de certificat).

Effectuez l'une des étapes suivantes :

```
> scp export device-state device <old serial#> to <connexion> @ <IP-du-serveur>: <chemin>
```

OU

```
> tftp export device-state device <old serial#> to <connexion> @ <IP-du-serveur>: <chemin>
```

STEP 7 | Remplacez le numéro de série de l'ancien pare-feu par celui du nouveau pare-feu de remplacement sur Panorama.

En remplaçant le numéro de série sur Panorama, vous permettez au nouveau pare-feu de se connecter à Panorama une fois la configuration restaurée sur le pare-feu.

1. Entrez la commande suivante en mode opérationnel :

```
> replace device old <old SN#> new <nouveau SN#>
```

2. Passer en mode Configuration et valider vos modifications.

```
> configure
# commit
```

3. Quitter le mode Configuration.

```
# exit
```

STEP 8 | Sur le nouveau pare-feu, importez l'état de périphérique et validez les modifications.

1. Accédez à l'interface Web du pare-feu géré.

© 2020 Palo Alto Networks, Inc.

2. Sélectionnez **Device (périphérique)** > **Setup (Configuration)** > **Operations (Opérations)** et cliquez sur le lien **Import Device State (Importer un état de périphérique)** dans la section Gestion de la configuration.
3. Naviguez pour localiser le fichier, puis cliquez sur **OK**.
4. **Commit (Validez)** vos modifications dans la configuration actuelle du pare-feu.

STEP 9 | À partir de panorama, vérifiez que vous avez restauré avec succès la configuration du pare-feu.

1. Accédez à l'interface Web Panorama et sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)**.
2. Vérifiez que la colonne connectée pour le nouveau pare-feu est activée.

STEP 10 | Synchroniser le pare-feu avec Panorama.

1. Accédez à l'interface Web Panorama, sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** et **Edit Selections (Modifier les sélections)** dans la portée d'application.
2. Sélectionnez **Device Groups (Groupes de périphériques)**, sélectionnez le groupe de périphériques contenant le pare-feu et **Include Device and Network Templates (Inclure les modèles de périphérique et de réseau)**.
3. Sélectionnez **Collector Groups (Groupes de collecteurs)** et sélectionnez le groupe de collecteurs qui contient le pare-feu.
4. Cliquez sur **OK** pour enregistrer les modifications dans la portée d'application.
5. **Commit and Push (Validez et appliquez)** vos modifications.



Si vous avez besoin de générer des rapports sur une période qui englobe le temps où l'ancien pare-feu était fonctionnel, et après l'installation du pare-feu de remplacement, vous devez générer une demande distincte pour chaque numéro de série de chaque pare-feu car le remplacement du numéro de série sur Panorama n'écrase pas les informations présentes dans les journaux.

© 2020 Palo Alto Networks, Inc.

Dépanner des échecs de validation

Si des échecs d'opérations d'application ou de validation se produisent sur le Panorama, vérifiez les conditions suivantes :

Symptôme	Condition	Résolution
Échec d'application au groupe de modèles ou de périphériques	La possibilité de recevoir des modifications de configuration de modèle de groupes et de dispositifs de Panorama est désactivée sur le pare-feu.	Accédez à l'interface web du pare-feu, sélectionnez **Device (périphérique)** > **Setup (Configuration)**, modifiez les paramètres de Panorama, puis cliquez sur **Enable Device and Network Template (Activer le périphérique et le modèle de réseau)** et **Enable Panorama Policy and Objects (activer la politique et les objets Panorama)**.
Échec de validation de Panorama ou échec d'application au modèle, groupe de périphériques ou groupe de collecteurs	Le serveur de gestion Panorama possède une version antérieure du logiciel que les collecteurs de journaux dédiés ou de pare-feux qu'il gère.	Mettre à niveau le serveur de gestion Panorama à la même version ou une version plus élevée que les pare-feu gérés, les collecteurs de journaux, les appareils et les clusters d'appareils WildFire. Pour plus d'informations, reportez-vous à la section Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire.

© 2020 Palo Alto Networks, Inc.

Résoudre les problèmes d'enregistrement ou erreurs de numéro de série

Sur l'appareil M-500 ou M-200, si la page de **Panorama (Panorama)** > **Support (Support)** n'indique pas les détails de la licence de support ou que la page **Panorama (Panorama)** > **Setup (Configuration)** > **Management (Gestion)** affiche inconnu pour le **Serial Number (numéro de série)**, même après avoir enregistré Panorama, procédez comme suit :

STEP 1 | Enregistrer le numéro de série du Panorama depuis le courriel d'exécution d'ordre que Palo Alto Networks vous a envoyé lorsque vous avez passé votre commande de Panorama.

STEP 2 | Sélectionnez **Panorama (Panorama)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les Paramètres Généraux.

STEP 3 | Entrez le **Serial Number (Numéro de série)** et cliquez sur **OK**.

STEP 4 | Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

© 2020 Palo Alto Networks, Inc.

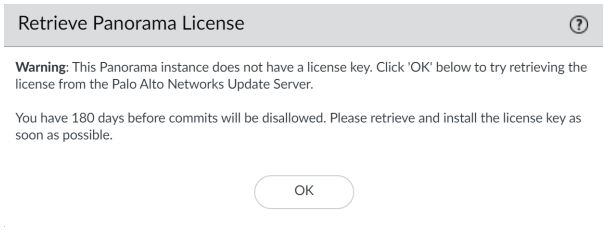
Dépannage des erreurs de déclaration

Si Panorama échoue à générer un rapport, ou que le rapport manque des données attendues, ses versions de contenu (par exemple, la base de données Applications) peuvent différer de celles des collecteurs gérés et des pare-feu. Les versions de contenu sur Panorama doivent être égales ou plus inférieures aux versions de contenu sur les collecteurs gérés et les pare-feu. Pour plus d'informations, reportez-vous à la section Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire.

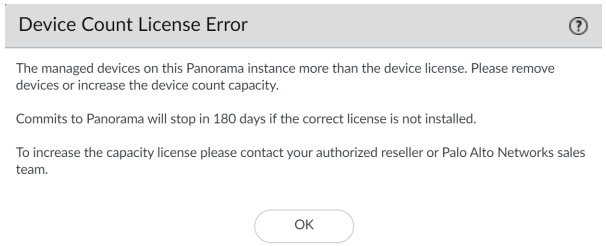
© 2020 Palo Alto Networks, Inc.

Résoudre les erreurs de licence de gestion des périphériques

À l'issue de la mise à niveau vers PAN-OS 8.1, l'appareil virtuel Panorama vérifie si une licence de gestion de périphérique a été correctement installée. Si une licence de gestion de périphérique n'a pas été installée avec succès ou si le nombre de pare-feu gérés par l'appareil virtuel Panorama dépasse la limite de licences de gestion de périphériques permise, vous disposez de 180 jours pour installer une licence de gestion de périphériques valide. Si aucune licence de gestion de périphériques valide n'a été installée, l'alerte suivante s'affiche chaque fois que vous vous connectez à l'interface Web de Panorama :



Si le nombre de pare-feu gérés par l'appareil virtuel Panorama dépasse la limite de licence de gestion de périphériques permise, les alertes suivantes apparaissent chaque fois que vous vous connectez à l'interface Web de Panorama :



Pour résoudre ce problème, vous devez enregistrer une licence de gestion de périphériques valide :

STEP 1 | Contactez votre représentant commercial Palo Alto Networks ou votre revendeur agréé pour acheter la licence de gestion de périphériques appropriée.

STEP 2 | Connectez-vous à l'interface Web Panorama.

STEP 3 | Activer / Récupérer une licence de gestion de périphérique selon que l'appareil virtuel Panorama est en ligne ou hors ligne.

- Activer / Récupérer une licence de gestion de pare-feu lorsque l'appareil virtuel Panorama est connectée à Internet.
- Activer / Récupérer une licence de gestion de pare-feu lorsque l'appareil virtuel Panorama n'est pas connecté à Internet.

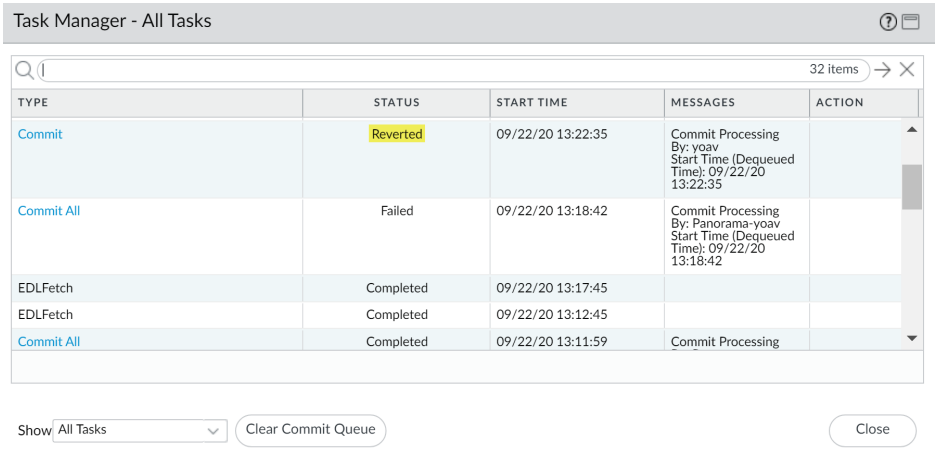
© 2020 Palo Alto Networks, Inc.

Dépannage des configurations de pare-feu automatiquement inversées

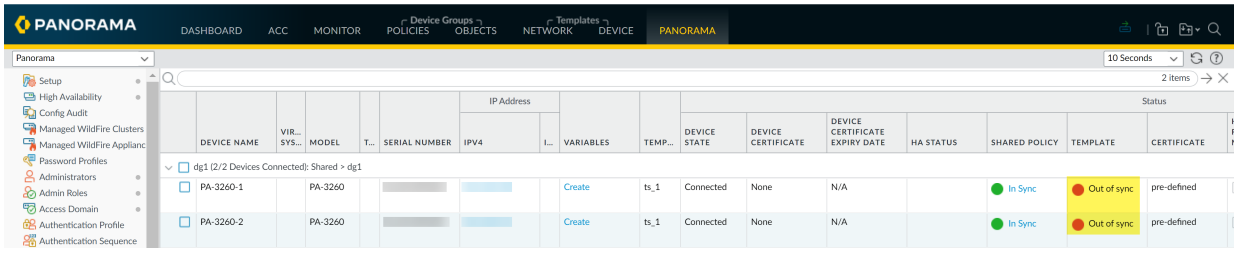
Si votre pare-feu géré fait un retour automatique de sa configuration à la suite d'un changement qui a provoqué l'interruption d'une connexion entre le serveur de gestion Panorama™ et le pare-feu, vous pouvez dépanner les pare-feux désynchronisés afin de déterminer les changements apportés et quels aspects de cette dernière modification de configuration ont provoqué le retour du pare-feu à sa configuration.

STEP 1 | Vérifiez que le pare-feu géré est automatiquement revenu à la dernière configuration en cours d'exécution.

- Sur le pare-feu
  1. Accédez à l'interface Web du pare-feu.
  2. Cliquez sur **Tasks (Tâches)**, en bas à droite de l'interface web.
  3. Vérifiez que la dernière opération de validation (transmise à partir de Panorama ou validée localement) affiche un statut `Reverted (Inversé)`.



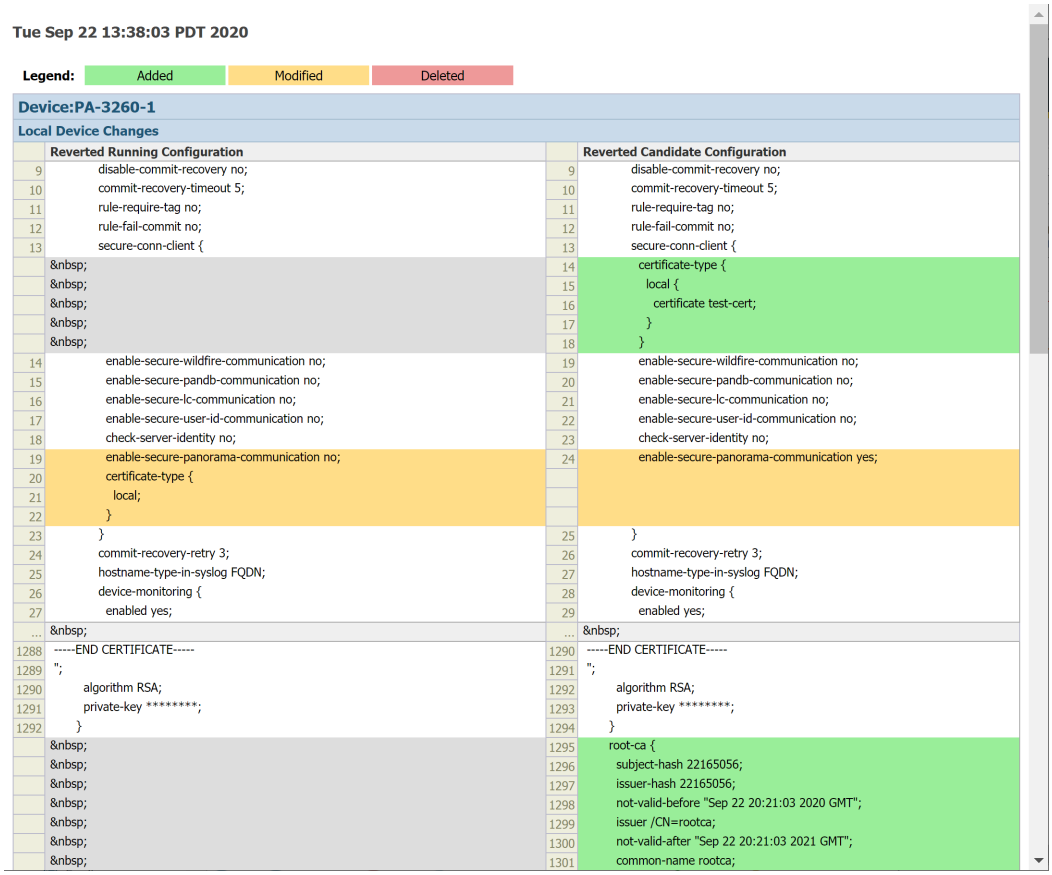
- Sur Panorama
  1. Se connecter à l'interface Web Panorama.
  2. Sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)** > **Summary (Récapitulatif)**.
  3. Consultez l'état de synchronisation des modèles et de la politique partagée. Si vous avez récemment transmis une configuration de Panorama à vos pare-feux gérés et que celle-ci a été inversée, la politique partagée ou le modèle s'affiche comme étant `Out of Sync (Désynchronisée)` (selon les modifications apportées à la configuration).



STEP 2 | Dans la colonne Last Merged Diff pour un pare-feu géré, **affichez Last Merged Config Diff** ( ) pour comparer la configuration en cours d'exécution et la configuration inversée. Dans

© 2020 Palo Alto Networks, Inc.

cet exemple, une règle de politique transmise par Panorama a refusé tout trafic entre le pare-feu géré et Panorama, ce qui a entraîné le retour arrière automatique de la configuration du pare-feu.



Tue Sep 22 13:38:03 PDT 2020

Legend: Added | Modified | Deleted

Device:PA-3260-1

Local Device Changes

	Reverted Running Configuration		Reverted Candidate Configuration
9	disable-commit-recovery no;	9	disable-commit-recovery no;
10	commit-recovery-timeout 5;	10	commit-recovery-timeout 5;
11	rule-require-tag no;	11	rule-require-tag no;
12	rule-fail-commit no;	12	rule-fail-commit no;
13	secure-conn-client {	13	secure-conn-client {
		14	certificate-type {
		15	local {
		16	certificate test-cert;
		17	}
		18	}
14	enable-secure-wildfire-communication no;	19	enable-secure-wildfire-communication no;
15	enable-secure-pandb-communication no;	20	enable-secure-pandb-communication no;
16	enable-secure-lc-communication no;	21	enable-secure-lc-communication no;
17	enable-secure-user-id-communication no;	22	enable-secure-user-id-communication no;
18	check-server-identity no;	23	check-server-identity no;
19	enable-secure-panorama-communication no;	24	enable-secure-panorama-communication yes;
20	certificate-type {		
21	local;		
22	}		
23	}	25	}
24	commit-recovery-retry 3;	26	commit-recovery-retry 3;
25	hostname-type-in-syslog FQDN;	27	hostname-type-in-syslog FQDN;
26	device-monitoring {	28	device-monitoring {
27	enabled yes;	29	enabled yes;
...		...	
1288	-----END CERTIFICATE-----	1290	-----END CERTIFICATE-----
1289	";	1291	";
1290	algorithm RSA;	1292	algorithm RSA;
1291	private-key ********;	1293	private-key ********;
1292	}	1294	}
		1295	root-ca {
		1296	subject-hash 22165056;
		1297	issuer-hash 22165056;
		1298	not-valid-before "Sep 22 20:21:03 2020 GMT";
		1299	issuer /CN=rootca;
		1300	not-valid-after "Sep 22 20:21:03 2021 GMT";
		1301	common-name rootca;

STEP 3 | Modifiez les objets de configuration selon vos besoins afin de ne pas rompre la connexion entre les pare-feux gérés et Panorama avant de rétablir la configuration.

© 2020 Palo Alto Networks, Inc.

Effectuer la mises à jour du contenu lorsque la paire HA de Panorama est en panne

Lors du déploiement des mises à jour de contenu aux périphériques gérés, si Panorama™ se trouve dans une configuration High Availability (Haute disponibilité ; HA), Panorama équilibre les tâches de mises à jour de contenu entre les homologues HA pour décroître la charge sur chaque Panorama. Dans l'éventualité où un homologue HA devient indisponible lors de la mise à jour de contenu, les tâches de mise à jour du contenu échouent pour les périphériques gérés auxquels l'homologue HA ayant échoué transmettrait normalement les mises à jour du contenu. Cela se produit pour les mises à jour du contenu planifiées et manuelles. Pour effectuer la mises à jour de contenu, vous devez manuellement transmettre la mise à jour de contenu aux périphériques gérés.

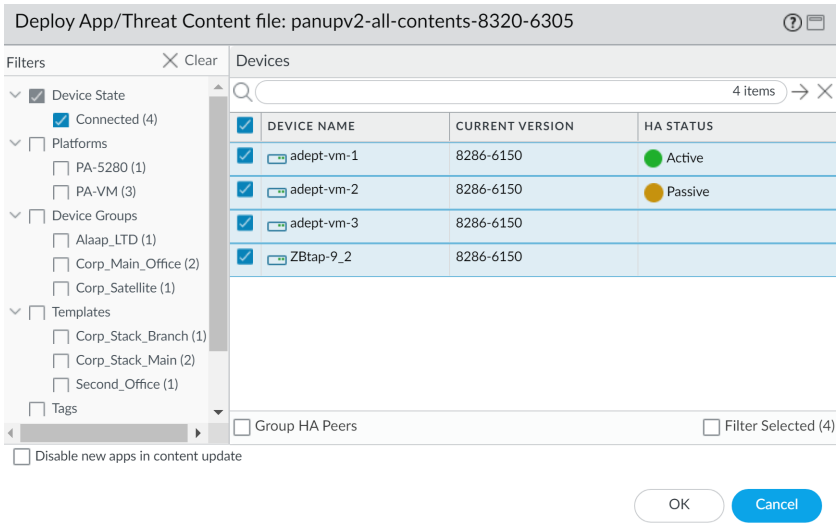
STEP 1 | Connectez-vous à l'ILC Panorama et désactiver l'équilibrage de charge pour les mises à jour du contenu :

```
admin> set dlsrvr distribute no
```

STEP 2 | Se connecter à l'interface Web Panorama.

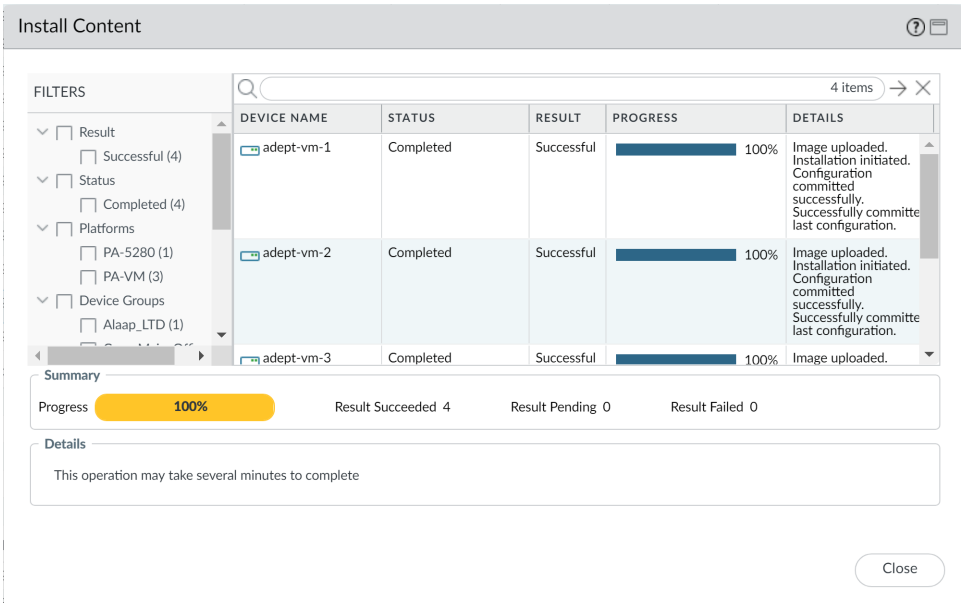
STEP 3 | Sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Dynamic Updates (Mises à jour dynamiques)** et **Install (Installer)** la mise à jour dynamique.

STEP 4 | Sélectionnez les périphériques gérés pour lesquels la mise à jour de contenu a échoué, puis cliquez sur **OK**.



STEP 5 | Vérifiez que la mise à jour de contenu a été transmise avec succès aux périphériques gérés sélectionnés.

© 2020 Palo Alto Networks, Inc.



STEP 6 | Connectez-vous à l'ILC Panorama et activer l'équilibrage de charge pour les mises à jour du contenu :

```
admin> set dlsrvr distribute yes
```


© 2020 Palo Alto Networks, Inc.

Affichage de l'état de réussite ou d'échec d'une tâche

Utilisez l'icône du gestionnaire de tâches 

en bas à droite de l'interface Web Panorama pour afficher la réussite ou l'échec d'une tâche. Le Gestionnaire de tâches affiche également un message détaillé pour vous aider à résoudre un problème. Pour plus d'informations, reportez-vous à la section Utilisez le Gestionnaire de Tâches Panorama.

© 2020 Palo Alto Networks, Inc.

Tester la correspondance aux politiques et la connectivité des périphériques gérés

Après avoir transmis avec succès les configurations du groupe de périphériques et de la piles de modèles à vos pare-feu, collecteurs de journaux et appareils WF-500, testez que le bon trafic correspond aux règles de politique transmises à vos périphériques gérés et que vos pare-feu peuvent se connecter à toutes les ressources réseaux appropriées.

- Résoudre les problèmes de correspondances du trafic à la règle de politique
- Résoudre les problèmes de connectivité aux ressources réseaux

Résoudre les problèmes de correspondances du trafic à la règle de politique

Pour tester la correspondance aux politiques, testez la configuration des règles de politique de vos périphériques gérés pour veiller à ce que la configuration active sécurité adéquatement votre réseau autorisant et en refusant le bon trafic. Une fois les résultats générés pour le trafic qui a été mis en correspondance avec les règles configurées, vous pouvez les **Export to PDF (Exporter au format PDF)** à des fins d'audit.

STEP 1 | Se connecter à l'interface Web Panorama.

STEP 2 | Sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)** > **Troubleshooting (Résolution des problèmes)** pour effectuer une correspondance de politique.

Vous pouvez également lancer un test de correspondance aux politiques à partir de l'onglet Policies (Politiques).

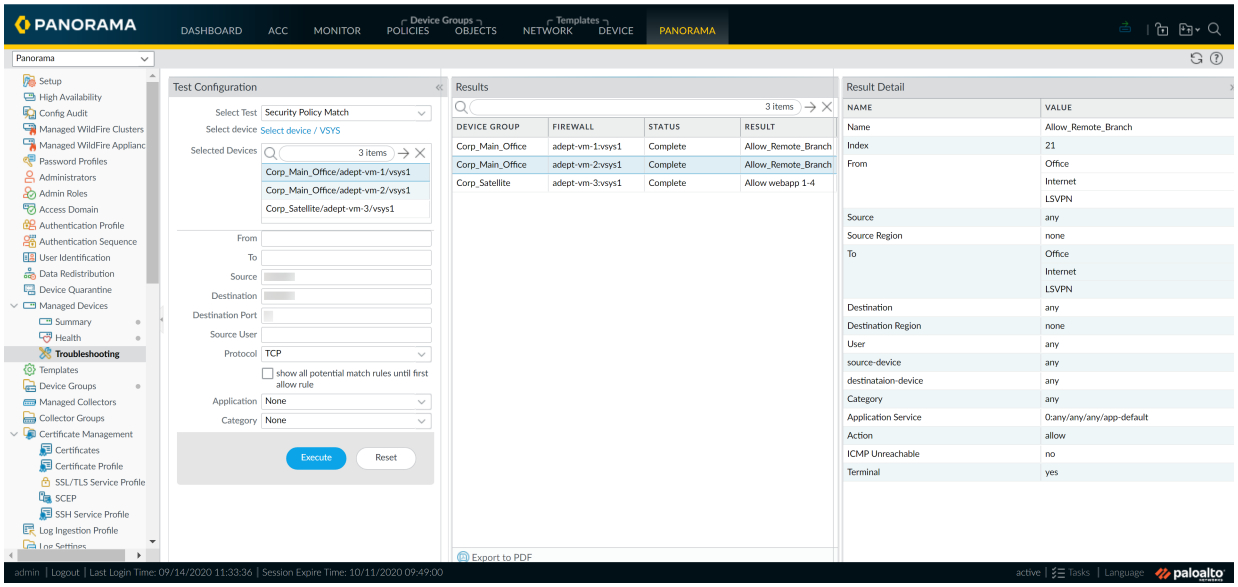
STEP 3 | Saisissez les informations requises pour effectuer le test de correspondance de la politique. Dans cet exemple, un test de correspondance aux politiques de sécurité est exécuté.

1. Sélectionnez **Security Policy Match (Correspondance aux politiques de sécurité)** dans la liste déroulante **Select Test (Sélectionner le test)**.
2. **Select device/VSYS (Sélectionner le périphérique/le système virtuel)** et sélectionnez les pare-feu gérés à tester.
3. Saisissez l'adresse IP source de laquelle provient le trafic.
4. Saisissez l'adresse IP de destination du périphérique cible pour le trafic.
5. Saisissez le protocole IP utilisé pour le trafic.
6. Au besoin, saisissez les informations supplémentaires qui sont pertinents pour effectuer le test de votre règle de politique de sécurité.

STEP 4 | **Execute (Exécutez)** le test de correspondance de la politique de sécurité.

STEP 5 | Sélectionnez les résultats de la correspondance aux politiques de sécurité pour passer en revue les règles de politique qui correspondent aux critères des tests.

© 2020 Palo Alto Networks, Inc.



Résoudre les problèmes de connectivité aux ressources réseaux

Effectuez les tests de connectivité pour les pare-feu gérés afin de vous assurer que vos périphériques gérés peuvent se connecter aux ressources réseau appropriées. Testez la configuration de vos périphériques gérés pour vous assurer que la configuration active sécurise adéquatement votre réseau en vous permettant de vérifier que les configurations transmises à vos périphériques gérés autorisent toujours ces périphériques à se connecter aux ressources, comme les collecteurs de journaux, les listes dynamiques externes configurées et le serveur de mises à jour de Palo Alto Networks. De plus, vous pouvez exécuter les tests de connectivité au routage, à WildFire®, au coffre-fort des meances, à ping et à traceroute pour vérifier que Panorama™ et les périphériques gérés peuvent accéder aux ressources réseau externes qui sont essentielles au fonctionnement et à la sécurité de votre réseau. Une fois les résultats générés, **Export to PDF (Exporter au format PDF)** à des fins d'audit.

Le test de connectivité Ping n'est pris en charge que sur les pare-feux exécutant les versions 9.0 ou ultérieures de PAN-OS.

STEP 1 | Se connecter à l'interface Web Panorama.

STEP 2 | Sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)** > **Troubleshooting (Résolution des problèmes)** pour effectuer un test de connectivité.

Vous pouvez également lancer un test de correspondance aux politiques à partir de l'onglet Policies (Politiques).

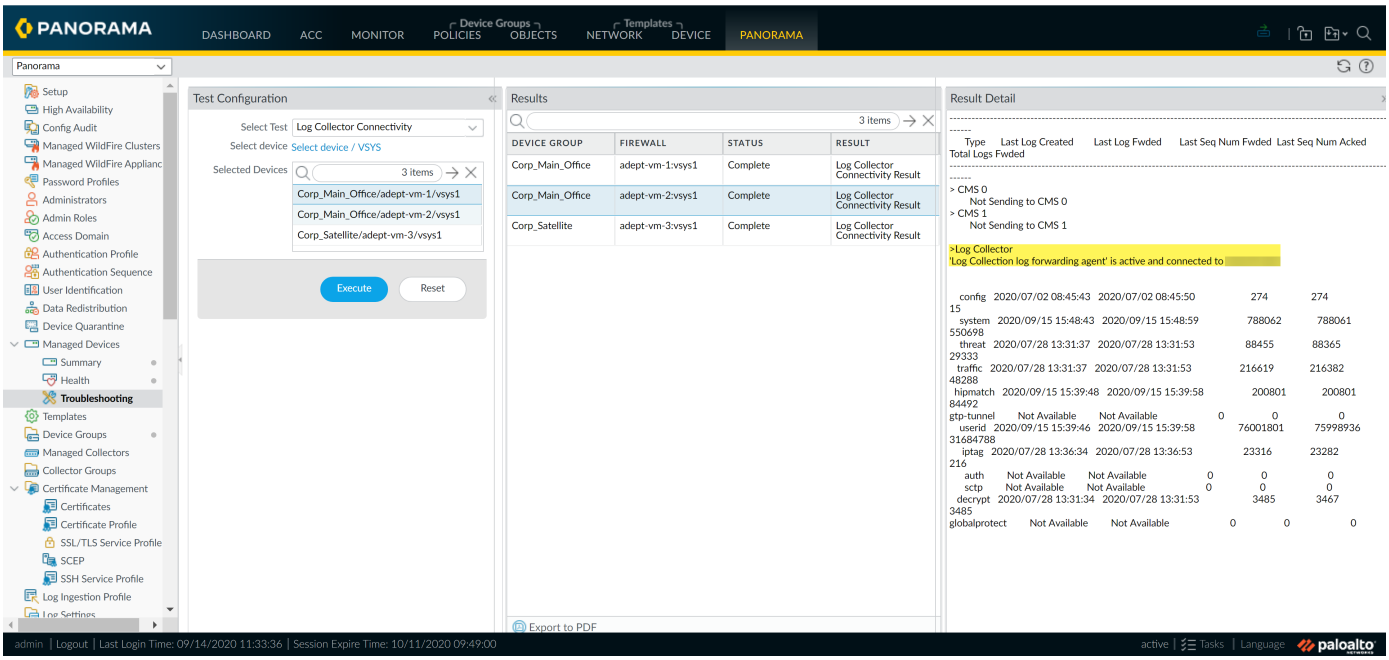
STEP 3 | Saisissez les informations requises pour effectuer le test de connectivité. Dans cet exemple, un test de connectivité du collecteur de journaux est exécuté.

1. Sélectionnez **Log Collector Connectivity (Connectivité du collecteur de journaux)** dans la liste déroulante **Select Test (Sélectionner le test)**.
2. **Select device/VSYS (Sélectionner le périphérique/le système virtuel)** et sélectionnez les pare-feu gérés à tester.
3. Au besoin, saisissez les informations supplémentaires qui sont pertinents pour effectuer le test de connectivité.

© 2020 Palo Alto Networks, Inc.

STEP 4 | **Execute (Exécuter)** le test de connectivité au collecteur de journaux.

STEP 5 | Sélectionnez les résultats du test de connectivité au collecteur de journaux pour passer en revue l'état de connectivité au collecteur de journaux pour les périphériques sélectionnés.



© 2020 Palo Alto Networks, Inc.

Downgrader vers Panorama 10.0

PAN-OS® 10.0 introduit la capacité de configurer des administrateurs locaux et Panorama pour les Collecteur de journaux dédiés et les appareils WildFire, la capacité de journaux sur des interfaces Ethernet, des mises à jour dynamiques automatisées pour les serveur de gestion Panorama™ à air gap, la capacité de procéder à des actions sur des règles filtrées dans l'optimiseur de politique et des filtres supplémentaires de 60 et 90 jours pour les rapports de surveillance, ACC et à la demande. Ces fonctionnalités ne sont toutefois pas compatibles avec Panorama s'il utilise PAN-OS 9.1 ou toute version antérieure. Utilisez les étapes suivantes pour downgrader les pare-feux avant de downgrader les collecteurs de journaux et Panorama exécutant une version Panorama 10.0 dans une version antérieure. Cette procédure fonctionne à la fois pour Panorama qui gère un collecteur de journaux local et pour Panorama qui gère un ou de plusieurs collecteurs de journaux dédiés.

Consultez la Matrice de compatibilité de Palo Alto Networks pour confirmer que les pare-feu et les appareils que vous avez l'intention de rétrograder sont compatibles avec la version de PAN-OS que vous voulez rétrograder. Pour les pare-feu et les appareils que vous pouvez rétrograder, vous devez également consulter les considérations de mise à niveau vers une version supérieure ou antérieure pour vous assurer que vous tenez compte de toutes les fonctionnalités et paramètres de configuration qui seront différents ou indisponibles après la rétrogradation.

STEP 1 | Enregistrez une sauvegarde des fichiers de configuration de Panorama et des périphériques gérés.

1. **Export Panorama and device configuration snapshot (Exporter un instantané de la configuration de l'appareil et de Panorama)** (**Panorama** > **Setup (Configuration)** > **Operations (Opérations)**).
2. Enregistrez le fichier .tgz exporté dans un emplacement externe à Panorama, aux collecteurs de journaux ou aux pare-feu. Vous pouvez utiliser cette sauvegarde pour restaurer la configuration en cas de problème qui vous forcerait à recommencer la procédure.

STEP 2 | Si vous avez configuré une authentification pour un Collecteur de journaux dédié et avez supprimé l'utilisateur **`admin`**, configurez et validez un nouvel utilisateur **`admin`** pour vos collecteurs de journaux dédiés.

Les Collecteurs de journaux dédiés doivent avoir l'utilisateur `admin` configuré afin de downgrader vers PAN-OS 9.1 et les versions antérieures.

STEP 3 | Downgradez chaque pare-feu exécutant une version de PAN-OS 10.0.

Si vous downgradez plus d'un pare-feu, rationalisez le processus en transférant chaque image PAN-OS 9.1 spécifique à un pare-feu sur Panorama avant de commencer le downgrade. Par exemple, pour downgrader les pare-feu PA-220 vers PAN-OS 9.1.0, téléchargez les images `PanOS_220-9.1.0` ou `PanOS_3000-9.1.0`.

Panorama exige que tous les pare-feu exécutent la même version ou une version antérieure de PAN-OS. Ainsi, avant de rétrograder Panorama, utilisez et répétez les tâches appropriées ci-dessous en fonction de votre environnement pour rétrograder tous les pare-feu gérés :

1. **Check Now (Vérifier maintenant)** les images disponibles (**Panorama** > **Device Deployment (Déploiement de périphériques)** > **Software (Logiciel)**).

© 2020 Palo Alto Networks, Inc.

2. Localisez l'image PAN-OS 9.1 pour chaque modèle ou série de pare-feu que vous souhaitez downgrader. Si l'image n'est pas déjà téléchargée, cliquez sur **Download (Télécharger)** pour la télécharger.

Pare-feu sans Haute Disponibilité / HD (High Availability / HA)

Cliquez sur **Install (Installer)** dans la colonne Action de la version de PAN-OS 9.1, sélectionnez tous les pare-feux que vous souhaitez rétrograder, sélectionnez **Reboot device after install (Redémarrer le périphérique après l'installation)** et cliquez sur **OK**.

Pare-feu HD actifs / actifs

1. Cliquez sur **Install (Installer)**, désactivez **Group HA Peers (Regrouper les homologues HD)**, sélectionnez un des homologues HD, sélectionnez **Reboot device after install (Redémarrer le périphérique après l'installation)**, puis cliquez sur **OK**. Attendez que le pare-feu termine le redémarrage avant de poursuivre.
2. Cliquez sur **Install (Installer)**,désactivez **Group HA Peers (Regrouper les homologues HD)**, sélectionnez l'homologue HD que vous n'avez pas mis à jour à l'étape précédente, sélectionnez **Reboot device after install (Redémarrer le périphérique après l'installation)**, puis cliquez sur **OK**.

Pare-feu HD actifs / passifs

Dans cet exemple, le pare-feu actif est appelé fw1 et le pare-feu passif fw2 :

1. Cliquez sur **Installer** dans la colonne Action de la mise à jour appropriée, désactivez **Group HA Peers (Regrouper les homologues HD)**, sélectionnez fw2, **Reboot device after install (Redémarrer le périphérique après l'installation)** et cliquez sur **OK**.
2. Après le redémarrage de fw2, vérifiez sur fw1 (widget **Dashboard (Tableau de bord)** > **High Availability (Haute disponibilité)**) que fw2 est toujours l'homologue passif (l'état du pare-feu local est `active` et l'homologue fw2 est `passive`).
3. Accédez à fw1 et **Suspend local device (Suspendre le périphérique local)** (**Device (Périphérique)** > **High Availability (Haute disponibilité)** > **Operational Commands (Commandes opérationnelles)**).
4. Accédez à fw2 (**Dashboard (Tableau de bord)** > **High Availability (Haute disponibilité)**) et vérifiez que l'état du pare-feu local est `active` et que l'homologue est `suspended`.
5. Accédez à Panorama, sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Software (Logiciel)**, cliquez sur **Install (Installer)** dans la colonne Action de la mise à jour appropriée, désactivez **Group HA Peers (Regrouper les homologues HD)**, sélectionnez fw1, **Reboot device after install (Redémarrer le périphérique après l'installation)**, puis cliquez sur **OK**. Attendez que fw1 termine le redémarrage avant de poursuivre.
6. Accédez à fw1 (widget **Dashboard (Tableau de bord)** > **High Availability (Haute disponibilité)**) et vérifiez que l'état du pare-feu local est `passive` et que l'homologue (fw2) est `active`.



Si vous avez activé la préemption dans les paramètres d'élection (Device (Périphérique) > High Availability (Haute disponibilité) > General (Général)), alors fw1 sera rétabli en tant qu'homologue actif après le redémarrage.

STEP 4 | Downgradez chaque collecteur de journaux exécutant Panorama 10.0.

1. **Check Now (Vérifier maintenant)** les images disponibles (**Panorama** > **Device Deployment (Déploiement de périphériques)** > **Software (Logiciel)**).
2. Localisez l'image de Panorama 9.1. Si l'image n'est pas déjà téléchargée, alors cliquez sur **Download (Télécharger)** pour la télécharger (colonne Action).
3. Une fois le téléchargement terminé, **Install (Installer)** l'image sur chaque collecteur de journaux exécutant Panorama 10.0. Sélectionnez **Reboot device after install (Redémarrer le périphérique après l'installation)** pour redémarrer automatiquement le périphérique lorsque la mise à niveau est terminée.

STEP 5 | Rétrogradez Panorama.

© 2020 Palo Alto Networks, Inc.

1. **Check Now (Vérifier maintenant)** les images disponibles (**Panorama** > **Device Deployment (Déploiement de périphériques)** > **Software (Logiciel)**).
2. Localisez l'image de Panorama 9.1. Si l'image n'est pas déjà téléchargée, cliquez sur **Download (Télécharger)** pour la télécharger.
3. Une fois le téléchargement terminé, **Install (Installer)** l'image sur Panorama.
4. Rédémarrez Panorama comme suit :
   - Si vous êtes invité à redémarrer, cliquez sur **Yes (Oui)**. Si une invite **CMS Login (Connexion CMS)** s'affiche, appuyez sur Entrée sans saisir de nom d'utilisateur ou de mot de passe. Lorsque l'invite de connexion Panorama s'affiche, saisissez le nom d'utilisateur/mot de passe définis lors de la configuration initiale.
   - Si vous n'êtes pas invité à redémarrer, sélectionnez **Panorama (Panorama)** > **Setup (Configuration)** > **Operations (Opérations)** et cliquez sur **Reboot Panorama (Redémarrer Panorama)** dans la section des opérations de périphérique.

STEP 6 | Migrer les journaux de Panorama vers le format de journal de PAN-OS 8.1.

Lors de la migration, les données des journaux ne sont pas visibles dans les onglets ACC ou Monitor (Surveillance). De plus, les nouvelles données des journaux ne sont pas transférées aux collecteurs de journaux avant que la migration a été effectuée.

1. Affichez le taux de journalisation entrant.

   Pour de meilleurs résultats, démarrez la migration des journaux lorsque le taux de journalisation entrant est faible. Pour vérifier le débit, exécutez la commande suivante depuis la CLI du collecteur de journaux :

```
admin@FC-M500-1> debug log-collector log-collection-stats show incoming-logs
```

   Une utilisation élevée du processeur (proche de 100 %) pendant la migration des journaux est attendue et les opérations continueront à fonctionner normalement. La migration des journaux est limitée en faveur des journaux entrants et d'autres processus en cas de conflit de ressources.
2. Commencez à migrer les journaux sur chaque collecteur de journaux au nouveau format.

   Pour commencer la migration, entrez la commande suivante depuis la CLI de chaque collecteur de journaux :

```
admin@FC-M500-1> request logdb migrate lc serial-number <ser_num> start
```
3. Consultez l'état de la migration des journaux pour estimer le temps nécessaire à la migration de tous les journaux existants vers le nouveau format.

```
admin@FC-M500-1> request logdb migrate lc serial-number <ser_num> status
 Slot: all
Migration State: In Progress
Percent Complete: 0.04
Estimated Time Remaining: 451 hour(s) 47 min(s)
```


© 2020 Palo Alto Networks, Inc.