paloalto
TECHDOCS

Administration de l’appareil WildFire

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

- For the most recent version of this guide or for access to 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

Last Revised

August 23, 2023

Table of Contents

Présentation de l’appareil WildFire 7

- À propos de l'appareil WildFire 8
- Cloud WildFire privé 9
- Cloud WildFire hybride : 10
- Interfaces de l'appareil WildFire 11
- Prise en charge des types de fichiers de l’appareil WildFire 12

Installation et gestion d'un appareil WildFire 15

- Configuration de l'appareil WildFire 16
- Transfert de fichiers pour analyse par l’appareil WildFire 24
- Envoi des échantillons malveillants ou des rapports à partir de l'appareil WildFire 32
- Configurer l'authentification à l'aide d'un certificat personnalisé sur un appareil WildFire autonome 34
  - Authentification mutuelle SSL des appareils WildFire 34
  - Configurer l'authentification avec des certificats personnalisés sur l'appareil WildFire 35
- Paramétrage de l'interface VM de l'appareil WildFire 38
  - Présentation de l'interface de machine virtuelle 38
  - Configuration de l'interface MV sur l'appareil WildFire 40
  - Connexion du pare-feu à l'interface MV de l'appareil WildFire 42
- Activation des fonctions d'analyse de l'appareil WildFire 44
  - Paramétrage des mises à jour de contenu de l'appareil WildFire 44
  - Activation de la génération de catégorie d'URL et de la signature locale 48
  - Envoi des logiciels malveillants découverts localement ou des rapports au cloud WildFire public 50
- Mise à niveau d’un appareil WildFire 52
- Installation du certificat de périphérique de l’appareil WildFire avec une connexion Internet 58

Surveillance de l’activité de l’appareil WildFire 63

- À propos des journaux et de la génération de rapports WildFire 64
- Utilisez le boitier WildFire pour surveiller l’état de l’analyse des échantillons 65
  - Affichage de l’utilisation de l’environnement d’analyse WildFire 65
  - Affichage des détails du traitement de l’analyse des échantillons WildFire 66
- Utilisez la CLI pour surveiller le boitier WildFire 68
  - Affichage des journaux système du boitier WildFire 68
- Utilisation du pare-feu pour surveiller les envois de l’appareil WildFire 70
- Affichage des journaux et des rapports d’analyse de l’appareil WildFire 71

Clusters d'appareils WildFire 75

Échelle et résilience des clusters d'appareils WildFire 76
Haute disponibilité des clusters d’appareils WildFire 78
Avantages de la gestion des clusters WildFire au moyen de Panorama 79
Gestion des clusters d'appareils WildFire 81
Déploiement d’un cluster d’appareils WildFire 86
Configuration locale d’un cluster sur des appareils WildFire 88
Configuration d’un cluster et ajout de nœuds localement 88
Configuration locale des paramètres généraux d’un cluster 95
Suppression locale d’un nœud d’un cluster 98
Configurer le chiffrement d'appareils-à-àppareils WildFire 102
Configurer le chiffrement d'appareil à appareil à l'aide de certificats prédéfinis via l'interface de ligne de commande 102
Configurer le chiffrement d'appareil à appareil à l'aide de certificats personnalisés via la CLI 103
Surveillance d’un cluster d’appareils WildFire 108
Affichage de l’état du cluster d’appareils WildFire au moyen de la CLI 108
États des applications Wildfire 119
États de service Wildfire 126
Mise à jour d’appareils WildFire appartenant à un cluster 128
Mise à niveau locale d’un cluster à partir d’une connexion Internet 128
Mise à niveau locale d’un cluster sans connexion Internet 133
Dépannage d’un cluster d’appareils WildFire 140
Dépannage des situations de « split brain » WildFire 140

Utilisation de la CLI de l’appareil WildFire 145

Concepts de la CLI du logiciel de l'appareil WildFire 146
Structure de la CLI du logiciel de l'appareil WildFire 146
Conventions des commandes de la CLI du logiciel de l'appareil WildFire 146
Messages des commandes de la CLI du logiciel de l'appareil WildFire 147
Symboles des options de commande de l'appareil WildFire 148
Niveaux de privilège de l'appareil WildFire 149
Modes des commandes de la CLI de WildFire 150
Mode Configuration de la CLI de l'appareil WildFire 150
Mode Opérationnel de la CLI de l'appareil WildFire 153
Accès à la CLI de l’appareil WildFire 154
Établissement d'une connexion de console directe 154
Établissement d'une connexion SSH 154
Opérations de la CLI de l’appareil WildFire 155
Accès aux modes Opérationnel et Configuration de l'appareil WildFire 155
Affichage options de commande de la CLI du logiciel de l'appareil WildFire 155

Restriction d'affichage des résultats des commandes de la CLI de l'appareil WildFire 156
Paramétrage du format de sortie des commandes de configuration pour l'appareil WildFire 157
Référence des commandes du mode Configuration de l'appareil WildFire 158
set deviceconfig cluster 158
set deviceconfig high-availability 159
set deviceconfig setting management 161
set deviceconfig setting wildfire 162
set deviceconfig system eth2 163
set deviceconfig system eth3 164
définir le système panorama de deviceconfig sur local-panorama-server 165
définir le panorama du système deviceconfig sur local-panorama panorama-server-2 166
set deviceconfig system update-schedule 167
set deviceconfig system vm-interface 168
Référence des commandes du mode Opérationnel de l'appareil WildFire 170
clear high-availability 171
create wildfire api-key 172
delete high-availability-key 173
delete wildfire api-key 173
delete wildfire-metadata 174
disable wildfire 175
edit wildfire api-key 175
load wildfire api-key 176
request cluster decommission 177
request cluster reboot-local-node 178
request high-availability state 179
request high-availability sync-to-remote 180
request system raid 181
request wildfire sample redistribution 182
request system wildfire-vm-image 183
request wf-content 184
save wildfire api-key 185
set wildfire portal-admin 186
show cluster all-peers 186
show cluster controller 187
show cluster data migration status 188
show cluster membership 189
show cluster task 191
show high-availability all 192

show high-availability control-link....193
show high-availability state....194
show high-availability transitions....195
show system raid....196
submit wildfire local-verdict-change....197
show wildfire....198
show wildfire global....199
show wildfire local....202
test wildfire registration....206

Présentation de l’appareil WildFire

WildFire™ assure la détection et la prévention de logiciels malveillants au jour 0 en combinant des analyses dynamiques et statiques en vue de détecter les menaces et de créer des protections pour bloquer les logiciels malveillants. WildFire étend les fonctionnalités des pare-feux Palo Alto Networks de nouvelle génération pour identifier et bloquer les logiciels malveillants ciblés et inconnus.

À propos de l'appareil WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

L'appareil WildFire fournit un cloud WildFire privé sur site vous permettant d'analyser des fichiers suspects dans un environnement bac à sable, sans que le pare-feu n'envoie de fichiers en dehors du réseau. Si vous souhaitez utiliser l'appareil WildFire pour héberger un cloud WildFire privé, configurez le pare-feu pour qu'il envoie des échantillons à l'appareil WildFire pour leur analyse. L'appareil WildFire place localement tous les fichiers dans son bac à sable et les analyse afin de détecter tout comportement malveillant à l'aide du même moteur que le cloud WildFire privé. En quelques minutes, le cloud privé renvoie les résultats de l'analyse journal des **WildFire Submissions (envois WildFire)** du pare-feu.

L’administration de l’appareil WildFire couvre la configuration et le paramétrage de l’appareil WildFire, mais partage une grande partie de la conception opérationnelle et des capacités avec le cloud public WildFire. Pour plus d’informations sur les capacités d’analyse WildFire, reportez-vous à l’administration Advanced Wildfire.

Vous pouvez activer un appareil WildFire pour :

- ❑ Générer localement des signatures antivirus et DNS pour les logiciels malveillants détectés, et pour assigner une catégorie d'URL aux liens malveillants. Vous pouvez ensuite permettre aux pare-feu connectés de récupérer les dernières signatures et catégories d'URL toutes les cinq minutes.
- ❑ Envoi des échantillons malveillants vers le cloud WildFire public. Le cloud WildFire public effectue une nouvelle analyse de l'échantillon et génère une signature pour détecter le logiciel malveillant ; cette signature peut être mise à la disposition des utilisateurs mondiaux en quelques minutes pour les protéger
- ❑ Envoyez les rapports de logiciel malveillant générés localement (sans envoyer le contenu de l'échantillon brut) au cloud WildFire public afin de contribuer aux statistiques sur les logiciels malveillants et aux données d'intelligence sur les menaces.

Vous pouvez configurer un maximum de 100 pare-feu Palo Alto Networks disposant chacun d'un abonnement valide à WildFire pour effectuer des transferts vers un appareil WildFire unique. En plus de l'abonnement au pare-feu WildFire, aucun autre abonnement WildFire n'est requis pour permettre le déploiement d'un cloud WildFire privé.

Vous pouvez gérer des appareils WildFire au moyen de la CLI locale de l’appareil, ou vous pouvez procéder centralement à la gestion des appareils WildFire au moyen de Panorama. À partir de PAN-OS 8.0.1, vous pouvez également grouper les appareils WildFire dans des clusters d'appareils WildFire et gérer les clusters globalement ou à partir de Panorama.

Cloud WildFire privé

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Dans un déploiement de cloud privé Palo Alto Networks, les pare-feu Palo Alto Networks transfèrent des fichiers vers un appareil WildFire installé sur le réseau de votre entreprise qui sert à l'hébergement d'un emplacement d'analyse sur un cloud privé. Un cloud WildFire privé peut recevoir et analyser des fichiers provenant d'un maximum de 100 pare-feu Palo Alto Networks.

Puisque le cloud WildFire privé est un bac à sable local, les échantillons bénins, indésirables et d’hameçonnage qui sont analysés ne quittent jamais votre réseau. De plus, par défaut, le cloud privé n'envoie pas les logiciels malveillants détectés hors de votre réseau ; cependant, vous pouvez choisir de transférer automatiquement les logiciels malveillants au cloud WildFire public pour la génération et la distribution de signature. Dans ce cas, le cloud WildFire public procède à une nouvelle analyse de l'échantillon, génère une signature pour identifier l'échantillon et distribue la signature à tous les pare-feu Palo Alto Networks qui disposent de licences de protection contre les menaces et WildFire.

Si vous ne souhaitez pas que le cloud WildFire privé transfère les échantillons malveillants hors de votre réseau, vous pouvez :

- Autoriser l'appareil WildFire à transférer le rapport de logiciel malveillant (et non pas l'échantillon en soi) au cloud WildFire public. Les rapports WildFire donnent des renseignements statistiques qui facilitent l'évaluation par Palo Alto Networks de la persistance et de la propagation des logiciels malveillants Pour plus d'informations, reportez-vous à la section Envoi des échantillons malveillants ou des rapports à partir de l'appareil WildFire.
- Charger manuellement les fichiers sur le portail WildFire au lieu de transférer automatiquement tous les logiciels malveillants, ou utiliser l’API WildFire pour envoyer les fichiers au cloud public WildFire.

Vous pouvez aussi réaliser l’Activation de la génération de catégorie d'URL et de la signature locale sur l’appareil WildFire. Les signatures générées par l'appareil WildFire sont distribuées aux pare-feu connectés pour que ces derniers puissent bloquer efficacement le logiciel malveillant lors de sa prochaine détection.

Les fichiers Android Application Package (APK) et MAC OSX ne sont pas pris en charge pour l'analyse sur le cloud WildFire privé.

Cloud WildFire hybride :

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Dans un déploiement de cloud WildFire hybride, un pare-feu peut transférer certains échantillons au cloud WildFire public hébergé par Palo Alto Networks et d'autres échantillons à un cloud WildFire privé hébergé par un appareil WildFire. Un déploiement de cloud WildFire hybride offre la souplesse nécessaire pour analyser des documents privés localement et dans votre réseau, tandis que le cloud WildFire public analyse des fichiers provenant d'Internet. Par exemple, transférez les données sur les cartes de paiement (PCI) et les renseignements personnels sur la santé exclusivement au cloud WildFire privé pour analyse, mais transférez les fichiers PE (portable executable/exécutable portable) au cloud WildFire public pour analyse. Si le cloud WildFire est déployé sous forme de cloud hybride, le transfert de fichiers vers le cloud public pour analyse vous permet d'obtenir un verdict rapide relativement aux fichiers qui ont déjà été traités dans le cloud WildFire public et libère les ressources de l'appareil WildFire, qui peuvent être allouées au traitement du contenu de nature délicate. De plus, vous pouvez transférer certains types de fichiers qui ne sont pas actuellement pris en charge pour analyse par l'appareil WildFire vers le cloud WildFire public, tels que les fichiers Android Application Package (APK).

Dans un déploiement de cloud WildFire hybride, il peut arriver qu’un fichier corresponde aux critères d’analyses du cloud public et du cloud privé. Dans ce cas, par mesure de précaution, le fichier n’est envoyé pour analyse qu’au cloud privé.

Pour configurer le transfert cloud hybride, consultez Transfert de fichiers pour analyse par l’appareil WildFire.

Interfaces de l'appareil WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Quatre ports Ethernet RJ-45 se trouvent à l’arrière des appareils WF-500. Ces ports sont nommés **MGT**, **1**, **2** et **3** et correspondent à des interfaces données.

L'appareil WildFire dispose de trois interfaces :

- **MGT** - Reçoit tous les fichiers transférés par les pare-feu et renvoie aux pare-feu des logs détaillant les résultats. Reportez-vous à la section Configuration de l'appareil WildFire.
- **Interface de la machine virtuelle (vm-interface)** - Fournit un accès réseau aux systèmes de bac à sable WildFire pour permettre aux échantillons de fichiers de communiquer avec Internet et à WildFire de mieux analyser le comportement des échantillons. Lorsque l'interface MV est configurée, WildFire peut observer les comportements malveillants qui ne se seraient pas manifestés sans accès réseau, tel que l'activité phone-home. Toutefois, pour éviter que votre bac à sable ne fasse entrer des logiciels malveillants dans votre réseau, configurez l'interface de la machine virtuelle sur un réseau isolé doté d'une connexion Internet. Vous pouvez également activer l'option Tor pour masquer l'adresse IP publique utilisée par votre entreprise des sites malveillants accessibles par l'échantillon. Pour plus d'informations sur l'interface MV, reportez-vous à la section Paramétrage de l'interface VM de l'appareil WildFire.
- **Interface de gestion du cluster** : procure une communication à l’échelle du cluster entre les nœuds de l’appareil WildFire qui sont membres d’un cluster d'appareils WildFire. Cette interface n’est pas la même que l’interface MGT qui sert aux opérations du pare-feu. Vous pouvez configurer l’interface Ethernet2 ou l’interface Ethernet3 (nommées **2** et **3**, respectivement) comme interface de gestion du cluster.

Procurez-vous les informations nécessaires pour configurer la connectivité réseau sur le port MGT, l'interface de machine virtuelle et l’interface de gestion du cluster (clusters d’appareils WildFire uniquement) auprès de votre administrateur réseau (adresse IP, masque de sous-réseau, passerelle, nom d'hôte, serveur DNS). Toutes les communications entre les pare-feu et l'appareil s'effectuent sur le port MGT, notamment l'envoi de fichiers, la distribution de logs WildFire et l'administration de l'appareil. Par conséquent, vérifiez que les pare-feu sont raccordés au port MGT de l'appareil. L'appareil doit également pouvoir se connecter au site updates.paloaltonetworks.com pour récupérer les mises à jour logicielles de son système d'exploitation.

Prise en charge des types de fichiers de l’appareil WildFire

Le tableau suivant répertorie les types de fichiers pris en charge pour l’analyse dans le cloud privé de l’appareil WildFire et par chargement direct sur le portail WildFire.

Types de fichiers pris en charge pour l’analyse	Cloud WildFire privé (appareil WildFire)	Portail WildFire | API (téléchargement direct ; toutes les régions)
Liens contenus dans les e-mails	✓	✓
Fichiers Android Application Package (APK).	✗	✓
Fichiers Adobe Flash	✓	✓
Fichiers Java Archive (JAR)	✓	✓
Fichiers Microsoft Office (y compris les fichiers SLK et IQY**)	✓	✓
Fichiers Portable Executable (PE) (y compris les fichiers MSI**)	✓	✓
Fichiers Portable Document Format (PDF)	✓	✓
Fichiers Mac OS X	✗	✓
Fichiers Linux (fichiers ELF et scripts Shell)	✗	✓
Fichiers d’archive (RAR, 7-Zip, ZIP)*	✓	✓
Fichiers de script (BAT, JS, VBS, PS1 et HTA)	✓	✓
Scripts de script (Perl et Python)	✗	✓

Types de fichiers pris en charge pour l’analyse	Cloud WildFire privé (appareil WildFire)	Portail WildFire | API (téléchargement direct ; toutes les régions)
Fichiers d’archive (ZIP [chargement direct] et ISO)*	✗	✓

* Les fichiers ZIP ne sont pas directement transférés vers le cloud Wildfire pour analyse. Au lieu de cela, ils sont d'abord décodés par le pare-feu, et les fichiers qui correspondent aux critères du profil d'analyse WildFire sont transférés séparément pour analyse.

** L’appareil WildFire ne prend pas en charge l’analyse de fichiers MSI, IQY et SLK.

Installation et gestion d'un appareil WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Il est possible de configurer l’appareil WildFire™ en tant que cloud WildFire privé hébergé localement. Les rubriques suivantes expliquent comment préparer l'appareil WildFire à recevoir les fichiers en vue de leur analyse, comment gérer l'appareil et comment activer l'appareil pour qu'il génère localement des signatures de menace et des catégories d'URL.

- À propos de l'appareil WildFire
- Configuration de l'appareil WildFire
- Configurer l'authentification à l'aide d'un certificat personnalisé sur un appareil WildFire autonome
- Paramétrage de l'interface VM de l'appareil WildFire
- Activation des fonctions d'analyse de l'appareil WildFire
- Installation du certificat de périphérique de l’appareil WildFire avec une connexion Internet

Configuration de l'appareil WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Cette section décrit les différentes étapes requises pour intégrer un appareil WildFire dans un réseau et procéder à un paramétrage de base.

STEP 1 | L'appareil WildFire doit être monté en rack et câblé.

Reportez-vous au Guide de référence du matériel de l’appareil WildFire pour obtenir des instructions.

STEP 2 | Connectez un ordinateur à l'appareil à l'aide du port MGT ou du port de console et mettez l'appareil sous tension.

1. Connectez-vous au port de console ou au port MGT. Les deux se trouvent à l'arrière de l'appareil
   - **Port de console** - Il s'agit d'un connecteur série mâle à 9 broches. Utilisez les paramètres suivants sur l'application de la console'A0;: 9600-8-N-1. Connectez le câble fourni au port série de l'ordinateur de gestion ou au convertisseur USB vers Série.
   - **Port MGT** - Il s'agit d'un port Ethernet RJ-45. Par défaut, l'adresse IP du port MGT est 192.168.1.1. L'interface de votre ordinateur de gestion doit se trouver sur le même sous-réseau que le port MGT. Par exemple, paramétrez l'adresse IP de l'ordinateur de gestion sur 192.168.1.5.
2. Mettez l'appareil sous tension.

   L'appareil est mis sous tension dès que vous branchez l'alimentation à la première source d'alimentation et un bip sonore d'avertissement retentit jusqu'à ce que vous branchiez la seconde alimentation. Si l'appareil est déjà branché et qu'il est arrêté, appuyez sur le bouton d'alimentation situé à l'avant de l'appareil pour le mettre sous tension.

STEP 3 | Enregistrez l'appareil WildFire.

1. Procurez-vous le numéro de série qui se trouve sur l'étiquette S/N de l'appareil ou exécutez la commande suivante et consultez le champ `serial` :

   ```
   admin@WF-500> afficher les informations système
   ```

2. Dans un navigateur, accédez au portail de support de Palo Alto Networks et connectez-vous.
3. Enregistrez le périphérique comme suit'A0;:
   - S'il s'agit du premier périphérique Palo Alto Networks que vous enregistrez et que vous ne disposez d'aucune information de connexion, cliquez sur **S'enregistrer** au bas de la page.

     Pour ce faire, entrez une adresse e-mail et le numéro de série du périphérique. Lorsque vous y êtes invité, configurez un nom d'utilisateur et un mot de passe pour accéder à la communauté de support de Palo Alto Networks.
   - Pour les comptes existants, connectez-vous et cliquez sur **Mes périphériques**. Accédez à la section **Enregistrer le périphérique** située en bas de l'écran, saisissez le numéro de série du périphérique, votre ville et votre code postal, puis cliquez sur **Enregistrer le périphérique**.
4. Pour confirmer l'enregistrement de WildFire sur l'appareil WildFire, connectez-vous à l'appareil à l'aide d'un client SSH ou en utilisant le port de console. Saisissez un nom d'utilisateur/mot de passe admin/admin. et saisissez la commande suivante sur l'appareil `:

   ```
   admin@WF-500> tester l’inscription wildfire
   ```

   La sortie suivante indique que l'appareil est enregistré avec l'un des serveurs du cloud WildFire de Palo Alto Networks.

   ```
   Tester l'inscription wildfire : téléchargement réussi de la
    liste des serveurs : sélection réussie du meilleur serveur :
    cs-s1.wildfire.paloaltonetworks.com
   ```


STEP 4 | Réinitialisez le mot de passe admin.

1. Définissez un nouveau mot de passe en exécutant la commande suivante'A0;:

```
admin@WF-500> définir le mot de passe
```

2. Saisissez l'ancien mot de passe, appuyez sur la touche Entrée et confirmez le nouveau mot de passe. Validez la configuration pour vous assurer que le nouveau mot de passe est enregistré en cas de redémarrage.

   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.*

3. Saisissez **exit** pour vous déconnecter, puis reconnectez-vous pour vérifier que le nouveau mot de passe a bien été défini.

STEP 5 | Configurez les paramètres de l'interface de gestion.

Cet exemple utilise les valeurs IPv4 suivantes, mais l'appareil est aussi compatible avec des adresses IPv6 :

- Adresse IPv4 : 10.10.0.5/22
- Masque de sous-réseau - 255.255.252.0
- Passerelle par défaut :10.10.0.1
- Nom d'hôte - wildfire-corp1
- Serveur DNS - 10.0.0.246

1. Connectez-vous à l'appareil à l'aide d'un client SSH ou en utilisant le port de console et passez en mode Configuration'A0;:

```
admin@WF-500> configurer
```

2. Définissez les informations relatives à l'adresse IP'A0;:

```
admin@WF-500# définir addresse ip du système deviceconfig
 10.10.0.5 netmask 255.255.252.0 default-gateway 10.10.0.1
 dns-setting serveurs principaux 10.0.0.246
```

Configurez un serveur DNS secondaire en remplaçant « primary » par « secondary » dans la commande ci-dessus, en excluant les autres paramètres relatifs à l'adresse IP. Par exemple :

```
admin@WF-500# définir système deviceconfig DNS-setting
 serveurs secondaires 10.0.0.247
```

3. Définissez le nom d'hôte (wildfire-corp1, dans cet exemple) :

```
admin@WF-500# définir le système deviceconfig hostname
 wildfire-corp1
```

4. Validez la configuration pour activer la nouvelle configuration de port de gestion (MGT)'A0;:

```
admin@WF-500# valider
```

5. Connectez le port de l'interface MGT à un commutateur réseau.
6. Replacez l'ordinateur de gestion sur votre réseau d'entreprise, ou sur n'importe quel réseau requis pour accéder à l'appareil sur le réseau de gestion.
7. Dans votre ordinateur de gestion, utilisez le client SSH pour vous connecter à la nouvelle adresse IP ou nom d'hôte attribué au port MGT de l'appareil. Dans cet exemple, l'adresse IP est 10.10.0.5.

STEP 6 | Activez l'appareil à l'aide du code d'autorisation WildFire que Palo Alto Networks vous a envoyé.

Même s'il fonctionnera sans code d'authentification, l'appareil WildFire ne pourra pas récupérer de mises à jour logicielles ou de contenu sans code d'authentification valide.

1. Passez en mode opérationnel :

```
admin@WF-500# sortir
```

2. Recherchez et installez la licence WildFire'A0;:

```
admin@WF-500> demande de licence pour récupérer le code
 d'authentification<auth-code>
```

3. Vérifiez la licence'A0;:

```
admin@WF-500> demander une vérification de l'assistance
```

Les informations sur le site et le contrat de support s'affichent. Vérifiez que la date affichée est valide.

STEP 7 | Configurez l'horloge de l'appareil WildFire.

Deux méthodes permettent d'y arriver. Vous pouvez définir manuellement la date, l'heure et le fuseau horaire ou vous pouvez configurer l'appareil WildFire pour qu'il synchronise son horloge local avec un serveur Network Time Protocol (protocole de diffusion du temps en réseau ; NTP).

- Pour régler l'horloge manuellement, entrez les commandes suivantes :

```
admin@WF-500> définir la date de l'horloge<YYYY/MM/
DD>heure<hh:mm:ss>admin@WF-500> configurer admin@WF-500# définir
 le fuseau horaire du système de configuration de l'appareil
 <timezone>
```

L'horodatage qui apparaîtra sur le rapport détaillé WildFire utilisera le fuseau horaire défini sur l'appareil. Si des administrateurs de plusieurs régions consulteront les rapports, définissez le fuseau horaire sur UTC.

- Pour configurer l'appareil WildFire afin qu'il se synchronise avec un serveur NTP, saisissez les commandes suivantes :

```
admin@WF-500> configurer admin@WF-500# définir le système
 deviceconfig ntp-servers primary-ntp-server ntp-server-
address<NTP primary server IP address>admin@WF-500# définir le
 système deviceconfig ntp-servers primary-ntp-server ntp-server-
address <NTP secondary server IP address>
```

L'appareil WildFire ne donne pas la priorité au serveur NTP principal ou secondaire ; il se synchronise avec l'un ou l'autre serveur.

STEP 8 | (Facultatif pour la configuration NTP) Définissez l’authentification du serveur NTP.

- Désactiver l'authentification NTP :

```
admin@WF-500# définir le système deviceconfig ntp-servers
 primary-ntp-server authentication-type sur aucun
```

- Activez l'échange de clés symétriques (secrets partagés) pour authentifier les mises à jour de l'heure du serveur NTP :

```
admin@WF-500# définir le système deviceconfig ntp-servers
 primary-ntp-server authentication-type symmetric-key
```

  Continuez à saisir l' **ID de clé** (1 - 65534), choisissez l' **algorithme** à utiliser dans l'authentification NTP (**MD5** ou **SHA1**), puis saisissez et confirmez l'algorithme d'authentification **authentication-key**.

- Utilisez la clé automatique (cryptographie à clé publique) pour authentifier les mises à jour de l'heure du serveur NTP :

```
admin@WF-500# définir le système deviceconfig ntp-servers
 primary-ntp-server authentication-type autokey
```

STEP 9 | Choisissez l'image de machine virtuelle que l'appareil devra utiliser pour l'analyse de fichiers.

L'image doit être basée sur les attributs qui représentent le plus exactement possible les logiciels installés sur les ordinateurs de vos utilisateurs finaux. Chaque image virtuelle contient différentes versions de systèmes d'exploitation et de logiciels, notamment Windows XP ou Windows 7 32 ou 64 bits, et des versions spécifiques d'Adobe Reader et Flash. Même si vous configurez l'appareil pour utiliser une configuration d'image de machine virtuelle, l'appareil utilise plusieurs instances de l'image afin d'améliorer les performances.

- Pour afficher une liste des machines virtuelles disponibles afin de déterminer celle qui représente le mieux votre environnement :

```
admin@WF-500> afficher wildfire vm-images
```

- Affichez l'image de machine virtuelle actuelle en exécutant la commande suivante et consultez le champ `Machine virtuelle sélectionnée`champ :

```
admin@WF-500> afficher état wildfire
```


- Sélectionnez l'image que l'appareil utilisera pour l'analyse :

```
admin@WF-500# définir le paramètre deviceconfig wildfire active-vm<vm-image-number>
```

Par exemple, pour utiliser vm-5 :

```
admin@WF-500# définir le paramètre deviceconfig wildfire active-vm vm-5
```

STEP 10 | Activez l'appareil WildFire afin d'observer les comportements malveillants, où le fichier en cours d'analyse cherche à accéder au réseau.

Paramétrage de l'interface VM de l'appareil WildFire.

STEP 11 | #unique_16

STEP 12 | (Optional (Facultatif)) Activez l’appareil WildFire pour qu’il effectue des recherches de verdict rapides et pour qu’il synchronise les verdicts avec le cloud WildFire public.

La commande de la CLI suivante permet d’activer l’appareil WildFire pour qu’il effectue des recherches de verdict rapides et pour qu’il synchronise les verdicts avec le cloud WildFire public. Cette fonction est désactivée par défaut ; définissez la commande sur **yes** pour activer cette fonction.

```
admin@WF-500# définir le paramètre deviceconfig wildfire cloud-intelligence cloud-query oui | non
```

STEP 13 | (Facultatif) Permettez à l'appareil WildFire d'obtenir des mises à jour de contenu quotidiennes de Palo Alto Networks pour faciliter et améliorer l'analyse des logiciels malveillants.

Activation des fonctions d'analyse de l'appareil WildFire

STEP 14 | (Facultatif) Permettez à l'appareil WildFire de générer les signatures DNS et antivirus et les catégories d'URL, et de distribuer les nouvelles signatures et catégories d'URL aux pare-feu connectés.

Activation de la génération de catégorie d'URL et de la signature locale

STEP 15 | (Facultatif) Envoyez automatiquement au cloud WildFire public les logiciels malveillants que le cloud WildFire privé détecte, pour soutenir la protection globale contre les logiciels malveillants.

Envoi des échantillons malveillants vers le cloud WildFire public.

STEP 16 | (Facultatif)Si vous ne souhaitez pas envoyer les échantillons de logiciels malveillants à l'extérieur du cloud WildFire privé, envoyez plutôt les rapports d'analyse au cloud WildFire public.

Si vous ne souhaitez pas envoyer les logiciels malveillants détectés localement au cloud WildFire public, il convient d'activer les envois de rapport d'analyse de logiciels malveillants pour améliorer et affiner les données d'intelligence WildFire sur les menaces.

Envoi des rapports d'analyse vers le cloud WildFire public.

STEP 17 | (Facultatif) Autorisez d'autres utilisateurs à gérer l'appareil WildFire.

Deux types de rôles peuvent être assignés : super utilisateur et super lecteur. Le rôle super utilisateur équivaut au compte admin et le rôle super lecteur dispose uniquement d'un accès en lecture.

Dans cet exemple, vous allez créer un compte super lecteur pour l'utilisateur bsimpson :

1. Passez en mode configuration :

```
admin@WF-500> configurer
```

2. Créez le compte utilisateur :

```
admin@WF-500# définir mgt-config users bsimpson<password>
```

3. Saisissez et confirmez un nouveau mot de passe.
4. Assignez le rôle super lecteur :

```
admin@WF-500# définir mgt-config users bsimpson permissions
 role-based superreader yes
```

STEP 18 | Configurez l'authentification RADIUS pour l'accès administrateur.

1. Créez un profil RADIUS à l'aide des options suivantes :

```
admin@WF-500# définir shared server-profile radius <profile-
name>
```

(Configurez le serveur'A0;RADIUS et d'autres attributs.)

2. Créez un profil d'authentification :

```
admin@WF-500# définir shared authentication-profile <profile-
name> method radius server-profile <server-profile-name>
```

3. Assignez le profil à un compte admin local :

```
admin@WF-500# définir mgt-config users username
 authentication-profile<authentication-profile-name>
```


Transfert de fichiers pour analyse par l’appareil WildFire

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Configurez les pare-feu Palo Alto Networks pour qu'ils transfèrent les fichiers ou les liens d'e-mail inconnus et les fichiers bloqués qui correspondent à des signatures antivirus existantes aux fins d’analyse. Utilisez le profil d’**analyse WildFire** pour définir les fichiers qui doivent être transférés au cloud privé WildFire (voire également sur le cloud public pour les déploiements cloud hybrides), puis associez le profil à une règle de sécurité qui déclenchera l’inspection des logiciels malveillants de type « zero-day ».

Précisez le trafic à transférer pour analyse selon l'application utilisée, le type de fichier détecté, les liens contenus dans les courriels ou le sens de transmission de l'échantillon (chargement, téléchargement ou les deux). Par exemple, vous pouvez configurer le pare-feu pour qu'il transfère les fichiers PE (Portable Executables/Exécutable portable) que les utilisateurs essaient de télécharger au cours d'une session de navigation Web. En plus des échantillons inconnus, le pare-feu transfère les fichiers bloqués qui correspondent aux signatures antivirus existantes. Palo Alto Networks dispose ainsi d’une source précieuse de renseignements sur les menaces qui se fondent sur les variantes des fichiers malveillants que les signatures ont réussi à bloquer, alors qu’ils n’avaient jamais été observés par WildFire, ni par le pare-feu.

Vous pouvez étendre les ressources d’analyses WildFire à un Cloud WildFire hybride : en configurant le pare-feu pour qu’il poursuive le transfert des fichiers de nature sensible vers votre cloud privé WildFire pour analyse locale et qu’il transfère les types de fichiers de nature moins sensible ou non pris en charge vers le cloud public WildFire.

De plus, vous pouvez consacrer les ressources des appareils WildFire à l’analyse de certains types de fichiers précis : soit des documents (fichiers Microsoft Office et PDF) ou des PE. Par exemple, si vous déployez un Cloud WildFire hybride : pour analyser les documents localement et les fichiers PE dans les clouds publics WildFire, vous pouvez consacrer tous les environnements d’analyse à l’analyse des documents. Ce faisant, vous pouvez délester l’analyse des fichiers PE vers le cloud public, ce qui vous permet d’allouer un plus grand nombre de ressources des appareils WildFire au traitement des documents de nature délicate.

Avant de commencer :

- ❑ S'il existe un autre pare-feu entre le pare-feu que vous configurez pour effectuer le transfert des fichiers et le cloud WildFire ou l'appareil WildFire, vérifiez que ce pare-feu autorise les ports suivants :

Port	Usage
443	• Enregistrement • Téléchargements PCAP • Téléchargements d’échantillons • Récupération du rapport • Envoi de fichiers • Téléchargements de rapports PDF

Port	Usage
10443	Mises à jour dynamiques

STEP 1 | (PA-7000 Series Firewalls Only (Pare-feu des séries PA-7000 uniquement)) Pour permettre à un pare-feu des séries PA-7000 de transférer des fichiers et des liens d'email pour analyse WildFire, vous devez d'abord configure a data port on an NPC as a Log Card interface (configurer un port de données sur un NPC comme interface de type carte de journal). Si vous disposez d'un appareil de la série PA-7000 équipé d'une LFC (log forwarding card (carte de transfert des journaux)), vous devez configure a port used by the LFC (configurer un port utilisé par la LFC). Lorsqu'il est configuré, le port de carte de journal ou l'interface LFC a priorité sur le port de gestion lors du transfert d'échantillons WildFire.

STEP 2 | Précisez le cloud privé ou hybride WildFire auquel vous souhaitez transférer des échantillons.

Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **WildFire**, puis modifiez les General Settings (Paramètres généraux) selon votre déploiement de cloud WildFire (public ou hybride).

Cloud WildFire privé :

1. Saisissez l'adresse IP ou FQDN de l'appareil WildFire dans le champ **WildFire Private Cloud (Cloud WildFire privé)**.

Cloud WildFire hybride :

1. Saisissez l'URL du **WildFire Public Cloud (cloud WildFire public)** :
   - États-Unis : **wildfire.paloaltonetworks.com**
   - Europe : **eu.wildfire.paloaltonetworks.com**
   - Japon : **jp.wildfire.paloaltonetworks.com**
   - Singapour : **sg.wildfire.paloaltonetworks.com**
   - United Kingdom: **uk.wildfire.paloaltonetworks.com**
   - Canada: **ca.wildfire.paloaltonetworks.com**
   - Australie : **au.wildfire.paloaltonetworks.com**
   - Allemagne : **de.wildfire.paloaltonetworks.com**
   - Inde : **in.wildfire.paloaltonetworks.com**
   - Suisse : **ch.wildfire.paloaltonetworks.com**
   - Pologne : **pl.wildfire.paloaltonetworks.com**
   - Indonésie : **id.wildfire.paloaltonetworks.com**
   - Taïwan : **tw.wildfire.paloaltonetworks.com**
   - France : **fr.wildfire.paloaltonetworks.com**
   - Qatar : **qatar.wildfire.paloaltonetworks.com**
   - Corée du Sud : **kr.wildfire.paloaltonetworks.com**
   - Israël : **il.wildfire.paloaltonetworks.com**
   - Arabie Saoudite : **sa.wildfire.paloaltonetworks.com**
   - Espagne : **es.wildfire.paloaltonetworks.com**
2. Saisissez l'adresse IP ou FQDN de l'appareil WildFire dans le champ **WildFire Private Cloud (Cloud WildFire privé)**.

STEP 3 | Définissez les limites de taille des fichiers que le pare-feu transfère à WildFire et configurez les paramètres de journalisation et de génération de rapports.

Continuez à modifier les paramètres généraux de WildFire (**Device (Périphérique)** > **Setup (Configuration)** > **WildFire (WildFire)**).

- Passez en revue les **limites de taille de fichier** pour les fichiers transférés à partir du pare-feu.

  Il est recommandé par WildFire de définir la taille de fichier pour les ***PE sur la limite de taille maximale de 10 Mo et de laisser la*** *Taille de fichier* ***pour tous les autres types de fichiers définie sur la valeur par défaut.***

- Sélectionnez **Report Benign Files (Rapporter les fichiers bénins)** pour permettre la journalisation des fichiers qui reçoivent un verdict WildFire bénin.
- Sélectionnez **Report Grayware Files (Signaler des fichiers indésirables)** pour permettre la journalisation des fichiers qui reçoivent un verdict WildFire indésirable.
- Définissez les informations de session qui sont consignées dans les rapports d'analyse WildFire en modifiant la section Session Information Settings (Paramètres d'informations de session). Par défaut, toutes les informations de session sont affichées dans les rapports d'analyse de WildFire. Décochez les cases correspondant à des champs pour les supprimer des rapports d'analyse WildFire, puis cliquez sur **OK (OK)** pour enregistrer les paramètres.

STEP 4 | (Panorama uniquement) Configurez Panorama pour la collecte d'informations complémentaires sur les échantillons recueillis auprès des pare-feu qui utilisent une version de PAN-OS antérieure à PAN-OS 7.0.

Certains champs de journal des envois WildFire introduits dans PAN-OS 7.0 ne sont pas remplis pour les échantillons envoyés par des pare-feu exécutant des versions de logiciel antécédentes. Si vous utilisez Panorama pour gérer les pare-feu exécutant des versions de logiciel antérieures à PAN-OS 7.0, Panorama peut communiquer avec WildFire pour recueillir les informations d'analyse relatives aux échantillons envoyés par ces pare-feu à partir du **WildFire Server (Serveur Wildfire)** (le cloud WildFire global, par défaut) afin de finaliser les détails des journaux.

Sélectionnez **Panorama (Panorama)** > **Setup (Configuration)** > **WildFire (WildFire)** et saisissez un **WildFire Server (Serveur WildFire)** si vous souhaitez modifier le paramètre par défaut pour permettre à Panorama de recueillir les détails à partir du cloud WildFire indiqué ou d'un appareil WildFire.

STEP 5 | Définissez le trafic à transférer vers WildFire pour analyse.

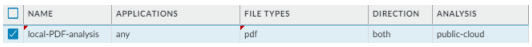
Si vous avez configuré un appareil WildFire, vous pouvez utiliser, à la fois, le cloud privé et le cloud public dans un déploiement de cloud hybride. Analysez les fichiers sensibles localement sur votre réseau, tandis que vous envoyez tous les autres fichiers inconnus au cloud WildFire public pour analyse approfondie et un renvoi de verdict rapide.

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **WildFire Analysis (Analyse WildFire)**, puis **Add (Ajouter)** un nouveau profil d'analyse WildFire et donnez un **Name (Nom)** descriptif au profil.
2. **Add (Ajoutez)** une règle au profil pour définir le trafic à transférer vers WildFire pour analyse et donnez à la règle un **Name (Nom)** descriptif, tel quel analyse-PDF-locale.
3. Définissez une règle de profil à faire correspondre au trafic inconnu pour le transfert des échantillons en vue de leur analyse selon les éléments suivants :
   - **Applications** : cette option permet le transfert des fichiers pour analyse selon l'application utilisée.
   - **File Types (Types de fichiers)** : cette option permet le transfert des fichiers pour analyse selon les types de fichiers, y compris les liens contenus dans les messages électroniques. Par exemple, sélectionnez **PDF (PDF)** pour envoyer, pour analyse, des PDF inconnus qui ont été détectés par le pare-feu.
   - **Direction (Sens)** : cette option permet le transfert des fichiers pour analyse selon le sens de transmission du fichier (chargement, téléchargement ou les deux). Par exemple, sélectionnez

both (les deux) pour transférer tous les PDF inconnus pour qu'ils soient analysés, peu importe le sens de transmission.

4. Définissez l'emplacement d'**Analysis (Analyse)** vers lequel le pare-feu transfère les fichiers qui satisfont la règle.
   - Sélectionnez **public-cloud (cloud public)** pour transférer les échantillons correspondants au cloud WildFire public pour analyse.
   - Sélectionnez **private-cloud (cloud privé)** pour transférer les échantillons correspondants à un cloud WildFire privé pour analyse.

   Par exemple, pour analyser des PDF qui contiennent des renseignements exclusifs sensibles sans envoyer ces documents hors de votre réseau, établissez l'emplacement de l'**Analysis (Analyse)** à **private-cloud (cloud privé)** pour la règle intitulée analyse-PDF-local.



Différentes règles peuvent transférer des échantillons correspondant à différents emplacements d'analyse selon vos besoins. L'exemple ci-dessus montre une règle qui transfère les types de fichiers sensibles pour l'analyse locale dans un cloud WildFire privé. Vous pourriez créer une autre règle pour transférer les types de fichiers moins sensibles, comme les PE, vers le cloud WildFire public. Cette flexibilité est prise en charge avec un déploiement de cloud WildFire hybride.

*Par mesure de précaution, lorsqu'un cloud hybride est déployé, les fichiers qui correspondent aux règles établies pour le **private-cloud (cloud privé)** ainsi qu'à celles établies pour le **public-cloud (cloud public)** sont transférés uniquement vers le cloud privé.*

5. (Facultatif) Continuez d'ajouter des règles au profil d'analyse WildFire, au besoin. Par exemple, vous pourriez ajouter une seconde règle au profil visant le transfert de fichiers de package APK Android, PE (Portable Executable/exécutable portable)et Flash vers le cloud WildFire public pour analyse.
6. Cliquez sur **OK** pour enregistrer le profil d'analyse WildFire.
7. (Facultatif) Continuez d'ajouter des règles au profil d'analyse WildFire, au besoin. Par exemple, vous pourriez ajouter une seconde règle au profil visant le transfert de fichiers de package APK Android, PE (Portable Executable/exécutable portable)et Flash vers le cloud WildFire public pour analyse.
8. Cliquez sur **OK** pour enregistrer le profil d'analyse WildFire.

STEP 6 | (Facultatif) Allouez les ressources des appareils WildFire à l'analyse des documents ou des fichiers exécutables.

Si vous déployez un cloud hybride pour analyser des types de fichiers précis localement et sur le cloud WildFire public, vous pouvez consacrer des environnements d'analyse au traitement d'un type de fichier. Vous pouvez ainsi mieux affecter vos ressources en fonction de la configuration de votre environnement d'analyse. Si vous ne consacrez pas de ressources à un environnement d'analyse, les ressources sont affectées selon les paramètres par défaut.

Utilisez la commande de la CLI suivante :

```
admin@WF-500# set deviceconfig setting wildfire preferred-analysis-environment documents | exécutables | défaut
```

Et sélectionnez l'une des options suivantes :

- documents (documents) : consacre les ressources d'analyse à une analyse simultanée de 25 documents, 1 Portable Executable (exécutable portable ; PE) et 2 liens d'e-mail.
- executables (exécutables) : consacre les ressources d'analyse à une analyse simultanée de 25 Portable Executables (exécutable portable ; PE), 1 document et 2 liens d'e-mail.
- defaut (par défaut) : consacre les ressources d'analyse à une analyse simultanée de 16 documents, 10 Portable Executables (exécutable portable ; PE) et 2 liens d'e-mail.

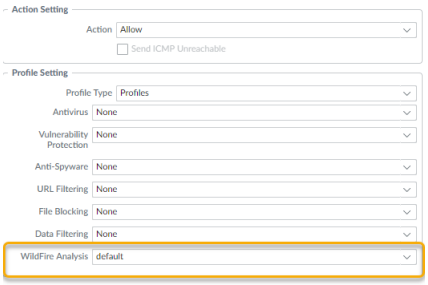
Confirmez que tous les processus des appareils WildFire fonctionnent en exécutant la commande suivante :

```
admin@WF-500> afficher l'état du logiciel système
```

STEP 7 | Associez le profil d'analyse WildFire à une règle de politique de sécurité.

Le trafic qui est autorisé par la règle de politique de sécurité est évalué selon le profil d'analyse WildFire joint ; les pare-feu transfèrent le trafic correspondant au profil pour analyse par WildFire.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et **Add (Ajoutez)** ou modifiez une règle de politique.
2. Cliquez sur l'onglet **Actions (Actions)** de la règle de politique.
3. Dans la section Paramètres des profils, sélectionnez **Profiles (Profils)** en tant que **Profile Type (Type de profil)** et sélectionnez un profil d'**WildFire Analysis (Analyse WildFire)** à joindre à la règle de politique



STEP 8 | Assurez-vous d’activer, sur le pare-feu, le transfert du trafic SSL décrypté pour analyse par WildFire.

C’est une meilleure pratique WildFire.

STEP 9 | Passez en revue les meilleures pratiques WildFire et appliquez-les.

STEP 10 | Cliquez sur **Commit (Valider)** pour appliquer les paramètres de WildFire.

STEP 11 | (Facultatif) Vérifiez les envois WildFire.

STEP 12 | Décidez ce que vous devez faire ensuite...

- Procédez à la vérification des envois WildFire pour confirmer que le pare-feu transfère correctement les fichiers pour analyse WildFire.
- Envoyez des échantillons malveillants ou des rapports à partir de l’appareil WildFire. Activez cette fonctionnalité pour transférer automatiquement les logiciels malveillants détectés dans votre cloud WildFire privé vers le cloud WildFire public. Le cloud WildFire public analyse de nouveau l'échantillon et génère une signature s'il est malveillant. La signature est distribuée à l'ensemble des utilisateurs à l'échelle mondiale par l'entremise des mises à jour de signatures WildFire.
- Effectuez la Surveillance de l’activité de l’appareil WildFire pour évaluer les alertes et les informations données sur les échantillons malveillants.

Envoi des échantillons malveillants ou des rapports à partir de l'appareil WildFire

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Activez la fonctionnalité d'intelligence du cloud de l'appareil WildFire afin d'envoyer automatiquement les échantillons malveillants détectés dans le cloud WildFire privé au cloud WildFire public. Le cloud WildFire public fait une analyse plus approfondie de l'échantillon malveillant et génère une signature pour identifier l'échantillon. La signature est ensuite ajoutée aux mises à jour de signatures WildFire et distribuée à l'ensemble des utilisateurs mondiaux pour empêcher toute exposition ultérieure à la menace. Si vous ne souhaitez pas envoyer les échantillons malveillants à l'extérieur de votre réseau, vous pouvez plutôt choisir d'envoyer seulement les rapports WildFire des échantillons malveillants qui ont été découverts sur votre réseau afin de les ajouter aux statistiques WildFire et aux renseignements sur les menaces.

- Envoi des échantillons malveillants vers le cloud WildFire public

  À partir de l'appareil WildFire, exécutez les commandes de la CLI suivantes afin de permettre à l'appareil d'envoyer automatiquement les échantillons malveillants vers le cloud WildFire public :

  ```
  admin@WF-500admin@WF-500# définir deviceconfig paramètre wildfire
   cloud-intelligence submit-sample oui
  ```

  Si la capture de paquet (PCAP) est activée sur le pare-feu qui a initialement envoyé l'échantillon pour analyse par le cloud WildFire privé, la PCAP de l'échantillon malveillant sera également transférée vers le cloud WildFire public.

- Envoi des rapports sur les échantillons malveillants vers le cloud WildFire public

  *Si l'*envoi des échantillons malveillants vers le cloud WildFire public *est activé sur l'appareil WildFire, vous n'avez pas à activer l'envoi de rapports sur les échantillons malveillants vers le cloud public sur l'appareil. Lorsqu'un échantillon malveillant est envoyé au cloud WildFire public, le cloud public génère un nouveau rapport d'échantillon malveillant pour cet échantillon.*

  Pour activer l'envoi automatique des rapports d'échantillons malveillants (plutôt que l'échantillon lui-même) au cloud WildFire public, exécutez la commande CLI suivante sur l'appareil WildFire :

  ```
  admin@WF-500# définir deviceconfig paramètre wildfire cloud-
  intelligence submit-report sur oui
  ```

- Vérification des paramètres de l'intelligence du cloud

  Confirmez que l'intelligence du cloud est activée pour envoyer les échantillons malveillants ou les rapports sur les échantillons malveillants vers le cloud WildFire public en exécutant la commande suivante :

  ```
  admin@WF-500> afficher l'état wildfire
  ```

  Consultez les champs `Submit sample` et `Submitreport`.

Configurer l'authentification à l'aide d'un certificat personnalisé sur un appareil WildFire autonome

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Par défaut, un appareil WildFire utilise des certificats prédéfinis pour l'authentification mutuelle afin d'établir les connexions SSL utilisées pour l'accès de gestion et la communication entre périphériques. 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 assurer une authentification mutuelle entre votre appareil WildFire et les pare-feu ou Panorama. 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.

Les rubriques suivantes décrivent comment configurer des appareils WildFire autonomes qui ne sont pas gérés par Panorama. Pour la configuration des certificats personnalisés pour les dispositifs WildFire et le cluster WildFire géré par Panorama, consultez le Guide d'administration de Panorama.

- Authentification mutuelle SSL des appareils WildFire
- Configurer l'authentification avec des certificats personnalisés sur l'appareil WildFire

Authentification mutuelle SSL des appareils WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Lorsqu'un pare-feu ou Panorama envoie un échantillon à un appareil WildFire pour analyse, le pare-feu agit en tant que client et l’appareil WildFire agit en tant que serveur. Pour s'authentifier mutuellement, chaque appareil présente un certificat pour s'identifier auprès de l'autre appareil.

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** : un appareil WildFire nécessite un certificat et un profil de certificat pour s'identifier auprès des pare-feu. 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 de l’appareil dans le nom commun du certificat (CN) ou le nom de l'attribut du sujet. Le pare-feu correspond au nom CN ou Subject Alt dans

le certificat que le serveur présente par rapport à l'adresse IP ou au FQDN du dispositif WildFire pour vérifier l'identité de l'appareil WildFire.

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.

- **Certificats clients et profil** : chaque pare-feu 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.

Configurer l'authentification avec des certificats personnalisés sur l'appareil WildFire

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Utilisez le flux de travail suivant pour remplacer les certificats prédéfinis par des certificats personnalisés dans votre déploiement WildFire. Lorsqu'un pare-feu ou Panorama envoie un échantillon à un appareil WildFire pour analyse, le pare-feu agit en tant que client et l'appareil WildFire agit en tant que serveur.

STEP 1 | Obtenez des paires de clés et des certificats d'autorité de certification (CA) pour l'appareil WildFire et le pare-feu ou Panorama.

STEP 2 | Importez le certificat CA pour valider le certificat sur le pare-feu.

1. Connectez-vous à la CLI sur l'appareil WildFire et passez en mode de configuration.

   ```
   admin@WF-500> configurer
   ```

2. Utilisez TFTP ou SCP pour importer le certificat.

   ```
   admin@WF-500#{tftp | scp} importer le certificat depuis
    le <value> fichier <value> remote-port <1-65535> source-
   ip au format<ip/netmask> certificate-name <value> phrase
    secrète <value> {pkcs12 | pem}
   ```

STEP 3 | Utilisez TFTP ou SCP pour importer la paire de clés contenant le certificat de serveur et la clé privée pour l'appareil WildFire.

```
admin@WF-500# {tftp | scp} importer la paire de clés depuis
 le<value> fichier <value> remote-port <1-65535> source-ip au
```



```
format <ip/netmask> certificate-name <value> phrase secrète<value>
{pkcs12 | pem}
```

STEP 4 | 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. Sur le CLI de l'appareil WildFire, saisissez le mode de configuration.

   ```
   admin@WF-500> configurer
   ```

2. Nommez le profil de certificat.

   ```
   admin@WF-500# définir shared certificate-profile <name>
   ```

3. Configurez le CA.

   Les commandes default-ocsp-url et ocsp-verify-cert sont facultatives.

   ```
   admin@WF-500# définir shared certificate-profile <name>
    Autorité de certification <name>
   ```

   ```
   admin@WF-500# définir shared certificate-profile <name>
    CA <name> [default-ocsp-url <value>]
   ```

   ```
   admin@WF-500# définir shared certificate-profile <name>
    Autorisation de certification <name> [ocsp-verify-
   cert <value>]
   ```


STEP 5 | Configurez un profil SSL / TLS pour l'appareil WildFire. Ce profil définit le certificat et la plage de protocoles SSL / TLS utilisés par l'appareil et les pare-feu WildFire pour les services SSL / TLS.

1. Identifiez le profil SSL/TLS.

```
admin@WF-500# définir shared ssl-tls-service-profile <name>
```

2. Sélectionnez le certificat.

```
admin@WF-500# définir un certificat shared ssl-tls-service-
profile <name> <value>
```

3. Définissez la plage SSL/TLS.

Les versions de PAN-OS 8.0 et les versions ultérieures prennent uniquement en charge les versions TLS 1.2 et les versions ultérieures. Vous devez définir la version maximale sur TLS 1.2 ou maximum.

```
admin@WF-500# définir shared ssl-tls-service-profile <name>
 protocol-settings min-version {tls1-0 | tls1-1 | tls1-2}
```

```
admin@WF-500# définir shared ssl-tls-service-profile <name>
 protocol-settings max-version {tls1-0 | tls1-1 | tls1-2 |
 max}
```

STEP 6 | Configurez la communication sécurisée avec le serveur sur l'appareil WildFire.

1. Définissez le profil de SSL/TLS. Ce profil de service SSL / TLS s'applique à toutes les connexions SSL entre WildFire et les machines clientes.

```
admin@WF-500# définir la gestion des paramètres deviceconfig
 secure-conn-server ssl-tls-service-profile <ssltls-profile>
```

2. Définissez le profil de certificat.

```
admin@WF-500# définir la gestion des paramètres deviceconfig
 secure-conn-server certificate-profile <certificate-profile>
```


Paramétrage de l'interface VM de l'appareil WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

L'interface de la machine virtuelle (vm-interface) assure la connectivité réseau externe des machines virtuelles bac à sable dans l'appareil WildFire pour permettre d'observer des comportements malveillants dans lesquels le fichier analysé tente d'accéder au réseau. Les sections suivantes décrivent l'interface MV et les étapes à suivre pour sa configuration. Vous pouvez également activer la fonctionnalité Tor sur l'interface MV ; celle-ci masque le trafic malveillant envoyé par l'appareil WildFire via l'interface MV, de manière à ce que les sites malveillants vers lesquels le trafic peut être envoyé ne puissent pas détecter votre adresse IP publique.

Cette section explique également les étapes à suivre pour connecter l'interface MV à un port dédié sur un pare-feu Palo Alto Networks afin d'activer la connectivité Internet.

- Présentation de l'interface de machine virtuelle
- Configuration de l'interface MV sur l'appareil WildFire
- Connexion du pare-feu à l'interface MV de l'appareil WildFire

Présentation de l'interface de machine virtuelle

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

L'interface MV (nommée **1** à l'arrière de l'appareil) est utilisée par WildFire pour améliorer les fonctionnalités de détection des logiciels malveillants. L'interface permet à un échantillon en cours d'exécution sur les machines virtuelles WildFire de communiquer avec Internet de sorte que l'appareil WildFire puisse mieux analyser le comportement de cet échantillon afin de déterminer s'il montre des caractéristiques propres à un logiciel malveillant.

- *Bien qu'il soit recommandé d'activer l'interface MV, il est très important que vous ne la connectiez pas à un réseau où n'importe lequel de vos serveurs/hôtes pourrait accéder, car les logiciels malveillants qui s'exécutent dans les machines virtuelles WildFire peuvent éventuellement utiliser cette interface pour se propager.*
- *Cette connexion peut être une ligne ADSL dédiée ou une connexion réseau qui autorise uniquement un accès direct à Internet depuis l'interface MV et qui limite tout accès à des serveurs internes/hôtes clients.*
- *L’interface VM sur vos appareils WildFire fonctionnant en mode FIPS/CC est désactivée.*

Le schéma suivant illustre deux options permettant de connecter l'interface MV au réseau.

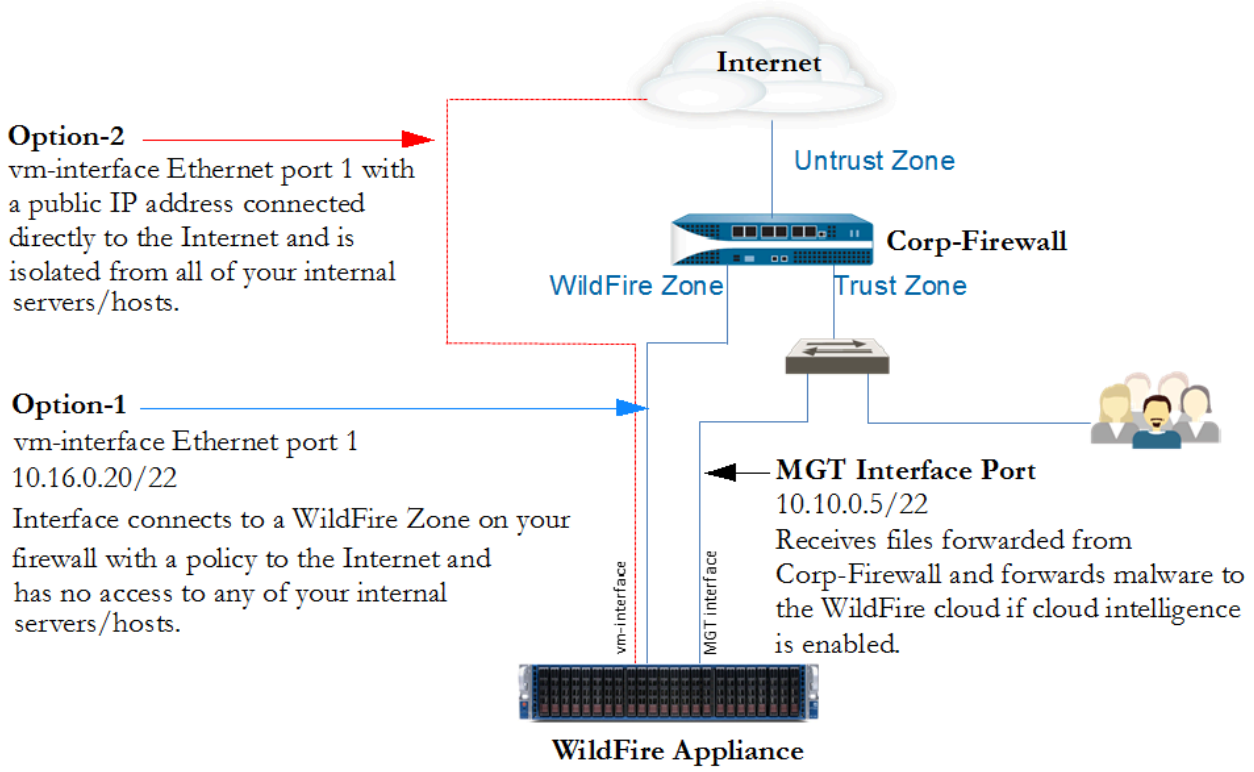


Figure 1: Exemple d'interface de machine virtuelle

- **Option 1** (recommandée) : connectez l'interface VM à une interface dans une zone dédiée sur un pare-feu dont la politique autorise uniquement l'accès à Internet. Cette politique est importante car les logiciels malveillants qui s'exécutent dans les machines virtuelles WildFire peuvent éventuellement utiliser cette interface pour se propager. Cette option est recommandée car les logs du pare-feu vont fournir une visibilité sur n'importe quel trafic généré par l'interface MV.
- **Option 2** - Utilisez une connexion dédiée à un fournisseur Internet, comme une connexion ADSL, pour connecter l'interface MV à Internet. Vérifiez que les serveurs/hôtes internes n'ont pas accès à cette connexion. Bien qu'il s'agisse d'une solution simple, le trafic généré par le logiciel malveillant de l'interface MV ne sera pas consigné à moins que vous placiez un pare-feu ou un outil de surveillance du trafic entre l'appareil WildFire et la connexion ADSL.

Configuration de l'interface MV sur l'appareil WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Cette section explique les différentes étapes requises pour configurer l'interface MV sur l'appareil WildFire en utilisant la configuration de l'option 1 détaillée dans l'exemple d'interface de machine virtuelle. Après avoir configuré l'interface MV en utilisant cette option, vous devez également configurer une interface sur un pare-feu Palo Alto Networks par lequel le trafic issu de l'interface MV sera acheminé, comme décrit dans la section Connexion du pare-feu à l'interface MV de l'appareil WildFire.

Par défaut, l'interface MV comporte les paramètres suivants :

- Adresse IP : 192.168.2.1
- Masque réseau : 255.255.255.0
- Passerelle par défaut : 192.168.2.254
- DNS : 192.168.2.254

Si vous prévoyez d'activer cette interface, configurez-la avec les paramètres adaptés à votre réseau. Si vous ne prévoyez pas d'utiliser cette interface, conservez les paramètres par défaut. Notez que cette interface doit disposer de valeurs réseau configurées ou la configuration échouera.

STEP 1 | Définissez les informations relatives à l'adresse IP pour l'interface MV sur l'appareil WildFire. Les valeurs IPv4 suivantes sont utilisées dans cet exemple mais l'appareil est aussi compatible avec des adresses IPv6 :

- Adresse IP : 10.16.0.20/22
- Masque de sous-réseau - 255.255.252.0
- Passerelle par défaut - 10.16.0.1
- Serveur DNS - 10.0.0.246

L'interface MV ne peut pas se trouver sur le même réseau que l'interface de gestion (MGT).

1. Passez en mode configuration :

```
admin@WF-500> configurer
```

2. Définissez les informations relatives à l'adresse IP pour l'interface MV :

```
admin@WF-500# définir deviceconfig system vm-interface ip-
address 10.16.0.20 netmask 255.255.252.0 default-gateway
 10.16.0.1 dns-server 10.0.0.246
```

Vous ne pouvez configurer qu'un seul serveur DNS sur l'interface MV. Il est recommandé d'utiliser le serveur DNS de votre ISP ou un service DNS ouvert.

STEP 2 | Activez l'interface MV.

1. Activez l'interface MV :

```
admin@WF-500# définir le paramètre deviceconfig wildfire vm-
network-enable oui
```

2. Validez la configuration :

```
admin@WF-500# valider
```

STEP 3 | Testez la connectivité de l'interface MV.

Exécutez une commande ping sur un système et spécifiez l'interface MV comme la source. Par exemple, si l'adresse IP de l'interface MV est 10.16.0.20, exécutez la commande suivante où *ip-ou-nom-hôte* est l'adresse IP ou le nom d'hôte d'un serveur/réseau sur lequel la commande ping est activée :

```
admin@WF-500> source du ping 10.16.0.20 host ip-or-hostname
```

Par exemple :

```
admin@WF-500> source du ping 10.16.0.20 host 10.16.0.1
```


STEP 4 | (Facultatif) Envoyez tout le trafic malveillant que le logiciel malveillant génère vers Internet. Le réseau Tor masque votre adresse IP publique, de manière à ce que les sites malveillants ne puissent pas déterminer la source du trafic.

1. Activez le réseau Tor :

```
admin@WF-500# définir le paramètre deviceconfig wildfire vm-network-use-tor
```

2. Validez la configuration :

```
admin@WF-500# valider
```

STEP 5 | (Facultatif) Vérifiez que la connexion au réseau Tor est active et fonctionnelle.

1. Lancez les commandes CLI suivantes pour chercher les ID d'événement Tor dans les journaux de l'appareil. Un appareil WildFire bien configuré et fonctionnel ne devrait générer aucun ID d'événement :
   - **admin@WF-500(active-controller)>show log system direction equal backward | match anonymous-network-unhealthy—**Le service Tor est inactif ou non fonctionnel. Songez à redémarrer votre service Tor pour vérifier s'il fonctionne correctement.
   - **admin@WF-500(active-controller)>show log system direction equal backward | match anonymous-network-unavailable—**Le service Tor fonctionne normalement, mais l'interface VM de l'appareil WildFire n'arrive pas à établir une connexion. Vérifiez vos paramètres de connexion réseau et testez le service de nouveau.

STEP 6 | Connexion du pare-feu à l'interface MV de l'appareil WildFire.

Connexion du pare-feu à l'interface MV de l'appareil WildFire

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

L'exemple de flux de travail suivant explique comment connecter l'interface MV à un port sur un pare-feu Palo Alto Networks. Avant de connecter cette interface au pare-feu, une zone non approuvée du pare-feu doit déjà être connectée à Internet. Dans cet exemple, vous configurez une nouvelle zone nommée wf-vm-zone qui contiendra l'interface MV utilisée pour connecter l'interface MV sur l'appareil au pare-feu. La politique associée à cette zone va uniquement autoriser les communications entre l'interface MV et la zone non approuvée.

STEP 1 | Configurez l'interface du pare-feu auquel l'interface MV va se connecter et paramétrez le routeur virtuel.

La zone wf-vm-zone ne doit contenir que l'interface (ethernet1/3 dans cet exemple) utilisée pour connecter l'interface MV sur l'appareil au pare-feu. Ceci permet d'empêcher le trafic généré par le logiciel malveillant de se propager sur d'autres réseaux.

1. Dans l'interface Web du pare-feu, sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)**, puis sélectionnez une interface, par exemple : **Ethernet 1/3 (Ethernet 1/3)**.
2. Dans la liste déroulante **Interface Type (Type d'interface)**, sélectionnez **Layer3 (Couche 3)**.
3. Dans l'onglet **Config (Configuration)**, cliquez sur la liste déroulante **Security Zone (Zone de sécurité)**, sélectionnez **New Zone (Nouvelle zone)**.
4. Dans le champ **Nom** de la boîte de dialogue Zone, saisissez wf-vm-zone, puis cliquez sur **OK**.
5. Dans la liste déroulante **Virtual Router (Routeur virtuel)**, sélectionnez **default (Par défaut)**.
6. Pour affecter une adresse IP à l'interface, sélectionnez l'onglet **IPv4** ou **IPv6** puis cliquez sur **Ajouter** dans la section IP et saisissez l'adresse IP, ainsi que le masque réseau à affecter à l'interface, par exemple, 10.16.0.0/22 (IPv4) ou 2001:db8:123:1::1/64 (IPv6).
7. Pour enregistrer la configuration de l'interface, cliquez sur **OK**.

STEP 2 | Créez une politique de sécurité sur le pare-feu pour autoriser l'accès à Internet depuis l'interface MV et bloquer l'ensemble du trafic entrant. Dans cet exemple, le nom de la politique est WildFire VM Interface. Étant donné que vous n'allez pas créer une politique de sécurité entre la zone non approuvée et la zone wf-vm-interface, l'ensemble du trafic entrant est bloqué par défaut.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**, puis cliquez sur **Add (Ajouter)**.
2. Dans l'onglet **General (Général)**, saisissez un **Name (Nom)**.
3. Dans l'onglet **Source (Source)**, définissez la **Source Zone (Zone source)** sur **wf-vm-zone (wf-vm-zone)**.
4. Dans l'onglet **Destination**, définissez la **zone de destination** sur **Untrust (Non approuvée)**.
5. Dans les onglets **Application (Application)** et **Service/URL Category (Catégorie de service/URL)**, conservez le paramètre par défaut **Any (Indifférent)**.
6. Dans l'onglet **Actions**, définissez **Action Setting (Paramètre d'action)** sur **Allow (Autoriser)**.
7. Sous **Log Setting (Paramètre des logs)**, cochez la case **Log at Session End (Se connecter à la fin de la session)**.

*Si vous craignez qu'une personne puisse ajouter involontairement d'autres interfaces à la zone wf-vm-zone, clonez la politique de sécurité de l'interface MV WildFire puis, dans l'onglet **Action** de la règle clonée, sélectionnez **Deny (Refuser)**. Vérifiez que cette nouvelle politique de sécurité s'affiche sous la politique de l'interface MV WildFire. Ceci remplacera la règle d'autorisation intra-zone implicite qui autorise les communications entre les interfaces d'une même zone et refuse/bloque toutes les communications intra-zone.*

STEP 3 | Connectez les câbles.

Connectez physiquement l'interface MV de l'appareil WildFire au port que vous avez configuré sur le pare-feu (Ethernet 1/3 dans cet exemple) à l'aide d'un câble RJ-45 droit. L'interface MV correspond au chiffre **1** à l'arrière de l'appareil.

Activation des fonctions d'analyse de l'appareil WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

- Paramétrage des mises à jour de contenu de l'appareil WildFire
- Activation de la génération de catégorie d'URL et de la signature locale
- Envoi des logiciels malveillants découverts localement ou des rapports au cloud WildFire public

Paramétrage des mises à jour de contenu de l'appareil WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Configurez les mises à jour de contenu quotidiennes sur l'appareil WildFire. Les mises à jour de contenu de l'appareil WildFire fournissent à l'appareil des renseignements sur les menaces, ce qui facilite la détection des logiciels malveillants, améliore la capacité de l'appareil à différencier les logiciels malveillants et bénins et garantit que l'appareil dispose des toutes dernières informations nécessaires à la génération de signatures.

- Installation des mises à jour de contenu WildFire directement à partir du serveur de mises à jour
- Installation des mises à jour de contenu WildFire à partir d'un serveur SCP

Installation des mises à jour de contenu WildFire directement à partir du serveur de mises à jour

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

STEP 1 | Vérifiez la connectivité entre l'appareil et le serveur de mises à jour, et identifiez la mise à jour du contenu à installer.

1. Connectez-vous à l'appareil WildFire et exécutez la commande suivante pour afficher la version du contenu actuelle :

```
admin@WF-500> Afficher les informations système | correspondre
 à wf-content-version
```

2. Vérifiez que l'appareil peut communiquer avec le serveur de mises à jour de Palo Alto Networks et affichez les mises à jour disponibles :

```
admin@WF-500> demande de mise à niveau du contenu wf
```

La commande interroge le serveur de mises à jour de Palo Alto Networks, renvoie des informations sur les mises à jour disponibles et identifie la version installée sur l'appareil.

```
Taille de la version Publiée sur Téléchargé Installé
 ------------------------------------------------- 2-253
 57MB 2014/09/20 20:00:08 PDT no no 2-39 44MB 2014/02/12
 14:04:27 PST oui actuel
```

Si l'appareil ne peut pas se connecter au serveur de mises à jour, vous devrez autoriser la connectivité entre l'appareil et le serveur de mises à jour de Palo Alto Network (updates.paloaltonetworks.com), ou télécharger et installer la mise à jour à l'aide de SCP comme décrit dans la section Installation des mises à jour de contenu WildFire à partir d'un serveur SCP.

STEP 2 | Téléchargez et installez la dernière mise à jour du contenu.

1. Téléchargez la dernière mise à jour du contenu :

```
admin@WF-500> demander la mise à niveau wf-content télécharger
 la plus récente
```

2. Affichez le statut du téléchargement :

```
admin@WF-500> afficher tous les emplois
```

Vous pouvez exécuter la commande **show jobs pending** pour afficher les tâches en attente. Le résultat suivant montre que le téléchargement (ID de tâche 5) est terminé (statut FIN) :

```
Résultat de l'état du type d'ID mis en file d'attente
 Terminé ------------------------------------------------
 22/04/2014 03:42:20 5 Downld FIN OK 03:42:23
```

3. Une fois le téléchargement terminé, installez la mise à jour :

```
admin@WF-500> demander la mise à niveau wf-content installer
 la dernière version
```

Exécutez de nouveau la commande **show jobs all** pour connaître le statut de l'installation.

STEP 3 | Vérifiez la mise à jour du contenu.

Exécutez la commande suivante et consultez le champ `wf-content-version` :

```
admin@WF-500> Afficher les informations système
```

Vous trouverez ci-dessous un exemple de résultat avec la version de mise à jour du contenu 2-253 installée :

```
admin@WF-500> afficher le nom d'hôte des informations système :
 Adresse IP de WildFire : Masque réseau 10.5.164.245 Passerelle par
 défaut : Adresse MAC 00:25:90:c3:ed:56 vm-interface-ip-address:
 192.168.2.2 vm-interface-netmask : 255.255.255.0 vm-interface-
default-gateway : 192.168.2.1 vm-interface-dns-server : 192.168.2.1
 heure: Lun Apr 21 09:59:07 2014 disponibilité: 17 jours, 23:19:16
 famille: m modèle: Série WildFire: abcd3333 sw-version: 6.1.0 wf-
content-version: 2-253 wfm-release-date: 20/08/2014 20:00:08 logdb-
version: 6.1.2 Famille de plateformes : m
```


STEP 4 | (Facultatif) Programmez l'installation quotidienne ou hebdomadaire des mises à jour de contenu.

1. Planifiez l'appareil pour qu'il télécharge et installe les mises à jour du contenu :

```
admin@WF-500# définir le système deviceconfig récurrence
 update-schedule wf-content [quotidienne | hebdomadaire]
 action [télécharger-et-installer | télécharger-seulement]
```

   Par exemple, pour télécharger et installer les mises à jour chaque jour à 8h du matin :

```
admin@WF-500# définir le système deviceconfig de récurrence de
 update-schedule wf-content sur quotidien action télécharger-
et-installer à 08:00
```

2. Validez la configuration.

```
admin@WF-500# valider
```

Installation des mises à jour de contenu WildFire à partir d'un serveur SCP

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

La procédure suivante décrit comment installer des mises à jour de contenu sur l'état des menaces sur un appareil WildFire qui n'a pas de connectivité directe avec le serveur de mises à jour de Palo Alto Networks. Vous aurez besoin d'un serveur SCP (Secure Copy/copie sécurisée) pour stocker temporairement la mise à jour de contenu.

STEP 1 | Récupérez le fichier de mise à jour du contenu sur le serveur de mises à jour.

1. Connectez-vous au portail de support Palo Alto Networks et cliquez sur **Dynamic Updates (Mises à jour dynamiques)**.
2. Dans la section WildFire Appliance (Appareil WildFire), cherchez la dernière mise à jour du contenu de l'appareil WildFire et téléchargez-la.
3. Copiez le fichier de mise à jour du contenu sur un serveur SCP et notez le nom du fichier et le chemin d'accès au répertoire.

STEP 2 | Installez la mise à jour du contenu sur l'appareil WildFire.

1. Connectez-vous à l'appareil WildFire et téléchargez le fichier de mise à jour du contenu à partir du serveur SCP :

   ```
   admin@WF-500> scp importer du wf-content depuis
    username@host:path
   ```

   Par exemple :

   ```
   admin@WF-500> scp importer du wf-content depuis
    bart@10.10.10.5:c:/updates/panup-all-wfmeta-2-253.tgz
   ```

   *Si votre serveur SCP est exécuté sur un port non standard ou si vous devez spécifiez l'adresse IP source, vous pouvez également définir ces options dans la commande **scp import**.*

2. Installez la mise à jour :

   ```
   admin@WF-500> demander un fichier d’installation de mise à
    niveau wf-content panup-all-wfmeta-2-253.tgz
   ```

3. Affichez le statut de l’installation :

   ```
   admin@WF-500> afficher tous les emplois
   ```

STEP 3 | Vérifiez la mise à jour du contenu.

Vérifiez la version du contenu :

```
admin@WF-500> Afficher les informations système | correspondre à
 wf-content-version
```

Le résultat suivant indique la version 2-253 :

```
wf-content-version: 2-253
```

Activation de la génération de catégorie d'URL et de la signature locale

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

L'appareil WildFire peut générer des signatures localement en fonction des échantillons reçus des pare-feu connectés et de l'API WildFire, plutôt que d'envoyer les logiciels malveillants au cloud public pour la génération des signatures. L'appareil peut générer les types de signatures suivants qui peuvent servir à bloquer les logiciels malveillants ainsi que le trafic de commande et de contrôle associé :

- **Signatures antivirus** : détectent et bloquent les fichiers malveillants. WildFire ajoute ces signatures aux mises à jour du contenu WildFire et antivirus.
- **Signatures DNS** : détectent et bloquent les domaines de rappel du trafic de commande et de contrôle associé à un logiciel malveillant. WildFire ajoute ces signatures aux mises à jour du contenu WildFire et antivirus.
- **Catégories d'URL** : classent les domaines de rappel comme malveillants et mettent à jour la catégorie d'URL dans PAN-DB.

Configurez les pare-feu pour qu'ils récupèrent les signatures générées par l'appareil WildFire toutes les cinq minutes. Vous pouvez également envoyer l'échantillon de logiciels malveillants au cloud WildFire public pour permettre la distribution des signatures à l'ensemble des utilisateurs mondiaux via les mises à jour de contenu Palo Alto Networks.

Même si vous utilisez l'appareil WildFire pour l'analyse de fichier locale, vous pouvez également permettre aux pare-feu connectés de recevoir les dernières signatures distribuées par le cloud WildFire public.

STEP 1 | Paramétrage des mises à jour de contenu de l'appareil WildFire.

L'appareil WildFire peut ainsi recevoir les dernières données d'intelligence sur les menaces de la part de Palo Alto Networks.

STEP 2 | Activez la génération de signatures et de catégories d'URL.

1. Connectez-vous à l'appareil et saisissez **`configure`** pour passer en mode Configuration.
2. Activez toutes les options de prévention des menaces :

```
admin@WF-500# définir le paramètre deviceconfig wildfire
 signature-generation av oui dns oui url oui
```

3. Validez la configuration :

```
admin@WF-500# valider
```

Vous pouvez afficher l'état d'une signature générée dans WildFire 8.0.1 ou dans un environnement ultérieur à l'aide de la commande suivante :

```
admin@WF-500# afficher wildfire global signature-status égal
 sha256 <sha-256
value>
```

Les appareils WildFire ne peuvent afficher l'état des signatures générées avant la mise à niveau vers WildFire 8.0.1.

STEP 3 | Définissez le calendrier pour que les pare-feu connectés récupèrent les signatures et les catégories d'URL générées par l'appareil WildFire.

Il est recommandé de configurer vos pare-feu pour extraire les mises à jour de contenu du cloud WildFire public et de l'appareil WildFire. Cette configuration garantit que vos pare-feu reçoivent des signatures en fonction des menaces détectées dans le monde entier en plus des signatures générées par votre appareil local.

- Pour plusieurs pare-feu gérés par Panorama :

  Lancez Panorama et sélectionnez **Panorama** > **Déploiement des périphériques** > **Mises à jour dynamiques**, cliquez sur **Planifications**, puis sur **Ajouter** des mises à jour de contenu planifiées pour les appareils gérés.

  Pour plus d'informations sur l'utilisation de Panorama pour configurer des pare-feu gérés afin de recevoir des signatures et des catégories d'URL d'un appareil WildFire, voir Planifier des mises à jour de contenu sur des appareils à l'aide de Panorama.

- Pour un seul pare-feu :

  1. Connectez-vous à l'interface Web du pare-feu et sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**.

     Pour les pare-feu configurés pour transférer des fichiers à un appareil WildFire (qu'il soit déployé sous forme de cloud privé ou hybride), la section WF-Private s'affiche.

  2. Définissez le **Schedule (Calendrier)** du téléchargement et des mises à jour de contenu à partir de l'appareil WildFire et de leur installation sur le pare-feu.

Envoi des logiciels malveillants découverts localement ou des rapports au cloud WildFire public

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Autorisez l'appareil WildFire à envoyer automatiquement les échantillons malveillants vers le cloud WildFire public. Le cloud WildFire public fait une analyse plus approfondie de l'échantillon malveillant et génère une signature pour identifier l'échantillon. La signature est ensuite ajoutée aux mises à jour de signatures WildFire et distribuée à l'ensemble des utilisateurs mondiaux pour empêcher toute exposition ultérieure à la menace. Si vous ne souhaitez pas envoyer les échantillons malveillants à l'extérieur de votre réseau, vous pouvez plutôt choisir d'envoyer seulement les rapports WildFire des échantillons malveillants qui ont été découverts sur votre réseau afin de contribuer et d'améliorer les statistiques WildFire et les renseignements sur les menaces.

- Envoi des échantillons malveillants vers le cloud WildFire public
  1. À partir de l'appareil WildFire, exécutez les commandes de la CLI suivantes afin de permettre à l'appareil d'envoyer automatiquement les échantillons malveillants vers le cloud WildFire public :

     ```
     admin@WF-500# définir le paramètre deviceconfig wildfire
      cloud-intelligence submit-sample sur oui
     ```

     Si la capture de paquet (PCAP) est activée sur le pare-feu qui a initialement envoyé l'échantillon pour analyse par le cloud WildFire privé, la PCAP de l'échantillon malveillant sera également transférée vers le cloud WildFire public.
  2. Accédez au portail WildFire pour afficher les rapports d'analyse des échantillons malveillants qui ont été automatiquement envoyés vers le cloud WildFire public. Lorsqu'un échantillon malveillant est envoyé au cloud WildFire public, le cloud public génère un nouveau rapport d'analyse pour cet échantillon.

- Envoi des rapports d'analyse vers le cloud WildFire public

  Pour envoyer automatiquement des rapports sur les échantillons malveillants au cloud WildFire public (plutôt que l'échantillon malveillant lui-même), exécutez la commande CLI suivante sur l'appareil WildFire :

  ```
  admin@WF-500# définir le paramètre deviceconfig wildfire cloud
   intelligence submit-report sur oui
  ```

  Si vous avez autorisé l'appareil WildFire à envoyer automatiquement les échantillons malveillants au cloud WildFire public, vous n'avez pas besoin d'activer cette option ; le cloud WildFire public générera un nouveau rapport d'analyse pour l'échantillon.

  Les rapports envoyés au cloud WildFire public ne peuvent pas être affichés sur le portail WildFire. Le portail WildFire affiche uniquement les rapports du cloud WildFire public.

- Vérifier les paramètres d'envoi des logiciels malveillants et des rapports

  Confirmez que l'intelligence du cloud est activée pour envoyer les échantillons malveillants ou les rapports sur les échantillons malveillants vers le cloud WildFire public en exécutant la commande suivante :

  ```
  admin@WF-500> afficher l'état wildfire
  ```

  Consultez les champs `Submit sample` et `Submitreport`.

Mise à niveau d’un appareil WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Utilisez le flux de travail suivant pour mettre à niveau le système d'exploitation de l'appareil WildFire. Si vous souhaitez mettre à niveau un appareil qui appartient à un cluster WildFire, reportez-vous à la section Mise à niveau d’appareils WildFire appartenant à un cluster. L'appareil ne peut utiliser qu'un seul environnement à la fois pour analyser des échantillons. Ainsi, après la mise à niveau de l'appareil, consultez la liste des images MV disponibles et choisissez l'image correspondant le mieux à votre environnement. Dans le cas de Windows 7, si votre environnement comporte des systèmes Windows 7 32 bits et Windows 7 64 bits, il est recommandé de choisir l'image Windows 7 64 bits. WildFire analysera donc les fichiers PE 32 et 64 bits. Même si vous configurez l'appareil pour utiliser une configuration d'image de machine virtuelle, l'appareil utilise plusieurs instances de l'image pour l'analyse de fichiers.

La durée nécessaire pour la mise à niveau du logiciel de l’appareil variera selon le nombre d’échantillons que l’appareil WildFire a analysés et stockés, car la mise à niveau entraîne la migration de tous les échantillons malveillants et des échantillons bénins des 14 derniers jours. Allouez 30 à 60 minutes pour la mise à jour d’un appareil WildFire que vous avez utilisé dans un environnement de production.

La procédure suivante utilise un exemple de nom de fichier tiré d’une version de PAN-OS 10.2.2. Le nom de fichier exact de la version que vous installez sur votre appareil WildFire peut différer en fonction de la version précise.

STEP 1 | Si vous configurez un appareil WildFire pour la première fois, commencez par procéder à la configuration de l'appareil WildFire.

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 (Périphérique)** > **Setup (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 :

```
admin@WF-500> afficher les derniers échantillons wildfire
```

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 cette mise à jour, l'appareil dispose des renseignements sur les menaces les plus récentes, ce qui lui permet de détecter avec précision les logiciels malveillants.

Ce processus peut prendre 6 heures ou plus sur les appareils plus anciens.

1. Vérifiez que vous exécutez la dernière mise à jour du contenu sur votre appareil WildFire.

```
admin@WF-500> demande de mise à niveau du contenu wf
```

2. Téléchargez le dernier package de mise à jour du contenu WildFire.

```
admin@WF-500> demander la mise à niveau wf-content télécharger la
 plus récente
```

   Si vous n'êtes pas connecté directement au serveur de mises à jour Palo Alto Networks, vous pouvez procéder au téléchargement et à l'installation des mises à jour de contenu WildFire à partir d'un serveur SCP.

3. Affichez l'état du téléchargement.

```
admin@WF-500> afficher tous les emplois
```

4. Une fois le téléchargement terminé, installez la mise à jour.

```
admin@WF-500> demander la mise à niveau wf-content installer la
 dernière version
```

STEP 4 | (Requis lors de la mise à niveau vers PAN-OS 10.2.2) Mettez à niveau les images VM sur l'appareil WildFire.

1. Connectez-vous et accédez à la page de téléchargement de logiciels du portail de support client de Palo Alto Networks. Vous pouvez également accéder manuellement à la page de téléchargement de logiciels à partir de la page d'accueil du support en accédant à **Updates (Mises à jour)** > **Software Updates (Mises à jour logicielles)**.

2. Sur la page des mises à jour logicielles, sélectionnez **WF-500 Guest VM Images (Images de VM invitée WF-500)** et téléchargez les fichiers d'image VM suivantes :

   Palo Alto Networks met régulièrement à jour les fichiers d'image VM. Par conséquent, le nom de fichier précis dépend de la version disponible. Assurez-vous de télécharger la dernière version, où la partie m-x.x.x dans le nom de fichier indique le numéro de version. En outre, vous pouvez vous aider de la date de publication pour déterminer la dernière version.

   - WFWinXpAddon3_m-1.0.1.xpaddon3
   - WFWinXpGf_m-1.0.1.xpgf
   - WFWin7_64Addon1_m-1.0.1.7_64addon1
   - WFWin10Base_m-1.0.1.10base
3. Chargez les images VM sur l'appareil WildFire.
   1. Importez l'image VM à partir du serveur SCP :

      ```
      admin@WF-500>scp import wildfire-vm-image from
       <username@ip_address>/<folder_name>/<vm_image_filename>
      ```

      Par exemple :

      ```
      admin@WF-500>scp import wildfire-vm-image from
       user1@10.0.3.4:/tmp/WFWin7_64Addon1_m-1.0.1.7_64addon1
      ```

   2. Pour vérifier l'état du téléchargement, utilisez la commande suivante :

      ```
      admin@WF-500>show jobs all
      ```

   3. Répétez l'opération pour les images VM restantes.
4. Installez l'image VM.
   1. ```
      admin@WF-500>request system wildfire-vm-image upgrade
       install file <vm_image_filename>
      ```
   2. Répétez l'opération pour les images VM restantes.
5. Vérifiez que les images VM ont été correctement installées et activées sur l'appareil WildFire.
   1. (Facultatif) Affichez la liste des images VM disponibles :

      ```
      admin@WF-500> show wildfire vm-images
      ```

      La sortie affiche les images VM disponibles.
   2. Validez la configuration :

      ```
      admin@WF-500# commit
      ```


      ```

3. Affichez les images VM actives en exécutant la commande suivante :

```
admin@WF-500> show wildfire status
```

STEP 5 | Téléchargez la version PAN-OS 10.2.2 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.

Les exemples présentés dans cette procédure indiquent comment passer à la version PAN-OS 10.2.2. Remplacez 10.2.2 par la version visée par la mise à niveau.

Téléchargez la version 10.2.2 du logiciel :

- Connexion Internet directe :
  1. ```
     admin@WF-500> request system software download version 10.2.2
     ```
  2. Pour vérifier l'état du téléchargement, utilisez la commande suivante :

     ```
     admin@WF-500> afficher tous les emplois
     ```
- Sans connexion Internet directe :
  1. Accédez au site de support de PaloAltoNetworks et, dans la section Tools (Outils), cliquez sur **Software Updates (Mises à jour logicielles)**.
  2. Téléchargez le fichier image du logiciel de l'appareil WildFire à installer sur un ordinateur exécutant le logiciel du serveur SCP.
  3. Importez l'image du logiciel depuis le serveur SCP.

     ```
     admin@WF-500> importer logiciel scp depuis
      <username@ip_address>/<folder_name>/<imagefile_name>
     ```

     Par exemple :

     ```
     admin@WF-500> scp import software from user1@10.0.3.4:/tmp/
     WildFire_m-10.2.2
     ```
  4. Pour vérifier l'état du téléchargement, utilisez la commande suivante :

     ```
     admin@WF-500> afficher tous les emplois
     ```

STEP 6 | Confirmez que tous les services fonctionnent.

```
admin@WF-500> afficher l’état du logiciel du système
```


```

**STEP 7 |** Installez la version 10.2.2 du logiciel.

```
admin@WF-500> request system software install version 10.2.2
```

STEP 8 | Terminez la mise à niveau du logiciel.

1. 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> afficher toutes les tâchesMises en file
    d’attente Sorties de la file d’attente ID Type Etat Résultat
    Terminé ----------------------------------------------------
    02:42:36 02:42:36 5 Installer FIN OK 02:43:02
   ```

2. Redémarrez l'appareil :

   ```
   admin@WF-500> demande de redémarrage système
   ```

   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.

STEP 9 | Vérifiez que l’appareil WildFire est prêt à reprendre l’analyse des échantillons.

1. Vérifiez que le champ `sw-version` indique 10.2.2 :

   ```
   admin@WF-500> Afficher les informations système | correspondre
    à sw-version
   ```

2. Confirmez que tous les processus fonctionnent :

   ```
   admin@WF-500> afficher l’état du logiciel du système
   ```

3. Confirmez que la tâche d’auto-validation(`AutoCom`) est terminée :

   ```
   admin@WF-500> afficher tous les emplois
   ```


STEP 10 | (Facultatif) Activez l’image de la machine virtuelle que l’appareil utilise pour mener l’analyse. Chaque image VM représente un seul système d’exploitation et prend en charge divers environnements d'analyse reposant sur ce système d’exploitation.

- *Si votre environnement comporte des systèmes Windows 7 32 bits et Windows 7 64 bits, il est recommandé de choisir l'image Windows 7 64 bits. WildFire analysera donc les fichiers PE 32 et 64 bits.*
- *Les environnements d’analyse actuellement disponibles sont vm-3 (Windows XP), vm-5 (Windows 7 64 bits) et vm-7 (Windows 10 64 bits).*

- Affichez l’image VM active en exécutant la commande suivante et consultez le champ `Selected VM` (VM sélectionnée) :

```
admin@WF-500> show wildfire status
```

- Afficher la liste des images de machines virtuelles disponibles :

```
admin@WF-500> afficher les images vm wildfire
```

La sortie suivante montre que `vm-5` est l’image Windows 7 64 bits :

```
vm-5 Windows 7 64 bits, Adobe Reader 11, Flash 11, Office 2010.
 Prise en charge de PE, PDF, Office 2010 et versions antérieures
```

- Définir l’image à utiliser pour l’analyse :

```
admin@WF-500# définir le paramètre deviceconfig wildfire active-
vm <vm-image-number>
```

Par exemple, pour utiliser vm-5, exécutez la commande suivante :

```
admin@WF-500# définir le paramètre deviceconfig wildfire active-
vm-5
```

Et validez la configuration:

```
admin@WF-500# commit
```

STEP 11 | Étapes suivantes :

- (Facultatif) Mettez à niveau les pare-feu vers PAN-OS 10.2.2. Reportez-vous aux instructions de mise à niveau du pare-feu comprises dans le Guide des nouvelles fonctions de PAN-OS 10.2. Les pare-feu qui utilisent des versions antérieures à PAN-OS 10.2.2 peuvent continuer à transmettre des échantillons à un appareil WildFire qui utilise la version 10.2.2.
- (Dépannage) Si, après la mise à niveau, vous constatez une erreur ou des problèmes liés à la migration des données, redémarrez l’appareil WildFire pour reprendre le processus de mise à niveau. Le redémarrage de l’appareil WildFire n’entraînera pas la perte des données.

Installation du certificat de périphérique de l’appareil WildFire avec une connexion Internet

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire ❑ Compte du portail de support client (CSP) avec l’un des rôles d’utilisateur suivants : Super utilisateur, utilisateur standard, utilisateur limité, chercheur sur les menaces, rôle d’essai AutoFocus, super utilisateur de groupe, utilisateur standard de groupe, utilisateur limité de groupe, chercheur sur les menaces de groupe, utilisateur du centre de support autorisé (ASC) et utilisateur du service complet ASC. ❑ Accès super utilisateur à l'appareil WildFire

Pour récupérer le certificat de périphérique sur l’appareil WF-500 lorsqu’une connexion Internet est disponible, vous devez vous connecter au portail de support de Palo Alto Networks pour générer un mot de passe à usage unique qui vous permettra d’accéder au certificat. Cet OTP est ensuite utilisé pour récupérer le certificat de périphérique sur l’appareil concerné.

Les appareils WF-500B sont équipés d’un module TPM (Trusted Platform Module, module de plateforme de confiance) qui leur permet de s’identifier en toute sécurité et de récupérer automatiquement le certificat de périphérique. Aucune intervention de l’utilisateur n’est nécessaire pour la gestion des certificats de périphérique WF-500B.

Si vous utilisez un Cloud WildFire privé et que vous ne vous connectez à aucun des services WildFire, vous n’avez pas besoin de mettre à jour les certificats de périphérique des appareils WildFire. En effet, l’appareil WildFire utilise des certificats prédéfinis pour l’authentification mutuelle afin d’établir les connexions SSL utilisées pour l’accès de gestion et la communication entre périphériques. Cependant, vous pouvez Configurer l'authentification à l'aide d'un certificat personnalisé sur un appareil WildFire autonome à la place.

Si votre appareil WF-500B n’est pas connecté à Internet, certaines tâches pourraient échouer lorsque l’appareil tente à plusieurs reprises de récupérer des certificats de périphérique.

Pour installer avec succès le certificat de périphérique sur votre pare-feu, les FQDN et les ports suivants doivent être autorisés sur votre réseau.

Nom de domaine complet	Ports
• http://ocsp.paloaltonetworks.com • http://crl.paloaltonetworks.com • http://ocsp.godaddy.com	TCP 80
• https://api.paloaltonetworks.com • http://apitrusted.paloaltonetworks.com • certificattrusted.paloaltonetworks.com • certificat.paloaltonetworks.com	TCP 443
• *.gpcloudservice.com	TCP 444 et TCP 443

STEP 1 | Vérifiez que vous exécutez l'une des versions PAN-OS suivantes sur l'appareil WildFire :

- PAN-OS 11.0.1 et versions ultérieures
- PAN-OS 10.2.4 et versions ultérieures
- PAN-OS 10.1.10 et versions ultérieures (non prises en charge sur l'appareil WF-500B)
- PAN-OS 10.0.12 et versions ultérieures (non prises en charge sur l'appareil WF-500B)
- PAN-OS 9.1.17 et versions ultérieures (non prises en charge sur l'appareil WF-500B)

STEP 2 | Générer le One-Time Password (mot de passe à usage unique ; OTP).

1. Connectez-vous au Customer Support Portal (Portail de support client) avec un rôle d'utilisateur autorisé à générer un OTP.
2. Sélectionnez **Products (Produits)** > **Device Certificates (Certificats de périphériques)** et **Generate OTP (Générer un OTP)**.
3. Pour **Device Type (Type de périphérique)**, sélectionnez **Generate OTP for WF-500 (Générer un OTP pour WF-500)**.
4. Sélectionnez le numéro de série de votre **WF-500 Device (Périphérique WF-500)**.
5. **Generate OTP (Générez un OTP)** puis copiez-le.

STEP 3 | Accédez à la CLI de l'appareil WF-500 avec des privilèges administratifs de super utilisateur.

STEP 4 | Configurez l'appareil WildFire pour qu'il se synchronise avec un serveur NTP :

```
admin@WF-500> configure admin@WF-500# set deviceconfig system ntp-
servers primary-ntp-server ntp-server-address <NTP primary server
 IP address> admin@WF-500# set deviceconfig system ntp-servers
 secondary-ntp-server ntp-server-address <NTP secondary server IP
 address>
```

STEP 5 | Téléchargez et installez le certificat de périphérique de l'appareil WF-500 à l'aide de la commande CLI suivante (n'oubliez pas d'utiliser le **One-time Password (Mot de passe à usage unique)** que vous avez généré dans le portail de support client) :

```
admin@WF-500> request certificate fetch otp <otp_value>
```

STEP 6 | Votre appareil WF-500 récupère et installe le certificat de périphérique.

STEP 7 | (Facultatif) Vérifiez que le téléchargement et l'installation d'un certificat de périphérique se sont déroulés correctement à l'aide de la commande CLI suivante :

```
admin@WF-500> show device-certificate status
```

Si l'installation du certificat de périphérique a réussi, la réponse suivante s'affiche :

```
Device Certificate information: Current device certificate status:
 Valid Not valid before: 2022/11/30 15:17:47 PST Not valid after:
 2023/02/28 15:17:47 PST Last fetched timestamp: 2022/11/30
 15:29:42 PST Last fetched status: success Last fetched info:
 Successfully fetched Device Certificate
```

STEP 8 | Actualisez les paramètres de l'appareil WildFire pour établir une connexion au cloud Advanced WildFire avec le certificat de périphérique mis à jour à l'aide de la commande CLI suivante :

Table 1:

Version PAN-OS exécutée sur l'appareil WildFire	Commande CLI
• PAN-OS 11.0.1 et versions ultérieures • PAN-OS 10.2.5 et versions ultérieures • PAN-OS 10.1.10 et versions ultérieures	`admin@WF-500> tester l'inscription wildfire`
• PAN-OS 10.2.4 • PAN-OS 10.0.12 et versions ultérieures • PAN-OS 9.1.17 et versions ultérieures	`admin@WF-500> demande de redémarrage système` *Ce processus peut prendre jusqu'à 20 minutes.*
Toute version configurée en tant que nœud de cluster WildFire	`admin@WF-500(active-controller)> request cluster reboot-local-node`

Version PAN-OS exécutée sur l'appareil WildFire	Commande CLI

	Vous pouvez afficher l'état de la tâche de redémarrage sur le nœud de contrôle WildFire à l'aide de la commande CLI suivante :
	`admin@WF-500(active-controller)> show cluster task pending`
	S'il ne reste aucune tâche en attente, utilisez la commande CLI suivante pour vérifier que le redémarrage a réussi :
	`admin@WF-500(active-controller)> show cluster task history`
	Une fois la commande terminée, vous devriez voir l'état `Finished: success at YYYY-MM-DD HH:MM:SS UTC`*, indiquant l'heure de fin du processus de redémarrage.*

Surveillance de l’activité de l’appareil WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Vous pouvez consulter les résultats d’analyse des échantillons envoyés à l’appareil WildFire en accédant au pare-feu qui a envoyé l’échantillon (ou à Panorama si vous gérez plusieurs pare-feu de manière centralisée), ou en utilisant l’API WildFire.

Une fois que WildFire a analysé un échantillon et rendu un verdict de fichier malveillant, indésirable ou bénin ou d’hameçonnage, un rapport d'analyse détaillé est généré pour l'échantillon. Les rapports d'analyse WildFire qui sont visualisés sur le pare-feu qui a envoyé l'échantillon comprennent également des informations sur la session au cours de laquelle l'échantillon a été détecté. Pour les échantillons qui sont identifiés comme étant malveillants, le rapport d'analyse WildFire donne des détails sur les signatures WildFire existantes qui pourraient être liées à ce logiciel malveillant qui vient d'être identifié et des renseignements sur les attributs, le comportement et l'activité du fichier qui ont indiqué que l'échantillon était malveillant.

Reportez-vous aux rubriques suivantes pour les détails sur la surveillance des envois WildFire, sur les rapports d'analyse WildFire pour les échantillons et pour définir des alertes et des avis fondés sur les envois et les résultats d'envoi :

- À propos des journaux et de la génération de rapports WildFire
- Utilisez la CLI pour surveiller le boitier WildFire
- Utilisation du pare-feu pour surveiller les envois de l’appareil WildFire

À propos des journaux et de la génération de rapports WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Vous pouvez surveiller les journaux de l’appareil WildFire sur le pare-feu, avec le portail WildFire ou avec l’API WildFire.

Pour chaque échantillon analysé par WildFire, WildFire classe l'échantillon sous la catégorie appropriée (logiciel malveillant, hameçonnage, fichier indésirable ou fichier bénin) et expose de façon détaillée de l'information sur l'échantillon ainsi que sur son comportement dans le rapport d'analyse WildFire. Les rapports d’analyse de WildFire sont accessibles sur le pare-feu qui a envoyé l’échantillon et sur le cloud WildFire (public ou privé) qui a analysé l’échantillon, ou peuvent être récupérés à l’aide de l’API WildFire :

- On the firewall (Sur le pare-feu) : tous les échantillons envoyés par un pare-feu pour analyse WildFire sont journalisés sous forme d'entrées des journaux d'envois WildFire (**Monitor (Surveillance)** > **WildFire Submissions (Envois WildFire)**). La colonne Action (Action) du journal d’envois WildFire indique si un fichier a été autorisé ou bloqué par le pare-feu. Pour chaque envoi WildFire, vous pouvez ouvrir une vue détaillée du journal afin de visualiser le rapport d'analyse WildFire qui correspond à l'échantillon ou télécharger le rapport au format PDF.
- Sur le portail WildFire : surveillance de l'activité WildFire, y compris le rapport d'analyse WildFire de chaque échantillon, qui peut également être téléchargé au format PDF. Si le cloud WildFire est déployé sous forme de cloud privé, le portail WildFire offre des précisions sur les échantillons qui sont manuellement chargés vers le portail et sur les échantillons qui sont envoyés par un appareil WildFire lorsque l'intelligence du cloud est activée.

  L'option pour consulter les rapports d'analyse WildFire sur le portail est uniquement prise en charge pour les appareils WildFire avec la fonction intelligence du cloud *activée.*
- Avec l'API WildFire : récupérez les rapports d'analyse WildFire à partir d'un appareil WildFire ou à partir du cloud WildFire public.

Utilisez le boitier WildFire pour surveiller l’état de l’analyse des échantillons

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Utilisez la CLI (interface de ligne de commande) WildFire pour surveiller les détails liés à l’analyse sur votre appareil WildFire. Vous pouvez consulter les informations relatives à l’utilisation de la plateforme d’analyse, la file d’attente des échantillons ainsi que les informations relatives au traitement des échantillons.

Reportez-vous aux sections suivantes pour obtenir de plus amples précisions sur l'utilisation de l’appareil WildFire pour surveiller l'activité WildFire :

- Affichage de l’utilisation de l’environnement d’analyse WildFire
- Affichage des détails du traitement de l’analyse des échantillons WildFire

Affichage de l’utilisation de l’environnement d’analyse WildFire

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

L’appareil WildFire utilise divers environnements d’analyse pour détecter les comportements malveillants au sein des échantillons. Vous pouvez voir les environnements d’analyse qui sont utilisés, le nombre d’entre eux qui sont disponibles ainsi que le nombre de fichiers dans la liste d’attente aux fins d’analyse. Si un environnement d’analyse est toujours utilisé à sa capacité de charge utile maximale (ou quasi-maximale), songez à affecter l’analyse des fichiers moins sensibles à un cloud public WildFire hébergé par Palo Alto Networks, à mettre à jour votre politique de transfert des fichiers ou à redéfinir les limites de transfert des fichiers (Palo Alto Networks recommande d’utiliser les valeurs de transfert de fichiers par défaut pour tous les types de fichiers).

STEP 1 | Accédez à la CLI et utilisez l’une des commandes suivantes en fonction de l’environnement d’analyse pour lequel vous souhaitez consulter les statistiques d’utilisation.

- Utilisation de l’environnement d’analyse des fichiers exécutables portables : **`show wildfire wf-vm-pe-utilization`**
- Utilisation de l’environnement d’analyse des documents : **`show wildfire wf-vm-doc-utilization`**
- Utilisation de l’environnement d’analyse des liens d’e-mail :**`show wildfire wf-vm-elinkda-utilization`**
- Utilisation de l’environnement d’analyse des archives : **`show wildfire wf-vm-archive-utilization`**

Pour un environnement d’analyse donné, l’application indique le nombre en cours d’utilisation et le nombre disponible :

```
{ available: 2, in_use: 1, }
```

STEP 2 | Affichez le nombre d’échantillons d’appareils WildFire qui attendent d’être analysés et leur répartition. Les échantillons sont traités au fur et à mesure que les environnements d’analyse deviennent disponibles.

`show wildfire wf-sample-queue-status`

```
{ DW-ARCHIVE : 4, DW-DOC : 2, DW-ELINK : 0, DW-PE : 21, DW-
URL_UPLOAD_FILE : 2, }
```

Affichage des détails du traitement de l’analyse des échantillons WildFire

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

L’appareil WildFire conserve des traces de l’activité d’analyse dans un journal d’événement. Vous pouvez afficher les détails relatifs aux services ou aux appareils connectés de votre réseau qui ont analysé un échantillon donné ainsi qu le nombre d’échantillons analysés au cours d’une période de temps donnée. Vous pouvez vous servir de ces informations pour surveiller l’activité et créer des politiques et des contre-mesures contre toute activité malveillante. Les activités très lourdes peuvent indiquer la présence d’une activité suspecte. Envisagez également d’utiliser un outil de collecte d’informations sur les menaces, comme AutoFocus, pour en apprendre davantage sur les menaces et en déterminer la nature.

STEP 1 | Affichez le nombre d’échantillons traités localement au cours d’une période de temps donnée ou en fonction d’un nombre maximum d’échantillons.

show wildfire local sample-processed {time [last-12-hrs| last-15-minutes | last-1-hr | last-24-hrs | last-30-days | last-7-days| last-calender-day | last-calender-month] \ count <number_of_samples>}.

```
Dernières informations sur les échantillons :
 +-----------------------------------------
 ---------------------+---------------------+------ -----
+------------+-----------+------------+------ --------------
+ | SHA256 | Créer du temps | Nom de fichier | Type
 de fichier | Taille du fichier | Malicieux | Etat |
 +-------------------------------------------------------------
 -----------------+---------------------+---------- -
+------------+-----------+------------+---------- ---------+ |
 ce752b7b76ac2012bdff2b76b6c6af18e132ae8113172028b9e02c6647ee19bb
 | 2018-12-09 16:55:53 | | Lien e-mail |
 31 522 | | téléchargement terminé | |
 349e57e51e7407abcd6eccda81c8015298ff5d5ba4cedf09c7353c133ceaa74b
 | 2018-12-09 16:53:40 | | Lien e-mail
 | 39 679 | | téléchargement terminé |
 +-------------------------------------------------------------
 -----------------+---------------------+---------- -+------------
+-----------+------------+---------- ---------+
```

STEP 2 | Identifiez le ou les périphériques qui ont soumis un échantillon spécifié à WildFire aux fins d’analyse.

show wildfire global sample-device-lookup sha256equal <SHA_256>.

```
 Exemple
 1024609813c57fe174722c53b3167dc3cf5583d5c7abaf4a95f561c686a2116e
 vu pour la dernière fois sur les appareils suivants :
 +-----------------------------------------------------
 --------------------+-----------+-----------+
 --------------------+ | SHA256 | Identifiant de
 l'appareil | IP de l'appareil | Heure de soumission |
 +-------------------------------------------------------------
 -----------------+-----------+-----------+-------- --------------+
 | 1024609813c57fe174722c53b3167dc3cf5583d5c7abaf4a95f561c686a2116e
 | Manuel | Manuel | 2019-08-05 19:24:39 |
 +-------------------------------------------------------------
 -----------------+-----------+-----------+-------- --------------
+
```


Utilisez la CLI pour surveiller le boitier WildFire

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Utilisez la CLI (interface de ligne de commande) WildFire™ pour afficher les journaux système interne. Vous pouvez passer en revue les événements de journalisation pour surveiller la santé et l’état des composantes WildFire, comme les nœuds de cluster, les services de base et d’analyseur ainsi que pour résoudre et vérifier la configuration du système. Pour plus d'informations sur les commandes PAN-OS, reportez-vous au Guide de mise en route de la ligne de commande PAN-OS.

- Affichage des journaux système du boitier WildFire

Affichage des journaux système du boitier WildFire

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Utilisez un émulateur de terminal, comme PuTTY, pour vous connecter à l’appareil WildFire au moyen d’une connexion Secure Shell (SSH) ou d’une connexion de série directe depuis une interface de série sur votre ordinateur de gestion jusqu’au port console de votre périphérique.

STEP 1 | Lancez le logiciel d’émulation du terminal, puis sélectionnez le type de connexion (série ou SSH).

- Pour établir une connexion SSH, saisissez le nom d'hôte WildFire ou l’adresse IP du périphérique que vous voulez connecter et régler le port sur **22**.
- Pour établir une connexion de série, connectez une interface de série du l’ordinateur de gestion au port console du périphérique. Configurez les paramètres de la connexion de série dans le logiciel d’émulation du terminal comme suit :
  - Débit de données'A0;: **9600**
  - Bits de données'A0;: **8**
  - Parité : **aucune**
  - Bits d'arrêt'A0;: **1**
  - Contrôle de flux : **aucun**

STEP 2 | Lorsque vous êtes invité à vous connecter, saisissez vos informations d'accès administratif.

STEP 3 | Saisissez la commande qui suit sur un appareil WildFire.

```
admin@WF-500>show log system subtype direction equal backward
```

Cette commande affiche tous les événements WildFire journalisés qui ont été classés en tant que sous-type d’appareil WildFire, du plus ancien au plus récent.

- Vous pouvez inverser l’affichage des journaux (du plus récent au plus ancien) en ajoutant l’argument de commande suivant : `direction equal backward`.
- Les messages journaux que renvoie la CLI de l’appareil WildFire peuvent comprendre de nombreux sous-types. Vous pouvez filtrer les journaux en fonction d’un mot-clé commun. Utilisez l’argument de commande suivant pour filtrer les journaux en fonction d’une chaîne donnée : `match queue < keyword>`

  Le journal de l’appareil WildFire suivant présente les processus d’initialisation du système lors du démarrage.

```
Heure Gravité Sous-type Objet IDEvénement ID
 Description ========================================
 ================================== 2017/03/29 12:04:33 moyen
 général général 0 Nom d'hôte changé en WF-500 2017/03/29 12:04:40
 info général général 0 VPN Disable mode = off 2017/03/29 12:04:41
 info hw ps-inse 0 Alimentation n°1 (en haut) insérée 2017 /03/29
 12:04:41 haut système général- 1 Le système démarre. 2017/03/29
 12:04:41 info raid pair-de 0 Nouvelle paire de disques A détectée.
 2017/03/29 12:04:41 info raid pair-de 0 Nouvelle paire de disques
 A détectée. 2017/03/29 12:04:41 info raid pair-de 0 Nouvelle
 paire de disques B détectée. 2017/03/29 12:04:41 info raid
 pair-de 0 Nouvelle paire de disques B détectée. 2017/03/29
 12:04:41 info cluster cluster 0 Le daemon de cluster est en cours
 d'initialisation. 2017/03/29 12:04:41 info port eth1 link-ch 0
 Port eth1 : Up 1Gb/s Full duplex 2017/03/29 12:04:41 info port MGT
 link-ch 0 Port MGT : Up 1Gb/s Full duplex 2017/03/29 12:04:41 info
 port eth3 link-ch 0 Port eth3 : Up 1Gb/s Full duplex 2017/03/29
 12:04:41 info port eth2 link-ch 0 Port eth2 : Up 1Gb/s Full duplex
 2017/03/29 12:04:41 info général général 0 L'alimentation n°1 (en
 haut) n'est pas présente au démarrage 2017/03/29 12:04:41 info
 général général 0 L'alimentation n°2 (en bas) n'est pas présent au
 démarrage
```


Utilisation du pare-feu pour surveiller les envois de l’appareil WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Les échantillons transférés par le pare-feu (vers les clouds privés et/ou publics WildFire) sont ajoutés en tant qu’entrées aux journaux des **envois WildFire**. Un rapport d'analyse WildFire détaillé s'affiche dans la vue agrandie de chacune des entrées du journal des Envois WildFire. Pour en savoir plus sur l’utilisation du pare-feu pour surveiller les logiciels malveillants, consultez Surveillance de l’activité WildFire.

Affichage des journaux et des rapports d’analyse de l’appareil WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Les journaux WildFire contiennent des informations sur des échantillons (fichiers et liens e-mail) analysés par WildFire. Il comprend des artefacts, qui sont des propriétés, des activités ou des comportements associés à l’événement enregistré, tels que le type d’application ou l’adresse IP d’un attaquant ainsi que des qualités spécifiques à WildFire, telles que des résultats d’analyse de haut niveau, y compris la catégorisation de l’échantillon comme malveillant, hameçonnage, indésirable ou bénin et détaille des informations sur l’échantillon. L’examen des journaux des envois WildFire peut également indiquer si un utilisateur de vos réseaux a téléchargé un fichier suspect. Le rapport d’analyse WildFire affiche des informations détaillées sur l’échantillon ainsi que des informations sur les utilisateurs ciblés, des informations d’en-tête d’e-mail (si activé), l’application contenant le fichier et toutes les URL impliquées dans la transmission ou dans l’activité de commande et contrôle du fichier. 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.

STEP 1 | Transfert de fichiers pour analyse par l’appareil WildFire.

STEP 2 | Configuration des paramètres du journal des envois WildFire.

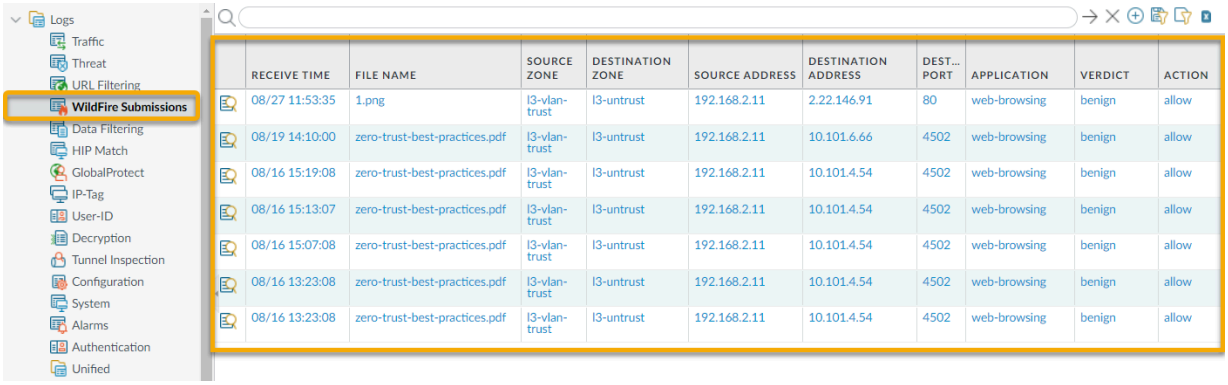
STEP 3 | Pour afficher les échantillons envoyés par un pare-feu à un cloud WildFire hybride, privé ou public, sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **WildFire Submissions (Envois WildFire)**. Une fois l'analyse WildFire d'un échantillon terminée, les résultats sont renvoyés au pare-feu qui a envoyé l'échantillon et sont accessibles dans les journaux des envois WildFire. Les journaux des envois comprennent des renseignements sur un échantillon donné, y compris les renseignements suivants :

- La colonne Verdict indique si l'échantillon est bénin, malveillant ou indésirable ou hameçonnage.
- La colonne Action (Action) indique si le pare-feu a autorisé ou bloqué l’échantillon.

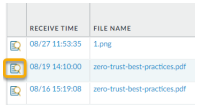
- La colonne Severity (Gravité) indique le degré de menace que pose un échantillon pour une organisation en se basant sur les valeurs suivantes : critique, élevé, moyen, faible et informatif.

  Les valeurs des degrés de gravité suivants sont déterminées par une combinaison de valeurs de verdict et d’action.

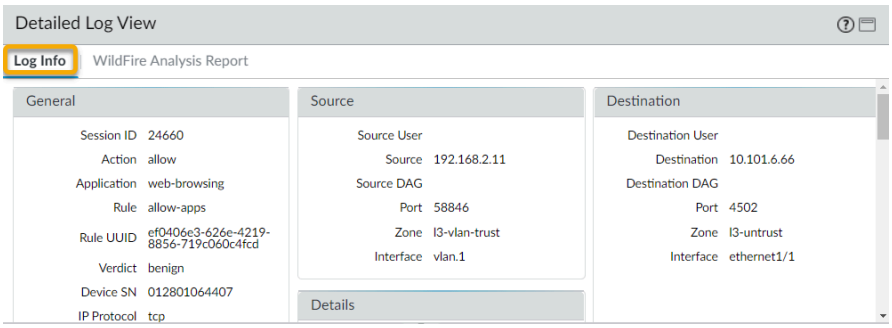
  - *Faible : échantillons indésirables dont l’action est définie sur autoriser.*
  - *Élevé : échantillons malveillants dont l’action est définie sur autoriser.*
  - *Informations :*
    - *échantillons bénins dont l’action est définie sur autoriser.*
    - *Les échantillons, peu importe le verdict, dont l'action est définie sur bloquer.*



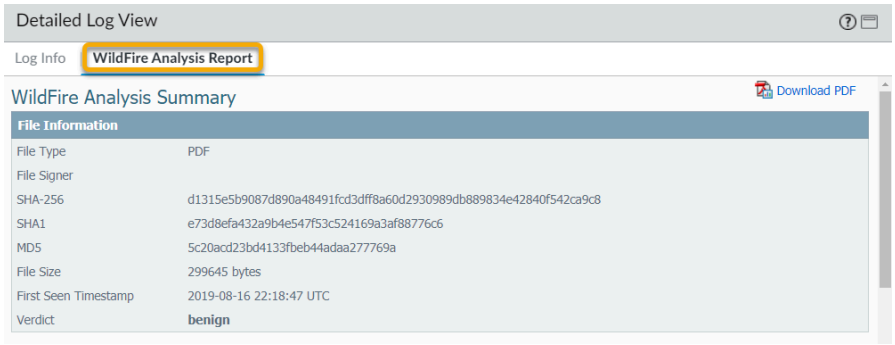
STEP 4 | Pour toute entrée, sélectionnez l'icône Détails du log pour ouvrir une vue détaillée pour chaque entrée du journal :



la vue détaillée du journal présente des informations sur le journal et le rapport d'analyse WildFire relatifs à l'entrée. Si la capture de paquet (PCAP) est activée pour le pare-feu, les échantillons de PCAP s'affichent également.



Pour tous les échantillons, le rapport d'analyse WildFire affiche le fichier et les détails de la session. Pour les échantillons de logiciels malveillants, le rapport d'analyse WildFire est élargi pour y inclure des détails sur le comportement et les attributs du fichier qui indiquaient son caractère malveillant.



STEP 5 | (Facultatif) **Download PDF (Téléchargez le PDF)** du rapport d'analyse WildFire.

Clusters d'appareils WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence 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. Les clusters s’avèrent particulièrement utilisant dans des environnements où il n’est pas permis d'accéder au cloud WildFire public. Vous pouvez configurer et gérer un maximum de vingt appareils WildFire dans un cluster d'appareils WildFire sur un seul réseau. Les clusters procurent également un seul package de signatures qu’ils distribuent à tous les pare-feu connectés, une architecture High-Availability (haute disponibilité ; HA) assurant une tolérance aux pannes et la possibilité d’une gestion centralisée au moyen de Panorama. Vous pouvez également gérer des appareils WildFire autonomes au moyen de Panorama.

Pour créer des clusters d'appareils WildFire, tous les appareils WildFire que vous souhaitez ajouter au cluster doivent utiliser Panorama 8.0.1 ou toute version ultérieure. Lorsque 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. Vous n'avez pas besoin d’une licence distincte pour créer et gérer des clusters d'appareils WildFire.

- Échelle et résilience des clusters d'appareils WildFire
- Gestion des clusters d'appareils WildFire
- Configuration locale d’un cluster sur des appareils WildFire
- Configurer le chiffrement d'appareils-à-àppareils WildFire
- Surveillance d’un cluster d’appareils WildFire
- Mise à jour d’appareils WildFire appartenant à un cluster
- Dépannage d’un cluster d’appareils WildFire

Échelle et résilience des clusters d'appareils WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

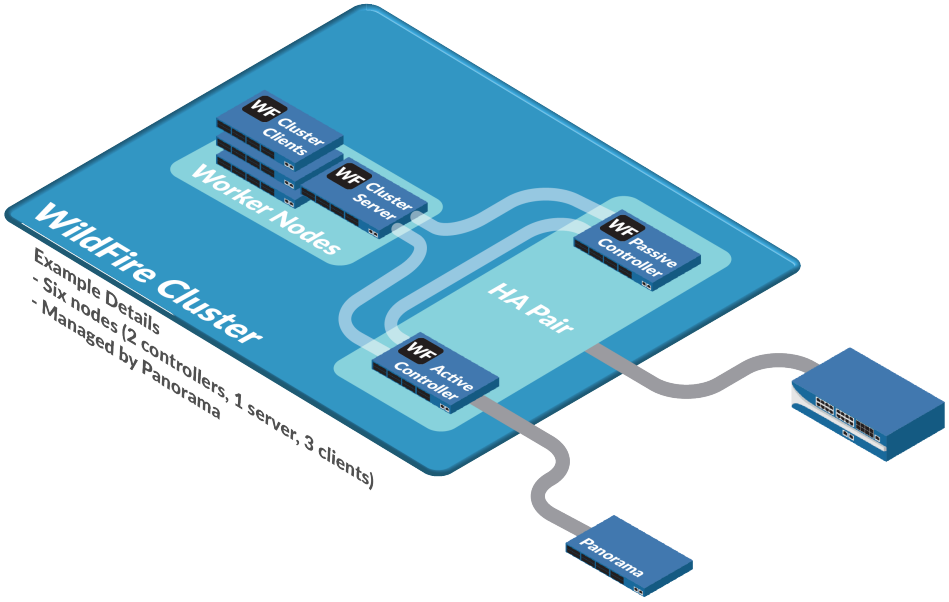
Les clusters d'appareils WildFire regroupent la capacité de stockage et d’analyse d’échantillons d’un maximum de vingt appareils WildFire, ce qui vous permet de prendre en charge d’importants déploiements de pare-feu sur un seul réseau. Vous disposez de la souplesse pour effectuer la gestion et la configuration locale d’un cluster sur des appareils WildFire au moyen de la CLI ou la gestion et la configuration centralisée d’un cluster sur Panorama (serveur d’appareils Panorama virtuels ou M-Series). L’environnement d’un cluster d'appareils WildFire comprend :

- De deux à vingt appareils WildFire que vous souhaitez grouper et gérer en tant que cluster. Au moins deux appareils WildFire configurés dans une paire High Availability (haute disponibilité ; HA).
- Des pare-feu qui transfèrent des échantillons au cluster aux fins d’analyse du trafic et de génération de signatures.
- (Facultatif) Un ou deux appareils Panorama pour la gestion centralisée du cluster, si vous décidez de ne pas gérer le cluster localement. Pour procurer la HA, utilisez deux appareils Panorama configurés en tant que paire HA.

Chaque appareil WildFire que vous ajoutez à un cluster d'appareils WildFire devient un nœud de ce cluster (il ne s’agit plus d’un appareil WildFire autonome). Panorama peut gérer un maximum de 10 clusters d'appareils WildFire et un total de 200 *nœuds de cluster* WildFire (10 clusters comportant un maximum de 20 nœuds).

Panorama peut gérer des appareils WildFire autonomes de même que des clusters d'appareils WildFire. Le nombre total combiné d’appareils WildFire autonomes et de nœuds de clusters d'appareils WildFire que Panorama peut gérer est fixé à 200. Par exemple, si Panorama gère trois clusters qui se composent d’un total de 15 nœuds de cluster WildFire et 8 appareils WildFire autonomes, Panorama gère alors un total de 23 appareils WildFire et peut en gérer 177 autres.

Il n’y a aucune limite d’enregistrement pour les appareils WildFire connectés à Panorama ; vous pouvez connecter le nombre de périphériques souhaités, sans incidence sur votre licence de capacité. Pour obtenir de plus amples renseignements sur la mise sous licence de Panorama, reportez-vous à la section Enregistrer Panorama et installer des licences.



Les nœuds de cluster jouent l'un des trois rôles suivants :

- **Nœud de contrôle** : deux nœuds de contrôle gèrent le service de file d'attente et la base de données, génère les signatures et gèrent le cluster localement, si vous ne gérez pas le cluster au moyen d'un appareil Panorama virtuel ou M-Series. Chaque cluster peut posséder un maximum de deux nœuds de contrôle. Pour procurer une tolérance aux pannes, chaque cluster d'appareils WildFire devrait posséder un minimum de deux nœuds configurés en tant que paire HA composée d'un nœud de contrôle principal et d'un nœud de contrôle de secours. À l'exception des échecs et de la maintenance ordinaire, chaque cluster devrait posséder deux nœuds de contrôle.
- **Nœud esclave (client du cluster)** : les nœuds de cluster qui ne sont pas des nœuds de contrôle sont des nœuds esclaves. Les nœuds esclaves augmentent la capacité d'analyse, la capacité de stockage et la résilience des données du cluster.
- **Nœud serveur (serveur du cluster)** : le troisième nœud d'un cluster WildFire est automatiquement configuré en tant que nœud serveur, un type particulier de nœud esclave qui offre la redondance des bases de données et de l'infrastructure en plus des capacités standard d'un nœud esclave.

Lorsqu'un pare-feu s'enregistre auprès d'un nœud de cluster, ou lorsque vous ajoutez un appareil WildFire qui a déjà enregistré des pare-feu auprès d'un cluster, le cluster transmet une liste d'enregistrement aux pare-feu qui sont connectés. La liste d'enregistrement indique tous les nœuds du cluster. En cas d'échec d'un nœud du cluster, les pare-feu qui sont connectés à ce nœud s'enregistrent auprès d'un autre nœud du cluster. Ce type de résilience est l'un des avantages que l'on peut tirer de la création de clusters d'appareils WildFire.

Avantage	Description
Échelle	Un cluster d'appareils WildFire augmente le débit d'analyse et la capacité de stockage disponibles sur un seul réseau, ce qui vous permet de disposer d'un plus important réseau de pare-feu sans segmenter votre réseau.
Haute disponibilité	En cas d'échec d'un nœud du cluster, la configuration HA procure une tolérance aux pannes afin d'empêcher la perte de services et de données

Avantage	Description
	critiques. Si vous gérez centralement les clusters au moyen de Panorama, la configuration HA de Panorama assure une tolérance aux incidents liés à la gestion centralisée.
Distribution d’un seul package de signatures	Tous les pare-feu connectés à un cluster reçoivent le même package de signatures, quel que soit le nœud du cluster qui a reçu ou analysé les données. Le package de signatures repose sur l'activité et les résultats de tous les membres du cluster, c’est-à-dire que chaque pare-feu connecté tire profit des connaissances combinées de tout le cluster.
Gestion centralisée (Panorama)	Vous sauvez du temps et simplifiez le processus de gestion lorsque vous utilisez Panorama pour gérer les clusters d'appareils WildFire. Une gestion d’un appareil ou d’un cluster WildFire qui repose sur Panorama plutôt que sur la CLI et les scripts vous procure une vue unique des périphériques de votre réseau. Vous pouvez également transmettre des configurations communes, des mises à jour de configuration et des mises à niveau logicielles à plusieurs clusters d'appareils WildFire à partir de l’interface Web de Panorama plutôt que la CLI de l’appareil WildFire.
Équilibrage de charge	Lorsqu’au moins deux nœuds sont actifs sur un cluster, celui-ci distribue et équilibre automatiquement la charge de l’analyse, de la génération de rapport, de la création de signatures, du stockage et de la distribution du contenu WildFire entre ses nœuds.

Haute disponibilité des clusters d’appareils WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

La haute disponibilité est un avantage décisif des clusters d'appareils WildFire, car la HA prévient la perte de services et de données critiques. Un cluster HA copie les données critiques, comme les résultats d’analyse, les rapports et les signatures, et les distribue à l’ensemble des nœuds afin d’empêcher que l’échec d’un nœud se traduise par une perte de données. Un cluster HA fournit également des services critiques redondants, comme la fonctionnalité d'analyse, l'API WildFire et la génération de signatures afin d'empêcher que l'échec d'un nœud se traduise par une interruption de service. Un cluster doit se composer d’au moins deux nœuds pour procurer les avantages de la haute disponibilité. L’échec d’un noeud du cluster n’a aucune incidence sur les pare-feu, car les pare-feu enregistrés à un nœud ayant échoué se servent de la liste d’enregistrement du cluster pour s’enregistrer auprès d’un autre nœud du cluster.

Les deux appareils qui composent la paire HA sont configurés par l’utilisateur en tant qu’appareils principal et secondaire. Selon les valeurs de priorité initiales qui ont été configurées, WildFire attribue également un état opérationnel aux appareils : Actif pour l’appareil principal et Passif pour le périphérique secondaire. Cet état détermine l’appareil WildFire qui est utilisé comme point de contact pour la gestion et les contrôles de l’infrastructure. Le périphérique passif est toujours synchronisé avec l’appareil actif et il est prêt à prendre ce rôle en cas d’échec d’un système ou d’un réseau. Par exemple, lorsque l’appareil

principal qui se trouve à l'état actif (actif-principal) échoue, un basculement se produit et il passe à un état passif-principal, tandis que l'appareil secondaire passe à l'état actif-secondaire. La valeur de priorité initialement attribuée demeure inchangée, peu importe l'état de l'appareil.

Un basculement se produit lorsque les homologues de la paire HA n'arrivent plus à communiquer entre eux, qu'ils deviennent inactifs ou qu'une erreur fatale s'est produite. La paire HA WildFire tentera de résoudre automatiquement les interruptions mineures. Cependant, les événements majeurs nécessiteront l'intervention de l'utilisateur. Un basculement peut également se produire lorsqu'un contrôleur est suspendu ou mis hors service par l'utilisateur.

Lors de la configuration d'un cluster, assurez-vous d'indiquer plus d'un nœud de contrôle. Chaque cluster devrait disposer d'une paire de contrôleurs HA. Un cluster devrait avoir un seul nœud de contrôle que dans des situations temporaires, par exemple, lorsque vous échangez des nœuds de contrôle ou qu'un nœud de contrôle échoue.

Dans une paire HA composée de deux nœuds de cluster, si un nœud de contrôle échoue, l'autre nœud de contrôle ne peut traiter les échantillons. Pour que le nœud de cluster qui demeure actif puisse traiter les échantillons, vous devez le configurer pour qu'il agisse comme un appareil WildFire autonome : supprimez les configurations de HA et de cluster sur le nœud de cluster actif et redémarrez le nœud. Le nœud redémarre en tant qu'appareil WildFire autonome.

Les clusters à trois nœuds possèdent une paire HA en plus d'un nœud de serveur, qui procure une redondance supplémentaire. Le serveur utilise les mêmes services de base de données et d'infrastructure serveur que le contrôleur, mais ne génère pas de signatures. Ce déploiement permet au cluster de fonctionner en cas d'échec d'un nœud de contrôle.

Les nœuds supplémentaires qui sont ajoutés à un cluster WildFire fonctionnent en tant que nœuds esclaves ou de serveur. Le troisième nœud est automatiquement configuré en tant que serveur, alors que les nœuds subséquents font office de nœuds esclaves.

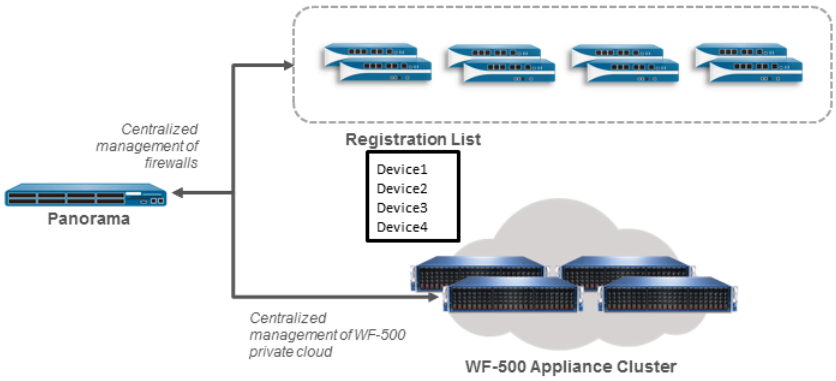
Avantages de la gestion des clusters WildFire au moyen de Panorama

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Si vous gérez les clusters d'appareils WildFire à l'aide de Panorama, vous pouvez effectuer la configuration de deux appareils M-Series ou virtuels Panorama en tant que paire HA pour permettre une redondance de gestion. Si vous ne configurez pas d'appareils Panorama redondants et que Panorama échoue, vous pouvez tout de même gérer les clusters localement depuis le nœud de contrôle.

Si vous utilisez une paire HA d'appareils Panorama pour gérer le cluster et qu'un appareil Panorama échoue, l'autre appareil Panorama reprend la gestion du cluster. En cas d'échec d'une paire HA d'appareils Panorama, rétablissez le service à partir de l'homologue qui a échoué dès que possible pour rétablir la HA de gestion.

Pour disposer d'une HA d'analyse, de stockage et de gestion centralisée, vous devez disposer d'au moins deux appareils WildFire que vous configurerez en tant que nœuds de contrôle et nœuds de contrôle de secours du cluster ainsi que de deux appareils Panorama M-Series ou virtuels.



Les pare-feu reçoivent une liste d’inscription dans laquelle figurent tous les appareils WildFire qui sont membres du cluster. Les pare-feu peuvent s'inscrire auprès de n’importe quel nœud du cluster, et le cluster équilibre automatiquement la charge entre ses nœuds.

Gestion des clusters d'appareils WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Pour gérer un cluster d'appareils WildFire, vous devez connaître les capacités des clusters et les recommandations en matière de gestion.

Catégorie	Description
Configuration et fonctionnement d’un cluster	Configurez tous les nœuds de cluster de manière identique pour garantir l’uniformité de l’analyse et de la communication d’un appareil à l’autre : • Tous les nœuds du cluster doivent utiliser la même version de PAN-OS (PAN-OS 8.0.1 ou version ultérieure). Panorama doit utiliser la même version du logiciel que les nœuds du cluster ou une version plus récente. Les pare-feu peuvent utiliser les mêmes versions du logiciel qui leur permettent d’envoyer des échantillons à un appareil WildFire. Les pare-feu n’ont pas besoin de disposer d’une version particulière du logiciel pour envoyer des échantillons à un cluster d'appareils WildFire. • Les nœuds du cluster héritent de la configuration du nœud de contrôle, à l’exception de la configuration de l'interface. Les membres du cluster surveillent la configuration du nœud de contrôle et mettent leurs propres configurations à jour lorsque le nœud de contrôle valide une configuration mise à jour. Les nœuds esclaves héritent de certains paramètres, comme les paramètres du serveur de mises à jour du contenu, les paramètres du serveur du cloud WildFire, l’image de l’analyse des échantillons, les durées de conservation des données des échantillons, les paramètres de l’environnement d'analyse, les paramètres de génération de signatures, les paramètres de journalisation, les paramètres d’authentification ainsi que les paramètres du serveur Panorama, du serveur DNS et du serveur NTP. • Lorsque vous gérez un cluster au moyen de Panorama, l’appareil Panorama transmet une configuration identique à tous les nœuds du cluster. Bien que vous puissiez modifier la configuration localement sur un nœud d’un appareil WildFire, Palo Alto Networks ne vous recommande pas de le faire, car la prochaine fois que Panorama transmettra une configuration, celle-ci remplacera la configuration active sur le nœud. Les modifications apportées localement sur les nœuds du cluster que Panorama gère entraînent souvent des erreurs de désynchronisation (Out of Sync). • Si la liste des nœuds qui appartiennent au cluster n’est pas identique sur les deux nœuds de contrôle, le cluster génère un avertissement de désynchronisation (Out of Sync). Pour éviter toute situation où les deux nœuds de contrôle mettent continuellement à jour la liste des membres désynchronisée pour l’autre nœud, l’appartenance au cluster cesse d’être

Catégorie	Description
	appliquée. Lorsque cela se produit, vous pouvez synchroniser la liste des membres à partir de la CLI locale du nœud de contrôle et du nœud de contrôle de secours en exécutant la commande opérationnelle suivante : **`request high-availability sync-to-remote running-configuration`**. 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. Sur chaque nœud de contrôle, exécutez la commande **`show cluster all-peers`**, puis comparez les listes de membres et corrigez-les. • Un cluster ne peut posséder que deux nœuds de contrôle (principal et de secours). Toute tentative visant à ajouter localement un troisième nœud de contrôle se soldera par un échec du cluster. (L'interface Web de Panorama vous empêche automatiquement d'ajouter un troisième nœud de contrôle.) Le troisième nœud ajouté à un cluster, de même que tous ceux qui suivent, doit être un nœud esclave. • Dans les configurations HA, le cluster distribue et conserve plusieurs copies de la base de données, des services de file d'attente et des envois d'échantillons, ce qui lui permet de procurer une redondance en cas d'échec de l'un de ses nœuds. L'exécution des services supplémentaires qui s'avèrent nécessaires pour procurer la redondance de la HA a une faible incidence sur le débit. • Le cluster vérifie automatiquement si des adresses IP doubles ont été utilisées pour le réseau de l'environnement d'analyse. • Si un nœud appartient à un cluster et que vous souhaitez l'intégrer à un autre cluster, vous devez d'abord le supprimer de son cluster actuel. • Ne modifiez pas l'adresse IP des appareils WildFire qui sont en train d'exécuter un cluster. Autrement, le pare-feu associé se désenregistrerait du nœud.
Politiques de conservation des données du cluster	Les politiques de conservation des données déterminent la durée pendant laquelle le cluster d'appareils WildFire stocke différents types d'échantillons. • **Échantillons bénins et indésirables** : le cluster conserve les échantillons bénins et indésirables pour une période de 1 à 90 jours (14 jours par défaut). • **Échantillons malveillants** : le cluster conserve les échantillons malveillants pour une période minimale de 1 jour (la valeur par défaut est indéfinie : ne jamais supprimer). Les échantillons malveillants peuvent comprendre des échantillons pour lesquels des verdicts d'hameçonnage ont été rendus. Configurez la même politique de conservation des données pour l'ensemble du cluster (4 dans configuration locale des paramètres généraux d'un cluster ou 4 dans configuration des paramètres généraux d'un cluster sur Panorama).

Catégorie	Description
Mise en réseau	Aucune communication n’est permise entre les clusters d'appareils WildFire. Les nœuds communiquent entre eux à l’intérieur d’un cluster donné, mais ne communiquent pas avec les nœuds des autres clusters. Tous les membres du cluster doivent : • Utiliser une interface de gestion dédiée au cluster pour la gestion et la communication du cluster (appliquée dans Panorama). • Disposer d’une adresse IP statique du même sous-réseau. • Utiliser des connexions à faible latence entre les nœuds du cluster. La latence maximale d’une connexion ne devrait pas être supérieure à 500 ms.
Interface de gestion dédiée au cluster	L’interface de gestion dédiée au cluster permet aux nœuds de contrôle de gérer le cluster. Ce n’est pas la même interface que l’interface de gestion standard (Ethernet0). Panorama oblige la configuration d’une interface de gestion dédiée au cluster. *En cas d’échec de la liaison de gestion du cluster entre les deux nœuds de contrôle d’une configuration à deux nœuds, l’analyse d’échantillons et les services du nœud de contrôle de secours continuent de s’exécuter même si ce dernier ne dispose d’aucune communication de gestion avec le nœud de contrôle principal. En effet, lorsque la liaison de gestion du cluster échoue, le nœud de contrôle de secours ne sait pas si le nœud de contrôle principal demeure fonctionnel, ce qui donne lieu à une situation de* split-brain*. Le nœud de contrôle de secours doit continuer à fournir des services au cluster au cas où le nœud de contrôle principal n’est pas fonctionnel. Une fois la liaison de gestion du cluster rétablie, les données des deux nœuds de contrôle sont fusionnées.*
DNS	Vous pouvez utiliser le nœud de contrôle d’un cluster d'appareils WildFire en tant que serveur DNS faisant autorité pour le cluster. (Un serveur DNS faisant autorité fournit les adresses IP des membres du cluster, tandis qu’un serveur DNS récursif interroge le serveur DNS faisant autorité et transmet les informations demandées à l’hôte qui a présenté la requête initiale.) Les pare-feu qui envoient des échantillons au cluster d'appareils WildFire devraient envoyer des requêtes DNS à leur serveur DNS habituel, par exemple, un serveur DNS d’entreprise interne. Le serveur DNS interne transmet la requête DNS au contrôleur du cluster d'appareils WildFire (selon le domaine de la requête). L’utilisation du contrôleur du cluster en tant que serveur DNS procure de nombreux avantages : • **Équilibrage de charge automatique** : lorsque le contrôleur du cluster résout le nom d’hôte utilisé pour la publication du service, les nœuds

Catégorie	Description
	du cluster hôte sont en ordre aléatoire, ce qui a pour effet d'équilibrer organiquement la charge sur les nœuds. • **Tolérance aux pannes** : si un nœud du cluster échoue, le contrôleur du cluster le supprime automatiquement de la réponse DNS, ce qui assure que les pare-feu envoient de nouvelles requêtes à des nœuds qui sont actifs. • **Souplesse et facilité de gestion** : lorsque vous ajoutez des nœuds au cluster, puisque le contrôleur met automatiquement à jour la réponse DNS, vous n'avez à apporter aucun changement sur le pare-feu et les requêtes sont automatiquement envoyées aux nouveaux nœuds ainsi qu'aux nœuds qui existaient auparavant. Bien que l'enregistrement DNS ne doive pas être mis en cache, pour le dépannage, si la recherche DNS réussit, la valeur TTL est 0. Toutefois, si la recherche DNS renvoie NXDOMAIN, la valeur TTL et la valeur TTL minimale sont toutes deux 0.
Administration	Vous pouvez administrer les clusters d'appareils WildFire au moyen de la CLI locale de WildFire ou de Panorama. Deux rôles administrateur sont disponibles localement sur les nœuds du cluster WildFire : • **Super lecteur** : accès en lecture seule. • **Super utilisateur** : accès en lecture / écriture
Enregistrement du pare-feu	Les clusters d'appareils WildFire transmettent à chaque pare-feu connecté à un nœud d'un cluster une liste d'enregistrement dans laquelle figurent tous les nœuds du cluster. Lorsque vous enregistrez un pare-feu auprès d'un appareil d'un cluster, le pare-feu reçoit la liste d'enregistrement. Lorsque vous ajoutez un appareil WildFire qui a déjà connecté des pare-feu à un cluster pour devenir un nœud de cluster, ces pare-feu reçoivent la liste d'enregistrement. En cas d'échec d'un nœud, les pare-feu connectés se servent de la liste d'enregistrement pour s'enregistrer auprès du prochain nœud qui figure sur la liste.
Migration de données	Pour procurer la redondance des données, les nœuds d'appareils WildFire d'un cluster partagent la base de données, les services de file d'attente et le contenu d'envoi d'échantillons. Toutefois, l'emplacement précis de ces données dépendra de la topologie du cluster. Par conséquent, les appareils WildFire d'un cluster sont soumis à des migrations de données ou à des réorganisations de données chaque fois que des changements sont apportés à la topologie. Les changements de topologie peuvent comprendre l'ajout ou la suppression de nœuds ainsi que la modification du rôle d'un nœud préexistant. Une migration de données peut également se produire lorsque les bases de données sont converties à une version plus récente, comme cela s'est produit lors du passage de WildFire 7.1 à 8.0.

Catégorie	Description
	On peut afficher l’état de la migration de données en déclenchant des commandes d’état à partir de la CLI WildFire. Ce processus peut prendre plusieurs heures selon la quantité de données qui est stockée sur les appareils WildFire.

Déploiement d’un cluster d’appareils WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Pour déployer un cluster d'appareils WildFire, vous devez mettre à niveau tous les appareils qui seront inscrits dans le cluster, créer le cluster WildFire, puis configurer les paramètres qui répondent le mieux à vos besoins. Vous pouvez effectuer ces tâches localement depuis la CLI de l’appareil WildFire ou par l’intermédiaire de Panorama, option qui vous permet d’appliquer rapidement les changements de configuration des appareils WildFire connectés et de les mettre à niveau.

La procédure suivante décrit la création et la configuration d’une paire High Availibility (haute disponibilité ; HA) d’appareils WildFire et l'ajout de nœuds d’appareils supplémentaires à un cluster.

STEP 1 | Procédez à la mise à niveau locale de vos appareils WildFire vers PAN-OS 8.0.1, la version minimale prise en charge pour faire fonctionner des clusters, ou vers une version ultérieure.

STEP 2 | Créez et configurez des nœuds, et ajoutez-en à un cluster d'appareils WildFire.

- Configuration d’un cluster et ajout de nœuds localement
- Configuration d’un cluster et ajout de nœuds sur Panorama

STEP 3 | Configurez les paramètres généraux d’un cluster d'appareils WildFire.

- Configuration locale des paramètres généraux d’un cluster
- Configuration des paramètres généraux d’un cluster sur Panorama

STEP 4 | (Facultatif) Chiffrer la communication d'appareil à appareil du cluster WildFire.

- Configurer le chiffrement d'appareil à appareil à l'aide de certificats prédéfinis via l'interface de ligne de commande
- Configurer le chiffrement d'appareil à appareil à l'aide de certificats personnalisés via la CLI
- Configurer le chiffrement d'appareil à appareil à l'aide de certificats prédéfinis de manière centralisée sur Panorama
- Configurer le chiffrement d'appareil à appareil à l'aide de certificats prédéfinis de manière centralisée sur Panorama

STEP 5 | Vérifiez que votre cluster d'appareils WildFire fonctionne normalement.

- Affichage de l’état du cluster d’appareils WildFire au moyen de la CLI
- Affichage de l’état du cluster d’appareils WildFire au moyen de Panorama

STEP 6 | (Facultatif) Mettez à niveaux les appareils WildFire qui sont déjà inscrits à un cluster.

- Mise à niveau locale d’un cluster à partir d’une connexion Internet
- Mise à niveau locale d’un cluster sans connexion Internet
- 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

Configuration locale d’un cluster sur des appareils WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Avant de configurer localement un cluster d’appareils WildFire, 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.

Si vous gérez votre cluster d'appareils WildFire à l'aide de Panorama, vous pouvez également configurer votre cluster WildFire de manière centralisée sur Panorama.

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. 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.*

Lorsque vos appareils WildFire sont disponibles, effectuez les tâches appropriées :

- Configuration d’un cluster et ajout de nœuds localement
- Configuration locale des paramètres généraux d’un cluster
- Suppression locale d’un nœud d’un cluster

Configuration d’un cluster et ajout de nœuds localement

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Lorsque vous ajoutez des nœuds à un cluster, le cluster établit automatiquement la communication entre les nœuds en fonction des interfaces que vous avez configurées pour le nœud de contrôle.

STEP 1 | Assurez-vous que chaque appareil WildFire que vous souhaitez ajouter au cluster utilise PAN-OS 8.0.1 ou une version ultérieure.

Sur chaque appareil WildFire, exécutez la commande suivante :

```
admin@WF-500> afficher les informations système | version
 correspondante
```


STEP 2 | Vérifiez que les appareils WildFire n'analysent pas d'échantillons et qu'ils sont autonomes (qu'ils n'appartiennent pas à un autre cluster).

1. Affichez sur chaque appareil s'il analyse des échantillons :

```
admin@WF-500> afficher l'analyse globale des échantillons
 wildfire
```

   Aucun échantillon ne devrait être à l'état `pending`. L'état de tous les échantillons devrait être terminé. Si les échantillons sont à l'état `pending`, attendez que l'analyse soit terminée. Les échantillons `Pending` s'affichent séparément des échantillons malveillants et inoffensifs. `Finish Date` indique la date et l'heure auxquelles l'analyse a pris fin.

2. Sur chaque appareil, vérifiez que tous les processus s'exécutent :

```
admin@WF-500> afficher l'état du logiciel système
```

3. Vérifiez que chaque appareil est autonome et qu'il n'appartient pas déjà à un cluster :

```
admin@WF-500> afficher l'appartenance au cluster Résumé
 du service : signature wfpc Nom du cluster : Address
 (Adresse) : 10.10.10.100 Nom d'hôte : Nom du nœud WF-500 :
 wfpc-000000000000-internal Numéro de série : 000000000000
 Mode nœud : autonome Rôle serveur : Véritable priorité
 HA : Dernière modification : Mon, 06 Mar 2017 16:34:25
 -0800 Services : wfcore signature wfpc infra État du
 moniteur : État de santé de Serf : passage de l'agent actif
 et accessible État de l'application : global-db-service :
 ReadyStandalone wildfire-apps-service :  Ready global-queue-
service: ReadyStandalone wildfire-management-service: Terminé
 siggen-db : Rapport ReadyMaster Diag : 10.10.10.100 : leader
 signalé '10.10.10.100', âge 0. 10.10.10.100 : le nœud local a
 réussi le contrôle d'intégrité.
```

   Les lignes surlignées indiquent que le nœud est en mode autonome et qu'il est prêt à être converti (appareil autonome à nœud d'un cluster).

   Le numéro de série à 12 chiffres qui figure dans ces exemples (`000000000000`) est un exemple générique. Il ne s'agit pas d'un véritable numéro de série. Les appareils WildFire de votre réseau possèdent des numéros de série uniques et véritables.

STEP 3 | Configurez le nœud de contrôle principal.

Il faut notamment configurer le nœud en tant que contrôleur principal de la paire HA, activer la HA et définir les interfaces que l'appareil utilise pour la connexion de la liaison de contrôle HA ainsi que pour la gestion et la communication du cluster.

1. Activez la haute disponibilité et configurez la connexion de l'interface de la liaison de contrôle au nœud de contrôle de secours, par exemple, sur l'interface eth3 :

   ```
   admin@WF-500# définir l'interface haute disponibilité
    activée deviceconfig sur oui ha1 port eth3 peer-ip-
   address <secondary-node-eth3-ip-address>
   ```

2. Configurez l'appareil en tant que nœud de contrôle principal :

   ```
   admin@WF-500# définir deviceconfig haute disponibilité
    election-option priorité principale
   ```

3. (Facultatif) Configurez l'interface haute disponibilité de secours entre le nœud de contrôle et le nœud de contrôle de secours, par exemple, sur l'interface de gestion :

   ```
   admin@WF-500# définir deviceconfig haute disponibilité
    interface ha1-backup gestion des ports peer-ip-
   address <secondary-node-management-ip-address>
   ```

4. Configurez l'interface dédiée pour la communication et la gestion au sein du cluster. Vous devez notamment préciser le nom du cluster et définir le rôle du nœud sur celui de nœud de contrôle :

   ```
   ad min@WF-500# définir le cluster de deviceconfig cluster-
   name<name>interface contrôleur de mode eth2
   ```

   Dans cet exemple, l'interface ethernet2 sert de port de communication dédié pour le cluster.

   Le nom du cluster doit être un nom de sous-domaine valide qui comporte un maximum de 63 caractères. Seuls les caractères en lettre minuscule et les chiffres sont autorisés. Les tirets et les points sont également autorisés s'ils ne sont pas utilisés au début ni à la fin du nom du cluster.

STEP 4 | Configurez le nœud de contrôle de secours.

Il faut notamment configurer le nœud en tant que contrôleur de secours de la paire HA, activer la HA et définir les interfaces que l'appareil utilise pour la connexion de la liaison de contrôle HA ainsi que pour la gestion et la communication du cluster.

1. Activez la haute disponibilité et configurez la connexion de l'interface de liaison de contrôle au nœud de contrôle principal sur la même interface utilisée sur le nœud de contrôle principal (eth3 dans le cas présent) :

   ```
   admin@WF-500# définir haute disponibilité sur activé
    oui de l'interface deviceconfig ha1 port eth3 peer-ip-
   address<primary-node-eth3-ip-address>
   ```

2. Configurez l'appareil en tant que nœud de contrôle de secours :

   ```
   admin @ WF-500 # définir la priorité secondaire de election-
   option sur haute disponibilité de deviceconfig
   ```

3. (Recommandé) Configurez l'interface haute disponibilité de secours entre le nœud de contrôle de secours et le nœud de contrôle, par exemple, sur l'interface de gestion :

   ```
   admin@WF-500# définir deviceconfig haute disponibilité
    interface ha1-backup gestion des ports peer-ip-
   address <primary-node-management-ip-address>
   ```

4. Configurez l'interface dédiée pour la communication et la gestion au sein du cluster. Vous devez notamment préciser le nom du cluster et définir le rôle du nœud sur celui de nœud de contrôle :

   ```
   ad min@WF-500# définir le cluster de deviceconfig cluster-name
    <name> interface contrôleur de mode eth2
   ```

STEP 5 | Validez les configurations sur les deux nœuds de contrôle.

Sur chaque nœud de contrôle :

```
admin@WF-500# valider
```

La validation de la configuration sur les deux nœuds de contrôle forme un cluster à deux nœuds.

STEP 6 | Vérifiez la configuration sur le nœud de contrôle principal.

Sur le nœud de contrôle principal :

```
admin@WF-500(active-controller)> afficher l'appartenance du
 cluster Récapitulatif du service : wfpc signature Nom du cluster :
 mycluster Adresse : 10.10.10.100 Nom d'hôte : Nom du nœud WF-500 :
 wfpc-000000000000-internal Numéro de série : 000000000000 Mode
 nœud : contrôleur Rôle serveur : Véritable priorité HA : dernière
 modification principale : Sam, 04 mars 2017 12:52:38 -0800
 Services : wfcore signature wfpc infra État du moniteur : État
 de santé de Serf : passage de l'agent actif et joignable État
```



```
 de l'application :  global-db-service : JoinedCluster  wildfire-
apps-service: Prêt  global-queue-service: JoinedCluster  wildfire-
management-service: Terminé  siggen-db : ReadyMaster Rapport de
 diagnostic : 10.10.10.110 : leader signalé '10.10.10.100', âge 0.
 10.10.10.100 : le nœud local a réussi le contrôle de santé
```

La ligne d'invite (`active-controller`) et la ligne surlignée `Application status` indiquent que le nœud est en mode contrôleur, qu'il est prêt et qu'il s'agit du nœud de contrôle principal.

STEP 7 | Vérifiez la configuration sur le nœud de contrôle secondaire.

Sur le nœud de contrôle secondaire :

```
admin@WF-500(passive-controller)> afficher l'appartenance au
 cluster Récapitulatif du service : signature wfpc Nom du cluster :
 mycluster Adresse : 10.10.10.110 Nom d'hôte : Nom du nœud WF-500 :
 wfpc-000000000000-internal Numéro de série : 000000000000 Mode
 nœud : contrôleur Rôle serveur : Véritable priorité HA :
 secondaire Dernière modification : Ven, 02 Dec 2016 16:25:57 -0800
 Services : wfcore signature wfpc infra État du moniteur : État
 de santé de Serf : passage de l'agent actif et joignable État
 de l'application :  global-db-service : JoinedCluster  wildfire-
apps-service: Prêt  global-queue-service: JoinedCluster  wildfire-
management-service: Terminé  siggen-db : ReadySlave Rapport de
 diagnostic : 10.10.10.110 : leader signalé '10.10.10.100', âge 0.
 10.10.10.110 : le nœud local a réussi le contrôle d'intégrité.
```

La ligne d'invite (`passive-controller`) et la ligne surlignée `Application status` indiquent que le nœud est en mode contrôleur, qu'il est prêt et qu'il s'agit du nœud de contrôle de secours.

STEP 8 | Testez la configuration du nœud.

Vérifiez que les clés API du nœud de contrôle peuvent être affichées globalement :

```
admin@WF-500(passive-controller)> afficher  wildfire global api-
keys Récapitulatif allService : wfpc signature Nom du cluster :
 mycluster
```

Les touches API des deux appareils devraient être consultables.

STEP 9 | Synchronisez manuellement les configurations haute disponibilité sur les nœuds de contrôle.

La synchronisation des nœuds de contrôle assure la correspondance des configurations. Vous ne devriez l'effectuer qu'une seule fois. Une fois les configurations de haute disponibilité synchronisées, les nœuds de contrôle conservent les configurations synchronisées ; vous n'avez plus à les synchroniser.

1. Sur le nœud de contrôle principal, synchronisez la configuration de la haute disponibilité au nœud de contrôle de l'homologue distant :

```
admin @ WF-500 (contrôleur actif)> demande la synchronisation
 haute disponibilité avec la configuration de fonctionnement à
 distance
```

   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.
2. Validez la configuration :

```
admin@WF-500# valider
```

STEP 10 | Vérifiez que le cluster fonctionne correctement.

Pour vérifier les renseignements relatifs au pare-feu, vous devez d'abord connecter au moins un pare-feu au nœud du cluster en sélectionnant ***Device (Périphérique)*** > ***Setup (Configuration)*** > ***WildFire (WildFire)*** *et en modifiant les* ***General Settings (Paramètres généraux)*** *pour qu'ils pointent vers le nœud.*

1. Affichez les homologues du cluster pour vous assurer que les deux contrôleurs sont membres du cluster :

```
admin@WF-500(active-controller)> afficher le cluster all-peers
```

2. Affichez les clés API des deux nœuds (si vous avez créé des clés API), à partir de n'importe quel nœud de contrôle :

```
admin @ WF-500 (contrôleur actif)> afficher toutes les clés
 API globales Wildfire
```

3. Accédez aux échantillons à partir de n'importe quel nœud de contrôle :

```
admin@WF-500(active-controller)> afficher l'état de
 l'échantillon wildfire global égal sha256<value>
```

4. Les pare-feu peuvent enregistrer et télécharger des fichiers sur les deux nœuds. Confirmez que le pare-feu transfère correctement les échantillons.
5. Les deux nœuds peuvent télécharger et analyser des fichiers.
6. Tous les fichiers analysés après la création du cluster indiquent deux emplacements de stockage, un sur chaque nœud.

STEP 11 | (Facultatif) Configurez un nœud esclave et ajoutez-le au cluster.

Les nœuds esclaves utilisent les paramètres du nœud de contrôle pour assurer l'uniformité de la configuration du cluster. Vous pouvez ajouter un maximum de 18 nœuds esclaves à un cluster, pour un maximum de 20 nœuds dans un cluster.

1. Sur le nœud de contrôle principal, ajoutez le nœud esclave à la liste des esclaves du nœud de contrôle :

   ```
   admin@WF-500(active-controller)> configurer
    admin@WF-500(active-controller)# définir le contrôleur du
    mode cluster de deviceconfig worker-list<ip>
   ```

   Le <*ip*> est l'adresse IP de l'interface de gestion des clusters du nœud esclave que vous voulez ajouter au cluster. Utilisez des commandes distinctes pour ajouter chaque nœud esclave au cluster.
2. Validez les configurations sur le nœud de contrôle :

   ```
   admin@WF-500(active-controller)# valider
   ```
3. Sur l'appareil WildFire que vous voulez convertir en noeud esclave du cluster, configurez le cluster à joindre, définissez l'interface de communications du cluster et placez l'appareil en mode `worker` :

   ```
   ad min@WF-500> configurer admin@WF-500# définir le cluster
    deviceconfig cluster-name<name>interface de travail en mode
    eth2
   ```

   L'interface de communications du cluster doit être identique à l'interface spécifiée sur les nœuds de contrôle pour les communications à l'intérieur du cluster. Dans le présent exemple, `eth2` est l'interface configurée sur les nœuds de contrôle pour la communication au sein du cluster.
4. Validez les configurations sur le nœud esclave :

   ```
   admin@WF-500# valider
   ```
5. Attendez que tous les services soient actifs sur le nœud esclave. Lancez **`show cluster membership (affichez l'adhésion au cluster)`** et vérifiez le `Applicationstatus (statut de l'application)`, qui indique tous les services et le `siggen-db` qui sont `Ready (prêts)` lorsque tous les services sont actifs.
6. Sur l'un ou l'autre des nœuds de contrôle, vérifiez que le nœud esclave a été ajouté :

   ```
   admin@WF-500> afficher tous les pairs du cluster
   ```

   Le nœud esclave que vous avez ajouté apparaît dans la liste des nœuds du cluster. Si, par mégarde, vous avez ajouté le mauvais appareil WildFire à un cluster, vous pouvez procéder à la suppression locale d'un nœud d'un cluster.

STEP 12 | Vérifiez la configuration sur le nœud esclave.

1. Sur le nœud esclave, vérifiez que le champ `Node mode` indique que le nœud est au mode esclave :

   ```
   admin@WF-500> afficher l'appartenance au cluster
   ```

2. Vérifiez que les pare-feu peuvent s’enregistrer sur le nœud esclave et que le nœud esclave peut télécharger et analyser les fichiers.

Configuration locale des paramètres généraux d’un cluster

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

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 :

- 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.

Procédez à la configuration des paramètres WildFire au moyen de la CLI sur le nœud de contrôle principal du cluster. Les autres nœuds du cluster utilisent les paramètres configurés sur le contrôleur du cluster.

STEP 1 | Configurez les paramètres généraux du cluster WildFire. Ce processus s’apparente à celui utilisé pour la configuration des paramètres de l’appareil WildFire.

1. (Recommandé) Réinitialisez le mot de passe admin.
2. Configurez les paramètres de l'interface de gestion. Définissez les adresses IP et la passerelle par défaut du nœud du cluster d'appareils WildFire. Chaque nœud du cluster d'appareils WildFire doit avoir une adresse IP statique du même sous-réseau. Définissez également les adresses IP du serveur DNS.
3. Configurez l'horloge de l'appareil WildFire. Définissez l’horloge manuellement ou en précisant les serveurs NTP, et définissez l’authentification du serveur NTP.
4. Choisissez l'image de machine virtuelle que l'appareil devra utiliser pour l'analyse de fichiers.
5. (Facultatif) Autorisez d'autres utilisateurs à gérer l'appareil WildFire. Ajoutez les comptes administrateur et attribuez-leur des rôles de gestion du cluster.
6. Configurez l'authentification RADIUS pour l'accès administrateur.

STEP 2 | (Facultatif) Connectez le cluster au cloud WildFire public et configurez les services de cloud que le cluster utilisera.

Si aucune raison d'affaires ne vous empêche de connecter le cluster d'appareils WildFire au cloud WildFire public, la connexion du cluster au cloud vous procure certains avantages, notamment :

- Utiliser les ressources du cloud pour analyser les échantillons dans plusieurs environnements au moyen de méthodes diverses.
- Interroger automatiquement le cloud pour obtenir des verdicts avant de procéder à une analyse locale et ainsi supprimer certaines tâches du cluster. (Cette option est désactivée par défaut.)
- Tirer profit des données d'intelligence de l'ensemble de la communauté WildFire et y contribuer.

Les fonctionnalités décrites dans cette rangée du tableau ne sont pas propres aux clusters. Vous pouvez également configurer ces fonctionnalités sur les appareils WildFire autonomes.

1. Tirer profit des données d'intelligence recueillies sur tous les appareils WildFire connectés :

   ```
   admin@WF-500(active-controller)# définir paramètre
    deviceconfig wildfire cloud-server<hostname-value>
   ```

   La valeur par défaut du nom d'hôte du serveur du cloud WildFire public est `wildfire-public-cloud`. Vous pouvez effectuer le transfert de fichiers pour analyse par WildFire vers n'importe quel cloud WildFire public.
2. Si vous connectez le cluster à un cloud WildFire public, vous devez décider de configurer, ou non, l'interrogation automatique du cloud public pour obtenir des verdicts avant d'effectuer l'analyse locale. L'interrogation du cloud public permet, dans un premier temps, de réduire la charge sur le cluster WildFire local :

   ```
   admin@WF-500(active-controller)# définir le paramètre
    deviceconfig wildfire cloud-intelligence cloud-query (non |
    oui)
   ```
3. Si vous connectez le cluster à un cloud WildFire public, configurez les types d'information pour lesquels vous souhaitez procéder à l'envoi des logiciels malveillants découverts localement ou des rapports au cloud WildFire public (données de diagnostic, rapports XML sur l'analyse des logiciels malveillants, échantillons malveillants). Si vous envoyez des échantillons malveillants, le cluster n'envoie pas de rapports.

   ```
   admin@WF-500(active-controller)# définir le paramètre
    deviceconfig wildfire cloud-intelligence submit-diagnostics
    (non | oui) submit-report (non | oui) submit-sample (non |
    oui)
   ```


STEP 3 | (Facultatif) Configurez le nœud de contrôle pour qu'il publie l'état du service au moyen du protocole DNS.

```
admin@WF-500(active-controller)# définir le contrôleur du mode
 cluster deviceconfig service-advertisement dns-service activé oui
```

STEP 4 | (Facultatif) Configurez des politiques de conservation des données applicables aux échantillons malveillants et indésirables.

1. Sélectionnez la durée de conservation des différents types de données :

   ```
   admin@WF-500(active-controller)# définir le paramètre
    deviceconfig wildfire file-retention malveillant <indefinite
    | 1-2000> non malveillant<1-90>
   ```

   Par défaut, la durée de conservation des échantillons malveillants est indéfinie (ne pas supprimer). Par défaut, la durée de conservation des échantillons qui ne sont pas malveillants (bénins et indésirables) est de 14 jours.

STEP 5 | (Facultatif) Configurez l'environnement d'analyse privilégié.

1. Si votre environnement d'analyse analyse principalement les échantillons de fichiers exécutables ou les échantillons de documents, vous pouvez allouer la majorité des ressources du cluster à l'analyse de ces types d'échantillons :

   ```
   admin@WF-500(active-controller)# définir le paramètre
    deviceconfig wildfire prefer-analysis-environment (Documents
    | Executables | défaut)
   ```

   Pour chaque appareil WildFire du cluster :

   - L'option `default` analyse simultanément 16 documents, 10 Portable Executables (exécutable portable ; PE) et 2 liens d'e-mail.
   - L'option Documents analyse simultanément 25 documents, 1 Portable Executable (exécutable portable ; PE) et 2 liens d'e-mail.
   - L'option Executables analyse simultanément 25 Portable Executables (exécutable portable ; PE), 1 document et 2 liens d'e-mail.

   Vous pouvez configurer un environnement d'analyse privilégié pour chaque nœud du cluster. (Si vous gérez le cluster depuis Panorama, Panorama peut définir l'environnement d'analyse de l'ensemble du cluster.)

STEP 6 | Configurez les paramètres d'analyse du nœud.

1. (Facultatif) Procédez au paramétrage des mises à jour de contenu pour améliorer l'analyse des logiciels malveillants.
2. Procédez à la Configuration de l'interface MV pour activer l'observation par le cluster des comportements malveillants, où le fichier en cours d'analyse cherche à accéder au réseau.
3. (Facultatif) Procédez à l'Activation de la génération de catégorie d'URL et de la signature locale pour générer les signatures DNS et antivirus et les catégories d'URL.

STEP 7 | Configurez la journalisation.

1. Configuration des paramètres du journal des envois WildFire.

Suppression locale d’un nœud d’un cluster

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Vous pouvez supprimer des nœuds d’un cluster à l’aide de la CLI locale. La procédure à suivre pour supprimer un nœud est différente si le cluster possède deux nœuds ou s’il en possède trois ou plus.

◉ Supprimez un nœud esclave d’un cluster composé d’au moins trois nœuds.

1. Mettez le nœud esclave hors service à partir de la CLI du nœud esclave :

```
admin@WF-500> démarrage de la mise hors service du cluster de
 demandes
```

La commande `decommission` ne fonctionne que pour les clusters qui possèdent trois nœuds ou plus. N’utilisez pas `decommission` pour supprimer un nœud d’un cluster à deux nœuds.

2. Confirmez que la mise hors service du nœud est réussie :

```
admin@WF-500> afficher l’appartenance aucluster
```

Cette commande renvoie `decommission: success` une fois que le nœud esclave a été supprimé du cluster. Si la commande n’indique pas que la mise hors service est réussie,

attendez quelques minutes pour permettre à la mise hors service de prendre find, puis exécutez la commande de nouveau.

3. Supprimez la configuration du cluster à partir de la CLI du nœud esclave :

```
admin@WF-500># supprimer le cluster deviceconfig
```

4. Validez la configuration :

```
admin@WF-500># valider
```

5. Vérifiez que tous les processus fonctionnent :

```
admin@WF-500> afficher l’état du logiciel du système
```

6. Supprimez le nœud esclave à partir de la liste des nœuds esclave du nœud de contrôle :

```
admin@WF-500(active-controller)# supprimer le contrôleur du
 mode cluster deviceconfig worker-list <worker-node-ip>
```

7. Validez la configuration :

```
admin@WF-500(active-controller)# valider
```

8. Sur le nœud de contrôle, assurez-vous que le nœud esclave a été supprimé :

```
admin@WF-500(active-controller)> afficher tous les pairs du
 cluster
```

Le nœud esclave que vous avez supprimé ne figure pas dans la liste des nœuds du cluster.

- Supprimez un nœud de contrôle d’un cluster à deux nœuds.

  Chaque cluster doit comporter deux nœuds de contrôle dans une configuration haute disponibilité fonctionnant dans des conditions normales. Il peut s’avérer toutefois nécessaire de supprimer un nœud de contrôle au moyen de la CLI pour effectuer la maintenance ou l’échange de nœuds de contrôle :

  1. Suspendez le nœud de contrôle que vous souhaitez supprimer :

     ```
     admin@WF-500(passive-controller)> interruption du débogage du cluster
     ```

  2. Sur le nœud de contrôle que vous souhaitez supprimer, supprimez la configuration haute disponibilité. Cet exemple illustre la suppression du nœud de contrôle de secours :

     ```
     admin@WF-500(contrôleur-passif)> configurer
      admin@WF-500(contrôleur-passif)# supprimer deviceconfig haute disponibilité
     ```

  3. Supprimez la configuration du cluster :

     ```
     admin@WF-500(contrôleur-passif)# supprimer le cluster deviceconfig
     ```

  4. Validez la configuration :

     ```
     admin@WF-500(contrôleur passif)# valider
     ```

  5. Attendez que les services soient restaurés. Exécutez la commande **`show cluster membership`** et vérifiez l’état de l’application `Application status`, qui présente tous les services et la `siggen-db` à l’état `Ready` lorsque tous les services sont actifs. Le `Node mode` devrait être `stand_alone`.
  6. Sur le nœud de cluster restant, vérifiez que le nœud a été supprimé :

     ```
     admin@WF-500(active-controller)> afficher tous les pairs du cluster
     ```

     Le nœud de contrôle que vous avez supprimé ne figure pas dans la liste des nœuds du cluster.
  7. Si un autre appareil WildFire est prêt, ajoutez-le dès que possible au cluster pour rétablir la haute disponibilité (Configuration d’un cluster et ajout de nœuds localement).

     Si aucun autre appareil WildFire n’est prêt à remplacer le nœud du cluster qui a été supprimé, vous devez supprimer les configurations de haute disponibilité et de cluster sur le nœud restant, puisque les clusters à un nœud ne sont pas recommandés et qu’ils ne procurent aucune haute

disponibilité. Il vaut mieux gérer un seul appareil WildFire en tant qu'appareil autonome, et non pas en tant que cluster à un nœud.

Pour supprimer les configurations de haute disponibilité et de cluster du nœud restant (dans cet exemple, le nœud de contrôle principal) :

```
admin@WF-500(contrôleur-actif)> configurer
 admin@WF-500(contrôleur-actif)# supprimer deviceconfig haute
 disponibilité admin@WF-500(contrôleur-actif)# supprimer le
 cluster deviceconfig admin@WF-500(contrôleur-actif)# valider
```

Attendez que les services soient restaurés. Exécutez la commande **show cluster membership** et vérifiez l'état de l'application `Application status`, qui présente tous les services et la `siggen-db` à l'état `Ready` lorsque tous les services sont actifs. Le `Node mode` devrait être `stand_alone`.

Configurer le chiffrement d'appareils-à-àppareils WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Vous pouvez chiffrer les communications WildFire entre les appareils déployés dans un cluster. Par défaut, les appareils WildFire envoient des données à l'aide de texte clair lorsqu’ils communiquent avec des appareils de gestion et des cluster WildFire homologues. Vous pouvez utiliser des certificats prédéfinis ou personnalisés pour authentifier les connexions entre les homologues de l'appareil WildFire à l'aide du protocole IKE / IPsec. Les certificats prédéfinis sont conformes aux exigences de certification et de conformité approuvées par FIPS / CC / UCAPL. Si vous souhaitez plutôt utiliser des certificats personnalisés, vous devez sélectionner un certificat conforme à FIPS / CC / UCAPL ; autrement, vous ne pourrez pas importer le certificat.

Vous pouvez configurer le chiffrement d'appareil à appareil WildFire localement à l'aide de l'interface de ligne de commande WildFire ou de façon centralisée via Panorama. Gardez à l'esprit que tous les appareils WildFire d'un cluster donné doivent exécuter une version de PAN-OS prenant en charge les communications cryptées.

Si les appareils WildFire de votre cluster utilisent le mode FIPS / CC, le cryptage est automatiquement activé à l'aide de certificats prédéfinis.

Selon la manière dont vous souhaitez déployer le chiffrement d'appareil à l’appareil, effectuez l'une des tâches suivantes :

- Configurer le chiffrement d'appareil à appareil à l'aide de certificats prédéfinis de manière centralisée sur Panorama
- Configurer le chiffrement d'appareil à appareil à l'aide de certificats prédéfinis de manière centralisée sur Panorama
- Configurer le chiffrement d'appareil à appareil à l'aide de certificats prédéfinis via l'interface de ligne de commande
- Configurer le chiffrement d'appareil à appareil à l'aide de certificats personnalisés via la CLI

Configurer le chiffrement d'appareil à appareil à l'aide de certificats prédéfinis via l'interface de ligne de commande

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Lors de la configuration du chiffrement d'appareil à appareil à l'aide de l'interface de ligne de commande, vous devez émettre toutes les commandes à partir de l'appareil WildFire désigné comme contrôleur actif. Les changements de configuration sont automatiquement distribués au contrôleur passif. Si vous utilisez un

cluster qui contient trois nœuds ou plus, vous devez également configurer les appareils du cluster WildFire faisant office de nœuds de serveur avec les mêmes paramètres que le contrôleur actif.

STEP 1 | Mettez à niveau chaque appareil WildFire géré vers la version 9.0 de PAN-OS.

STEP 2 | Vérifiez que votre cluster d'appareils WildFire a été correctement configuré et qu'il fonctionne correctement.

STEP 3 | Activez la communication de cluster sécurisée sur l'appareil WildFire désigné en tant que contrôleur actif.

```
définir le cryptage du cluster deviceconfig activé oui
```

STEP 4 | (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.

```
définir le cryptage haute disponibilité de deviceconfig
 activé oui
```

STEP 5 | (Clusters d'appareils avec 3 nœuds ou plus uniquement) Répétez les étapes 2 à 4 pour le troisième nœud de serveur d'appareil WildFire inscrit dans le cluster.

Configurer le chiffrement d'appareil à appareil à l'aide de certificats personnalisés via la CLI

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Lors de la configuration du chiffrement d'appareil à appareil à l'aide de l'interface de ligne de commande, vous devez émettre toutes les commandes à partir de l'appareil WildFire désigné comme contrôleur actif. Les changements de configuration sont automatiquement distribués au contrôleur passif. Si vous utilisez un cluster qui contient trois nœuds ou plus, vous devez également configurer les appareils du cluster WildFire faisant office de nœuds de serveur avec les mêmes paramètres que le contrôleur actif.

STEP 1 | Mettez à niveau chaque appareil WildFire géré vers la version 9.0 de PAN-OS.

STEP 2 | Vérifiez que votre cluster d'appareils WildFire a été correctement configuré et qu'il fonctionne correctement.

STEP 3 | Importez (ou éventuellement générez) un certificat avec une clé privée et son certificat d'autorité de certification. 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. Pour importer un certificat personnalisé, entrez ce qui suit à partir de l'interface de ligne de commande de l'appareil WildFire : **certificat d'importation scp à partir du <value> fichier <value> remote-port <1-65535> source-ip format<ip/netmask> certificate-name <value> phrase secrète <value><value>**
2. Pour générer un certificat personnalisé, saisissez ce qui suit à partir de la CLI du boitier WildFire : **request certificate generate certificate-name name digest country-code state locality organization email filename ca signed-by | ocsp-responder-url days-till-expiry hostname [...] request certificate generate certificate-name name digest country-code state locality organization email filename ca signed-by | ocsp-responder-url days-till-expiry ip [...] request certificate generate certificate-name name**

STEP 4 | Importez la paire de clés de l'appareil WildFire contenant le certificat de serveur et la clé privée.

```
importation scp keypair depuis le <value> fichier <value> remote-
port <1-65535> source-ip <ip/netmask> certificate-name <value>
 format de phrase secrète <value>  <pkcs12|pem>
```


STEP 5 | Configurez et spécifiez un profil SSL / TLS pour définir le certificat et le protocole que les appareils WildFire utilisent pour les services SSL / TLS.

définir gestion des paramètres deviceconfig secure-conn-server ssl-tls-service-profile <profile name>

1. Créez un profil SSL/TLS.

   ```
   définir ssl-tls-service-profile partagé <name>
   ```

2. Spécifiez un certificat personnalisé.

   ```
   définir un <name> certificat <value> shared ssl-tls-service-profile
   ```

3. Définissez la plage SSL/TLS.

   ```
   définir <name> protocol-settings min-version <tls1-0|tls1-1|tls1-2> de  shared ssl-tls-service-profile
   ```

   ```
   définir les paramètres de protocole ssl-tls-service-profile <name> _ssl-profile_max-version partagés <tls1-0|tls1-1|tls1-2|max>
   ```

4. Spécifiez le profil SSL/TLS. Ce profil de service SSL / TLS s'applique à toutes les connexions entre les appareils WildFire et le pare-feu, ainsi qu'aux homologues de l'appareil WildFire.

   ```
   définir la gestion des paramètres deviceconfig secure-conn-server ssl-tls-service-profile <ssltls-profile>
   ```


STEP 6 | Configurez et spécifiez un certificat de profil pour définir le certificat et le protocole que les appareils WildFire utilisent pour les services SSL / TLS.

1. Créez le profil de certificat.

```
définir shared certificate-profile <name>
```

2. (Facultatif) Définissez le nom du sujet (nom commun) ou l'autre nom du sujet.

```
définir shared certificate-profile <name> username-field
 subject <common-name>
```

```
définir shared certificate-profile <name> username-field
 subject-alt <email|principal-name>
```

3. (Facultatif) Définissez le domaine de l'utilisateur.

```
définir le <name> domaine <value> de shared certificate-
profile
```

4. Configurez le CA.

```
définir <name> autorité de certification <name> de shared
 certificate-profile
```

```
définir <name> autorité de certification <name> de shared
 certificate-profile sur default-ocsp-url <value>
```

```
définir <name> autorité de certification <name> de shared
 certificate-profile sur ocsp-verify-cert <value>
```

5. Indiquez le profil de certificat.

```
définir la gestion des paramètres deviceconfig secure-conn-
server certificate-profile <certificate-profile>
```

STEP 7 | Importez le certificat et la paire de clés privées.

STEP 8 | 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 9.

1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificats)**.
2. Configuration d'un profil de certificat.

3. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion) > Secure Communication Settings (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.
4. 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 créé à l'étape 2.
5. Sous Customize Communication (Personnaliser la communication), sélectionnez **WildFire Communication (Communication WildFire)**.
6. Cliquez sur **OK**.

STEP 9 | Désactivez l'utilisation du certificat prédéfini.

```
set deviceconfig setting management secure-conn-server disable-pre-defined-cert yes
```

STEP 10 | Spécifiez le nom DNS utilisé pour l'authentification qui se trouve dans le certificat personnalisé (généralement le SubjectName ou le SubjectAltName). Par exemple, le nom de domaine par défaut est **`wfpc.service.mycluster.paloaltonetworks.com`**.

```
définir les paramètres wildfire deviceconfig sur custom-dns-name <custom_dns_name>
```.

STEP 11 | (Clusters d'appareils avec 3 nœuds ou plus uniquement) Répétez les étapes 2 à 10 pour le troisième nœud de serveur d'appareil WildFire inscrit dans le cluster.

Surveillance d’un cluster d’appareils WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Vous pouvez vérifier l’état opérationnel de votre cluster d’appareils WildFire au moyen de la CLI ou de Panorama. Vous pouvez ainsi vérifier que les applications et les services qui s’exécutent sur un nœud donné fonctionnent correctement. Pour qu’un cluster WildFire fonctionne correctement, les applications et les services appropriés doivent être actifs sur chaque nœud et l’état de chacun d’entre eux doit être sain. Les clusters qui fonctionnent hors de ces paramètres pourraient ne pas s’exécuter dans des conditions optimales ou pourraient pointer vers d’autres problèmes, comme des problèmes de configuration.

La CLI affiche des informations qui ne sont pas disponibles à partir de Panorama. Il est hautement recommandé d’utiliser la CLI WildFire lorsque vous corrigez des problèmes liés au cluster.

Vous pouvez afficher l’état actuel d’un nœud de contrôle WildFire en exécutant une série de commandes show à partir de la CLI WildFire. La commande affiche les détails sur la configuration, les applications et les services qui sont actifs sur l’appareil ainsi que les messages d’erreur et d’état. Vous pouvez ensuite vous servir de ces détails pour déterminer l’état de votre cluster. L’affichage de l’état n’interrompt aucun service Wildfire. Vous pouvez exécuter cette commande en tout temps.

Consultez les sections suivantes pour plus de détails sur la surveillance de votre appliance WildFire :

- Affichage de l’état du cluster d’appareils WildFire au moyen de la CLI
- Affichage de l’état du cluster d’appareils WildFire au moyen de Panorama
- États des applications Wildfire
- États de service Wildfire

Affichage de l’état du cluster d’appareils WildFire au moyen de la CLI

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Pour confirmer le fonctionnement de votre cluster d’appareils WildFire selon les paramètres de fonctionnement normaux, vous devez exécuter les commandes show suivantes :

- **`show cluster controller`** : affiche l’état des nœuds actifs/passifs du cluster WildFire.
- **`show cluster all-peers`** : affiche les informations concernant tous les membres d’un cluster d’appareils WildFire donné.
- **`show cluster membership`** : affiche les informations relatives aux appareils WildFire appartenant à des nœuds de cluster ou des nœuds autonomes.

- **`show cluster data-migration-status`** : affiche l’état actuel du processus de migration des données.
- **`show log system`** : affiche le journal des événements WildFire, y compris les détails relatifs à l’état du système.

STEP 1 | Sur le nœud de contrôle d’un appareil WildFire, exécutez la commande suivante :

```
admin@WF-500(active-controller)>show clustercontroller
```

Un cluster WildFire sain affiche les détails suivants :

- Le nom du cluster auprès duquel l’appareil est inscrit et son rôle configuré.
- `K/V API online status` indique `True` lorsque l’interface interne du cluster fonctionne correctement. Un état `False` peut indiquer un problème réseau et la mauvaise configuration du nœud.
- `Task processing` affiche `True` sur les contrôleurs actifs (principaux) et `False` sur les contrôleurs passifs (de secours).
- Les adresses IP de tous les noeuds WildFire du cluster sont indiquées sous `App Service Avail`.
- Un maximum de trois `Good Core Servers` s'affiche. Le nombre de `Good Core Servers` dépend du nombre de nœuds qui s’exécutent dans le cluster. Si un troisième nœud fonctionne dans un cluster, il est automatiquement configuré en tant que nœud serveur pour optimiser l’intégrité du cluster.
- Aucun `Suspended Nodes`.
- `Current Task` fournit des informations générales sur les opérations exécutées au niveau du cluster, comme le redémarrage, la mise hors service et les tâches suspendues.

Cet exemple montre le résultat que l'on obtient d’un contrôleur actif configuré dans un cluster WildFire à deux nœuds qui fonctionne correctement :

```
Nom du cluster : API WildFire_Cluster K/V en ligne : Traitement des
 tâches réelles : sur Contrôleur actif Publicité DNS réelle : Nom
 DNS d’App Service : App Service Disponible : 2.2.2.14, 2.2.2.15
 Serveurs principaux : 009701000026 : 2.2.2.15 009701000043 :
 2.2.2.14 Bons serveurs principaux : 2 nœuds suspendus : Tâche
 en cours : * Affichage de la dernière tâche terminée Demande :
 démarrage depuis qa14 (009701000043/80025) at 2017-09-18 21:43:34
 UTC null Réponse: autorisé par qa15 à 2017-09-18 21:45:15 UTC 1/2
 serveurs principaux disponibles. Terminé : succès le 2017-09-18
 21:43:47 UTC
```


STEP 2 | Sur le nœud de contrôle d'un appareil WildFire, exécutez la commande suivante :

```
admin@WF-500> afficher tous les pairs du cluster
```

Un cluster WildFire sain affiche les détails suivants :

- Les informations générales concernant les nœuds WildFire du cluster sont indiquées sous `Address`, `Mode`, `Server`, `Node` et `Name`.
- Tous les noeuds du cluster WildFire utilisent le service `wfpc`, un service d'analyse d'échantillons de fichiers interne.
- Les nœuds actifs, passifs et serveur affichent `Serverrole applied` en regard de `Status`. Si le nœud est configuré pour être un serveur, mais qu'il ne fonctionne pas comme un serveur, le champ `status` affiche `Serverrole assigned`.

  Dans un déploiement à trois nœuds, le troisième nœud, soit le nœud serveur, entre dans la catégorie des nœuds esclaves.
- Les nœuds récemment supprimés peuvent être présents, mais la mention `Disconnected` s'affiche. Il faut parfois attendre plusieurs jours avant qu'un nœud déconnecté ne soit supprimé de la liste des nœuds du cluster.
- Le nœud de contrôle actif affiche `siggen-db:ReadyMaster`.
- Le nœud de contrôle passif affiche `siggen-db:ReadySlave`.

  Pour obtenir de plus amples informations sur les états de service et des applications WildFire, reportez-vous aux sections États de service Wildfire *et* États des applications Wildfire.
- `Diag report` présente les événements système et les messages d'erreur du cluster :

Message d'erreur	Description
`Unreachable`	Le nœud n'a jamais pu être atteint à partir du contrôleur du cluster.
`Unexpected member`	Le nœud ne fait pas partie de la configuration du cluster. Il se peut que le nœud ait été récemment supprimé de la configuration du cluster ou il peut s'agit d'une mauvaise configuration.
`Left cluster`	Le nœud ne peut plus être atteint à partir du contrôleur du cluster.
`Incorrect cluster name`	Le nœud possède un nom de cluster qui est mal configuré.
`Connectivity unstable`	La connexion entre le nœud et le contrôleur du cluster est instable.

Message d'erreur	Description
`Connectivity lost`	La connectivité entre le nœud et le contrôleur du cluster a été perdue.
`Unexpected server serial number`	La présence inattendue d'un nœud serveur a été détectée.

Cet exemple présente un cluster WildFire à trois nœuds qui fonctionne correctement :

```
Adresse Mode Nom du nœud du serveur ------- ---- ------ ---------
 2.2.2.15 contrôleur Auto Réel qa15 Service : signature infra
 wfcore wfpc Etat : Connecté, rôle de serveur appliqué Modifié :
 Mon, 18 Sep 2017 15:37:40 -0700 WF App : global-db-service :
 JoinedCluster wildfire-apps-service : Arrêté global-queue-service:
 JoinedCluster wildfire-management-service: Terminé siggen-db :
 Contrôleur ReadySlave 2.2.2.14 Pair réel qa14 Service : signature
 infra wfcore wfpc Etat : Connecté, rôle de serveur appliqué
 Modifié : Mon, 18 Sep 2017 15:37:40 -0700 WF App: global-db-
service: commit-lock wildfire-apps-service: Arrêté global-queue-
service: Service de gestion des feux de forêt ReadyStandalone :
 Terminé siggen-db : ReadyMaster 2.2.2.16 esclave réel wf6240
 Service : infra wfcore wfpc Etat : Connecté, rôle de serveur
 appliqué Modifié : Mer, 22 février 2017 11:11:15 -0800 WF App :
 wildfire-apps-service : Prêt global-db-service : Service de file
 d'attente global JoinedCluster : Service de base de données locale
 JoinedCluster : Rapport DataMigrationFailed Diag : 2.2.2.14:
 reported leader '2.2.2.15', age 0. 2.2.2.15: le nœud local a
 réussi la vérification de santé
```

STEP 3 | Sur le nœud de contrôle d'un appareil WildFire, exécutez la commande suivante :

```
admin@WF-500>afficher l'appartenance aucluster
```

Un cluster WildFire sain affiche les détails suivants :

- Les détails généraux sur la configuration de l'appareil WildFire, comme le nom du cluster, l'adresse IP de l'appareil, le numéro de série, etc.
- `Server role` indique si l'appareil WildFire fonctionne ou non comme un serveur du cluster. Les serveurs du cluster exploitent des services et des applications d'infrastructure supplémentaires. Vous pouvez ajouter trois serveurs maximum par cluster.
- `Node mode` décrit le rôle d'un appareil WildFire. Les appareils WildFire qui sont inscrits à un cluster peuvent être un nœud de contrôle (`controller`) ou esclave (`worker`), selon votre

configuration et le nombre de nœuds qui sont inclus dans votre déploiement. `Stand_alone` s'affiche si l'appareil ne fait pas partie d'un cluster.

- Les `Services` suivants sont exploités selon le rôle que joue le nœud du cluster :

Type de nœud	Services exploités sur le nœud
Nœud de contrôle (actif ou passif)	• `infra` • `wfpc` • `Signature` • `wfcore`
Nœud serveur	• `infra` • `wfpc` • `wfcore`
Nœud esclave	• `infra` • `wfpc`

- `HA priority` indique principal ou secondaire selon le rôle configuré. Ce paramètre est toutefois indépendant de l'état HA actuel de l'appareil.
- `Work queue status` montre les analyses d'échantillon en retard ainsi que les échantillons qui sont en cours d'analyse. Vous y découvrirez également la charge qu'un appareil WildFire reçoit.

Pour obtenir de plus amples informations sur les états de service et des applications WildFire, reportez-vous aux sections États de service WildFire *et* États des applications WildFire.

Cet exemple présente un contrôleur WildFire qui fonctionne correctement :

```
Résumé du service : signature wfpc Nom du cluster : qa-
auto-0ut1 Adresse : 2.2.2.15 Nom d'hôte : qa15 Nom de nœud :
 wfpc-009701000026-internal Numéro de série : 009701000026
 Mode nœud : contrôleur Rôle serveur : Véritable priorité HA :
 secondaire Dernière modification : Ven, 22 Sep 2017 11:30:47
 -0700 Services : wfcore signature wfpc infra État du moniteur :
 État d'intégrité du serf: passage de l'agent vivant et accessible
 Vérification de l'infrastructure du service: réussi Etat de
 l'application: global-db-service: ReadyLeader wildfire-apps-
service: global-queue-service prêt: ReadyLeader wildfire-
management-service: Terminé siggen-db : État de la file d'attente
 prêt à travailler : analyse de l'échantillon en file d'attente :
 0 analyse d'échantillon en cours : 0 exemple de copie en file
 d'attente : 0 exemple de copie en cours d'exécution : 0 Rapport
 de diagnostic : 2.2.2.14: reported leader '2.2.2.15', age 0.
 2.2.2.15: le nœud local a réussi la vérification de santé
```


STEP 4 | Sur le nœud de contrôle d'un appareil WildFire, exécutez la commande suivante :

admin@WF-500(active-controller)>show clusterdata-migration-status

L'appareil WildFire affiche les détails suivants sur la migration des données :

- Ne transférez pas les fichiers au cluster d'appareils WildFire lorsque la migration des données est en cours. Lorsque la migration de données est terminée, la commande affiche l'horodatage d'achèvement.
- Les changements topologiques apportés au cluster WildFire (par exemple, l'ajout ou le retrait de nœuds ou la modification des rôles des nœuds déclenchent les événements de migration des données.
- La migration des données peut se produire lors de la mise à niveau vers une nouvelle version de WildFire. Après la mise à niveau, veillez à vérifier l'état opérationnel de votre cluster WildFire et vérifier son bon fonctionnement.

L'exemple suivant présente le progrès de la migration des données dans un cluster d'appareils WildFire :

```
admin@WF-500(active-controller)> : afficher l'état de migration des
 données terminé à 100 % le lundi 9 septembre 21:44:48 PDT 2019
```

STEP 5 | Sur les nœuds actifs, passifs et de serveur d'un appareil WildFire, exécutez :

admin@WF-500(active-controller)>show log systemsubtype direction equal backward

Cette commande affiche tous les événements WildFire journalisés qui ont été classés en tant que sous-type d'appareil WildFire, du plus récent au plus ancien.

- Vous devez entrer cette commande pour tous les nœuds d'un cluster. Par exemple, si vous utilisez un cluster à trois nœuds, vous devez vérifier l'état sur le contrôleur actif, sur le contrôleur passif et sur le nœud du serveur.
- Les messages journaux que renvoie la CLI de l'appareil WildFire peuvent comprendre de nombreux sous-types. Vous pouvez filtrer les journaux en fonction d'un mot-clé commun relatif au sous-type. Utilisez l'argument de commande suivant pour filtrer les journaux en fonction d'une composante donnée :
  - global-queue : **matchqueue**, par exemple **show log system directionequal backward | match queue**
  - global-database : **match global**, par exemple **show log system direction equal backward | matchglobal**

- signature-generation : **`match signature`**, par exemple **`show log system direction equal backward| match signature`**

- Les clusters d’appareils WildFire qui fonctionnent normalement renvoient les états suivants pour chaque nœud d’un cluster à deux nœuds. Les nœuds WildFire qui fonctionnent bien renvoient des états différents, selon le rôle d’un appareil.

  Utilisez la liste de contrôle suivante pour vérifier que les services de l’appareil WildFire fonctionnent correctement dans votre déploiement de cluster.

  - **Contrôleur actif**

Composant	État du contrôleur actif
`global-queue`	❑ `infowildfire cluster 0 Global queue (rabbitmq) cluster formation succeeded withstatus ReadyLeader` ❑ `info general general 0 Setup policy for global-queue service`
`global-database`	❑ `infogeneral general 0 I’m cluster leader, bootstrap for global-db service` ❑ `info general general 0 Setup policy for global-queue service`
`signature-generation`	❑ `infowildfir cluster 0 Signature generation service status set to ReadyMaster` ❑ `info wildfir cluster 0 Signature generationservice status set to ReadyMaster`

*Les messages journaux renvoyés par les appareils WildFire sont affichés du plus récent au plus ancien. Si vous n’utilisez pas l’argument de commande **`direction equal backward`** comme il est indiqué dans la procédure ci-dessus, la CLI de l’appareil WildFire renvoie les messages journaux dans l’ordre du plus ancien au plus récent.*

  - **Contrôleur passif**

Composant	Exemple d’état du contrôleur passif
`global-queue`	❑ `infogeneral general 0 Setup policy for global-queue service` ❑ `info wildfire cluster 0 Global queue (rabbitmq)cluster formation succeeded with status JoinedCluster` ❑ `info general general 0 Join cluster for global-queueservice - succeeded`

Composant	Exemple d’état du contrôleur passif
	❑ info general general 0 Setup policy for global-queue service
global-database	❑ infogeneral general 0 Setup policy for global-queue service ❑ info general general 0 Restore applications:done, For global-db bootstrap and join cluster ❑ info general general 0 Start vm_mgr, For global-dbbootstrap and join cluster ❑ info general general 0 Start uwsgi, For global-dbbootstrap and join cluster ❑ info general general 0 Start wf_services, Forglobal-db bootstrap and join cluster ❑ info general general 0 Suspend applications:done, For global-db bootstrap and join cluster ❑ info general general 0 Stop vm_mgr, For global-dbbootstrap and join cluster ❑ info general general 0 Stop uwsgi, For global-dbbootstrap and join cluster ❑ info general general 0 Stop wf_services, Forglobal-db bootstrap and join cluster ❑ info general general 0 Bootstrap and join clusterfor global-db service
signature-generation	❑ infowildfir cluster 0 Signature generation service status set to ReadySlave ❑ info wildfir cluster 0 Signature generationservice status set to ReadySlave

Les messages journaux renvoyés par les appareils WildFire sont affichés du plus récent au plus ancien. Si vous n’utilisez pas l’argument de commande ***direction equal backward*** *comme il est indiqué dans la procédure ci-dessus, la CLI de l’appareil WildFire renvoie les messages journaux dans l’ordre du plus ancien au plus récent.*

- Les clusters d’appareils WildFire qui fonctionnent normalement renvoient les états suivants pour chaque nœud d’un cluster à trois nœuds. Les nœuds WildFire qui fonctionnent bien renvoient des états différents, selon le rôle d’un appareil.

  Utilisez la liste de contrôle suivante pour vérifier que les services de l’appareil WildFire fonctionnent correctement dans votre déploiement de cluster.

  - **Contrôleur actif**

Composant	État du contrôleur actif
`global-queue`	❑ `infowildfire cluster 0 Global queue (rabbitmq) cluster formation succeeded withstatus JoinedCluster` ❑ `info general general 0 Join cluster for global-queueservice - succeeded` ❑ `info general general 0 Setup policy for global-queue service`
`global-database`	❑ `infogeneral general 0 Restore applications: done, For global-db bootstrap andjoin cluster` ❑ `info general general 0 Start vm_mgr, For global-dbbootstrap and join cluster` ❑ `info general general 0 Start uwsgi, For global-dbbootstrap and join cluster` ❑ `info general general 0 Start wf_services, Forglobal-db bootstrap and join cluster` ❑ `info general general 0 Suspend applications:done, For global-db bootstrap and join cluster` ❑ `info general general 0 Stop vm_mgr, For global-dbbootstrap and join cluster` ❑ `info general general 0 Stop uwsgi, For global-dbbootstrap and join cluster` ❑ `info general general 0 Stop wf_services, Forglobal-db bootstrap and join cluster` ❑ `2019/07/19 14:40:19 info general general 0Bootstrap and join cluster for global-db service`
`signature-generation`	❑ `infowildfire cluster 0 Signature generation service status set to ReadyMaster`

Composant	État du contrôleur actif

Les messages journaux renvoyés par les appareils WildFire sont affichés du plus récent au plus ancien. Si vous n'utilisez pas l'argument de commande ***direction equal backward*** *comme il est indiqué dans la procédure ci-dessus, la CLI de l'appareil WildFire renvoie les messages journaux dans l'ordre du plus ancien au plus récent.*

- **Contrôleur passif**

Composant	État du contrôleur passif
global-queue	❑ infogeneral general 0 Setup policy for global-queue service ❑ info general general 0 Setup policy for global-queue service ❑ info wildfire cluster 0 Global queue (rabbitmq)cluster formation succeeded with status ReadyLeader ❑ info general general 0 Setup policy for global-queue service
global-database	❑ infogeneral general 0 I'm cluster leader, bootstrap for global-db service ❑ info general general 0 Setup policy for global-queue service
signature-generation	❑ infowildfire cluster 0 Signature generation service status set to ReadySlave ❑ info wildfire cluster 0 Signature generationservice status set to ReadySlave

Les messages journaux renvoyés par les appareils WildFire sont affichés du plus récent au plus ancien. Si vous n'utilisez pas l'argument de commande ***direction equal backward*** *comme il est indiqué dans la procédure ci-dessus, la CLI de l'appareil WildFire renvoie les messages journaux dans l'ordre du plus ancien au plus récent.*

- **Nœud serveur**

Composant	État du nœud serveur
global-queue	❑ infowildfire cluster 0 Global queue (rabbitmq) cluster formation succeeded withstatus JoinedCluster

Composant	État du nœud serveur
	❑ info general general 0 Join cluster for global-queueservice - succeeded ❑ info general general 0 Setup policy for global-queue service ❑ info wildfire cluster 0 Global queue (rabbitmq)cluster formation succeeded with status StandbyAsWorker
global-database	❑ infogeneral general 0 Restore applications: done, For global-db bootstrap andjoin cluster ❑ info general general 0 Start vm_mgr, For global-dbbootstrap and join cluster ❑ info general general 0 Start uwsgi, For global-dbbootstrap and join cluster ❑ info general general 0 Start wf_services, Forglobal-db bootstrap and join cluster ❑ info general general 0 Suspend applications:done, For global-db bootstrap and join cluster ❑ info general general 0 Stop vm_mgr, For global-dbbootstrap and join cluster ❑ info general general 0 Stop uwsgi, For global-dbbootstrap and join cluster ❑ info general general 0 Stop wf_services, Forglobal-db bootstrap and join cluster ❑ 2019/07/19 14:32:50 info general general 0Promote worker node and join cluster for global-db service
signature-generation	❑ infowildfire cluster 0 Signature generation service status set to Stopped ❑ critical wildfire cluster 0 Signature DataMigrationDone

Les messages journaux renvoyés par les appareils WildFire sont affichés du plus récent au plus ancien. Si vous n'utilisez pas l'argument de commande ***direction equal backward*** *comme il est indiqué dans la procédure ci-dessus, la CLI de l'appareil WildFire renvoie les messages journaux dans l'ordre du plus ancien au plus récent.*

États des applications Wildfire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

L’appareil WildFire exploite une série d’applications internes liées à la gestion et à la coordination du traitement des données d’échantillons. Ces applications et leurs états requis sont indiqués lorsque vous affichez l’état d’un cluster d'appareils WildFire.

La liste suivante indique les composantes du cluster, leur objectif ainsi que les conditions d’état :

Name (Nom)	Description	Conditions d’état possibles	Definition
global-db-service	Cette base de données d'application est utilisée pour stocker les données d’analyse WildFire.	AcquiringSessionSpinLock	Attendre le verrouillage total de l'UCT de session jusqu’à obtention du verrou ou du délai.
		Bootstrapping	L’application de base de données échantillon est actuellement en mode autoamorçage.
		BootstrappingNoMeet	Le service de base de données échantillon local a commencé à fonctionner sans former de cluster avec d’autres appareils WildFire.
		FailedToBecomeWorker	N’a pas réussi à joindre le cluster en tant que nœud esclave.
		FailedToBootstrap	Le processus d'autoamorçage a échoué.
		FailedToJoinCluster	N’a pas réussi à joindre le cluster.
		FailedToStartServices	Les services de base de données internes n’ont pas réussi à démarrer.
		MaintenanceDecommission	Lancement du processus de mise hors service des services de base de données.

Name (Nom)	Description	Conditions d’état possibles	Definition
		MaintenanceDecommissionDone	Le service de base de données a été mis hors service.
		MaintenanceFailover	Lancement du processus visant à rétrograder le service local et à forcer le basculement d’une réplique du nœud de sauvegarde.
		MaintenanceFailed	Échec du basculement de service.
		MaintenanceFailoverDone	Basculement de service terminé.
		MaintenanceRecoverFromSplitbrain	Si l'appareil WildFire est actuellement en mode split-brain, l'état du service de base de données sera défini sur MaintenanceRecoverFromSplitbrain au démarrage du service.
		MaintenanceSuspend	Le service de base de données est sur le point d’être suspendu parce que l’utilisateur a déclenché l’une des commandes suivantes : debug cluster suspend ou request cluster decommission.
		MaintenanceSuspendDone	Le service de base de données a terminé le processus de suspension.
		DataMigration	Les contenus de la base de données locale sont en cours de fusion avec la base de données principale. Une telle migration se produit lorsqu’un appareil WildFire se joint à un cluster.
		DataMigrationDone	Le processus de migration des données est terminé.

Name (Nom)	Description	Conditions d’état possibles	Definition
		DataMigrationFailed	Le processus de migration des données a échoué.
		JoinedCluster	Le service de base de données local s’est joint au cluster.
		Ready	Le service de base de données est en mode prêt.
		ReadyLeader	Le service de base de données est en mode prêt, et l’appareil est configuré en tant que leader.
		ReadyStandalone	Le service de base de données est en mode prêt, et l’appareil fonctionne en tant qu’appareil autonome.
		Splitbrain	Une situation de « split brain » a été détectée, et les services de base de données sont entrés en mode « split brain ». Le service passera en mode ReadyStandalone sous peu.
		StandbyAsWorker	Le service de base de données du nœud esclave est en mode veille.
		WaitingforLeaderReady	Le nœud local est en attente pour joindre le nœud leader.

Name (Nom)	Description	Conditions d’état possibles	Definition
global-queue-service	Gère la gestion et l’établissement de la priorité des échantillons envoyés pour analyse WildFire.	Bootstrapping	L’application du service de file d’attente est actuellement en mode autoamorçage.
		FailedToBecomeWorker	N’a pas réussi à joindre le cluster en tant que nœud esclave.
		FailedToBootstrap	Le processus d'autoamorçage a échoué.

Name (Nom)	Description	Conditions d’état possibles	Definition
		FailedToJoinCluster	N’a pas réussi à joindre le cluster.
		FailedToStartServices	Les services de file d’attente internes n’ont pas réussi à démarrer.
		MaintenanceDecommission	Lancement du processus de mise hors service des services de file d'attente.
		MaintenanceDecommissionDone	Le service de file d’attente a été mis hors service.
		MaintenanceFailover	Lancement du processus visant à rétrograder le service local et à forcer le basculement d’une réplique du nœud de sauvegarde.
		MaintenanceFailed	Échec du basculement de service.
		MaintenanceFailoverDone	Basculement de service terminé.
		MaintenanceRecoverFromSplitbrain	Si l’appareil WildFire se trouve actuellement en mode « split brain », l’état du service de file d’attente sera défini sur
		MaintenanceSuspend	Le service de file d’attente est sur le point d’être suspendu parce que l’utilisateur a déclenché l’une des commandes suivantes : debug cluster suspend ou request cluster decommission.
		MaintenanceSuspendDone	Le service de file d'attente a terminé le processus de suspension.
		JoinedCluster	Le service de file d’attente s’est joint au cluster.

Name (Nom)	Description	Conditions d’état possibles	Definition
		Ready	Le service de file d’attente est en mode prêt.
		ReadyLeader	Le service de file d’attente est en mode prêt, et l’appareil est configuré en tant que leader.
		ReadyStandalone	Le service de file d'attente est en mode prêt, et l’appareil fonctionne en tant qu’appareil autonome.
		Splitbrain	Une situation de « split brain » a été détectée, et les services de file d’attente sont entrés en mode « split brain ». Le service passera en mode ReadyStandalone sous peu.
		StandbyAsWorker	Le service de file d’attente du nœud esclave est en mode veille.

Name (Nom)	Description	Conditions d’état possibles	Definition
siggen-db	Génère les signatures privées de WildFire et les échantillons à analyser.	DatabaseFailover	Lorsqu’un basculement HA se produit, le contrôleur passif devient le contrôleur actif. Le service de signature du contrôleur passif devient le service principal et l’état est défini sur DatabaseFailover.
		DatabaseFailoverFaild	Échec du basculement de la base de données de signatures.
		DataMigration	Les contenus de la base de données de signatures locale sont en cours de fusion avec la base de données principale. Une telle migration se produit lorsqu’un appareil WildFire se joint à un cluster.

Name (Nom)	Description	Conditions d’état possibles	Definition
		DataMigrationDone	Le processus de migration des données est terminé.
		DataMigrationFailed	Le processus de migration des données a échoué.
		Deregistered	Le service de base de données de signatures a été révoqué.
		MaintenanceDecommission	Lancement du processus de mise hors service des services de base de données de signatures.
		MaintenanceDecommissionDone	Le service de file d’attente a été mis hors service.
		MaintenanceFailover	Lancement du processus visant à rétrograder le service local et à forcer le basculement d’une réplique du nœud de sauvegarde.
		MaintenanceFailoverDone	Basculement de service terminé.
		MaintenanceSuspend	Le service de base de données de signatures est sur le point d’être suspendu parce que l’utilisateur a déclenché l’une des commandes suivantes : debug cluster suspend ou request cluster decommission.
		MaintenanceSuspendDone	Le service de base de données de signatures a terminé le processus de suspension.
		MigrateMalwareDatabase	Lors de la mise à niveau de PAN-OS 7.1 vers 8.0, les données d’échantillons sont converties à un autre format. Ces états indiquent la progression du processus de migration de données.
		MigrateSiggenDatabaseStage1	
		MigrateSiggenDatabaseStage2	
		MigrateSiggenDatabaseStage3	

Name (Nom)	Description	Conditions d’état possibles	Definition
		Ready	Le service de base de données de signatures est en mode prêt.
		ReadyMaster	Le service de base de données de signatures est en mode principal et il s’exécute sur le contrôleur actif.
		ReadySlave	Le service de base de données de signatures est en mode sauvergarde et il s’exécute sur le contrôleur passif.
		ReadyStandalone	Le service de base de données de signatures est en mode prêt, et l’appareil fonctionne en tant qu’appareil autonome.
		Splitbrain	Une situation de « split brain » a été détectée, et le service de base de données de signatures est entré en mode « split brain ». Le service passera en mode ReadyStandalone sous peu.
		Stopped	Le service de base de données de signatures a cessé sur l’appareil.

Name (Nom)	Description	Conditions d’état possibles	Definition
wildfire-management-service	Service de gestion du mode de fonctionnement de WildFire.	Running	Le service de gestion de WildFire est en mode opérationnel.
		Done	L’exécution du service de gestion de WildFire est terminée.

Name (Nom)	Description	Conditions d’état possibles	Definition
wildfire-apps-service	Applications de l’infrastructure de WildFire.	Deregistered	Le service d’applications WildFire a été révoqué.

Name (Nom)	Description	Conditions d’état possibles	Definition
		Ready	Le service d’applications WildFire est en mode prêt.
		Restored	Le service d’applications WildFire a terminé les procédures de maintenance.
		Scheduling	Le service d’applications WildFire est en mode planification.
		SetupSampleStorage	Le service d’applications WildFire fonctionne lors de la mise à niveau de WildFire (version 7.1 à 8.0).
		Stopped	Le service d’applications WildFire a cessé sur l’appareil.
		Suspended	Le service d’applications WildFire a été suspendu en raison de la maintenance.

États de service Wildfire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

L’appareil WildFire exploite une série de services internes liés à la gestion et à la coordination du traitement des données d’échantillons. Ces services et leurs états requis sont indiqués lorsque vous affichez l’état d’un cluster d'appareils WildFire.

La liste suivante présente les composantes de service Wildfire, leurs descriptions, leurs conditions d’état et leurs autres détails pertinents :

Name (Nom)	Objectif	Nœuds touchés	État
`infra`	Indique qu’un service d’infrastructure d’un cluster WildFire est actif sur un nœud donné.	Tous les nœuds	S’affiche à l’écran de l’état de la CLI lorsque le service est actif. Si ces services ne sont pas présents pour un

Name (Nom)	Objectif	Nœuds touchés	État
wfpc	Indique que le service d’analyse de fichiers échantillons (cloud WildFire privé) peut effectuer l’analyse des fichiers et générer les rapports.		nœud donné, vérifiez la configuration de l’appareil.
Signature	Génère les signatures privées de WildFire et les échantillons à analyser.	Contrôleur actif (principal) / passif (de secours)	
wfcore	Indique que le nœud agit en tant que serveur pour les services d’infrastructure du cluster WildFire.	Nœud serveur	

Mise à jour d’appareils WildFire appartenant à un cluster

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Vous pouvez utiliser la CLI pour mettre individuellement à niveau des appareils WildFire inscrits dans un cluster ou utiliser Panorama pour mettre à niveau le cluster en tant que groupe.

La durée nécessaire pour la mise à niveau du logiciel de l’appareil variera selon le nombre d’échantillons que l’appareil WildFire a analysés et stockés, car la mise à niveau entraîne la migration de tous les échantillons malveillants et des échantillons bénins des 14 derniers jours. Allouez 30 à 60 minutes pour chaque appareil WildFire que vous avez utilisé dans un environnement de production.

- *Tous les nœuds d’un cluster doivent utiliser la même version du système d’exploitation.*
- *Panorama peut gérer des appareils et des clusters d’appareils WildFire qui utilisent PAN-OS 8.0.1 ou toute version ultérieure.*
- *Assurez-vous que les périphériques sont branchés à une source d’alimentation fiable. La perte de puissance au cours d’une mise à niveau peut rendre les périphériques inutilisables.*

Selon votre déploiement, exécutez l’une des tâches suivantes pour mettre à niveau votre cluster WildFire :

- 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
- Mise à niveau locale d’un cluster à partir d’une connexion Internet
- Mise à niveau locale d’un cluster sans connexion Internet

Mise à niveau locale d’un cluster à partir d’une connexion Internet

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Pour mettre un cluster à niveau localement, vous devez individuellement mettre à niveau chaque appareil WildFire inscrit dans le cluster. Lorsqu’un appareil est mis à niveau, il se réinscrit automatiquement au cluster auquel il était initialement affecté.

STEP 1 | 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 :

```
admin@WF-500 (contrôleur passif)> afficher les derniers
 échantillons de wildfire
```

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 2 | Installez la dernière mise à jour de contenu pour l'appareil WildFire. Grâce à cette mise à jour, l'appareil dispose des renseignements sur les menaces les plus récentes, ce qui lui permet de détecter avec précision les logiciels malveillants.

Ce processus peut prendre 6 heures ou plus sur les appareils plus anciens.

1. Vérifiez que vous exécutez la dernière mise à jour du contenu sur votre appareil WildFire.

```
admin@WF-500> demande de mise à niveau du contenu wf
```

2. Téléchargez le dernier package de mise à jour du contenu WildFire.

```
admin@WF-500> demander la mise à niveau wf-content télécharger la
 plus récente
```

   Si vous n'êtes pas connecté directement au serveur de mises à jour Palo Alto Networks, vous pouvez procéder au téléchargement et à l'installation des mises à jour de contenu WildFire à partir d'un serveur SCP.
3. Affichez l'état du téléchargement.

```
admin@WF-500> afficher tous les emplois
```

4. Une fois le téléchargement terminé, installez la mise à jour.

```
admin@WF-500> demander la mise à niveau wf-content installer la
 dernière version
```


STEP 3 | (Requis lors de la mise à niveau vers PAN-OS 10.2.2) Mettez à niveau les images VM sur l'appareil WildFire.

1. Connectez-vous et accédez à la page de téléchargement de logiciels du portail de support client de Palo Alto Networks. Vous pouvez également accéder manuellement à la page de téléchargement de logiciels à partir de la page d'accueil du support en accédant à **Updates (Mises à jour)** > **Software Updates (Mises à jour logicielles)**.

2. Sur la page des mises à jour logicielles, sélectionnez **WF-500 Guest VM Images (Images de VM invitée WF-500)** et téléchargez les fichiers d'image VM suivantes :

   Palo Alto Networks met régulièrement à jour les fichiers d'image VM. Par conséquent, le nom de fichier précis dépend de la version disponible. Assurez-vous de télécharger la dernière version, où la partie m-x.x.x dans le nom de fichier indique le numéro de version. En outre, vous pouvez vous aider de la date de publication pour déterminer la dernière version.

   - WFWinXpAddon3_m-1.0.1.xpaddon3
   - WFWinXpGf_m-1.0.1.xpgf
   - WFWin7_64Addon1_m-1.0.1.7_64addon1
   - WFWin10Base_m-1.0.1.10base
3. Chargez les images VM sur l'appareil WildFire.
   1. Importez l'image VM à partir du serveur SCP :

      ```
      admin@WF-500>scp import wildfire-vm-image from
       <username@ip_address>/<folder_name>/<vm_image_filename>
      ```

      Par exemple :

      ```
      admin@WF-500>scp import wildfire-vm-image from
       user1@10.0.3.4:/tmp/WFWin7_64Addon1_m-1.0.1.7_64addon1
      ```

   2. Pour vérifier l'état du téléchargement, utilisez la commande suivante :

      ```
      admin@WF-500>show jobs all
      ```

   3. Répétez l'opération pour les images VM restantes.
4. Installez l'image VM.
   1. ```
      admin@WF-500>request system wildfire-vm-image upgrade
       install file <vm_image_filename>
      ```
   2. Répétez l'opération pour les images VM restantes.
5. Vérifiez que les images VM ont été correctement installées et activées sur l'appareil WildFire.
   1. (Facultatif) Affichez la liste des images VM disponibles :

      ```
      admin@WF-500> show wildfire vm-images
      ```

      La sortie affiche les images VM disponibles.
   2. Validez la configuration :

      ```
      admin@WF-500# commit
      ```


      ```

3. Affichez l’image VM active en exécutant la commande suivante :

```
admin@WF-500> show wildfire status
```

STEP 4 | Vérifiez que la version du logiciel de l'appareil WildFire que vous souhaitez installer est disponible.

```
admin@WF-500 (contrôleur passif)> demande de vérification du
 logiciel système
```

STEP 5 | Téléchargez la version PAN-OS 10.2.2 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. Les exemples présentés dans cette procédure indiquent comment passer à la version PAN-OS 10.2.2. Remplacez 10.2.2 par la version visée par la mise à niveau.

Téléchargez la version 10.2.2 du logiciel.

```
admin@WF-500(passive-controller)> request system software download
 version 10.2.2
```

Pour vérifier l'état du téléchargement, utilisez la commande suivante :

```
admin@WF-500 (contrôleur passif)> afficher tous les travaux
```

STEP 6 | Confirmez que tous les services fonctionnent.

```
admin@WF-500(passive-controller)> show system software status
```

STEP 7 | Installez la version 10.2.2 du logiciel.

```
admin@WF-500(passive-controller)> request system software install
 version 10.2
```

STEP 8 | Terminez la mise à niveau du logiciel.

1. 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)> afficher tous les travaux
 mis en file d'attente retirés de la file d'attente Type
 d'ID État Résultat Terminé ----------------------------
 ------------------------ 14:53:15 14:53:15 5 Installer FIN OK
 14:53:19
```


2. Redémarrez l’appareil en douceur :

```
admin@WF-500 (contrôleur passif)> demande de redémarrage du
 cluster-nœud-local
```

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.

STEP 9 | Répétez les étapes 1 à 8 pour chaque nœud esclave WildFire du cluster.

STEP 10 | (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)> afficher les tâches en attente du
 cluster
```

STEP 11 | Vérifiez que l’appareil WildFire est prêt à reprendre l’analyse des échantillons.

1. Vérifiez que le champ sw-version affiche la version mise à niveau :

```
admin@WF-500 (contrôleur passif)> afficher les informations
 système | correspondre à la version logiciel
```

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 (contrôleur passif)> afficher tous les travaux
```

4. Confirmez que la migration des données a été effectuée avec succès. Exécutez la commande `show cluster data-migration-status` pour afficher le progrès de la fusion des bases de données. Une fois la fusion des données terminée, l’horodatage d’achèvement indique :

```
100 % terminé le lundi 9 septembre 21:44:48 PDT 2019
```

La durée d’une fusion de données dépend de la quantité de données stockées sur l’appareil WildFire. Allouez plusieurs heures à la récupération, car le processus de fusion de données peut durer très longtemps.

Mise à niveau locale d’un cluster sans connexion Internet

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Pour mettre un cluster à niveau localement, vous devez individuellement mettre à niveau chaque appareil WildFire inscrit dans le cluster. Lorsqu'un appareil est mis à niveau, il se réinscrit automatiquement au cluster auquel il était initialement affecté.

STEP 1 | 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 :

```
admin@WF-500 (contrôleur passif)> afficher les derniers
 échantillons de wildfire
```

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 2 | Récupérez le fichier de mise à jour du contenu sur le serveur de mises à jour.

1. Connectez-vous au portail de support Palo Alto Networks et cliquez sur **Dynamic Updates (Mises à jour dynamiques)**.
2. Dans la section WildFire Appliance (Appareil WildFire), cherchez la dernière mise à jour du contenu de l'appareil WildFire et téléchargez-la.
3. Copiez le fichier de mise à jour du contenu sur un serveur SCP et notez le nom du fichier et le chemin d'accès au répertoire.

STEP 3 | Installez la mise à jour du contenu sur l'appareil WildFire.

1. Connectez-vous à l'appareil WildFire et téléchargez le fichier de mise à jour du contenu à partir du serveur SCP :

   ```
   admin@WF-500> scp importer du wf-content depuis
    username@host:path
   ```

   Par exemple :

   ```
   admin@WF-500> scp importer du wf-content depuis
    bart@10.10.10.5:c:/updates/panup-all-wfmeta-2-253.tgz
   ```

   *Si votre serveur SCP est exécuté sur un port non standard ou si vous devez spécifiez l'adresse IP source, vous pouvez également définir ces options dans la commande **scp import**.*

2. Installez la mise à jour :

   ```
   admin@WF-500> demander un fichier d’installation de mise à
    niveau wf-content panup-all-wfmeta-2-253.tgz
   ```

3. Affichez le statut de l’installation :

   ```
   admin@WF-500> afficher tous les emplois
   ```

STEP 4 | Vérifiez la mise à jour du contenu.

Vérifiez la version du contenu :

```
admin@WF-500> Afficher les informations système | correspondre à
 wf-content-version
```

Le résultat suivant indique la version 2-253 :

```
wf-content-version: 2-253
```

STEP 5 | (Requis lors de la mise à niveau vers PAN-OS 10.2.2) Mettez à niveau les images VM sur l’appareil WildFire.

1. Connectez-vous et accédez à la page de téléchargement de logiciels du portail de support client de Palo Alto Networks. Vous pouvez également accéder manuellement à la page de téléchargement de logiciels à partir de la page d’accueil du support en accédant à **Updates (Mises à jour)** > **Software Updates (Mises à jour logicielles)**.

2. Sur la page des mises à jour logicielles, sélectionnez **WF-500 Guest VM Images (Images de VM invitée WF-500)** et téléchargez les fichiers d'image VM suivantes :

   Palo Alto Networks met régulièrement à jour les fichiers d'image VM. Par conséquent, le nom de fichier précis dépend de la version disponible. Assurez-vous de télécharger la dernière version, où la partie m-x.x.x dans le nom de fichier indique le numéro de version. En outre, vous pouvez vous aider de la date de publication pour déterminer la dernière version.

   - WFWinXpAddon3_m-1.0.1.xpaddon3
   - WFWinXpGf_m-1.0.1.xpgf
   - WFWin7_64Addon1_m-1.0.1.7_64addon1
   - WFWin10Base_m-1.0.1.10base
3. Chargez les images VM sur l'appareil WildFire.
   1. Importez l'image VM à partir du serveur SCP :

      ```
      admin@WF-500>scp import wildfire-vm-image from
       <username@ip_address>/<folder_name>/<vm_image_filename>
      ```

      Par exemple :

      ```
      admin@WF-500>scp import wildfire-vm-image from
       user1@10.0.3.4:/tmp/WFWin7_64Addon1_m-1.0.1.7_64addon1
      ```

   2. Pour vérifier l'état du téléchargement, utilisez la commande suivante :

      ```
      admin@WF-500>show jobs all
      ```

   3. Répétez l'opération pour les images VM restantes.
4. Installez l'image VM.
   1. ```
      admin@WF-500>request system wildfire-vm-image upgrade
       install file <vm_image_filename>
      ```

   2. Répétez l'opération pour les images VM restantes.
5. Vérifiez que les images VM ont été correctement installées et activées sur l'appareil WildFire.
   1. (Facultatif) Affichez la liste des images VM disponibles :

      ```
      admin@WF-500> show wildfire vm-images
      ```

      La sortie affiche les images VM disponibles.
   2. Validez la configuration :

      ```
      admin@WF-500# commit
      ```


      ```

3. Affichez les images VM actives en exécutant la commande suivante :

```
admin@WF-500> show wildfire status
```

STEP 6 | Vérifiez que la version du logiciel de l'appareil WildFire que vous souhaitez installer est disponible.

```
admin@WF-500 (contrôleur passif)> demande de vérification du
 logiciel système
```

STEP 7 | Téléchargez la version PAN-OS 10.2.2 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. Les exemples présentés dans cette procédure indiquent comment passer à la version PAN-OS 10.2.2. Remplacez 10.2.2 par la version visée par la mise à niveau.

Téléchargez la version 10.2.2 du logiciel :

1. Accédez au site de support de PaloAltoNetworks et, dans la section Tools (Outils), cliquez sur **Software Updates (Mises à jour logicielles)**.
2. Téléchargez le fichier image du logiciel de l'appareil WildFire à installer sur un ordinateur exécutant le logiciel du serveur SCP.
3. Importez l'image du logiciel depuis le serveur SCP.

```
admin@WF-500> logiciel d'importation scp à partir de
 <username@ip_address>/<folder_name>/<imagefile_name>
```

Par exemple :

```
admin@WF-500> scp import software from user1@10.0.3.4:/tmp/
WildFire_m-10.2.2
```

4. Pour vérifier l'état du téléchargement, utilisez la commande suivante :

```
admin@WF-500> afficher tous les emplois
```

STEP 8 | Confirmez que tous les services fonctionnent.

```
admin@WF-500(passive-controller)> show system software status
```

STEP 9 | Installez la version 10.2.2 du logiciel.

```
admin@WF-500(passive-controller)> request system software install
 version 10.2.2
```


STEP 10 | Terminez la mise à niveau du logiciel.

1. 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)> afficher tous les travaux
 mis en file d'attente retirés de la file d'attente Type
 d'ID État Résultat Terminé ----------------------------
 ------------------------ 14:53:15 14:53:15 5 Installer FIN OK
 14:53:19
```

2. Redémarrez l'appareil en douceur :

```
admin@WF-500 (contrôleur passif)> demande de redémarrage du
 cluster-nœud-local
```

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.

STEP 11 | Répétez les étapes 1 à 10 pour chaque nœud esclave WildFire du cluster.

STEP 12 | (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)> afficher les tâches en attente du
 cluster
```


STEP 13 | Vérifiez que l’appareil WildFire est prêt à reprendre l’analyse des échantillons.

1. Vérifiez que le champ sw-version affiche la version mise à niveau :

   ```
   admin@WF-500 (contrôleur passif)> afficher les informations
    système | correspondre à la version logiciel
   ```

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 (contrôleur passif)> afficher tous les travaux
   ```

4. Confirmez que la migration des données a été effectuée avec succès. Exécutez la commande `show cluster data-migration-status` pour afficher le progrès de la fusion des bases de données. Une fois la fusion des données terminée, l’horodatage d’achèvement indique :

   ```
   100 % terminé le lundi 9 septembre 21:44:48 PDT 2019
   ```

   La durée d’une fusion de données dépend de la quantité de données stockées sur l’appareil WildFire. Allouez plusieurs heures à la récupération, car le processus de fusion de données peut durer très longtemps.

Dépannage d’un cluster d’appareils WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Consultez les rubriques suivantes pour diagnostiquer et dépanner les problèmes liés aux clusters d’appareils WildFire :

- Dépannage des situations de « split brain » WildFire

Dépannage des situations de « split brain » WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Un cluster High Availability (haute disponibilité ; HA) d’appareils WildFire à deux nœuds subit une situation de « split brain » lorsque l’un des nœuds (ou les deux homologues HA) croit que l'autre ne fonctionne plus. Cette situation se produit lorsque des problèmes de configuration ou de connectivité réseau entraîne l’échec des connexions HA et du cluster, mais que les appareils continuent à pouvoir traiter les échantillons. Dans une telle situation, les deux appareils WildFire prennent le rôle de contrôleur actif (ou principal) sans secours, ce qui annule les avantages d’un déploiement HA, comme la redondance et l’équilibrage de charge. De plus, les appareils WildFire n'arrivent plus à utiliser efficacement les ressources d’analyse. Lorsqu’ils subissent une interruption mineure, les clusters WildFire tentent automatiquement de récupérer des situations de « split brain ». Des événements plus graves exigeront une intervention manuelle.

Lorsque surgit une situation de « split brain », les conditions suivantes s’appliquent :

- Aucun des homologues WildFire n'est au courant de l’état ni du rôle HA de l’autre homologue.
- Les deux homologues WildFire deviennent le serveur principal et continuent à recevoir des échantillons des pare-feu ; ils fonctionnent toutefois de manière indépendante.
- Les tâches liées au cluster sont suspendues lorsque la HA n’est pas disponible.

Lorsqu’ils sont bien configurés, les clusters d'appareils WildFire à trois nœuds ne devraient pas subir de situations de « split brain » en raison de la redondance supplémentaire offerte par le troisième nœud de serveur.

Quelle est la cause d’une situation de « split brain » ?

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Une situation de « split brain » est un correctif apporté lors de l'échec d'un seul nœud d'un cluster à deux noeuds, dans lequel les homologues de la paire haute disponibilité d'appareils WildFire n'arrivent plus à communiquer entre eux, tout en continuant de fournir des fonctionnalités restreintes. Bien que la haute disponibilité et l'équilibrage de charge ne soient plus disponibles, vous pouvez continuer à transférer des échantillons à WildFire pour qu'il les analyse. Une situation de « split brain » s'explique par l'une des causes suivantes :

- Problèmes matériels ou panne de courant.
- Problèmes de connectivité réseau, comme l'échec d'un routeur ou d'un commutateur, le battement du réseau ou une partition du réseau.
- Problèmes de connectivité ou de configuration de l'appareil WildFire.

  Palo Alto Networks recommande d'utiliser une connexion directe au moyen d'un câble pour la liaison des interfaces du cluster et HA.
- Nœud WildFire qui ne fonctionne pas correctement.

Déterminer si un cluster WildFire se trouve dans une situation de « split brain »

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Lorsque les appareils d'un cluster WildFire à deux nœuds entrent dans une situation de « split brain », l'échec ou les échecs de service génèrent des avertissements dans la CLI de WildFire et dans l'appareil Panorama de gestion (le cas échéant).

STEP 1 | (CLI de l'appareil WildFire uniquement) Sur un contrôleur d'un appareil WildFire, exécutez la commande suivante :

```
admin@WF-500>afficher l'appartenance aucluster
```

Le noeud du cluster WildFire touché affiche `Cluster:splitbrain` à côté de `Service Summary`.

L'exemple suivant présente un nœud d'un cluster WildFire à deux nœuds qui se trouve dans une situation de « split brain » :

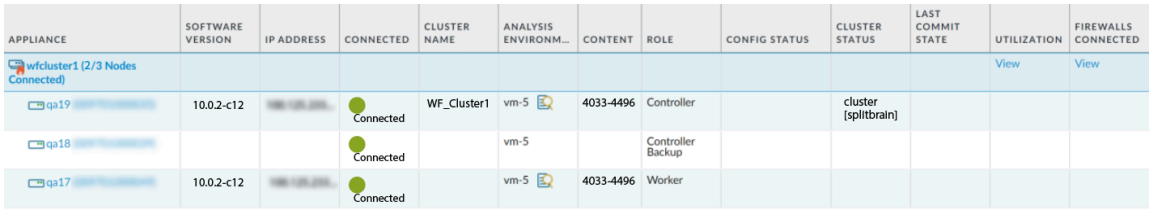
```
Résumé du service : Cluster:splitbrain Nom du cluster : adresse
 WF_Cluster_1 : 2.2.2.114 Nom d'hôte : wf1 Nom du nœud :
 wfpc-009707000380-interne Numéro de série : 009707000380 Mode
 nœud : rôle serveur du contrôleur : Véritable priorité HA :
 secondaire Dernière modification : Tue, 24 Oct 2017 15:13:18
 -0700 Services: wfcore signature wfpc infra État du moniteur:
 État d'intégrité du serf: passage de l'agent vivant et accessible
 Vérification de l'infrastructure du service: réussi Etat de
 l'application: global-db-service: ReadyLeader wildfire-apps-
service: global-queue-service prêt: ReadyLeader wildfire-
management-service: Terminé siggen-db: État de la file d'attente
 de travail ReadyMaster : exemple d'analyse en file d'attente :
 0 exemple d'analyse en cours d'exécution : 0 exemple de copie
```



```
en file d'attente : 0 exemple de copie en cours d'exécution :
0 Rapport Diag : 2.2.2.114: reported leader '2.2.2.114', age 0.
2.2.2.114: le nœud local a réussi la vérification de santé
```

STEP 2 | (Panorama uniquement) Sur l'appareil Panorama qui gère le cluster WildFire :

1. Sélectionnez **Panorama (Panorama) > Managed WildFire Clusters (Clusters WildFire gérés)**.
2. Dans la colonne **Cluster Status (État du cluster)**, vérifiez la présence de **cluster [splitbrain] (cluster [splitbrain])**. Elle indique que l'appareil est en mode « split brain ».



APPLIANCE	SOFTWARE VERSION	IP ADDRESS	CONNECTED	CLUSTER NAME	ANALYSIS ENVIRONM...	CONTENT	ROLE	CONFIG STATUS	CLUSTER STATUS	LAST COMMIT STATE	UTILIZATION	FIREWALLS CONNECTED
wfcluster1 (2/3 Nodes Connected)											View	View
qa19	10.0.2-c12		Connected	WF_Cluster1	vm-5	4033-4496	Controller		cluster [splitbrain]			
qa18			Connected		vm-5		Controller Backup					
qa17	10.0.2-c12		Connected		vm-5	4033-4496	Worker					

Récupération d'une situation de « split brain »

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Pour résoudre une situation de « split brain », déboguez vos problèmes de réseau, puis restaurez la connectivité entre les homologues WildFire HA. Les clusters d'appareils WildFire tentent automatiquement de récupérer d'une situation de « split brain ». Toutefois, en cas d'échec de ces mesures, vous devez manuellement lancer le processus de récupération.

STEP 1 | Vérifiez que votre réseau fonctionne normalement et que l'appareil WildFire transmet et reçoit le trafic.

1. Activez la possibilité d'envoyer des requêtes ping à une interface de l'appareil WildFire.
   - Activer l'envoi de requêtes ping sur une interface donnée de l'appareil :`setdeviceconfig system <interface_number> service disable-icmp no`
   - Activer l'envoi de requêtes ping sur toutes les interfaces de l'appareil : `setdeviceconfig system service disable-icmp no`
2. Générez du trafic ping d'une interface WildFire vers un périphérique externe. Vérifiez que les valeurs des compteurs de réception et de transmission ont augmenté.

   ```
   ping source <wildfire-interface-ip> host<destination-ip-address>
   ```

STEP 2 | Déterminez quel appareil WildFire n'est pas en santé. Reportez-vous à la section Affichage de l'état du cluster d'appareils WildFire au moyen de la CLI ou Affichage de l'état du cluster d'appareils WildFire au moyen de Panorama pour afficher l'état de l'appareil.

STEP 3 | Redémarrez en douceur le nœud *qui pose problème* au moyen de la commande suivante :

```
request cluster reboot-local-node
```

L’appareil WildFire qui redémarre devrait s’inscrire automatiquement au cluster WildFire pour lequel il a été configuré.

L'autre nœud de contrôle qui se trouve en mode « split brain » doit être en santé.

STEP 4 | Attendez la fin de la migration de données. Exécutez la commande `show cluster data-migration-status` pour afficher le progrès de la fusion des bases de données. Une fois la fusion des données terminée, l’horodatage d’achèvement indique :

```
100 % terminé le lundi 9 septembre 21:44:48 PDT 2019
```

La durée d’une fusion de données dépend de la quantité de données stockées sur l’appareil WildFire. Allouez plusieurs heures à la récupération, car le processus de fusion de données peut durer très longtemps.

STEP 5 | Vérifiez l’état du cluster sur Panorama ou via la CLI de l’appareil WildFire.

Utilisation de la CLI de l’appareil WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Les rubriques suivantes décrivent les commandes de la CLI spécifiques au logiciel de l'appareil WildFire™. Toutes les autres commandes, telles que la configuration des interfaces, la validation de la configuration et la définition des informations système, sont identiques à celles de PAN-OS et sont également affichées dans la hiérarchie. Pour plus d'informations sur les commandes PAN-OS, reportez-vous au Guide de mise en route de la ligne de commande PAN-OS.

- Concepts de la CLI du logiciel de l'appareil WildFire
- Modes des commandes de la CLI de WildFire
- Accès à la CLI de l’appareil WildFire
- Opérations de la CLI de l’appareil WildFire
- Référence des commandes du mode Configuration de l'appareil WildFire
- Référence des commandes du mode Opérationnel de l'appareil WildFire

Concepts de la CLI du logiciel de l'appareil WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Cette section présente et décrit l'utilisation de l'interface de ligne de commande (CLI) du logiciel de l'appareil'A0;WildFire'A0;:

- Structure de la CLI du logiciel de l'appareil WildFire
- Conventions des commandes de la CLI du logiciel de l'appareil WildFire
- Messages des commandes de la CLI du logiciel de l'appareil WildFire
- Symboles des options de commande de l'appareil WildFire
- Niveaux de privilège de l'appareil WildFire

Structure de la CLI du logiciel de l'appareil WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

La CLI du logiciel de l'appareil'A0;WildFire vous permet de gérer l'appareil. La CLI est la seule interface de l'appareil. Celle-ci vous permet non seulement d'afficher les informations d'état et de configuration, mais aussi de modifier la configuration de l'appareil. Accédez à la CLI du logiciel de l'appareil'A0;WildFire via SSH ou directement à partir de la console l'aide du port de la console.

La CLI du logiciel de l'appareil'A0;WildFire fonctionne en deux modes'A0;:

- **Mode Opérationnel** : affichez l'état du système, parcourez la CLI du logiciel de l'appareil WildFire et passez en mode Configuration.
- **Mode Configuration** : affichez et modifiez la hiérarchie de configuration.

Conventions des commandes de la CLI du logiciel de l'appareil WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

L'invite de commande de base incorpore le nom d'utilisateur et le nom d'hôte de l'appareil'A0;:

```
username@hostname>
```

Exemple :


```
admin@WF-500>
```

Lorsque vous passez en mode Configuration, l'invite passe de **>** à **#** :

```
username@hostname> (mode opérationnel) username@hostname> configurer
 Entrer en mode configuration [modifier] username@hostname# (mode
 configuration)
```

En mode Configuration, le contexte hiérarchique actuel est affiché par la bannière `[edit...]` présentée entre crochets lorsqu'une commande est émise.

Messages des commandes de la CLI du logiciel de l'appareil WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Des messages peuvent s'afficher lors de l'émission d'une commande. Ces messages fournissent des informations contextuelles et peuvent vous aider à corriger les commandes non valides. Dans les exemples suivants, le message s'affiche en gras.

Exemple : Commande inconnue

```
username@hostname# application-group Commande inconnue : application-
group [edit network] username@hostname #
```

Exemple : changement de mode

```
username@hostname# quitter Quitter le mode de configuration
 username@hostname>
```

Exemple : Syntaxe non valide

```
 username@hostname> debug 17 Commande non reconnue Syntaxe non
 valide. username@hostname>
```

La CLI vérifie la syntaxe de chaque commande. Si la syntaxe est correcte, elle exécute la commande et les modifications apportées de la hiérarchie candidate sont enregistrées. Si la syntaxe est incorrecte, un message de syntaxe non valide s'affiche, comme dans l'exemple suivant'A0;:

```
username@hostname# définir le paramètre deviceconfig wildfire cloud-
intelligence submit-sample sur oui Command non reconnue Syntaxe non
 valide. [modifier] username@hostname #
```


Symboles des options de commande de l'appareil WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Le symbole précédant une option peut fournir des informations supplémentaires sur la syntaxe de la commande.

Symbole	Description
*	Cette option est obligatoire.
>	Des options imbriquées supplémentaires sont disponibles pour cette commande.
+	Des options imbriquées supplémentaires sont disponibles pour cette commande à ce niveau.
|	Une option permettant de spécifier une valeur d'exception ou une valeur de correspondance est disponible pour restreindre la commande.
“ “	Bien que les guillemets doubles ne soient pas le symbole d'une option de commande, ils doivent être utilisés lors de la saisie d'expressions multimots dans les commandes de la CLI. Par exemple, pour créer un groupe d'adresses nommé Test Group et pour ajouter l'utilisateur nommé user1 à ce groupe, vous devez encadrer de guillemets le nom du groupe comme suit : set address-group “Test Group” user1. Si vous n’encadrez pas de guillemets doubles le nom du groupe, la CLI interprète le mot Test comme le nom du groupe et Group comme le nom d’utilisateur. L’erreur suivante s’affiche alors : `testis not a valid name`. *Un guillemet simple ne serait également pas valide dans cet exemple.*

Les exemples suivants indiquent comment ces symboles sont utilisés.

Exemple : Dans la commande suivante, le mot-clé `from` est obligatoire :

```
username@hostname> configuration d'importation scp ? + numéro de
 port SSH du port distant sur l'hôte distant * à partir de la source
 (username@host:path) username@hostname> configuration d'importation
 scp Exemple : Le résultat de cette commande montre les options
```



```
définies avec + et >. username@hostname# définir la règle de
base règles de sécurité règles1 ? + action action + application
application + destination destination + disabled disabled + from
from + log-end log-end + log-setting log-setting + log-start
log-start + negate-destination negate-destination + negate-source
negate-source + schedule schedule + service service + source source
+ to to > profiles profiles <Enter> Saisie terminée [modifier]
username@hostname# définir règle de base règles de sécurité règle1
```

Chaque option désignée par + peut être ajoutée à la commande.

Le mot-clé profiles (avec >) dispose d'options supplémentaires :

```
username@hostname# définir règle de base règles de sécurité profils
 règle1 ? + virus Help string for virus + spyware Help string
 for spyware + vulnerability Help string for vulnerability +
 group Help string for group <Enter> Saisie terminée [modifier]
 username@hostname# définir règle de base règles de sécurité profils
 règle1
```

Niveaux de privilège de l'appareil WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Les niveaux de privilèges déterminent les commandes que l'utilisateur est autorisé à exécuter et les informations qu'il est autorisé à afficher.

Niveau	Description
Super lecteur	Dispose d'un accès en lecture seule à l'appareil.
Super utilisateur	Dispose d'un accès en lecture/écriture à l'appareil.

Modes des commandes de la CLI de WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Les rubriques suivantes décrivent les modes utilisés pour interagir avec la CLI du logiciel de l'appareil WildFire :

- Mode Configuration de la CLI de l'appareil WildFire
- Mode Opérationnel de la CLI de l'appareil WildFire

Mode Configuration de la CLI de l'appareil WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

La saisie de commandes en mode Configuration modifie la configuration candidate. La configuration candidate modifiée est stockée dans la mémoire de l'appareil et conservée pendant l'exécution de l'appareil.

Chaque commande de configuration implique une action et peut inclure des mots-clés, options et valeurs.

Cette section décrit le mode Configuration et la hiérarchie de configuration.

- Utilisation des commandes du mode Configuration
- Hiérarchie de configuration
- Chemins d'accès à la hiérarchie
- Navigation dans la hiérarchie

Utilisation des commandes du mode Configuration

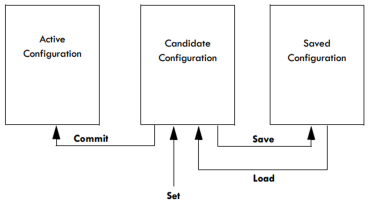
Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Les commandes suivantes vous permettent de stocker et d'appliquer les modifications apportées à la configuration'A0;:

- `save` : enregistre la configuration candidate dans la mémoire non volatile sur l'appareil. La configuration enregistrée est conservée jusqu'à ce qu'elle soit remplacée par les commandes **save** suivantes. Veuillez noter que cette commande n'active pas la configuration.
- `commit` : applique la configuration candidate à l'appareil. Une configuration validée devient la configuration active du périphérique.
- `set` : modifie une valeur dans la configuration candidate.

- `load` : affecte la dernière configuration enregistrée ou une configuration spécifiée comme configuration candidate.

> *Si vous quittez le mode Configuration sans émettre la commande* ***`save`*** *ou* ***`commit`****, les modifications apportées à la configuration peuvent être perdues si l'appareil n'est plus alimenté.*



La gestion d'une configuration candidate et la séparation des étapes d'enregistrement et de validation confèrent d'importants avantages par rapport aux architectures'A0;CLI classiques'A0;:

- La distinction entre les concepts d'enregistrement et de validation permet d'effectuer plusieurs modifications simultanément et de réduire la vulnérabilité du système.
- Les commandes peuvent être facilement adaptées pour des fonctions similaires. Par exemple, lors de la configuration de deux interfaces'A0;Ethernet, chacune disposant d'une adresse'A0;IP différente, vous pouvez modifier la configuration de la première interface, copier la commande, modifier uniquement l'interface et l'adresse'A0;IP, puis appliquer les modifications à la seconde interface.
- La structure de la commande est toujours cohérente.

Comme la configuration candidate est toujours unique, toutes les modifications autorisées apportées à celle-ci sont cohérentes.

Hiérarchie de configuration

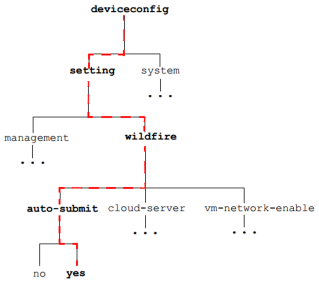
Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

La configuration de l'appareil est organisée hiérarchiquement. La commande `show` vous permet d'afficher une partie du niveau hiérarchique actif. Saisissez show pour afficher la hiérarchie complète, et `show` avec des mots-clés pour afficher une partie de la hiérarchie. Par exemple, lorsque vous exécutez la commande `show` à partir du niveau supérieur du mode Configuration, toute la configuration s'affiche. Lorsque vous exécutez la commande `edit mgt-config` et que vous saisissez `show`, ou si vous exécutez ***`showmgt-config`***, seule la partie mgt-config de la hiérarchie s’affiche.

Chemins d'accès à la hiérarchie

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Lors de la saisie de commandes, le chemin d'accès à la hiérarchie est comme suit :

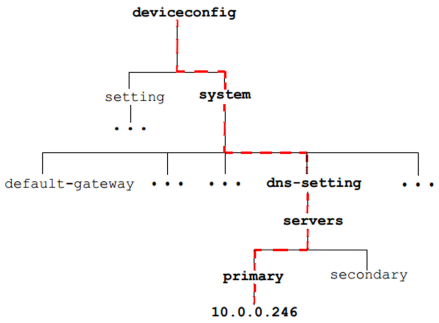


Par exemple, la commande suivante affecte le serveur'A0;DNS principal 10.0.0.246 à l'appareil'A0;:

```
[modifier] username@hostname# définir le système deviceconfig dns-setting sur serveurs principaux 10.0.0.246
```

Cette commande génère un nouvel élément dans la hiérarchie et dans le résultat de la commande `show` suivante :

```
[edit] username@hostname# afficher le système deviceconfig system
 dns-settings dns-setting { servers { primary 10.0.0.246 } }
 [modifier] username@hostname#
```



Navigation dans la hiérarchie

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

La bannière [edit...] présentée sous la ligne d'invite de commande du mode Configuration affiche le contexte hiérarchique actif.

```
[Modifier]
```

indique que le contexte relatif est le niveau supérieur de la hiérarchie, tandis que


```
[modifier deviceconfig]
```

indique que le contexte relatif est le niveau deviceconfig.

Les commandes répertoriées ci-dessous vous permettent de parcourir la hiérarchie de configuration.

Niveau	Description
Modifier	Définit le contexte de la configuration dans la hiérarchie de commande.
Up	Passe le contexte au niveau supérieur suivant de la hiérarchie.
top	Passe le contexte au niveau le plus élevé de la hiérarchie.

*La commande **`set`** émise après l'utilisation des commandes **`up`** et **`top`** est exécutée à partir du nouveau contexte.*

Mode Opérationnel de la CLI de l'appareil WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Lors de la connexion initiale au périphérique, la CLI du logiciel de l'appareil'A0;WildFire s'ouvre en mode Opérationnel. Les commandes du mode Opérationnel impliquent des actions qui sont immédiatement exécutées. Celles-ci n'affectent pas la configuration et ne doivent pas être enregistrées ni validées.

Les commandes du mode Opérationnel sont de plusieurs types :

- **Accès réseau** : accédez à un autre hôte. SSH est pris en charge.
- **Surveillance et dépannage** : effectuez des tâches de diagnostic et d'analyse. Les commandes sont les suivantes : `debug` et `ping`.
- **Commandes d'affichage** : affichez ou effacez les informations actives. Les commandes sont les suivantes : `clear` et `show`.
- **Commandes de navigation dans la CLI du logiciel de l'appareil WildFire** : passez en mode Configuration ou quittez la CLI du logiciel de l'appareil WildFire. Les commandes sont les suivantes : `configure`, `exit` et `quit`.
- **Commandes système** : émettez des requêtes au niveau du système ou redémarrez. Les commandes sont les suivantes : `set` et `request`.

Accès à la CLI de l’appareil WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Cette section décrit l'accès à la CLI du logiciel de l'appareil WildFire :

- Établissement d'une connexion de console directe
- Établissement d'une connexion SSH

Établissement d'une connexion de console directe

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Utilisez les paramètres suivants pour une connexion de console directe'A0;:

- Débit de données'A0;: 9600
- Bits de données'A0;: 8
- Parité'A0;: aucune
- Bits d'arrêt'A0;: 1
- Contrôle de flux'A0;: None

Établissement d'une connexion SSH

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Pour accéder à la CLI du logiciel de l'appareil WildFire :

STEP 1 | Utilisez le logiciel d'émulation de terminal pour établir une connexion de console SSH avec l'appareil WildFire.

STEP 2 | Saisissez le nom d'utilisateur de l'administrateur. La valeur par défaut est admin.

STEP 3 | Saisissez le mot de passe de l'administrateur. La valeur par défaut est admin.

La CLI du logiciel de l'appareil'A0;WildFire s'ouvre en mode Opérationnel et l'invite d'interface de ligne de commande s'affiche'A0;:

```
username@hostname>
```


Opérations de la CLI de l’appareil WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

- Accès aux modes Opérationnel et Configuration de l'appareil WildFire
- Affichage options de commande de la CLI du logiciel de l'appareil WildFire
- Restriction d'affichage des résultats des commandes de la CLI de l'appareil WildFire
- Paramétrage du format de sortie des commandes de configuration pour l'appareil WildFire

Accès aux modes Opérationnel et Configuration de l'appareil WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Lors de la connexion, la CLI du logiciel de l'appareil'A0;WildFire s'ouvre en mode Opérationnel. Vous pouvez basculer entre les modes Opérationnel et Configuration à tout moment.

- Pour passer du mode Opérationnel au mode Configuration, utilisez la commande **`configure`** :

```
username@hostname> configurer Entrer en mode de configuration
 [modifier] username@hostname#
```

- Pour quitter le mode Configuration et revenir en mode Opérationnel, utilisez la commande **`quit`** ou **`exit`** :

```
username@hostname# quitter Sortir du mode de configuration
 username@hostname>
```

Pour passer du mode Configuration au mode Opérationnel, utilisez la commande **`run`**. Par exemple, pour afficher les ressources système en mode Configuration, utilisez la commande **`run show system resources`**.

Affichage options de commande de la CLI du logiciel de l'appareil WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Utilisez **?** (ou Meta-H) pour afficher une liste des options de commande, en fonction du contexte :

- Pour afficher une liste des commandes opérationnelles, saisissez **?** dans l'invite de commande.

```
username@hostname> ? Effacer les paramètres d’exécution configurer
Manipuler les informations de configuration logicielle créer créer
des commandes déboguer et diagnostiquer supprimer Supprimer les
fichiers du disque dur désactiver désactiver les commandes modifier
les commandes quitter Quitter cette session trouver Trouver des
commandes CLI avec mot-clé grep Recherche fichier pour les lignes
contenant un modèle correspondant moins Examiner le contenu du
fichier de débogage ping hôtes et réseaux quitter Quitter cette
demande de session Faire des demandes au niveau du système scp
Utiliser scp pour importer / exporter des fichiers définir définir
des paramètres opérationnels afficher Afficher les paramètres
opérationnels ssh Démarrer un shell sécurisé à un autre hôte
soumettre des extrémités de commandes Imprimer les 10 dernières
lignes de contenu de fichier de débogage telnet Démarrer une session
telnet à un autre test d’hôte vérifier les paramètres système avec
des cas de test tftp Utiliser tftp pour importer / exporter des
fichiers traceroute Imprimer l’itinéraire des paquets à l’hôte
réseau username@hostname>
```

- Pour afficher les options disponibles pour une commande spécifique, saisissez la commande suivie de **?**.

Exemple :

```
username@hostname> ping ? + bypass-routing table de routage,
utiliser l’interface spécifiée + nombre de requêtes à envoyer
(1..2000000000 paquets) + do-not-fragment Ne pas fragmenter les
paquets de demande d’écho (IPv4) + intervalle Délai entre les
requêtes (secondes) + no-resolve Ne pas essayer d’imprimer les
adresses symboliquement + modèle Modèle de remplissage hexadécimal
+ taille des paquets de demande (0..65468 octets) + source Adresse
source de la demande d’écho + valeur de type de service IP tos
(0..255) +  ttl IP time-to-live value (IPv6 hop-limit value) (0..255
hops) + verbose Afficher la sortie détaillée * host Hostname ou
adresse IP de l’hôte distant
```

Restriction d'affichage des résultats des commandes de la CLI de l'appareil WildFire

Certaines commandes opérationnelles incluent une option permettant de restreindre le résultat affiché. Pour restreindre le résultat, saisissez le symbole de barre verticale suivi de **except** ou **match** et de la valeur à exclure ou inclure :

Exemple :

Le résultat suivant est pour la commande show system info :

```
username@hostname> afficher les informations systèmenom d’hôte :
Adresse IP de WildFire : Masque réseau 192.168.2.20 : Passerelle par
défaut 255.255.255.0 : Adresse mac 192.168.2.1 : 00:25:90:95:84:76
```



```
 vm-interface-ip-address: 10.16.0.20 vm-interface-netmask :
 255.255.252.0 vm-interface-default-gateway : 10.16.0.1 vm-
interface-dns-server : 10.0.0.247 heure: Mon Apr 15 13:31:39
 2013 uptime: 0 jours, 0:02:35 famille: m modèle: Série WF-500 :
 009707000118 sw-version: 8.0.1 wf-content-version: 702-283 wf-
content-release-date: version logdb inconnue: 8.0.15 famille de
 plates-formes : m mode opérationnel : normal username@hostname>
 L’exemple suivant affiche uniquement les informations du modèle
 système : username@hostname> afficher les informations système |
 modèle de correspondance modèle : WF-500 username@hostname>
```

Paramétrage du format de sortie des commandes de configuration pour l'appareil WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Modifiez le format de sortie des commandes de configuration à l'aide de la commande **`set cli config-output-format`** en mode Opérationnel. Les options sont les suivantes : Format par défaut, JSON (JavaScript Object Notation), Définir le format et Format XML. Le format par défaut est un format hiérarchique dans lequel les sections de configuration sont présentées une par ligne et entre accolades.

Référence des commandes du mode Configuration de l'appareil WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Cette section contient des informations de référence sur les commandes du mode Configuration suivantes qui sont spécifiques au logiciel de l'appareil'A0;WildFire. Toutes les autres commandes du logiciel de l’appareil WildFire sont identiques à celles de PAN-OS, telles qu’elles sont décrites dans le Guide de mise en route de la CLI PAN-OS 11.0.

- set deviceconfig cluster
- set deviceconfig high-availability
- set deviceconfig setting management
- set deviceconfig setting wildfire
- set deviceconfig system eth2
- set deviceconfig system eth3
- définir le système panorama de deviceconfig sur local-panorama-server
- définir le panorama du système deviceconfig sur local-panorama panorama-server-2
- set deviceconfig system update-schedule
- set deviceconfig system vm-interface

set deviceconfig cluster

Description

Configurez les paramètres du cluster d'appareils WildFire sur l'appareil WildFire. Vous pouvez configurer le nom du cluster, l’interface utilisée pour la communication du cluster et le mode (rôle) de l’appareil au sein du cluster : contrôleur ou esclave. Sur les appareils WildFire que vous configurez en tant que contrôleurs du cluster, vous pouvez ajouter des appareils WildFire au cluster et établir si le contrôleur offre un service DNS sur son interface de gestion.

Emplacement de la hiérarchie

```
définir deviceconfig
```

Syntaxe

```
cluster { nom-cluster <name>; interface {eth2 | eth3} ; mode
 { contrôleur { service-publicité dns-service activé {non | oui};
 worker-list {adresse-ip} } worker ; } }
```


Options

`+ cluster-name` : nommez le cluster. Le nom doit être une section de nom de domaine valide.

`+ interface` : configurez l’interface à utiliser pour la communication du cluster. L’interface de communication du cluster doit être identique pour tous les membres du cluster.

`> mode` : configurez l’appareil WildFire en tant que nœud de contrôle ou que nœud esclave. Dans le cas de nœuds de contrôle, vous pouvez décider si le contrôleur fournit un service DNS sur l’interface de gestion (`service-advertisement`) et ajouter des nœuds esclaves au cluster (`worker-list`). Chaque cluster d'appareils WildFire devrait posséder deux nœuds de contrôle pour procurer la haute disponibilité. Vous pouvez ajouter deux contrôleurs et un maximum de 18 nœuds esclaves à un cluster, pour un maximum de 20 nœuds.

Exemple de résultat

```
admin@wf-500(active-controller)# afficher le cluster deviceconfig
 cluster { cluster-name sid-6 ; interface eth2 ; mode { contrôleur
 { worker-list { 2.2.2.115 ; } } } }
```

Niveau de privilège requis

superuser, deviceadmin

set deviceconfig high-availability

Description

Configurez les paramètres de haute disponibilité du cluster d'appareils WildFire.

Emplacement de la hiérarchie

```
définir deviceconfig
```

Syntaxe

```
haute disponibilité { enabled {no | yes}; option de choix
 { preemptive {no | yes}; priorité {primary | secondary}; minuteries
 { advanced {heartbeat interval <value> | hello-interval <value>
 | preemption-hold-time <value> | promotion-hold-time <value>}
 aggressif; conseillé; } } interface { ha1 { peer-ip-address <ip-
address>; port {eth2 | eth3 | management}; chiffrement activé {no |
 yes}; } ha1-backup { peer-ip-address <ip-address>; port {eth2 | eth3
 | management}; } } }
```

Options

`+ enabled` : activez la HA sur les deux nœuds de contrôle pour assurer la tolérance aux pannes du cluster. Chaque cluster d'appareils WildFire devrait posséder deux nœuds de contrôle configurés en tant que paire HA.

`> election-option` : configurez les valeurs d’option préemptives, de priorité et du minuteur HA.

`+ preemptive` : option à sélectionner pour permettre à la paire HA passive (le nœud de contrôle de secours) de remplacer la paire HA active (le nœud de contrôle principal) selon les paramètres de priorité (`priority`) HA. Par exemple, en cas d’échec du nœud de contrôle principal, le nœud de contrôle secondaire (passif) reprend le contrôle du cluster. Une fois le nœud de contrôle principal restauré, le contrôleur secondaire continue de contrôler le cluster et le contrôleur principal agit en tant que nœud de contrôle de secours si vous n’avez pas configuré la préemption. Toutefois, si vous configurez la préemption sur les deux homologues HA, une fois le contrôleur principal restauré, il remplace le contrôleur secondaire en reprenant le contrôle du cluster. Le contrôleur secondaire reprend son ancien rôle de nœud de contrôle de secours. Pour que la préemption fonctionne, vous devez configurer ce paramètre sur les deux homologues HA.

`+ priority` : option à sélectionner pour configurer la priorité de préemption de chaque contrôleur de la paire HA. Configurez la préemption sur les deux membres de la paire de contrôleurs HA.

`> timers` : configurez les minuteurs des options de sélection HA. L’appareil WildFire propose deux options de minuteurs préconfigurées (les paramètres `aggressive` et `recommended`). Vous pouvez également configurer les minuteurs séparément. Les minuteurs `Advanced` vous permettent de configurer les valeurs individuellement :

- L’option `heartbeat-interval` définit l’intervalle, en millisecondes, d’envoi de requêtes ping de pulsation. La plage de valeurs se situe entre 1 000 et 60 000 ms ; la valeur par défaut est définie sur 2 000 ms.
- L’option `hello-interval` définit l’intervalle, en millisecondes, d’envoi de messages Hello. La plage de valeurs se situe entre 8 000 et 60 000 ms ; la valeur par défaut est définie sur 8000 ms.
- L’option `preemption-hold-time` définit l’intervalle, en minutes, pendant lequel l’appareil doit rester en mode passive (contrôleur de secours) avant de remplacer le nœud de contrôle actif (principal). La plage de valeurs se situe entre 1 et 60 minutes ; la valeur par défaut est définie sur 1 minute.
- L’option `promtion-hold-time` définit l’intervalle, en millisecondes, qu’il faut attendre avant de passer de l’état passive (contrôleur de secours) à l’état actif (principal). La plage de valeurs se situe entre 0 et 60 000 ms ; la valeur par défaut est définie sur 2 000 ms.

`> interface` : configurez les paramètres de l’interface HA pour les interfaces de liaison de contrôle principale (`ha1`) et de secours (`ha1-backup`). Les interfaces de liaison de contrôle permettent à la paire de contrôleurs HA de demeurer synchronisée et prête à faire face à un basculement en cas d’échec du nœud de contrôle principal. La configuration de l’interface `ha1` et de l’interface `ha1-backup` procure une connectivité redondante entre les contrôleurs en cas d’échec d’une liaison. Définissez :

- L’adresse IP de l'homologue (`peer-ip-address`). Pour chaque interface, configurez l'adresse IP de l'homologue HA. L’interface homologue `ha1` possède l’adresse IP de l’interface `ha1` qui se trouve sur l’autre nœud de contrôle de la paire HA. L’interface homologue `ha1-backup` possède l’adresse IP de l’interface `ha1-backup` qui se trouve sur l’autre nœud de contrôle de la paire HA.
- Le `port`. Sur chaque nœud de contrôle,configurez le port à utiliser pour l’interface `ha1` et le port à utiliser pour l’interface `ha-backup`. Vous pouvez utiliser `eth2`, `eth3` ou le port de gestion (`management`) (eth0) pour les interfaces de liaison de contrôle HA. Vous ne pouvez pas utiliser l’interface du réseau de l’environnement d'analyse (eth1) comme interface de liaison de contrôle `ha1` ou `ha1-backup`. Utilisez la même interface `ha1` sur les deux homologues HA et la même `ha1-backup` (interface autre que l’interface `ha1`) sur les deux homologues HA. Par exemple, configurez

`eth3` en tant qu'interface `ha1` sur les deux nœuds de contrôle et configurez l’interface de gestion (`management`) en tant qu’interface `ha1-backup` sur les deux nœuds de contrôle.

Exemple de résultat

```
admin@wf-500(active-controller)# afficher haute disponibilité
 deviceconfig haute disponibilité { election-option { priority
 primary; } activé non; interface { ha1 { peer-ip-address
 10.10.10.150; port eth2 } ha1-backup { peer-ip-address 10.10.10.160;
 port management } } }
```

Niveau de privilège requis

superuser, deviceadmin

set deviceconfig setting management

Description

Configurez les paramètres de la session de gestion administrative sur l'appareil WildFire. Vous pouvez configurer des délais d’expiration pour mettre fin aux sessions administratives si leur inactivité dure trop longtemps ainsi que le nombre de tentatives de connexion (tentatives de connexion échouées) nécessaires pour verrouiller un administrateur.

Emplacement de la hiérarchie

```
définir le paramètre deviceconfig
```

Syntaxe

```
gestion { idle-timeout {0 | <value>} admin-lockout { failed-attempts
 <value> lockout-time <value> } }
```

Options

`+ idle-timeout` : délai d'inactivité de session administrative par défaut en minutes. Configurez un délai d'inactivité allant de 1 à 1 440 minutes ou définissez la valeur du délai d'expiration sur 0 (zéro) pour que la session n'expire jamais.

`> admin-lockout` : configurez le nombre de tentatives (`failed-attempts`) dont l'administrateur dispose pour se connecter à l’appareil avant qu’il ne soit verrouillé du système (de 0 à 10) et la durée `lockout-time` en minutes (de 0 à 60) pendant laquelle l'administrateur ne peut accéder au système s’il dépasse le seuil d’échecs de tentatives (`failed-attempts`) défini.

Exemple de résultat

```
gestion { idle-timeout 0; admin-lockout { failed-attempts 3; lockout-
time 5; } }
```


set deviceconfig setting wildfire

Description

Configurez des paramètres WildFire sur l'appareil WildFire. Vous pouvez configurer le transfert de fichiers malveillants, définir le serveur de cloud qui reçoit les fichiers infectés et activer ou désactiver l'interface vm-interface.

Emplacement de la hiérarchie

```
définir le paramètre deviceconfig
```

Syntaxe

```
wildfire { active-vm {vm-1 | vm-2 | vm-3 | vm-4 | vm-5 | <value>};
 cloud-server <value>; custom-dns-name <value>; preferred-analysis-
environment {Documents | Exécutables | par défaut}; vm-network-
enable {no | yes}; vm-network-use-tor {enable | disable}; cloud-
intelligence { cloud-query {no | yes};submit-diagnostics {no |
 yes}; submit-report {no | yes}; submit-sample {no | yes}; } file-
retention { malicious {indefinite | <1-2000>}; non-malicious <1-90> }
 signature-generation { av {no | yes}; dns {no | yes}; url {no |
 yes}; } }
```

Options

`+ active-vm` : sélectionnez l'environnement de machine virtuelle que WildFire utilisera pour l'analyse d'échantillon. Chaque MV dispose d'une configuration différente comme Windows XP, des versions Flash, Adobe Reader, etc. Pour afficher la MV sélectionnée, exécutez la commande : **`show wildfire status`** et consultez le champ Selected VM (Machine virtuelle sélectionnée). Pour afficher les informations sur l'environnement VM, exécutez la commande suivante **`: show wildfire vm-images.`**

`+ cloud-server` : nom d'hôte du serveur du cloud auquel l'appareil transférera les échantillons/rapports malveillants pour nouvelle analyse. Le serveur du cloud par défaut est wildfire-public-cloud. Pour configurer le transfert, utilisez la commande suivante : **`set deviceconfig setting wildfire cloud-intelligence`**.

`+ custom-dns-name` : configurez un nom DNS personnalisé à utiliser dans les certificats du serveur et dans la liste de serveur Wildfire à la place du nom DNS par défaut `wfpc.sevice.<clustername>.<domain>`.

`+ preferred-analysis-environment` : allouez la majorité des ressources à l’analyse des documents ou à l’analyse des exécutables, selon le type d’échantillons le plus souvent analysé dans votre environnement. L’affectation pas défaut répartit les ressources de manière équilibrée entre les échantillons de fichiers exécutables et de documents. Par exemple, pour allouer la majorité des ressources d'analyse aux documents : **`set deviceconfig setting wildfire preferred-analysis-environment Documents`**.

`+ vm-network-enable` : activez ou désactivez le réseau vm-network. Lorsqu'il est activé, les échantillons de fichiers exécutés dans le bac à sable de la machine virtuelle ont accès à Internet. Ceci permet à WildFire de mieux analyser le comportement du logiciel malveillant afin de rechercher des informations comme l'activité du téléphone personnel.

`+ vm-network-use-tor` : activez ou désactivez le réseau Tor pour l'interface vm-interface. Lorsque cette option est activée, tout trafic malveillant provenant des systèmes de bac à sable de l'appareil WildFire lors de l'analyse d'échantillon est envoyé via le réseau Tor. Le réseau Tor masque votre adresse IP publique, de manière à ce que les sites malveillants ne puisse pas déterminer la source du trafic.

`> cloud-intelligence` : configurez l'appareil afin qu'il envoie des diagnostics, des rapports ou des échantillons WildFire au cloud WildFire de Palo Alto Networks ou qu’il demande automatiquement des informations au cloud WildFire public avant d’effectuer l’analyse locale pour préserver les ressources de l’appareil WildFire. L'option d'envoi de rapport envoie des rapports pour des échantillons malveillants au cloud à des fins de statistiques. L'option d'envoi d'échantillon envoie des échantillons malveillants au cloud. Si l'option submit-sample est activée, vous n'avez pas besoin d'activer l'option submit-report, car le cloud analyse de nouveau l'échantillon, et un nouveau rapport et une signature sont générés si l'échantillon est malveillant.

`> file-retention` : configurez la durée de conservation des échantillons malveillants (malveillants et hameçonnage) et des échantillons non malveillants (indésirables et bénins). Par défaut, la durée de conservation des échantillons malveillants est indéfinie (ne jamais supprimer). Par défaut, la durée de conservation des échantillons qui ne sont pas malveillants est de 14 jours. Par exemple, voici la commande à utiliser pour conserver des échantillons qui ne sont pas malveillants pour une durée de 30 jours : **`set deviceconfig setting wildfire file-retention non-malicious 30`**.

`> signature-generation` : activez l'appareil pour qu'il génère des signatures localement, supprimant ainsi la nécessité d'envoyer des données au cloud public pour bloquer le contenu malveillant. L'appareil WildFire analysera les fichiers qui lui sont transférés par les pare-feu Palo Alto Networks ou l'API WildFire et générera des signatures antivirus et DNS qui bloquent les fichiers malveillants ainsi que le trafic de commande et de contrôle associé. Lorsque l'appareil détecte une URL malveillante, il l'envoie à PAN-DB qui la classe dans une catégorie de logiciel malveillant.

Exemple de résultat

Vous trouverez ci-dessous un exemple de résultat des paramètres WildFire.

```
admin@WF-500# afficher le paramètre wildfire de deviceconfig wildfire
 { signature-generation { av yes; dns yes; url yes; } intelligence
 cloud { submit-report no; submit-sample yes; submit-diagnostics
 yes; cloud-query yes; } conservation de fichier { non-malicious
 30; malicious 1000; { active-vm vm-5; cloud-server wildfire-public-
cloud; vm-network-enable yes; }
```

set deviceconfig system eth2

Description

Configurez l'interface eth2.

Emplacement de la hiérarchie

```
définir le système deviceconfig sur eth2
```

Syntaxe

```
eth2 { default-gateway <ip-address>; ip-address <ip-address>; mtu
 <value>; netmask <ip-netmask>; vitesse-duplex {100Mbps-full-duplex
 | 100Mbps-half-duplex | 10Mbps-full-duplex | 10Mbps-half-duplex |
 1Gbps-full-duplex | 1Gbps-half-duplex | auto-negotiate}; permitted-
ip <ip-address/netmask>; service disable-icmp {no | yes}; }
```

Options

+ `default-gateway` : adresse IP de la passerelle par défaut de l’interface eth2.

+ `ip-address` : adresse IP de l'interface eth2.

+ `mtu` : maximum Transmission Unit (unité de transmission maximale ; MTU) pour l'interface eth2.

+ `netmask` : masque réseau de l'interface eth2.

+ `speed-duplex` : vitesse de l’interface (10 Mbits/s, 100 Mbits/s, 1 Gbits/s ou automatiquement négociée) et mode duplex (intégral ou semi) de l’interface eth2.

> `permitted-ip` : adresses IP autorisées à accéder à l’interface eth2. Si vous spécifiez un masque réseau avec l’adresse IP, le masque réseau doit être au format de notation contenant des barres obliques. Par exemple, pour spécifier une adresse de Classe C, saisissez : 10.10.10.100/24 (not 10.10.10.100 255.255.255.0).

> `service-disable` : désactivez ICMP pour l’interface eth2.

Exemple de résultat

```
admin@wf-500(active-controller)# afficher le système deviceconfig
 eth2 eth2 { ip-address 10.10.10.120; masque de réseau 255.255.255.0;
 service { disable-icmp no; } speed-duplex auto-negotiate; mtu
 1500; }
```

Niveau de privilège requis

superuser, deviceadmin

set deviceconfig system eth3

Description

Configurez l'interface eth3.

Emplacement de la hiérarchie

```
définir le système deviceconfig sur eth2
```

Syntaxe

```
eth3 { default-gateway <ip-address>; ip-address <ip-address>; mtu
 <value>; netmask <ip-netmask>; speed-duplex {100Mbps-full-duplex
 | 100Mbps-half-duplex | 10Mbps-full-duplex | 10Mbps-half-duplex |
 1Gbps-full-duplex | 1Gbps-half-duplex | auto-negotiate}; permitted-
ip <ip-address/netmask>; service disable-icmp {no | yes}; }
```

Options

+ `default-gateway` : adresse IP de la passerelle par défaut de l’interface eth3.

+ `ip-address` : adresse IP de l'interface eth3.

+ `mtu` : maximum Transmission Unit (unité de transmission maximale ; MTU) pour l'interface eth3.

+ `netmask` : masque réseau de l'interface eth3.

+ `speed-duplex` : vitesse de l’interface (10 Mbits/s, 100 Mbits/s, 1 Gbits/s ou automatiquement négociée) et mode duplex (intégral ou semi) de l’interface eth3.

> `permitted-ip` : adresses IP autorisées à accéder à l’interface eth3. Si vous spécifiez un masque réseau avec l’adresse IP, le masque réseau doit être au format de notation contenant des barres obliques. Par exemple, pour spécifier une adresse de Classe C, saisissez : 10.10.10.100/24 (not 10.10.10.100 255.255.255.0).

> `service-disable` : désactivez ICMP pour l’interface eth3.

Exemple de résultat

```
admin@wf-500(active-controller)# afficher le système deviceconfig
 eth3 eth3 { ip-address 10.10.20.120; netmask 255.255.255.0; service
 { disable-icmp no; } speed-duplex auto-negotiate; mtu 1500; }
```

Niveau de privilège requis

superuser, deviceadmin

définir le système panorama de deviceconfig sur local-panorama-server

Description

Configurez le serveur Panorama principal pour la gestion du cluster d’appareils WildFire ou de l’appareil WildFire.

Emplacement de la hiérarchie

```
définir le panorama du système deviceconfig sur local-panorama
```

Syntaxe

```
serveur panorama {adresse IP | FQDN};
```

Options

`+ panorama-server` : configurez l'adresse IP ou le Fully Qualified Domain Name (nom de domaine complet ; FQDN) du serveur Panorama principal que vous utiliserez pour gérer le cluster d’appareils WildFire ou l’appareil WildFire.

Exemple de résultat

Le résultat est tronqué pour indiquer uniquement la strophe qui affiche les paramètres du serveur Panorama.

```
admin@wf-500(active-controller)# afficher le système deviceconfig
 système { panorama-server 10.10.10.100; panorama-server-2
 10.10.10.110 hostname myhost; ip-address 10.10.20.120; netmask
 255.255.255.0; default-gateway 10.10.10.1; update-server
 updates.paloaltonetworks.com; service { disable-icmp no; disable-ssh
 no; disable-snmp yes; } ...
```

Niveau de privilège requis

superuser, deviceadmin

définir le panorama du système deviceconfig sur local-panorama panorama-server-2

Description

Configurez le serveur Panorama de secours pour la gestion du cluster d’appareils WildFire ou de l’appareil WildFire. La configuration d’un serveur Panorama de secours procure une haute disponibilité aux fins de la gestion du cluster ou des appareils individuels.

Emplacement de la hiérarchie

```
définir le panorama du système deviceconfig sur local-panorama
```

Syntaxe

```
serveur-panorama-2 {adresse IP | FQDN} ;
```


Options

`+ panorama-server-2` : configurez l'adresse IP ou le Fully Qualified Domain Name (nom de domaine complet ; FQDN) du serveur Panorama de secours que vous utiliserez pour gérer le cluster d’appareils WildFire ou l’appareil WildFire.

Exemple de résultat

Le résultat est tronqué pour indiquer uniquement la strophe qui affiche les paramètres du serveur Panorama.

```
admin@wf-500(active-controller)# afficher le système deviceconfig
 système { panorama-server 10.10.10.100; panorama-server-2
 10.10.10.110 hostname myhost; ip-address 10.10.20.120; netmask
 255.255.255.0; default-gateway 10.10.10.1; update-server
 updates.paloaltonetworks.com; service { disable-icmp no; disable-ssh
 no; disable-snmp yes; } ...
```

Niveau de privilège requis

superuser, deviceadmin

set deviceconfig system update-schedule

Description

Planifiez les mises à jour de contenu sur un appareil WildFire. Ces mises à jour de contenu fournissent à l'appareil les toutes dernières informations sur les menaces afin de détecter précisément les logiciels malveillants et d'améliorer la capacité de l'appareil à différencier les logiciels malveillants et bénins.

Emplacement de la hiérarchie

```
set deviceconfig system update-schedule
```

Syntaxe

```
récurrence de wf-content { daily at <value> action {download-and-
install | download-only}; weekly { action {download-and-install |
 download-only}; at <value>; day-of-week {friday | monday | saturday
 | sunday | thursday | tuesday | wednesday}; } }
```

Options

`> wf-content` : mises à jour de contenu WildFire.

`> daily` : planifiez une mise à jour chaque jour.

`+ action` : spécifiez l'action à exécuter. Vous pouvez planifier l'appareil pour qu'il télécharge et installe la mise à jour ou qu'il la télécharge seulement et que vous l'installiez ensuite manuellement.

`+ at` : spécification de l'heure hh:mm (ex : 20:10).

> `hourly` : planifiez une mise à jour chaque heure.

`+ action` : spécifiez l'action à exécuter. Vous pouvez planifier l'appareil pour qu'il télécharge et installe la mise à jour ou qu'il la télécharge seulement et que vous l'installiez ensuite manuellement.

`+ at` : minutes après l'heure.

> `weekly` : planifiez une mise à jour chaque semaine.

`+ action` : spécifiez l'action à exécuter. Vous pouvez planifier l'appareil pour qu'il télécharge et installe la mise à jour ou qu'il la télécharge seulement et que vous l'installiez ensuite manuellement.

`+ at` : spécification de l'heure hh:mm (ex : 20:10).

`+ day-of-week` : jour de la semaine (Friday, Monday, Saturday, Sunday, Thursday, Tuesday, Wednesday)

Exemple de résultat

```
admin@WF-500# afficher le calendrier des mises à jour { wf-content
 { recurring { weekly { at 19:00; action download-and-install; day-
of-week friday; } } } }
```

Niveau de privilège requis

superuser, deviceadmin

set deviceconfig system vm-interface

Description

L'interface vm-interface est utilisée par les logiciels malveillants exécutés sur le bac à sable de la machine virtuelle de l'appareil WildFire pour accéder à Internet. L'activation de ce port est recommandée car elle permet à WildFire de mieux identifier l'activité malveillante si le logiciel malveillant accède à Internet pour une activité phone-home ou autre. Il est important que cette interface dispose d'une connexion isolée à Internet. Si votre appareil WildFire fonctionne en mode FIPS/CC, l’interface vm est désactivée. Pour obtenir de plus amples renseignements, reportez-vous à la section Paramétrage de l'interface VM de l'appareil WildFire.

Une fois que l'interface vm-interface est configurée, activez-la en exécutant la commande suivante :

```
définir le paramètre wildfire deviceconfig vm-network-enable sur oui
```

Emplacement de la hiérarchie

```
définir le système deviceconfig sur eth2
```


Syntaxe

```
définir vm-interface { default-gateway <ip_address>; dns-server
 <ip_address>; ip-address <ip_address>; link-state; mtu; netmask
 <ip_address>; speed-duplex; {
```

Options

+ `default-gateway` : passerelle par défaut pour l'interface VM.
+ `dns-server` : serveur DNS par défaut pour l'interface VM.
+ `ip-address` : adresse IP de l'interface VM.
+ `link-state` : définir si l'état de la liaison est ascendant ou descendant.
+ `mtu` : unité de transmission maximale pour l'interface VM.
+ `netmask` : masque réseau IP de l'interface VM.
+ `speed-duplex` : vitesse et duplex pour l'interface VM.

Exemple de résultat

Vous trouverez ci-dessous une interface vm-interface configurée.

```
vm-interface { ip-address 10.16.0.20; netmask 255.255.252.0; default-
gateway 10.16.0.1; dns-server 10.0.0.246; }
```

Niveau de privilège requis

superuser, deviceadmin

Référence des commandes du mode Opérationnel de l'appareil WildFire

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Appareil WildFire	❑ Licence WildFire

Cette section contient des informations de référence sur les commandes du mode Opérationnel suivantes qui sont spécifiques au logiciel de l'appareil WildFire. Toutes les autres commandes du logiciel de l’appareil WildFire sont identiques à celles de PAN-OS. Pour plus d’informations sur ces commandes, consultez le Guide de mise en route de la CLI PAN-OS 11.0.

- clear high-availability
- create wildfire api-key
- delete high-availability-key
- delete wildfire api-key
- delete wildfire-metadata
- disable wildfire
- edit wildfire api-key
- load wildfire api-key
- request cluster decommission
- request cluster reboot-local-node
- request high-availability state
- request high-availability sync-to-remote
- request system raid
- request wildfire sample redistribution
- request system wildfire-vm-image
- request wf-content
- save wildfire api-key
- set wildfire portal-admin
- show cluster all-peers
- show cluster controller
- show cluster membership
- show cluster task
- show cluster data migration status
- show high-availability all
- show high-availability control-link

- show high-availability state
- show high-availability transitions
- show system raid
- show wildfire
- show wildfire global
- show wildfire local
- submit wildfire local-verdict-change
- test wildfire registration

clear high-availability

Description

Effacez les statistiques sur les liaisons de contrôle High-Availability (haute disponibilité ; HA) et les statistiques sur les transitions du nœud de contrôle d’un cluster d'appareils WildFire.

Syntaxe

```
créer { high-availability { control-link { statistics; }
 transitions; } }
```

Options

`> control-link>` : effacez les statistiques sur les liaisons de contrôle HA.

`> transitions>` : effacez les statistiques sur les transitions HA (événements qui surviennent lors des basculements HA).

Exemple de résultat

Après avoir effacé les statistiques sur les transitions ou sur les liaisons de contrôle, le cluster d’appareils WildFire remet toutes les valeurs à zéro (0).

```
admin@wf-500(active-controller)> afficher les statistiques de liaison
 de contrôle haute disponibilité Haute disponibilité : Statistiques
 de liaison de contrôle : HA1 : Messages-TX : 0 Messages-RX : 0
 Capacité-Msg-TX : 0 Capacité-Msg-RX : 0 Error-Msg-TX : 0 Error-
Msg-RX : 0 Preempt-Msg-TX : 0 Preempt-Msg-RX : 0 Preempt-Ack-Msg-
TX : 0 Preempt-Ack-Msg-RX : 0 Primary-Msg-TX : 0 Primary-Msg-RX :
 0 Primary-Ack-Msg-TX : 0 Primary-Ack-Msg-RX : 0 Hello-Msg-TX : 0
 Hello-Msg-RX : 0 Hello-Timeouts : 0 Hello-Failures : 0 MasterKey-
Msg-TX : 0 MasterKey-Msg-RX : 0 MasterKey-Ack-Msg-TX : 0 MasterKey-
Ack-Msg-RX : 0 Connection-Failures : 0 Connection-Tries-Failures :
 0 Connection-Listener-Tries : 0 Connection-Active-Tries : 0 Ping-
TX : 0 Ping-Fail-TX : 0 Ping-RX : 0 Ping-Timeouts : 0 Ping-Failures :
 0 Ping-Error-Msgs : 0 Ping-Autres-Msgs : 0 Ping-Last-Rsp : 0
 admin@wf-500(contrôleur actif)> afficher les transitions haute
 disponibilité Haute disponibilité : Statistiques de transition :
```



```
 Inconnu : 0 Suspendu : 0 Initial : 0 Non-Fonctionnel : 0 Passif 0
 Actif 0
```

Niveau de privilège requis

superuser, deviceadmin

create wildfire api-key

Description

Générez des clés API sur un appareil WildFire que vous utiliserez sur un système externe pour soumettre des échantillons à l’appareil, pour rechercher des rapports ou pour récupérer des échantillons et des Packet Captures (captures de paquets ; PCAP) de l'appareil.

Syntaxe

```
créer { wildfire { api-key { key <value>; name <value>; { { {
```

Options

+ `key` : créez une clé API en saisissant manuellement une valeur de clé. La valeur doit être composée de caractères (a-z) ou chiffres (0-9) 64 bits. Si vous ne précisez pas l'option key, l'appareil génère automatiquement une clé.

+ `name` : donnez éventuellement un nom à la clé API. Le nom de clé API est simplement utilisé pour étiqueter les clés afin de simplifier l'identification des clés affectées à des utilisations spécifiques et n'a aucun effet sur la fonctionnalité de la clé.

Exemple de résultat

La sortie suivante montre que l'appareil comporte trois clés API et qu'une clé est nommée `ma-clé-api`.

```
admin@WF-500> afficher toutes less clés api wildfire global
 +-----------------------------------------------------+------------+
 | Apikey | Name |
 +-----------------------------------------------------
+------------+ | <API KEY> | my-api-key | | <API
 KEY> | my-api-key | | <API KEY> | my-api-key |
 +-----------------------------------------------------+------------
+ +---------+--------------------+--------------------+ | Etat
 | Heure de création | Heure dernière utilisation | +---------
+--------------------+--------------------+ | Activé | 2017-03-02
 19:14:36 | 2017-03-02 19:14:36 | | Activé | 2016-02-06 12:13:22 |
 2017-03-01 12:10:20 | | Enabled | 2014-08-04 17:00:42 | 2017-03-01
 11:12:52 | +---------+--------------------+--------------------+
```

Niveau de privilège requis

superuser, deviceadmin

delete high-availability-key

Description

Supprimez la clé de chiffrement de l’homologue utilisée pour la High Availability (haute disponibilité ; HA) sur les liaisons de contrôle du cluster du nœud contrôleur du cluster d'appareils WildFire.

Syntaxe

```
supprimer { high-availability-key; }
```

Options

No additional options.

Exemple de résultat

La ligne surlignée de l'exemple de résultat indique que le chiffrement n'est pas activé sur les liaisons de contrôle HA.

```
admin@wf-500(contrôleur actif)> afficher l’état high-availability
 Haute disponibilité : Informations locales : Version : 1
 État: contrôleur actif (1 derniers jours) Informations sur le
 périphérique: Adresse IPv4 de gestion : 10.10.10.14/24 Adresse
 IPv6 de gestion : Configuration conjointe des liaisons de contrôle
 HA1 :  Chiffrement activé : aucune information sur l’option de
 choix : Priorité : préemption primaire : pas de compatibilité de
 version : Version du logiciel : Faites correspondre la compatibilité
 du contenu de l'application : Faites correspondre la compatibilité
 antivirus : Correspondance des informations sur les pairs :
 Etat de la connexion : up Version : 1 État : contrôleur passif
 (derniers 1 jours) Informations sur l'appareil : Adresse IPv4
 de gestion : 10.10.20.112/24 Adresse IPv6 de gestion : Connexion
 en place ; Informations sur l'option d'élection du lien HA1
 principal : Priorité : secondaire Préemptif : non Configuration
 Synchronisation : Activé : oui Configuration en cours d'exécution :
 synchronisé
```

Niveau de privilège requis

superuser, deviceadmin

delete wildfire api-key

Description

Supprimez une clé API de l'appareil WildFire. Les systèmes configurés pour utiliser l'API afin d'exécuter des fonctions d'API sur l'appareil ne pourront plus accéder à l'appareil lorsque vous supprimez la clé.

Syntaxe

```
supprimer { wildfire { api-key { key <value>; { { {
```

Options

`+ key <value>` : la valeur de la clé que vous voulez supprimer. Pour afficher une liste des clés API, exécutez la commande suivante :

```
admin@WF-500> afficher toutes les clés api wildfire global
```

Exemple de résultat

```
admin@WF-500> supprimer la clé wildfire api-key <API KEY> Clé API
 <API Key> supprimé
```

Niveau de privilège requis

superuser, deviceadmin

delete wildfire-metadata

Description

Supprimez des mises à jour de contenu sur l'appareil WildFire. Pour plus d'informations sur les mises à jour de contenu et sur leur installation, reportez-vous à la section request wf-content.

Syntaxe

```
supprimer { wildfire-metadata update <value>; {
```

Options

`+ update <value>` : définissez la mise à jour de contenu que vous souhaitez supprimer.

Exemple de résultat

Le résultat suivant montre la suppression d'une mise à jour nommée :

```
panup-all-wfmeta-2-181.candidate.tgz. admin@WF-500> supprimer la mise
 à jour des métadonnées wildfire panup-all-wfmeta-2-181.candidate.tgz
 supprimé avec succès panup-all-wfmeta-2-181.candidate.tgz
```

Niveau de privilège requis

superuser, deviceadmin

disable wildfire

Description

Désactive la signature de domaine ou la signature d’échantillon pour l’exclure de la prochaine version de contenu de WildFire.

Syntaxe

```
désactiver wildfire { domain-signature { domain <value>; } OU...
 sample-signature { sha256 { equal <value>; } }
```

Options

`> domain-signature` : désactive la signature de domaine pour l’exclure de la prochaine version de contenu de WildFire.

`> sample-signature` : désactive la signature d’échantillon pour l’exclure de la prochaine version de contenu de WildFire.

Exemple de résultat

Un échantillon ou un domaine qui a été désactivé ne produit aucun résultat.

```
admin@WF-500> désactiver la signature d’échantillon wildfire sha256
 égal à
 d1378bda0672de58d95f3bff3cb42385f2d806a4a15b89cdecfedbdb1ec08228
```

Niveau de privilège requis

superuser, deviceadmin

edit wildfire api-key

Description

Modifiez un nom de clé API ou l'état de la clé (activée/désactivée) sur un appareil WildFire.

Syntaxe

```
modifier{ wildfire { api-key [nom | état] key <value>; { {
```

Options

`+ name` : renommer une clé API.

`+ status` : activer ou désactiver une clé API.

`* key` : spécifier la clé à modifier.

Exemple de résultat

La valeur de clé est requise dans cette commande. Par exemple, pour renommer la clé `stu` en `stu-key1`, saisissez la commande suivante :

Dans la commande suivante, vous n'avez pas besoin de saisir l'ancien nom de clé ; saisissez simplement le nouveau.

```
admin@WF-500> modifier le nom de la clé api wildfire stu-
key1 clé <API KEY> Pour modifier l’état de stu-key1 sur
 désactivé, entrez la commande suivante : admin@WF-500> modifier
 l’état de la clé api wildfire désactiver la clé <API KEY>
 Exemple de sortie indiquant que stu-key1 est désactivé :
 admin@WF-500> afficher toutes les clés api globales wildfire
 +-----------------------------------------------------+------------+
 | | Apikey Nom |
 +-----------------------------------------------------+------------+
 | <API KEY> | stu-key1 |
 +-----------------------------------------------------+------------
+ +----------+---------------------+---------------------+ |
 État | Créer des | de temps Dernière | de temps d’utilisation
 +----------+---------------------+---------------------+ | |
 Désactivé 2017-03-02 19:14:36 | 2017-03-02 19:14:36 | +----------
+---------------------+---------------------+
```

Niveau de privilège requis

superuser, deviceadmin

load wildfire api-key

Description

Après l'importation de clés API sur l'appareil WildFire, vous devez utiliser la commande load pour que les clés puissent être utilisées. Utilisez cette commande pour remplacer toutes les clés API existantes. Vous pouvez également fusionner les clés du fichier importé avec la base de données de clés existante.

Syntaxe

```
charger { wildfire { from <value> mode [fusionner | remplacer]; { {
```

Options

* `from` : spécifiez le nom du fichier de clés API que vous souhaitez importer. Les fichiers de clés portent l'extension .keys. Par exemple, mes-clés-api.keys. Pour afficher la liste des clés pouvant être importées, saisissez la commande suivante :

```
admin@WF-500> charger la clé API wildfire à partir de ?
```


`+ mode` : (Facultatif) Passez en mode d'importation (merge/replace). Par exemple, pour remplacer la base de données de clés sur l'appareil par le contenu du nouveau fichier de clés, saisissez la commande suivante :

```
admin@WF-500> charger le remplacement du mode clé api wildfire à
 partir de my-api-keys.keys
```

Si vous ne spécifiez pas l'option **mode**, l'action par défaut fusionnera les nouvelles clés.

Niveau de privilège requis

superuser, deviceadmin

request cluster decommission

Description

Supprimez un nœud d’un cluster d’appareils WildFire qui possède trois nœuds ou plus. N’utilisez pas cette commande pour supprimer un nœud d’un cluster à deux nœuds. Au lieu, effectuez la suppression locale d’un nœud d’un cluster au moyen des commandes `delete deviceconfig high-availability` et `delete deviceconfig cluster`.

Emplacement de la hiérarchie

request cluster

Syntaxe

```
demande { cluster { decommission { show; start; stop; } } }
```

Options

`Show` : affichez l’état de la tâche de mise hors service du nœud.

`start` : commencez la mise hors service du nœud.

`stop` : interrompez la mise hors service du nœud.

Exemple de résultat

Le champ `Node mode` confirme la mise hors service du nœud du cluster, car le mode indiqué est `stand_alone` plutôt que `controller` ou `worker`.

```
admin@wf-500> afficher l’appartenance au cluster Résumé du service :
 signature wfpc Nom du cluster : Address (Adresse) : 10.10.10.86
 Nom d’hôte : wf-500 Nom du nœud : wfpc-009707000xxx-numéro
 de série interne : 009707000xxx Mode nœud : stand_alone rôle
 serveur : Véritable priorité HA : Dernière modification : Mer,
 15 Feb 2017 00:05:11 -0800 Services: wfcore signature wfpc infra
 État du moniteur: État de santé du serf: passage de l’agent
 vivant et accessible État de l’application: wildfire-apps-
```



```
service: Prêt global-db-service : Service de file d’attente global
 ReadyStandalone : ReadyStandalone local-db-service: ReadyMaster
```

Niveau de privilège requis

superuser, deviceadmin

request cluster reboot-local-node

Description

Redémarrez doucement le nœud local du cluster WildFire.

Emplacement de la hiérarchie

```
request cluster
```

Syntaxe

```
demande { cluster { reboot-local-node ; } }
```

Options

No additional options.

Exemple de résultat

Il existe plusieurs façons de vérifier que le nœud local du cluster a redémarré ou qu’il est en train de redémarrer :

- `show cluster task local` : affichez les tâches demandées sur le nœud local.
- `show cluster task current` : affichez les tâches en cours d’exécution sur le nœud local ou la dernière tâche effectuée (nœuds de contrôle uniquement).
- `show cluster task pending` : affichez les tâches de la file d’attente qui n’ont pas encore été exécutées sur le nœud local (controller nodes only).
- `show cluster task history` : affichez les tâches qui ont été exécutées sur le nœud local (nœuds de contrôle uniquement).

Par exemple, la commande suivante montre que les tâches de redémarrage du cluster à deux nœuds ont été terminées avec succès :

```
admin@qa15(passive-controller)> afficher l’historique des tâches du
 cluster Demande :        redémarrer depuis qa16 (009701000044/35533)
 à 2017-02-17 19:21:53 UTC                Redémarrage demandé par
 l’admin Réponse:       autorisé par qa15 à 2017-02-17 22:11:31 UTC
                demande n’affectant pas le serveur principal sain.
 Progression:        Attendez que le magasin kv soit prêt pour la
 requête...                Le magasin KV est prêt, attendez que le
 cluster de tête soit disponible...                Le cluster de
```



```
 tête est 2.2.2.16...                  La vérification est que sysd
 et clusterd sont actifs ...                  Vérification si cluster-
mgr est prêt...                Vérification de la préparation
 du cluster global-db...                  Arrêt du serveur de file
 d'attente globale et sortie du cluster...                  Arrêt des
 serveurs global-db et basculement... redémarrage... Terminé : succès
 au 2017-02-17 22:17:56 UTC Demande : redémarrage à partir de qa16
 (009701000044/35535) au 2017-02-17 22:45:50 UTC Redémarrage demandé
 par l'administrateur Réponse : autorisation de qa15 au 2017-02 -17
 23:06:44 La demande UTC n'affecte pas le serveur principal sain.
 Progression:        Attendez que le magasin kv soit prêt pour la
 requête...                Le magasin KV est prêt, attendez que le
 cluster de tête soit disponible...                 Le cluster de
 tête est 2.2.2.15...                  La vérification est que sysd
 et clusterd sont actifs ...                  Vérification si cluster-
mgr est prêt...                Vérification de la préparation
 du cluster global-db...                  Arrêt du serveur de file
 d'attente globale et sortie du cluster...                  Arrêt des
 serveurs global-db et basculement... redémarrage... Terminé : succès
 le 2017-02-17 23:12:53 UTC
```

Niveau de privilège requis

superuser, deviceadmin

request high-availability state

Description

Sur un cluster d'appareils WildFire, rendez l’état High Availability (haute disponibilité ; HA) du nœud de contrôle local ou homologue fonctionnel.

Emplacement de la hiérarchie

```
request high-availability
```

Syntaxe

```
demande { high-availability { state { functional; } pair {
 functional; } } }
```

Options

> `functional` : rendez fonctionnel l’état HA du nœud de contrôle local.

> `peer` : rendez fonctionnel l’état HA du nœud de contrôle homologue.

Exemple de résultat

Les lignes surlignées de l'exemple de résultat indiquent que l’état HA du nœud de contrôle local est fonctionnel dans le rôle de contrôleur actif (principal) et que l’état HA du nœud de contrôle homologue est fonctionnel dans le rôle de contrôleur passif (de secours).


```
admin@wf-500(active-controller)> afficher l'état high-disponibility
 Haute disponibilité : Informations locales : Version : 1 État :
 contrôleur actif (derniers 1 jours) Informations sur l'appareil :
 Adresse IPv4 de gestion : 10.10.10.14/24 Adresse IPv6 de
 gestion : Configuration conjointe des liaisons de contrôle HA1 :
 Chiffrement activé : aucune information sur l'option de choix
 Priorité : préemption primaire : pas de compatibilité de version :
 Version du logiciel : Faites correspondre la compatibilité du
 contenu de l'application : Faites correspondre la compatibilité
 antivirus : Correspondance des informations sur les pairs :
 Etat de la connexion : up Version : 1 État : contrôleur passif
 (derniers 1 jours) Informations sur l'appareil : Adresse IPv4
 de gestion : 10.10.20.112/24 Adresse IPv6 de gestion : Connexion
 en place ; Informations sur l'option d'élection du lien HA1
 principal : Priorité : secondaire Préemptif : non Configuration
 Synchronisation : Activé : oui Configuration en cours d'exécution :
 synchronisé
```

Niveau de privilège requis

superuser, deviceadmin

request high-availability sync-to-remote

Description

Sur un cluster d'appareils WildFire, synchronisez la configuration active ou la configuration candidate du nœud de contrôle local, ou l’horloge (date et heure) du nœud de contrôle local avec le nœud de contrôle homologue High-Availability (haute disponibilité ; HA).

Emplacement de la hiérarchie

request high-availability

Syntaxe

```
demande { high-availability { sync-to-remote { candidate-config;
 clock; running-config; } } }
```

Options

`> candidate-config` : synchronisez la configuration candidate du nœud de contrôle homologue local avec le nœud de contrôle homologue HA distant.

`> candidate-config` : synchronisez l’horloge (heure et date) du nœud de contrôle homologue local avec le nœud de contrôle homologue HA distant.

`> running-config` : synchronisez la configuration active du nœud de contrôle homologue local avec le nœud de contrôle homologue HA distant.

Exemple de résultat

La ligne surlignée de l'exemple de résultat indique que l’état de la configuration HA est synchronisé sur le nœud de contrôle homologue HA.

```
admin@wf-500(active-controller)> afficher l'état high-disponibility
 Haute disponibilité : Informations locales : Version : 1
 État: contrôleur actif (1 derniers jours) Informations sur le
 périphérique: Adresse IPv4 de gestion : 10.10.10.14/24 Adresse
 IPv6 de gestion : Configuration conjointe des liaisons de contrôle
 HA1 : Chiffrement activé : aucune information sur l'option de choix
 Priorité : préemption primaire : pas de compatibilité de version :
 Version du logiciel : Faites correspondre la compatibilité du
 contenu de l'application : Faites correspondre la compatibilité
 antivirus : Correspondance des informations sur les pairs :
 Etat de la connexion : up Version : 1 État : contrôleur passif
 (derniers 1 jours) Informations sur l'appareil : Adresse IPv4
 de gestion : 10.10.20.112/24 Adresse IPv6 de gestion : Connexion
 en place ; Informations sur l'option d'élection du lien HA1
 principal : Priorité : secondaire Préemptif : non Configuration
 Synchronisation : Activé : oui Configuration en cours d'exécution :
 synchronisé
```

Niveau de privilège requis

superuser, deviceadmin

request system raid

Description

Cette option vous permet de gérer les paires'A0;RAID installées sur l'appareil'A0;WildFire.
L'appareil WF-500 est fourni avec quatre lecteurs ; ces derniers se trouvent dans les quatre premières baies de lecteur (A1, A2, B1 et B2). Les lecteurs'A0;A1 et A2 sont une paire RAID'A0;1, et les lecteurs'A0;B1 et B3 sont une seconde paire RAID'A0;1.

Emplacement de la hiérarchie

request system

Syntaxe

```
raid { remove <value>; OR... copy { from <value>; to <value>; } OR...
 add {
```

Options

- `add` : ajoutez un lecteur à la paire de disques RAID correspondante.
- `copy` : copiez et migrez les données d’un lecteur à un autre lecteur du logement.
- `remove` : lecteur à supprimer de la paire de disques RAID.

Exemple de résultat

Le résultat suivant indique un appareil WF-500 doté d'un RAID correctement configuré.

```
admin@WF-500> afficher le raid du système Paire de disques A Id
 de disque disponible A1 Id de disque présent A2 Présent Paire
 de disques B Id de disque disponible B1 Présent ID de disque B2
 Présent
```

Niveau de privilège requis

superuser, deviceadmin

request wildfire sample redistribution

Description

Redistribuez les échantillons du nœud du cluster d'appareils WildFire local vers un autre nœud du cluster tout en conservant éventuellement des échantillons sur le nœud local.

Emplacement de la hiérarchie

```
request system
```

Syntaxe

```
demande { wildfire { sample { redistribution {   keep-local-copy {oui
 | non};   numéro de série <value>; } } } }
```

Options

* `keep-local-copy` : conservez, ou non, une copie des échantillons redistribués sur le nœud de l’appareil WildFire local.

* `serial-number` : numéro de série du nœud auquel vous avez redistribué les échantillons.

Exemple de résultat

`Storage Nodes` affiche l’autre nœud auquel le nœud local redistribue les échantillons. Si le nœud local ne redistribue par d’échantillons, l’emplacement d’un seul nœud de stockage s'affiche. Si le noeud local redistribue les échantillons, `Storage Nodes` indique deux emplacements de stockage. Les lignes surlignées de l'exemple de résultat indiquent deux nœuds de stockage qui stockent les échantillons (le nœud local et le nœud vers lequel le nœud local redistribue les échantillons) et vérifient que la redistribution des échantillons s’effectue.

```
admin@WF-500> afficher l'analyse globale des échantillons
 wildfire Dernière création de 100 échantillons
 malveillants +------------------------------
 ----------------------------------------+ |
 SHA256 | Date de fin | Date de création | Malicieux |
```



```
+------------------------------------------------------------
--------------------+ | <HASH VALUE> | 2017-03-24 17:27:40 |
2017-03-24 15:41:47 | Oui | | <HASH VALUE> | 2017-03-24 17:26:46
| 2017-03-24 15:41:45 | Oui | | <HASH VALUE> | 2017-03-24
17:26:54 | 2017-03-24 15:41:45 | Oui | | <HASH VALUE> |
2017-03-24 17:25:12 | 2017-03-24 15:41:44 | Oui | | <HASH VALUE>
| 2017-03-24 17:24:28 | 2017-03-24 15:41:44 | Oui | | <HASH
VALUE> | 2017-03-24 17:23:58 | 2017-03-24 15:41:44 | Oui | |
<HASH VALUE> | 2017-03-24 17:26:52 | 2017-03-24 14:55:23 | Oui |
| <HASH VALUE> | 2017-03-24 17:23:32 | 2017-03-24 14:55:23 | Oui
| | <HASH VALUE> | 2017-03-24 17:24:58 | 2017-03-24 14:55:23 | Oui
| | <HASH VALUE> | 2017-03-24 17:22:02 | 2017-03-24 14:55:23 | Oui
| +------------------------------------------------------------
--------------------+ +--------------------------------
----------------------------------------+ | Nœuds de
stockage | Nœuds d'analyse | Statut | Type de fichier |
+------------------------------------------------------------
-------------------+ | 0907:ld2_2,065:ld2_2 | qa116 | Notifier
Terminer | JAR Java | | 0097:ld2_2,004:ld2_2 | qa117 | Notifier
Terminer | Classe Java | | 0524:ld2_2,006:ld2_2 | qa117 | Notifier
Terminer | Classe Java | | 0656:ld2_2,524:ld2_2 | qa117 | Notifier
Terminer | Classe Java | | 0024:ld2_2,056:ld2_2 | qa117 | Notifier
Terminer | DLL | | 0324:ld2_2,006:ld2_2 | qa117 | Notifier Terminer
| JAR Java | | 0682:ld2_2,006:ld2_2 | qa116 | Notifier Terminer
| JAR Java | | 0092:ld2_2,016:ld2_2 | qa116 | Notifier Terminer
| DLL | | 0682:ld2_2,002:ld2_2 | qa116 | Notifier Terminer |
DLL | | 0056:ld2_2,824:ld2_2 | qa117 | Notifier Terminer | DLL
| +------------------------------------------------------------
--------------------* lignes 1-10
```

Niveau de privilège requis

superuser, deviceadmin

request system wildfire-vm-image

Procédez à des mises à niveau sur les images de bac à sable de Virtual Machine (machine virtuelle ; MV) de l'appareil WildFire utilisées pour analyser les fichiers. Pour récupérer de nouvelles images MV du serveur de mises à jour de Palo Alto Networks, vous devez tout d'abord télécharger l'image manuellement, l'héberger sur un serveur SCP, puis récupérer l'image sur l'appareil à l'aide du client SCP. Une fois l'image téléchargée sur l'appareil, vous pouvez l'installer à l'aide de cette commande.

Emplacement de la hiérarchie

request system

Syntaxe

```
demande { system { wildfire-vm-image { upgrade install file
 <value>; } } }
```


Options

`> wildfire-vm-image` : installez des images de Virtual Machine (machine virtuelle ; MV).

`+ upgrade install file` : procédez à une mise à niveau vers l'image MV. Après l'option file, saisissez `?` pour afficher la liste des images MV disponibles. Par exemple, exécutez la commande suivante pour répertorier les images disponibles :

```
admin@WF-500> demande le fichier d'installation de mise à niveau du
 système wildfire-vm-image ?
```

Exemple de résultat

Pour obtenir la liste des images MV disponibles, exécutez la commande suivante :

```
admin@WF-500> demande le fichier d'installation de mise à niveau
 du système wildfire-vm-image ? Pour installer une image de machine
 virtuelle (Windows 7 64-bits dans cet exemple), exécutez la commande
 suivante : admin@WF-500> request system wildfire-vm-image upgrade
 install file WFWin7_64Base_m-1.0.0_64base
```

Niveau de privilège requis

superuser, deviceadmin

request wf-content

Procédez à des mises à jour de contenu sur un appareil WildFire. Ces mises à jour de contenu fournissent à l'appareil les toutes dernières informations sur les menaces afin de détecter précisément les logiciels malveillants et d'améliorer la capacité de l'appareil à différencier les logiciels malveillants et bénins. Pour planifier l'installation automatique des mises à jour de contenu, consultez set deviceconfig system update-schedule et delete wildfire-metadata pour la suppression de mises à jour de contenu sur l'appareil WildFire.

Emplacement de la hiérarchie

```
demande
```

Syntaxe

```
demande wf-content { downgrade install {previous | <value>}; mettre
 à niveau { check download latest info install { file <filename>
 version latest; } } }
```

Options

`> downgrade` — Installer une version de contenu précédente Utilisez l'option previous pour installer le package de contenu précédemment installé ou saisissez une valeur de mise à niveau antérieure vers un numéro de package de contenu spécifique.

`> upgrade` — Exécuter des fonctions de mise à niveau de contenu

`> check` — Obtenir des informations sur les packages de contenu disponibles sur le serveur de mises à jour de Palo Alto Networks

`> download` — Télécharger un package de contenu

`> info` — Afficher des informations sur les packages de contenu disponibles

`> install` — Installer un package de contenu

`> file` — Spécifier le nom du fichier contenant le package de contenu

`> version` — Télécharger ou mettre à niveau en fonction du numéro de version du package de contenu

Exemple de résultat

Pour obtenir la liste des mises à jour de contenu disponibles, exécutez la commande suivante :

```
admin@WF-500> demande de vérification de la mise à
 niveau de wf-content Taille de la version Publié le
 Téléchargé Installé -------------------------------
 ---------------------------------------- 2-217 58 Mo 2014/07/29
 13:04:55 PDT oui actuel 2-188 58 Mo 2014/07/01 13:04:48 PDT oui
 précédent 2-221 59 Mo 2014/08/02 13:04:55 PDT non non
```

Niveau de privilège requis

superuser, deviceadmin

save wildfire api-key

Description

Utilisez la commande save pour enregistrer toutes les clés API sur l'appareil WildFire dans un fichier. Vous pouvez ensuite exporter le fichier de clés à des fins de sauvegarde ou pour modifier les clés par lot. Pour plus de détails sur l'utilisation de l'API WildFire sur un appareil WildFire, reportez-vous au Guide de référence de l'API WildFire.

Emplacement de la hiérarchie

```
enregistrer
```

Syntaxe

```
enregistrer { wildfire { api-key to <value>; { {
```

Options

`* to` — Entez le nom du fichier d'exportation de clé. Par exemple, pour exporter toutes les clés API sur l’appareil WildFire dans un fichier nommé mes-clés-wf, saisissez la commande suivante :


```
admin@WF-500> enregistrer la clé API Wildfire dans my-wf-keys
```

Niveau de privilège requis

superuser, deviceadmin

set wildfire portal-admin

Description

Définit le mot de passe du compte d'administrateur qu'un administrateur utilisera pour afficher les rapports d'analyse WildFire générés par un appareil WildFire. Le nom du compte (admin) et le mot de passe sont requis lors de l'affichage du rapport sur le pare-feu ou à partir de Panorama dans **Monitor (Surveillance)** > **WildFire Submissions (Envois WildFire)** > **View WildFire Report (Afficher le rapport WildFire)**. Le nom d'utilisateur et le mot de passe par défaut est admin/admin.

Le compte Admin du portail est le seul compte que vous pouvez configurer sur l'appareil pour afficher les rapports à partir de l'appareil ou du Panorama. Vous ne pouvez pas créer de nouveaux comptes ou renommer le compte. Ce compte Admin est différent de celui utilisé pour gérer l'appareil.

Emplacement de la hiérarchie

```
Modifier wildfire
```

Syntaxe

```
définir { wildfire { portal-admin { password <value>; } }
```

Exemple de résultat

Vous trouverez ci-dessous le résultat de cette commande.

```
admin@WF-500> définir le mot de passe de l'administrateur du portail
 Wildfire Entrez le mot de passe : Confirmez le mot de passe :
```

Niveau de privilège requis

superuser, deviceadmin

show cluster all-peers

Description

Permet d'afficher sur le nœud de contrôle du cluster d'appareils WildFire l’état de tous les membres du cluster d'appareils WildFire, y compris le mode de l’appareil WildFire (contrôleur ou travailleur), l’état de la connexion et l’état de service de l’application.

Emplacement de la hiérarchie

```
afficher le cluster
```

Syntaxe

```
tous les pairs ;
```

Options

No additional options.

Exemple de résultat

```
admin@thing1(active-controller)> afficher tous les pairs du cluster
 Adresse Mode Serveur Noeud Nom ------- ---- ------ ---------
 10.10.10.14    contrôleur Auto Réel thing1 Service: infra signature
 wfcore wfpc Etat : Connecté, rôle de serveur appliqué Modifié :
 Wed, 15 Feb 2017 09:12:01 -0800 WF App: wildfire-apps-service: Prêt
 global-db-service : Service de file d'attente global JoinedCluster :
 JoinedCluster siggen-db : ReadyMaster 10.10.10.112   contrôleur
 Pair Réel thing2 Service: infra signature wfcore wfpc Etat :
 Connecté, rôle de serveur appliqué Modifié : Wed, 15 Feb 2017
 09:13:00 -0800 WF App: wildfire-apps-service: Prêt global-db-
service : Service de file d'attente global ReadyLeader : ReadyLeader
 siggen-db : ReadySlave Diag report: 10.10.10.112: reported leader
 '10.10.10.112', age 0. 10.10.10.14: le nœud local a réussi la
 vérification de santé
```

Niveau de privilège requis

superuser, deviceadmin

show cluster controller

Description

Sur un nœud de contrôle d’un cluster d'appareils WildFire, affiche l’état des contrôleurs du cluster d’appareils WildFire, y compris le nom du cluster et le rôle du nœud de contrôle local (si le champ `Active Controller` affiche `True`, le contrôleur local est le contrôleur principal, si le champ `Active Controller` affiche `False`, le contrôleur local est le contrôleur de secours).

Emplacement de la hiérarchie

```
afficher le cluster
```


Syntaxe

```
contrôleur;
```

Options

No additional options.

Exemple de résultat

```
admin@thing1(active-controller)> afficher le contrôleur du cluster
 Nom du cluster : satriani1 K/V API online : Traitement des tâches
 réelles : sur Contrôleur actif Publicité DNS réelle : Nom DNS d’App
 Service : App Service Disponible : Serveurs principaux 10.10.10.112,
 10.10.10.14 : 009707000742: 10.10.10.112 009701000043 10.10.10.14
 Serveurs principaux bons: 2 nœuds suspendus : Tâche en cours :
 aucune tâche trouvée
```

Niveau de privilège requis

superuser, deviceadmin

show cluster data migration status

Description

Utilisez cette commande à partir d’un nœud de contrôle du cluster d’appareils WildFire pour afficher l’état de la migration de données qui est en cours. La commande affiche le moment où la migration de données a commencé et son progrès. Lorsque la migration de données est terminée, la commande affiche l’horodatage d’achèvement. En cas d’échec de la migration de données, l’état affichera `0% completed`.

Emplacement de la hiérarchie

```
afficher le cluster
```

Syntaxe

```
État de migration des données ;
```

Options

No additional options.

Exemple de résultat

```
adminWF-500(active-controller)> afficher l’état de la migration des
 données du cluster 100% completed on Mon Sep 9 21:44:48 PDT 2019
```


Niveau de privilège requis

superuser, deviceadmin

show cluster membership

Description

Affichez les renseignements sur l’appartenance d’un nœud de cluster ou d’un appareil WildFire autonome à un cluster d'appareils WildFire, notamment l’adresse IP, le nom d’hôte le numéro de série de l’appareil WildFire, le rôle de l’appareil (`Node mode`), la priorité de haute disponibilité et l’état de l’application.

Emplacement de la hiérarchie

```
afficher le cluster
```

Syntaxe

```
appartenance ;
```

Options

No additional options.

Exemple de résultat

Vous pouvez afficher les renseignements sur l’appartenance des nœuds membres d’un cluster d'appareils WildFire (nœuds de contrôle et nœuds esclaves) et des appareils WildFire autonomes pour vérifier leur appartenance, ou non, à un cluster, leur état d’application et les autres renseignements sur l’hôte local. Le résultat diffère légèrement selon le rôle de l’appareil WildFire. Voici les différences :

- L’invite indique le nœud de contrôle actif (principal) et le nœud de contrôle passif (de secours), mais n’indique pas le rôle s’il s'agit d’un nœud esclave ou d’appareil autonome.
- Le `Node mode` indique si l’appareil WildFire est un nœud de contrôle (`controller node`), un nœud esclave (`worker node`) ou un appareil WildFire autonome (`stand_alone`).
- `HA priority` affiche `primary` pour le nœud de contrôle actif, `secondary` pour le nœud de contrôle passif (de secours), et le champ est vide pour les nœuds esclaves et les appareils WildFire autonomes.
- Les champs `Application status` affichent des valeurs différentes, selon les champs. Dans les champs `global-db-service` et `global-queue-service`, `ReadyLeader` ou `JoinedCluster` s’affichera pour les membres du cluster et `ReadyStandalone` s’affichera pour les appareils autonomes.

  Dans le champ `siggen-db`, `ReadyMaster` s'affichera pour le nœud de contrôle principal du cluster d'appareils WildFire, `ReadySlave` s’affichera pour le nœud de contrôle secondaire du cluster

d'appareils WildFire, `Ready` s’affichera pour les nœuds esclaves du cluster d'appareils WildFire et `ReadyMaster` s’affichera pour les appareils WildFire autonomes.

Pour éviter de dévoiler les vrais numéros de série, les quatre derniers chiffres du numéro de série de chaque appareil WildFire sont remplacés par « xxxx » à l’écran.

Résultat obtenu sur le nœud de contrôle principal d’un cluster d'appareils WildFire :

```
admin@thing1(active-controller)> afficher l'appartenance au
 cluster Résumé du service : wfpc signature Nom du cluster :
 satriani1 Adresse : 10.10.10.14 Nom de l’hôte: thing1 Nom du
 nœud: wfpc-00970100xxxx-internal Numéro de série : 00970100xxxx
 Mode nœud : contrôleur Rôle serveur : Véritable priorité HA :
 primaire Dernière modification : Mer, 15 février 2017 09:12:01
 -0800 Services : wfcore signature wfpc infra État du moniteur : État
 de santé de Serf : passage de l'agent actif et accessible État de
 l'application : wildfire-apps-service : Prêt global-db-service :
 Service de file d'attente global JoinedCluster : JoinedCluster
 siggen-db : ReadyMaster
```

Résultat obtenu sur le nœud de contrôle de secours d’un cluster d'appareils WildFire :

```
admin@thing2(passive-controller)> afficher l'appartenance au
 cluster Résumé du service : wfpc signature Nom du cluster :
 satriani1 Adresse : 10.10.10.112 Nom d'hôte : thing2 Nom de nœud :
 wfpc-00970700xxxx-internal Numéro de série : 009707000xxxx Mode
 nœud : contrôleur Rôle serveur : Véritable priorité HA : secondaire
 Dernière modification : Mer, 15 février 2017 09:13:10 -0800
 Services : wfcore signature wfpc infra État du moniteur : État
 de santé de Serf : passage de l'agent actif et accessible État de
 l'application : wildfire-apps-service : Prêt global-db-service :
 Service de file d'attente global ReadyLeader : ReadyLeader siggen-
db : ReadySlave
```

Résultat obtenu sur le nœud esclave d’un cluster d'appareils WildFire :

```
admin@grinch> afficher l'appartenance au cluster Résumé du service :
 wfpc Nom du cluster : satriani1 Adresse : 10.10.10.19 Nom d'hôte :
 grinch Nom du nœud : wfpc-00970100xxxx-internal Numéro de série :
 00970100xxxx Mode nœud :  Rôle serveur esclave : Véritable
 priorité HA : Dernière modification : Jeu, 09 février 2017 15:55:55
 -0800 Services : wfcore wfpc infra État du moniteur : État de
 santé de Serf : passage de l'agent actif et accessible État de
 l'application : wildfire-apps-service : Prêt global-db-service :
 Service de file d'attente global JoinedCluster : JoinedCluster
 siggen-db : Ready
```

Résultat obtenu sur un appareil WildFire autonome (pas un membre d’un cluster d'appareils WildFire) :

```
admin@max> affiche l'appartenance au cluster Résumé du service :
 signature wfpc Nom du cluster : Address (Adresse) : 10.10.10.90
 Nom d'hôte : max Nom de nœud : wfpc-00970700xxxx-internal Numéro
```



```
 de série : 00970700xxxx Mode nœud : stand_alone Rôle serveur :
 Véritable priorité HA : Dernière modification : Lundi 13 février
 2017 02:54:52 -0800 Services : wfcore signature wfpc infra État
 du moniteur : État de santé de Serf : passage de l'agent actif
 et accessible État de l'application : wildfire-apps-service :
 Prêt global-db-service : Service de file d'attente global
 ReadyStandalone : Siggen-db ReadyStandalone : ReadyMaster
```

Niveau de privilège requis

superuser, deviceadmin

show cluster task

Description

Affichez les renseignements sur les tâches du cluster d'appareils WildFire pour le nœud local du cluster ou pour tous les nœuds du cluster ou affichez l’historique des tâches du cluster qui ont été exécutées ou qui sont en attente.

Emplacement de la hiérarchie

```
afficher le cluster
```

Syntaxe

```
tâche { current; history; local; pending; }
```

Options

`> current` : affichez les tâches actuellement autorisées sur le cluster d'appareils WildFire. Disponible uniquement sur les nœuds de contrôle du cluster.

`> history` : affichez les tâches du cluster qui ont été exécutées. Disponible uniquement sur les nœuds de contrôle du cluster.

`> local` : affichez les tâches qui sont en attente sur le nœud local du cluster d'appareils WildFire.

`> pending` : affichez les tâches qui sont en attente sur l’ensemble du cluster d'appareils WildFire. Disponible uniquement sur les nœuds de contrôle du cluster.

Exemple de résultat

```
admin@WF-500(active-controller)> afficher cluster tâche local
 Requête : redémarrage depuis WF-500 (009701000034/74702) au
 2017-02-21 03:06:45 UTC Redémarrage demandé par l'administrateur En
 file d'attente : par WF-500 2 /3 serveurs principaux disponibles.
 redémarrage non autorisé pour maintenir le quorum Demande :
 redémarrage depuis WF-500 (009701000034/74704) au 2017-02-21
 03:10:27 UTC Redémarrage demandé par l'administrateur En file
 d'attente : par WF-500 2/3 serveurs principaux disponibles.
```



```
 redémarrage non autorisé pour maintenir le quorum admin@WF-500
 (contrôleur actif)> afficher la tâche de cluster actuelle aucune
 tâche trouvée admin@WF-500 (contrôleur actif)> afficher la tâche
 de cluster en attente Demande : redémarrer à partir de WF-500
 (009701000034/74702 ) au 2017-02-21 03:06:45 UTC Redémarrage demandé
 par l'administrateur En file d'attente : par les serveurs principaux
 WF-500 2/3 disponibles. redémarrage non autorisé pour maintenir le
 quorum Demande : redémarrage depuis WF-500 (009701000034/74704) au
 2017-02-21 03:10:27 UTC Redémarrage demandé par l'administrateur
 En file d'attente : par WF-500 2/3 serveurs principaux disponibles.
 redémarrage non autorisé pour maintenir le quorum admin@WF-500B
 (contrôleur passif)> afficher l'historique des tâches du cluster :
 permis par WF-500B au 2017-02-17 22:11:31 UTC la demande n'affecte
 pas le serveur principal sain. Progression :       Attendez
 que le magasin kv soit prêt pour la requête...
  Le magasin KV est prêt, attendez que le cluster de tête soit
 disponible...                Le cluster de tête est 10.10.10.100...
                La vérification est que sysd et clusterd sont
 actifs ...                  Vérification si cluster-mgr est prêt...
                Vérification de la préparation du cluster global-
db...                Arrêt du serveur de file d'attente globale et
 sortie du cluster...                Arrêt des serveurs global-db
 et basculement... redémarrage... Terminé : succès le 2017-02-17
 22:17:56 UTC
```

Niveau de privilège requis

superuser, deviceadmin

show high-availability all

Description

Affichez toutes les informations relatives à la High Availability (haute disponibilité ; HA) du cluster d'appareils WildFire, y compris la liaison de contrôle HA, l’état HA et les informations sur les transitions de HA, les informations sur le logiciel installé sur l’homologue, sur la mise à jour du contenu et sur la compatibilité antivirus ainsi que les informations sur la connexion et le rôle de l’homologue.

Emplacement de la hiérarchie

```
afficher tous les haute disponibilité
```

Syntaxe

```
Tous ;
```

Options

No additional options.

Exemple de résultat

```
admin@thing1(active-controller)> afficher tous les high-availability
 haute disponibilité : Informations locales : Version : 1
 État: contrôleur actif (1 derniers jours) Informations sur le
 périphérique: Adresse IPv4 de gestion : 10.10.10.14/24 Adresse IPv6
 de gestion : Configuration conjointe des liaisons de contrôle HA1 :
 Intervalle du moniteur de liaison : Cryptage 3000 ms activé : aucune
 information de liaison de contrôle HA1 : IP address: 10.10.10.140/24
 Adresse MAC: 00:00:5e:00:53:ff Interface: eth3 État du lien: Up ;
 Paramètre Clé 1Gb/s-full importée : aucune information sur l’option
 d’élection : Priorité : préemption principale : pas d’intervalle de
 suspension de promotion : Intervalle de message Hello de 2000 ms :
 Intervalle de ping de pulsation de 8000 ms: Intervalle de préemption
 de 2000 ms: Intervalle de maintien en échec du moniteur de 1 min :
 Intervalle de maintien du maître addon de 0 ms: Informations sur
 la version 500 ms : Version de build : Base de données URL 8.0.1-
c31 : Contenu de l’application non installé : 497-2688 Antivirus : 0
 Compatibilité de version: Version du logiciel : Faites correspondre
 la compatibilité du contenu de l'application : Faites correspondre
 la compatibilité antivirus : Correspondance des informations sur
 les pairs : Etat de la connexion : up Version : 1 État : contrôleur
 passif (derniers 1 jours) Informations sur l'appareil : Adresse IPv4
 de gestion : 10.10.10.30/24 Adresse IPv6 de gestion : Informations
 sur le lien de contrôle HA1 : IP address: 10.10.10.130 Adresse
 MAC: 00:00:5e:00:53:00 Connexion; Lien primaire HA1 Informations
 sur l’option de choix : Priorité : secondaire Préemptif : pas
 d’informations de version : Version de build : Base de données
 URL 8.0.1-c31 : Contenu de l’application non installé : 497-2688
 Antivirus : 0 Moniteur initial Maintenir inactif; Autoriser le
 réseau/les liens à s’installer : Les échecs de surveillance des
 liens et des chemins d’accès ont été respectés Synchronisation de
 la configuration : Activé : oui Configuration en cours d'exécution :
 synchronisé
```

Niveau de privilège requis

superuser, deviceadmin

show high-availability control-link

Description

Affichez les statistiques relatives à la haute disponibilité du cluster d'appareils WildFire pour la liaison de contrôle HA établie entre les nœuds de contrôles principal et de secours, notamment le nombre de types de messages différents transmis et reçus sur la liaison de contrôle HA, les échecs de connexion et l'activité ping.

Emplacement de la hiérarchie

```
afficher tous les haute disponibilité
```


Syntaxe

```
liaison de contrôle { statistics; }
```

Options

`> statistics` : affichiez les statistiques relatives à la liaison de contrôle HA établie entre les nœuds de contrôle du cluster d'appareils WildFire.

Exemple de résultat

```
admin@thing1(active-controller)> afficher les statistiques de liaison
 de contrôle haute disponibilité haute disponibilité : Statistiques
 du lien de contrôle : HA1 : Messages-TX : 13408 Messages-RX : 13408
 Capacité-Msg-TX : 2 Capacité-Msg-RX : 2 Erreur-Msg-TX : 0 Erreur-
Msg-RX : 0 Preempt-Msg-TX : 0 Preempt-Msg-RX : 0 Preempt-Ack-Msg-
TX : 0 Preempt-Ack-Msg-RX : 0 Primaire-Msg-TX : 1 Primaire-Msg-RX :
 1 Primaire-Acq-Msg-TX : 1 Primaire-Acq-Msg-RX : 1 Hello-Msg-TX :
 13402 Hello-Msg-RX : 13402 Hello-Timeouts : 0 Hello-Failures :
 0 MasterKey-Msg-TX : 1 MasterKey-Msg-RX : 1 MasterKey-Ack-Msg-
TX : 1 MasterKey-Ack-Msg-RX : 1 Echecs de connexion : 0 tentatives
 de connexion-échecs : 12 tentatives d'écoute de connexion : 1
 tentatives de connexion actives : 12 Ping-TX : 53614 Ping-Échec-TX :
 0 Ping-RX : 53613 Ping-Timeouts : 0 Échecs de ping : 0 Ping-Error-
Msgs : 0 Ping-Autres-Msgs : 0 Ping-Dernier-Rsp : 1
```

Niveau de privilège requis

superuser, deviceadmin

show high-availability state

Description

Affichez les informations relatives à l’état High Availability (haute disponibilité ; HA) du cluster d'appareils WildFire pour les nœuds de contrôle locaux et homologues du cluster, notamment si le nœud de contrôle est actif (principal) ou passif (de secours) et depuis combien de temps, la configuration HA, si les configurations du nœud de contrôle local et homologue sont synchronisées ainsi que la compatibilité des versions de l’antivirus, des mises à jour de contenu et des logiciels entre les homologues.

Emplacement de la hiérarchie

```
afficher tous les haute disponibilité
```

Syntaxe

```
État
```


Options

No additional options.

Exemple de résultat

```
admin@thing1(active-controller)> afficher l'état de haute
 disponibilité Haute disponibilité Informations locales : Version :
 1 État: contrôleur actif (1 derniers jours) Informations sur le
 périphérique: Adresse IPv4 de gestion : 10.10.10.14/24 Adresse
 IPv6 de gestion : Configuration conjointe des liaisons de contrôle
 HA1 : Chiffrement activé : aucune information sur l'option de choix
 Priorité : préemption primaire : pas de compatibilité de version :
 Version du logiciel : Faites correspondre la compatibilité du
 contenu de l'application : Faites correspondre la compatibilité
 antivirus : Correspondance des informations sur les pairs :
 Etat de la connexion : up Version : 1 État : contrôleur passif
 (derniers 1 jours) Informations sur l'appareil : Adresse IPv4
 de gestion : 10.10.10.30/24 Adresse IPv6 de gestion : Connexion
 en place ; Informations sur l'option d'élection du lien HA1
 principal : Priorité : secondaire Préemptif : non Configuration
 Synchronisation : Activé : oui Configuration en cours d'exécution :
 synchronisé
```

Niveau de privilège requis

superuser, deviceadmin

show high-availability transitions

Description

Affichez les renseignements sur les transitions de High-Availability (haute disponibilité ; HA) du cluster d'appareils WildFire concernant des événements qui surviennent lors du basculement HA des nœuds de contrôle du cluster.

Emplacement de la hiérarchie

```
afficher tous les haute disponibilité
```

Syntaxe

```
transitions ;
```

Options

No additional options.

Exemple de résultat

```
admin@thing1(active-controller)> afficher les transitions de haute
 disponibilité  Haute disponibilité : Statistiques de transition :
 Inconnu : 1 Suspendu : 0 Initial : 0 Non-Fonctionnel : 0 Passif 0
 Actif 3
```

Niveau de privilège requis

superuser, deviceadmin

show system raid

Description

Affichez la configuration RAID de l'appareil WildFire. L'appareil WF-500 est fourni avec quatre lecteurs ; ces derniers se trouvent dans les quatre premières baies de lecteur (A1, A2, B1 et B2). Les lecteurs'A0;A1 et A2 sont une paire RAID'A0;1, et les lecteurs'A0;B1 et B3 sont une seconde paire RAID'A0;1.

Emplacement de la hiérarchie

```
afficher le système
```

Syntaxe

```
raid { detail; {
```

Options

No additional options.

Exemple de résultat

Vous trouverez ci-dessous la configuration RAID sur un appareil WF-500 fonctionnel.

```
admin@WF-500> afficher les détails du raid système Paire de disques
 A État disponible Nettoyer ID de disque A1 Modèle actuel : Taille
 ST91000640NS : 953869 Mo partition_1 : synchronisation active
 partition_2 : synchronisation active ID de disque A2 Modèle actuel :
 Taille ST91000640NS : 953869 Mo partition_1 : synchronisation
 active partition_2 : synchronisation active Paire de disques B
 Disponible Statut propre ID de disque B1 Modèle actuel : Taille
 ST91000640NS : 953869 Mo partition_1 : synchronisation active
 partition_2 : synchronisation active ID de disque B2 Modèle actuel :
 Taille ST91000640NS : 953869 Mo partition_1 : synchronisation active
 partition_2 : synchronisation active
```

Niveau de privilège requis

superuser, superreader

submit wildfire local-verdict-change

Description

Modifiez localement les verdicts de WildFire rendus pour les échantillons envoyés à partir du pare-feu. Les modifications de verdicts ne concernent que les échantillons envoyés à l’appareil WildFire ; le verdict du même échantillon demeure inchangé dans le cloud WildFire public. Vous pouvez afficher les échantillons dont les verdicts ont été modifiés en utilisant la commande show wildfire global.

Le WildFire private cloud content package (module de contenu du cloud WildFire privé) est mis à jour pour inclure les modifications que vous apportez aux verdicts (sur le pare-feu, sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)** > **WF-Private (WildFire privé)** pour activer les mises à jour de contenu du cloud WildFire privé). Lorsque vous faites passer le verdict d’un échantillon à malveillant, l’appareil WildFire génère une nouvelle signature pour détecter le logiciel malveillant et ajoute la signature au module de contenu du cloud WildFire privé. Lorsque vous faites passer le verdict d’un échantillon à bénin, l’appareil WildFire retire la signature du module de contenu du cloud WildFire privé.

On peut également utiliser un appel API pour modifier les verdicts des échantillons locaux. Pour plus d'informations, consultez le Guide de référence de l'API WildFire.

Emplacement de la hiérarchie

```
Envoyer à wildfire
```

Syntaxe

```
envoyer { wildfire { local-verdict-change { hash <value>; verdict
 <value>; comment <value>; } }
```

Options

* `hash (hâchage)` : spécifiez le hachage SHA-256 du fichier dont vous souhaitez modifier le verdict.

* `verdict` : saisissez le nouveau verdict du fichier : indiquez 0 pour un échantillon bénin ; 1 pour un échantillon malveillant ; 2 pour un échantillon indésirable.

* `comment` : ajoutez un commentaire pour décrire la modification de verdict.

Exemple de résultat

Vous trouverez ci-dessous le résultat de cette commande.

```
admin@WF-500> envoyer hâchage test de commentaire wildfire local-
verdict-change
 c323891a87a8c43780b0f2377de2efc8bf856f02dd6b9e46e97f4a9652814b5c
 verdict 2 Veuillez saisir 'Y' pour valider: (y ou n) le verdict est
 modifié (ancien verdict: 1, nouveau verdict:2)
```


Niveau de privilège requis

superuser, deviceadmin

show wildfire

Description

Affichez diverses informations sur l’appareil WildFire, notamment des informations sur les périphériques globaux et locaux ainsi que des informations liées aux échantillons, l’état de l'appareil ainsi que la machine virtuelle qui est sélectionnée pour mener l’analyse.

Emplacement de la hiérarchie

```
show wildfire
```

Syntaxe

```
état | vm-images | wf-vm-pe-utilisation | wf-vm-doc-utilisation |
 wf-vm-email-lien-utilisation | wf-vm-utilisation de l'archive | wf-
exemple-file-état }
```

Options

`> status` — Affichez l'état de l'appareil ainsi que des informations de configuration comme la machine virtuelle (MV) utilisée pour l'analyse de l'échantillon, si des échantillons/rapports sont envoyés ou non au cloud, le réseau vm-network, et des informations d'enregistrement.

`> vm-images` — Affichez les attributs des images de machine virtuelle disponibles utilisées pour l'analyse de l'échantillon. Pour afficher l'image active actuelle, exécutez la commande suivante :

```
admin@WF-500> afficher l'état de wildfire
```

et afficher le `champ VM`.

`> wf-sample-queue-status` : affiche le nombre d’échantillons d’appareils WildFire qui attendent d’être analysés et leur répartition.

`> wf-vm-doc-utilization` : affiche le nombre d’environnements d’analyse qui ont été utilisés pour traiter les fichiers de documents qui sont disponibles et utilisés.

`> wf-vm-elinkda-utilization` : affiche le nombre d’environnements d’analyse utilisés pour traiter les liens contenus dans les e-mails qui sont disponibles et utilisés.

`> wf-vm-pe-utilization` : affiche le nombre d’environnements d’analyse utilisés pour traiter les fichiers exécutables qui sont disponibles et utilisés.

Exemple de résultat

Vous trouverez ci-dessous le résultat de cette commande.


```
admin@WF-500> afficher l'état de wildfire Informations de connexion :
 Nuage Wildfire : s1.wildfire.paloaltonetworks.com Statut :
 Inactif Soumettre un échantillon : désactivé Soumettre un
 rapport : désactivé VM sélectionnée : vm-5 Connexion Internet VM :
 désactivée Réseau VM utilisant Tor : désactivé Meilleur serveur :
 s1.wildfire.paloaltonetworks.com Périphérique enregistré : oui
 Adresse IP de la route de service : 10.3.4.99 Vérification de la
 signature : activer Sélection du serveur : activer Via un proxy :
 non admin@WF-500> afficher wildfire vm-images Images de VM prises
 en charge : vm-1 Windows XP, Adobe Reader 9.3.3, Flash 9, Office
 2003. Prend en charge PE, PDF, Office 2003 et versions antérieures
 vm-2 Windows XP, Adobe Reader 9.4.0, Flash 10n, Office 2007. Prend
 en charge PE, PDF, Office 2007 et versions antérieures vm-3 Windows
 XP, Adobe Reader 11, Flash 11, Office 2010. Prend en charge PE, PDF,
 Office 2010 et versions antérieures vm-4 Windows 7 32 bits, Adobe
 Reader 11, Flash 11, Office 2010. Prend en charge PE, PDF, Office
 2010 et versions antérieures vm-5 Windows 7 64 bits, Adobe Reader
 11, Flash 11, Office 2010. Prend en charge PE, PDF, Office 2010 et
 versions antérieures vm-6 Windows XP, Internet Explorer 8, Flash 11.
 Prise en charge des liens E-MAIL admin@WF-500> afficher wildfire wf-
sample-queue-status DW-ARCHIVE : 4, DW-DOC : 2, DW-ELINK : 0, DW-PE :
 21, DW-URL_UPLOAD_FILE : 2, admin@WF-500> afficher wildfire wf-vm-
pe-utilization { available : 2, in_use: 1, }
```

Niveau de privilège requis

superuser, superreader

show wildfire global

Description

Affichez diverses informations sur les périphériques globaux ainsi que sur l’état des échantillons, comme les clés API disponibles, les informations d’enregistrement, les changements apportés aux verdicts rendus pour les échantillons, l’activité, l’origine des échantillons et les échantillons qui ont récemment été analysés par l’appareil.

Emplacement de la hiérarchie

```
show wildfire global
```

Syntaxe

```
clés api { all { details; } key <value>; } devices-reporting-data;
 last-device-registration { all; } local-verdict-change { all; sha256
 <value>; } } sample-analysis { number; type; } } sample-device-
lookup { sha256 { equal <value>; } sample-status { sha256 { equal
 <value>; } } signature-status { sha256 { equal <value>; } }
```


Options

`> api-keys` : affichez des détails sur les clés API générées sur l'appareil WildFire. Vous pouvez afficher l'heure de dernière utilisation de la clé, le nom de la clé, l'état (activée ou désactivée), et la date/heure de génération de la clé.

`> devices-reporting-data` : affichez la liste des dernières activités d'enregistrement.

`> last-device-registration` : affichez la liste des dernières activités d'enregistrement.

`> local-verdict-change` : affichez les échantillons dont les verdicts ont été modifiés.

`> sample-analysis` : affichez les résultats de l’analyse WildFire pour un maximum de 1 000 échantillons.

`> sample-status` : affichez l'état de l'échantillon WildFire. Saisissez la valeur SHA256 du fichier pour afficher l'état de l'analyse actuelle.

`> sample-device-lookup` : affiche le pare-feu qui a envoyé l’échantillon SHA256 spécifié.

`> signature-status` : affichez l'état de la signature WildFire. Saisissez la valeur SHA256 du fichier pour afficher l'état de l'analyse actuelle.

Exemple de résultat

Vous trouverez ci-dessous le résultat de cette commande.

```
admin@WF-500> afficher toutes les clés API globales wildfire
 +------------+-----------+---------+--------------------
+---------------------+ | Clé api | Nom| Etat | Créer Heure |
 Heure dernière utilisation | +------------+-----------+---------
+---------------------+---------------------+ | <API KEY> |
 happykey1 | Activé | 2017-03-01 23:21:02 | 2017-03-01 23:21:02
 | +------------+-----------+---------+--------------------
+---------------------+ admin@WF-500> afficher wildfire global
 devices-reporting-data +--------------+--------------------
+-------------+------------+----------+--------+ | _ID appareil |
 Dernier enregistrement |  IP appareil | Version logiciel | Modèle
 HW | Etat | +--------------+----------------------+-------------
+------------+----------+--------+ | 000000000000 | 2017-03-01
 22:28:25 | 10.1.1.1 | 8.1.4 | PA-220 | OK | +--------------
+---------------------+-------------+------------+----------
+--------+ admin@WF-500> afficher wildfire global last-device-
registration all +--------------+----------------------+-------------
+------------+----------+--------+ | ID appareil | dernier
 enregistrement | IP appareil | Version logiciel | Modèle HW
 | Etat | +--------------+----------------------+-------------
+------------+----------+--------+ | 000000000000 | 2017-07-31
 12:35:53 | 10.1.1.1 | 8.1.4 | PA-220 | OK | +--------------
+---------------------+-------------+------------+----------+--------
+ admin@WF-500> afficher wildfire global local-verdict-change
 +-------------------------------------------------------------------
+---------+--------+ | SHA256 | Verdict | Source |
 +-------------------------------------------------------------------
+---------+--------+ |
 c883b5d2e16d22b09b176ca0786128f8064d47edf26186b95845aa3678868496| 2
 -> 1 | Oui |
```



```
 +-------------------------------------------------------------------
+---------+--------+ admin@WF-500> afficher wildfire global sample-
analysis 100 derniers échantillons malveillants créés +--------------
+---------------------+---------------------+-----------+ | SHA256
 | Date de fin | date de création | Malveillant | +--------------
+---------------------+---------------------+-----------+ |
 <HASH VALUE> | 2017-03-01 23:27:57 | 2017-03-01 23:27:57 | Oui
 | +--------------+---------------------+--------------------
+-----------+ +---------------------+----------------
+---------------+----------------+ | Nœuds de stockage | Nœuds
 d’analyse | Etat | Type de fichier | +----------------------
+----------------+---------------+----------------+ |
 00926ld1_2,0094:d1_2 | qa16 | Notifier la fin | Fichier Elink
 | +----------------------+----------------+---------------
+-----------------+ Derniers 100 échantillons non malveillants
 créés +--------------+---------------------+--------------------
+-----------+ | SHA256 | Date de fin | Date de création | Malicious
 | +--------------+---------------------+--------------------
+-----------+ | <HASH VALUE> | 2017-03-01 23:31:15 | 2017-03-01
 23:24:29 | Non | +--------------+--------------------
+---------------------+-----------+ +----------------------
+-----------------+---------------+--------------------+ |
 Nœuds de stockage | Nœuds d’analyse | Etat | Type de fichier
 | +----------------------+----------------+---------------
+--------------------+ | 0712:smp_27,94:smp_7 | qa16 | Notifier la
 fin | document MS Office | +----------------------+----------------
+---------------+--------------------+ admin@WF-500> afficher
 wildfire global sample-device-lookup sha256 equal
 d75f2f71829153775fa33cf2fa95fd377f153551aadf0a642704595100efd460
 Echantillon
 1024609813c57fe174722c53b3167dc3cf5583d5c7abaf4a95f561c686a2116e
 consulté pour la dernière fois sur les appareils suivants:
 +-------------------------------------------------------------------
+-----------+-----------+--------------------+ |
 SHA256 | ID appareil | IP appareil | Heure d’envoi |
 +-------------------------------------------------------------------
+-----------+-----------+--------------------+ |
 1024609813c57fe174722c53b3167dc3cf5583d5c7abaf4a95f561c686a2116e
 | Manuel | Manuel | 2019-08-05 19:24:39 |
 +-------------------------------------------------------------------
+-----------+-----------+--------------------+
 admin@WF-500> afficher wildfire global sample-status sha256 equal
 dc9f3a2a053c825e7619581f3b31d53296fe41658b924381b60aee3eeea4c088
 +---------------------+---------------------+-----------
+---------------------------+ | Date de fin | Date
 de création | Malveillant | Nœuds de stockage |
 +---------------------+---------------------+-----------
+---------------------------+ | 2017-03-01 22:34:17 |
 2017-03-01 22:28:23 | Non | 009026:smp_27,097010smp_27 |
 +---------------------+---------------------+-----------
+---------------------------+ +----------------+--------------
+------------------+ | Nœuds d’analyse | Etat | Type de
 fichier | +----------------+--------------+-----------------
+ | qa15 | Notifier la fin | Fichier Adobe Flash |
 +----------------+--------------+------------------+
 admin@WF-500> afficher wildfire global signature-status sha256
```



```
 equalc883b5d2e16d22b09b176ca0786128f8064d47edf26186b95845aa3678868496
 Signature Nom: Virus/Win32.WPCGeneric.cr Etat actuel: publié
 Historique de publication: +---------------+--------------------
+---------+-------------+----------+ | Version | Horodatage | UTID
 | ID interne | Status | +---------------+--------------------
+---------+-------------+----------+ | 155392 | 2017-02-03 10:11:06
 | 5000259 | 10411 | publié | +---------------+--------------------
+---------+-------------+----------+
```

Niveau de privilège requis

superuser, superreader

show wildfire local

Description

Affichez diverses informations sur les échantillons et les périphériques locaux, sur l’activité et sur les échantillons récemment analysés par l’appareil ainsi que des statistiques WildFire de base.

Emplacement de la hiérarchie

```
show wildfire local
```

Syntaxe

```
dernier { analysis { filter malicious|benign; sort-by SHA256|Submit
 Time|Start Time|Finish Time|Malicious|Status; sort-direction
 asc|desc; limit 1-20000; days 1-7; } OU... échantillons { filter
 malicious|benign; sort-by SHA256|Create Time|File Name|File Type|
File Size|Malicious|Status; sort-direction asc|desc; limit 1-20000;
 days 1-7; } échantillon traité { count 1-1000; time {last-1-hr|
last-12-hrs|last-15-minutes|last-24-hrs|last-30-days|last-7-days|
last-calender-day|last-calender-month; } état de l’échantillon
 { sha256 { equal <value>; } } statistics days <1-31> | hours <0-24>
 | minutes <0-60>; }
```

Options

`> latest` : affichez les 30 dernières activités, ce qui inclut les 30 dernières activités d'analyse, les 30 derniers fichiers analysés, les informations de session sur les fichiers analysés, et les fichiers chargés sur le serveur du cloud public.

`> sample-processed` : affiche le nombre d’échantillons traités localement dans un délai spécifié ou le nombre d’échantillons maximum.

`> sample-status` : affichez l'état de l'échantillon WildFire. Saisissez la valeur SHA256 du fichier pour afficher l'état de l'analyse actuelle.

`> statistics` : Affichez des statistiques WildFire de base.

Exemple de résultat

Vous trouverez ci-dessous le résultat de cette commande.

```
admin@WF-500> afficher la dernière analyse wildfire
 Dernières informations d'analyse : +--------------------
+---------------------- +---------------------+--------------------
+ | SHA256 | Heure de soumission | Heure de début | Heure de fin |
 +---------------------+---------------------+---------------------
 --------+---------------------+ | <HASH VALUE>| 2017-03-01 14:28:26
 | 2017-03-01 14:28:26 | 2017-03-01 14:34:24 | | <HASH VALUE>|
 2017-03-01 14:28:25 | 2017-03-01 14:28:25 | 2017-03-01 14:28:41
 | | <HASH VALUE>| 2017-03-01 14:28:25 | 2017-03-01 14:28:25 |
 2017-03-01 14:28:26 | +---------------------+---------------------
+---------------------- --------+---------------------+ +------------
+----- ------------------------------------------------
 ----+-----------+ | Malveillant | Image de
 machine virtuelle | Etat | +--------------------
+-------------------------------------------------
 ------------------------+-----------+ | Oui | Windows 7 x64
 SP1, Adobe Reader 11, Flash 11, Office 2010 | terminé | |
 Non | Analyseur statique Java/Jar | terminé | | Suspect |
 Analyseur statique Java/Jar | terminé | +--------------------
+-------------------------------------------------
 ------------------------+-----------+ admin@WF-500> afficher les
 derniers échantillons locaux de wildfire Dernières informations
 sur les échantillons : +---------------------+--------------------
+----------- -----+---------------+ | SHA256 | Heure de création
 | Nom de fichier | Type de fichier | +--------------------
+----------------------+----------- ----+---------------+
 | <HASH VALUE> | 2017-03-01 14:28:25 | | Classe JAVA | |
 <HASH VALUE> | 2017-03-01 14:28:25 | | Classe JAVA | | <HASH
 VALUE> | 2017-03-01 14:28:25 | | PE | +--------------------
+----------------------+----------- ----+---------------+
 +-------------+-----------+- ------------------+ | Taille du
 fichier | Malveillant | Etat | +-------------+----------
+---------------------------+ | 20 407 | Non | analyse terminée
 | | 1 584 | Oui | analyse terminée | | 259 024 | Non | analyse
 terminée | +-------------+-----------+-------------+ admin@
 WF-500> affiche le nombre d'échantillons locaux traités par wildfire
 2 Fenêtre de temps : 15 dernières minutes Affichage du nombre :
 2 : +-------------------------------------------------------------
 ------------------+---------------------+-------- ---
+-----------+----------+-----------+-------- ----------
+ | SHA256 | Heure de création | Nom de fichier | Type
 de fichier | Taille du fichier | Malveillant |Etat |
 +-------------------------------------------------------------
 ----------------+--------------------+---------- -
+-----------+----------+-----------+---------- ---------+ |
 ce752b7b76ac2012bdff2b76b6c6af18e132ae8113172028b9e02c6647ee19bb
 | 2018-12-09 16:55:53 | | Lien e-mail | 31 522 | | téléchargement
 terminé | |
 349e57e51e7407abcd6eccda81c8015298ff5d5ba4cedf09c7353c133ceaa74b
 | 2018-12-09 16:53:40 | | Lien e-mail | 39 679 | | téléchargement
 terminé |
 +-------------------------------------------------------------
```



```
 ----------------+--------------------+---------- -
+-----------+----------+-----------+---------- ---------+
 admin@WF-500> afficher wildfire local sample-status sha256 égal
 0f2114010d00d7fa453177de93abca9643f4660457536114898c56149f819a9b
 Informations sur l'échantillon : +--------------------- +----------
+-----------------------------------+ | Heure de création | Nom
 de fichier | Type de fichier | +--------------------+----------
+-------------- -------------------+ | 2017-03-01 22:28:24 |
 rmr.doc | Document Microsoft Word 97 - 2003 | +--------------------
+----------+-------------- --------------------+ +----------
+----------+---- --------------+ | Taille du fichier | Malveillant
 | Etat | +----------+----------+-----------------+ | 133120 |
 Oui | analyse terminée | +----------+----------+-----------------
+ Informations sur l'analyse : +- -------------------
+--------------------+------- -------------+-----------+ | Heure
 de soumission | Heure de début | Heure de fin | Malveillant |
 +--------------------+--------------------+----- ----------------
+------------+ | 2017-03-01 22:28:24 | 2017-03-01 22:28:24 |
 2017-03-01 22:28:24 | Suspect | | 2017-03-01 22:28:24 | 2017-03-01
 22:28:24 | 2017-03-01 22:34:07 | Oui | +--------------------
+----------------------+----- ---------------+-----------+
 +---------------------- ----------------------------------------
+--------- --+ | Image de machine virtuelle | Etat |
 +-----------------------------------------------------------------
 ----------------------+ | Analyseur statique DOC/CDF | terminé | |
 Windows 7 x64 SP1, Adobe Reader 11, Flash 11, Office 2010 | terminé
 | +-----------------------------------------------------------------
 ---------------------+ admin@WF-500> afficher les
 statistiques locales wildfire 2017-03-01 17:44:31 Reçu
 après : 2017-02-28 17:44:31 Reçu avant : 2017-03-01
 17:44:31 ---------------------------------------
 ------------------------------------------- | Statistiques
 wildfire |
 +-----------------------------------------------------------------
 ---------------------------------+ |+--------------------
 ----------------------------------------------
 ------------------+| || Exécutable || |
+-----------------------------------------------------------------
 ---------------------------------+| || TypeFichier
 | Soumis | Analysé | En attente | Logiciels
 malveillants | Graywares | bénin | Erreur || |
+-----------------------------------------------------------------
 ---------------------------------+| || exe | 2 | 2 | 0 | 0 | 0 | 2 |
 0 || |+-----------------------------------------------------------------
 ---------------------------------+| || dll | 0 | 0 | 0 | 0 | 0 | 0 |
 0 || |+-----------------------------------------------------------------
 ---------------------------------+| Résumé de
 l'analyse de l'environnement pour l'exécutable :
 Utilisation de la MV 0/10 Fichiers analysés : 2
 +-----------------------------------------------------------------
 ---------------------------------+ || Non exécutable || |
+-----------------------------------------------------------------
 ---------------------------------+| || TypeFichier
 | Soumis | Analysé | En attente | Logiciels
 malveillants | Graywares | bénin | Erreur || |
+-----------------------------------------------------------------
```



```
 ---------------------------------+| || pdf | 0 | 0 | 0 | 0 | 0 | 0 |
 0 || |+-------------------------------------------------------------
 ---------------------------------+| || pot | 0 | 0 | 0 | 0 | 0 | 0 |
 0 || |+-------------------------------------------------------------
 ---------------------------------+| || doc | 1 | 1 | 0 | 1 | 0 | 0 |
 0 || |+-------------------------------------------------------------
 ---------------------------------+| || ppt | 0 | 0 | 0 | 0 | 0 | 0 |
 0 || |+-------------------------------------------------------------
 ---------------------------------+| || xl | 0 | 0 | 0 | 0 | 0 | 0 |
 0 || |+-------------------------------------------------------------
 ---------------------------------+| || docx | 0 | 0 | 0 | 0 | 0 | 0
 | 0 || |
+-------------------------------------------------------------
 ---------------------------------+| || pptx | 0 | 0 | 0 | 0 | 0 | 0
 | 0 || |
+-------------------------------------------------------------
 ---------------------------------+| || xlsx | 0 | 0 | 0 | 0 | 0 | 0
 | 0 || |
+-------------------------------------------------------------
 ---------------------------------+| || rtf | 0 | 0 | 0 | 0 | 0 | 0 |
 0 || |+-------------------------------------------------------------
 ---------------------------------+| || classe | 2 | 2 | 0 | 1 | 0 |
 1 | 0 || |
+-------------------------------------------------------------
 ---------------------------------+| || swf | 1 | 1 | 0 | 0 | 0 | 1 |
 0 || |+-------------------------------------------------------------
 ---------------------------------+| Résumé de
 l'analyse de l'environnement pour les non-exécutables :
 Utilisation de la MV 0/16 Fichiers analysés : 4
 +-------------------------------------------------------------
 ---------------------------------+ || Liens || |
+-------------------------------------------------------------
 ---------------------------------+| || TypeFichier
 | Soumis | Analysé | En attente | Logiciels
 malveillants | Graywares | bénin | Erreur || |
+-------------------------------------------------------------
 ---------------------------------+| || elien | 1 | 1 | 0 | 1 | 0 | 0
 | 0 || |
+-------------------------------------------------------------
 ---------------------------------+| Résumé de l'analyse
 de l'environnement pour les liens : Fichiers analysés : 1
 ------------------------------------------------- --------- |
 Statistiques générales |
 +-------------------------------------------------------------
 -------+ Utilisation totale du disque : 67/1283(Go) (5%) ||
+------------------------------+---------- -+-+-----------+||
 ||| File d'attente d'échantillons ||| ||+-----------------
+--------------------+--------- -----+|| ||| SOUMIS | ANALYSÉ | EN
 ATTENTE ||| ||+----------------------+----------+-+------ -----+||
 ||| 7 | 7 | 0 ||| ||+----------------------+----------+-+------
 ----+||| |+--------------------------+------------------- ------+|
 ||| Verdicts ||| ||+-------------------------+-------------------
 -----+|| ||| Logiciels malveillants | Graywares | bénin |
 Erreur ||| ||+------------------------------+-----------------
 -----+|| ||| 3 | 0 | 4 | 0 ||| ||+----------------------
+-----------+-+------ ----+||| |+--------------------------
```



```
+--------------------- ------+| ||| Nombre de sessions
 et de téléchargements ||| ||+-------------------------
+--------------------- -----+|| ||| Séances | Téléchargements ||| ||
+-------------------------+-------------------- -----+|| ||| 7 | 5
 ||| ||+-------------------------+-------------------- -----+||
```

Niveau de privilège requis

superuser, superreader

test wildfire registration

Description

Exécute un test pour vérifier l'état d'enregistrement d'un appareil WildFire ou d'un pare-feu Palo Alto Networks sur un serveur WildFire. Si le test réussit, l'adresse IP ou le nom du serveur WildFire s'affiche. Un enregistrement est requis pour qu'un appareil WildFire ou un pare-feu puisse transférer des fichiers vers le serveur WildFire.

Syntaxe

```
test { wildfire { registration; } }
```

Options

No additional options.

Exemple de résultat

Vous trouverez ci-dessous un résultat réussi sur un pare-feu pouvant communiquer avec un appareil WildFire. S'il s'agit d'un appareil WildFire pointant vers le cloud WildFire de Palo Alto Networks, le nom du serveur de l'un des serveurs cloud s'affiche dans le champ `select the best server:`.

```
Test de wildfire Enregistrement de wildfire dans le cloud public :
 téléchargement réussi liste de serveurs : sélection du meilleur
 serveur réussie : ca-s1.wildfire.paloaltonetworks.com
```

Niveau de privilège requis

superuser, superreader

