Panorama 管理者ガイド

Version 10.0 (EoL)

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

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

About the Documentation

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

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

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

Last Revised

December 4, 2020

Table of Contents

Panorama の概要 11
Panorama について 12
Panorama モデル 14
ファイアウォール設定および更新の中央管理について 17
ファイアウォールと Panorama 間のコンテキスト切り替え 17
Panorama の合計コンフィグレーションサイズ 17
テンプレートおよびテンプレート スタック 18
Device Groups (デバイス グループ) 19
ログとレポートの中央管理 25
管理対象コレクタおよびコレクタ グループ 25
ローカルおよび分散ログ収集 26
複数のログ コレクタを含むコレクタ グループに関する注意事項 27
ログ転送オプション 29
一元的なレポート 30
Panorama を使用したデータの再配信 31
ロールベースのアクセス制御 32
管理ロール 32
認証プロファイルと認証シーケンス 34
アクセス ドメイン 34
管理認証 34
Panorama のコミット、検証、およびプレビュー操作 36
Panorama のデプロイ計画 37
Panorama のデプロイ：タスクの概要 39

Panorama のセットアップ 41
Panorama のログ保持要件を決定 42
Panorama バーチャル アプライアンスのセットアップ 44
Panorama バーチャル アプライアンスのセットアップ前提条件 44
Panorama バーチャル アプライアンスのインストール 47
Panorama バーチャル アプライアンスの初期設定の実行 77
ログ コレクタを使用する Panorama バーチャル アプライアンスのセットアップ 80
ローカル ログ コレクタを使用する Panorama バーチャル アプライアンスのセットアップ 86
Panorama モードの Panorama バーチャル アプライアンスのセットアップ 90
管理専用モードの Panorama バーチャル アプライアンスのセットアップ 91
Panorama バーチャル アプライアンスでのログ ストレージ容量の拡張 92
Panorama バーチャル アプライアンスの CPU およびメモリを増やす 111
Panorama バーチャルアプライアンスにシステムディスクを追加する 117
Panorama バーチャル アプライアンスのセットアップの完了 122
M-Series アプライアンスのセットアップ 123
M-Series アプライアンス インターフェイス 123
M-Series アプライアンスの初期設定 125
M-Series のセットアップの概要 129
M-Series アプライアンスをログ コレクタとしてセットアップ 130
M-Series アプライアンスのストレージの拡張 137
複数のインターフェイスを使用するように Panorama を設定 144
Panorama の登録とライセンスのインストール 151
Panorama の登録 151

Panorama サポート ライセンスのアクティベーション.....152
Panorama バーチャル アプライアンスがインターネットに接続している時のファイアウォール管理ライセンスのアクティベーション/取得.....153
Panorama バーチャル アプライアンスがインターネットに接続していない時のファイアウォール管理ライセンスのアクティベーション/取得.....154
M-Series アプライアンスにおけるファイアウォール管理ライセンスのアクティベーション/取得.....156
Panorama デバイス証明書のインストール.....159
Panorama のコンテンツ更新とソフトウェア更新のインストール.....161
Panorama、ログ コレクタ、ファイアウォール、および WildFire のバージョン互換性.....161
HA 設定の Panorama に更新をインストール.....162
Panorama からインターネットに接続できる場合の更新のインストール.....163
Panorama からインターネットに接続できない場合の更新のインストール.....167
インターネットに接続せずにPanoramaのアップデートを自動的にインストールする.....171
Panorama ログの新しいログ形式への移行.....176
別の Panorama モデルへの移行.....178
Panorama バーチャル アプライアンスから M-Series アプライアンスへの移行.....178
Panorama バーチャル アプライアンスから異なるハイパーバイザへの移行.....181
M-Series アプライアンスから Panorama バーチャル アプライアンスへの移行.....185
M-100 アプライアンスから M-500 アプライアンスへの移行.....190
Panorama 管理インターフェイスへのアクセスおよびナビゲート.....193
Panorama Web インターフェイスへのログイン.....193
Panorama Web インターフェイスへのナビゲート.....193
Panorama CLI へのログイン.....194
Panorama への管理アクセスのセットアップ.....196
管理者ロール プロファイルの設定.....196
アクセス ドメインの設定.....197
管理者アカウントおよび認証の設定.....197
カスタム証明書を使用する認証のセットアップ.....210
SSL/TLS 接続を相互に認証する方法.....210
Panorama でのカスタム証明書を使用する認証の設定.....211
管理対象デバイスでのカスタム証明書を使用する認証の設定.....213
新しいクライアント デバイスの追加.....214
証明書の変更.....215

ファイアウォールの管理.....219
管理対象デバイスとしてのファイアウォールの追加.....220
管理対象ファイアウォールのデバイス証明書のインストール.....225
管理対象ファイアウォールのデバイス証明書のインストール.....225
複数の管理対象ファイアウォールのデバイス証明書のインストール.....227
ゼロタッチプロビジョニングのセットアップ.....230
ZTP の概要.....230
ZTP プラグインのインストール.....232
ZTP インストーラ管理者アカウントの設定.....238
Panorama への ZTP ファイアウォールの追加.....239
ZTP タスクでの CLI の使用.....243
ZTP プラグインのアンインストール.....245
デバイス グループの管理.....247
デバイス グループの追加.....247
デバイス グループの階層を作成.....248
共有またはデバイス グループ ポリシーで使用するオブジェクトの作成.....250

継承したオブジェクトの値を復元 251
未使用の共有オブジェクトの管理 252
継承したオブジェクトの優先度を管理 252
ポリシー ルールあるいはオブジェクトを別のデバイス グループに移動/コピー 253
Panorama で URL フィルタリング ベンダーを選択 255
ファイアウォールのサブセットにポリシー ルールをプッシュ 259
ルール階層の管理 261
テンプレートおよびテンプレート スタックの管理 264
テンプレートの機能および例外 264
テンプレートの追加 264
テンプレート スタックの設定 266
テンプレートまたはテンプレートスタック変数の設定 269
既存のテンプレートスタック変数のインポートおよび上書き 272
テンプレートまたはテンプレートスタック値のオーバーライド 273
テンプレート設定の無効化/削除 276
Panorama からマスターキーを管理 277
エンタープライズ データ消失防止 (DLP) のセットアップ 281
エンタープライズ データ漏洩防止 (DLP) の概要 281
エンタープライズ データ損失防止 (DLP) のサポート対象。 283
事前定義済みデータ フィルタリングプロファイル 285
エンタープライズ データ漏洩防止 (DLP) プラグインのインストール 286
データ パターンの作成 289
データ フィルタリング プロファイルの作成 290
エンタープライズ データ漏洩防止 (DLP) の有効化 293
エンタープライズ データ消失防止 (DLP) のログ詳細を見る 296
既存のデータ パターンの有効化とプロファイルのフィルタリングの有効化 297
エンタープライズ データ消失防止 (DLP) の設定の編集 298
エンタープライズ データ消失防止 (DLP) プラグインのアンインストール 302
データをマネージドファイアウォールに再配信する 304
ファイアウォールを Panorama 管理に移行 306
Panorama 管理への変更を計画 306
ファイアウォールを Panorama 管理に移行 307
ファイアウォール HA ペアを Panorama 管理に移行 311
ファイアウォールの設定の一部を Panorama に読み込む 314
Panoramaでのデバイスモニタリング 317
デバイス健康状態の監視 317
ポリシー ルール使用状況のモニター 318
「ユース ケース：Panorama を使用してファイアウォールを構成 324
このユース ケースにおけるデバイス グループ 324
このユース ケースのテンプレート 325
中央管理設定とポリシーのセットアップ 326

大規模なファイアウォールのデプロイを管理 333
最適な大規模ファイアウォールのデプロイソリューションを決定 334
M-600 および Panorama バーチャル アプライアンスのデバイス管理能力の強化 335
デバイス管理能力要件の強化 335
Panorama をデプロイしてデバイス管理を強化 336
Panorama Interconnect 339
Panorama Interconnect の概要 339
Panorama Interconnect の要件 340
Panorama Controller およびノード間の認証を有効化 342
Panorama Interconnect プラグインのセットアップ 347
Panorama Interconnect の同期 350

Panorama Interconnect でファイアウォールを管理.....351
Panorama Interconnect プラグインのアップグレード..... 360

ログ収集の管理.....363
管理対象コレクタの設定..... 364
専用のログ コレクタの認証の設定.....367
専用のログ コレクタの管理者アカウントの設定.....367
専用のログ コレクタの RADIUS 認証の設定..... 368
専用のログ コレクタの TACACS+ 認証を設定する.....371
専用のログ コレクタの LDAP 認証の設定.....373
コレクタ グループの管理.....377
コレクタ グループの設定.....377
ログ コレクタ間でのカスタム証明書を用いる認証の設定.....379
ログ コレクタを別のコレクタ グループに移動.....381
コレクタ グループからのファイアウォールの削除.....382
Panorama へのログ転送の設定.....384
外部の宛先への syslog 転送の設定.....388
Cortex Data Lake へのログの転送.....392
Panorama へのログ転送の確認.....393
ログ転送とバッファのデフォルトの変更.....395
Panorama から外部の宛先へのログ転送を設定..... 397
ログ収集のデプロイメント..... 400
専用のログ コレクタを使用する Panorama のデプロイ..... 400
ローカル ログ コレクタを使用する Panorama M-Series アプライアンスのデプロイ.....406
ローカル ログ コレクタを使用する Panorama バーチャル アプライアンスのデプロイ.....411
ローカル ログ収集を使用するレガシー モードの Panorama バーチャル アプライアンスのデプロイ.....416

WildFire アプライアンスの管理.....419
Panorama で管理するスタンドアロン WildFire アプライアンスの追加.....420
Panorama での WildFire アプライアンスの基本設定..... 423
WildFire アプライアンスの認証の設定.....423
WildFire アプライアンスとクラスタのカスタム証明書を使用する認証のセットアップ.....434
Panorama の管理対象の WildFire アプライアンスのカスタム証明書を設定する.... 434
WildFire クラスタ用の単一のカスタム証明書で認証を設定する..... 436
Panorama で設定された WildFire アプライアンスにカスタム証明書を適用する.... 438
Panorama 管理からの WildFire アプライアンスの削除.....440
WildFire クラスタの管理.....441
Panoramaで集中的にクラスタを構成する..... 441
PanoramaをWildFireクラスタのステータスの表示..... 461
インターネット接続を使用してクラスタをセンターでアップグレードする..... 462
インターネット接続を使用してクラスタをセンターでアップグレードする..... 464

ライセンスの管理と更新.....469
Panorama を使用したファイアウォールのライセンス管理.....470
Panorama を使用したファイアウォール、ログ コレクタ、および WildFire アプライアンスへの更新のデプロイ.....472
サポートされている更新.....472

Panorama を使用してコンテンツ更新のスケジュールを設定 473
Panorama がインターネットに接続されている状態でログ コレクタをアップグレード 474
Panorama がインターネットに接続されていない状態でログ コレクタをアップグレード 477
Panorama がインターネットに接続されている状態でファイアウォールをアップグレード 481
Panorama がインターネットに接続されていない状態でファイアウォールをアップグレード 486
ZTP ファイアウォールのアップグレード 491
Panorama でコンテンツのアップデートを元に戻す 492

ネットワーク アクティビティのモニター 493
Panorama を使用した可視化 494
ACC およびアプリケーション スコープを使用したネットワークのモニタリング 494
ログ データの分析 496
レポートの生成、スケジュール設定、および電子メール送信 497
スケジュールされたレポートの鍵制限の設定 500
Panorama への Traps ESM ログの取り込み 502
「ユース ケース：Panorama を使用したアプリケーションのモニタリング 504
「ユース ケース：Panoramaを使用してインシデントに対処 507
インシデントの通知 507
ACC でウィジットを確認 507
脅威ログの確認 508
WildFire ログの確認 509
データ フィルタリング ログの確認 509
セキュリティ ルールの更新 510

Panorama の高可用性 511
Panorama HA の前提条件 512
HA 設定の Panorama での優先度とフェイルオーバー 514
フェイルオーバーのトリガー 515
HA ハートビート ポーリングおよび Hello メッセージ 515
HA パス モニタリング 515
Panorama HA でのロギングに関する考慮事項 516
レガシー モードの Panorama バーチャル アプライアンスでのロギングのフェイルオーバー 516
Panorama モードの M-Series アプライアンスまたは Panorama バーチャル アプライアンスでのロギングのフェイルオーバー 517
Panorama HA ピア間の同期 518
Panorama HA ペアの管理 519
Panorama での HA のセットアップ 519
HA ピア間のカスタム証明書を使用する認証のセットアップ 521
Panorama HA フェイルオーバーのテスト 522
Panorama のフェイルオーバーにより NFS ロギングが再開された後の優先度の切り替え 522
プライマリ Panorama のアクティブ状態への復元 523

Panorama の管理 525
設定変更のプレビュー、検証、コミット 526

自動コミットリカバリを有効化.....529
Panorama およびファイアウォールの設定のバックアップを管理.....531
設定ファイルのエクスポートのスケジュール設定.....531
Panorama およびファイアウォールの設定の保存およびエクスポート.....532
Panorama の設定変更を元に戻す.....535
Panorama に保存される設定バックアップ ファイルの上限数の設定.....537
管理対象ファイアウォールでの設定バックアップ ファイルのロード.....538
Panorama の設定変更の比較.....539
設定変更を制限するためのロックの管理.....540
Panorama にカスタム ロゴを追加.....542
Panorama タスク マネージャの使用.....543
ログおよびレポートのストレージ割り当ておよび有効期間を管理.....544
ログおよびレポートの保存.....544
ログおよびレポートの有効期間.....545
ログおよびレポートのストレージ割り当ておよび有効期間を設定.....545
Panorama レポートのランタイムの設定.....547
Panorama のモニタリング.....548
Panorama のシステム ログと設定ログ.....548
SNMP を使用して Panorama およびログ コレクタの統計を監視.....548
Panorama の再起動またはシャットダウン.....551
Panorama のパスワード プロファイルおよび複雑性の設定.....552

Panorama プラグイン.....553
Panorama プラグインについて.....554
Panorama プラグインをインストール.....555
VM-Series プラグインおよび Panorama プラグイン.....557
Panorama への VM-Series プラグインのインストール.....557

トラブルシューティング.....559
Panorama システムの問題のトラブルシューティング.....560
Panorama の診断ファイルの生成.....560
Panorama がサスペンド状態になっている場合の診断.....560
ファイル システム整合性チェックの監視.....560
ソフトウェア更新とコンテンツ更新が格納される Panorama ストレージの管理.....561
Panorama HA デプロイ環境でのスプリット ブレインからの回復.....562
ログ ストレージと接続に関する問題のトラブルシューティング.....563
Panorama　ポートの使用状況の確認.....563
コレクタ グループのログ保存エリアがゼロと表示される問題を解決する.....565
故障した M-Series アプライアンスのディスクを交換.....566
ESXi サーバーの仮想ディスクを交換.....566
vCloud Air サーバーの仮想ディスクを交換.....566
ログ コレクタ モードでログを新しい M-Series アプライアンスに移行.....567
Panorama モードでログを新しい M-Series アプライアンスに移行.....572
高可用性の Panorama モードで新しい M-Series アプライアンス モデルにログを移行.....578
高可用性の Panorama モードで同じ M-Series アプライアンス モデルにログを移行.....585
非 HA の Panorama で障害/RMA が発生した後のログ コレクタの移行.....591
M-Series アプライアンスの RAID ペアのメタデータを再生成.....594
ログ クエリ ジョブの閲覧.....595
RMA ファイアウォールの交換.....597
ファイアウォールの部分的なデバイス状態の生成.....597

RMA ファイアウォール交換の前準備 597
交換後のファイアウォール設定の復元 598
コミット エラーのトラブルシューティング 602
登録あるいはシリアル番号のエラーのトラブルシューティング 603
レポート エラーのトラブルシューティング 604
デバイス管理ライセンスエラーのトラブルシューティング 605
自動復帰ファイアウォール設定のトラブルシューティング 606
Panorama HA ピアがダウンした際の完全なコンテンツ更新 608
タスクの成否の確認 610
管理対象デバイスのポリシーマッチと接続のテスト 611
ポリシー ルールのトラフィックマッチのトラブルシューティング 611
ネットワーク リソースへの接続のトラブルシューティング 612
Panorama 10.0 からのダウングレード 614

Panorama の概要

Panorama™ 管理サーバーでは、Palo Alto Networks の次世代ファイアウォールおよび WildFire アプライアンスとアプライアンス クラスタを一元的に監視、管理できます。1つの画面からすべてのアプリケーション、ユーザー、ネットワークを通過するコンテンツを管理し、ここから得られる情報を使用してネットワーク全体を保護および制御するアプリケーション有効化ポリシーを作成することができます。Panorama を使用してポリシーとファイアウォールを中央管理すると、ファイアウォールの分散ネットワークを効率的に管理および維持できます。WildFire アプライアンスおよび WildFire アプライアンス クラスタの一元的な管理に Panorama を使用すると、1 つのネットワークでサポートできるファイアウォールの数が増えて、耐障害性のために高可用性が提供され、管理効率が上がります。

- Panorama について
- Panorama モデル
- ファイアウォール設定および更新の中央管理について
- ログとレポートの中央管理
- Panorama を使用したデータの再配信
- ロールベースのアクセス制御
- Panorama のコミット、検証、およびプレビュー操作
- Panorama のデプロイ計画
- Panorama のデプロイ：タスクの概要

Panorama について

Panorama では、中央管理により、Palo Alto Networks ファイアウォールを効果的に設定、管理、およびモニターできます。以下の主な 3 つのエリアで Panorama の付加価値が得られます。

- 一元的な設定およびデプロイ – ネットワーク上のファイアウォールおよび WildFire アプライアンスの中央管理と迅速なデプロイを簡略化するには、Panorama を使用して、デプロイのためにファイアウォールおよび WildFire アプライアンスを事前に設定します。次に、ファイアウォールをグループにまとめて、ネットワークおよびデバイスの基本設定を適用する各種テンプレートを作成し、デバイスグループを使用して共有ポリシーとローカル ポリシー ルールをグローバルに管理できます。ファイアウォール設定および更新の中央管理についてを参照してください。
- 分析およびレポートの中央管理による集約ロギング – ネットワーク上のすべての管理対象ファイアウォールのアクティビティに関する情報を収集して一元的に分析し、データの調査とレポートを行います。このようにネットワーク トラフィック、ユーザー アクティビティおよび関連タスクの包括的なビューを提供することで、ネットワーク上のアプリケーションを安全に有効化できる豊富なポリシーセットを使用して、潜在的な脅威に対応できるようになります。一元的なロギングおよびレポーティングを参照してください。
- 分散管理 – グローバル/ローカルのファイアウォール設定およびポリシーへのアクセスを委任または制限できます。分散管理での適切なアクセス レベルの委任の詳細は、ロールベースのアクセス制御を参照してください。

4つの Panorama モデル が利用可能です。Panorama バーチャル アプライアンス、M-600 アプライアンス、M-500 アプライアンス、および M-200 アプライアンスは PAN-OS 10.0 に対応しています。Panorama 中央管理 は、Panorama を高可用性 (HA) 構成でデプロイして、ファイアウォールを管理する方法を示しています。

© 2019 Palo Alto Networks, Inc.

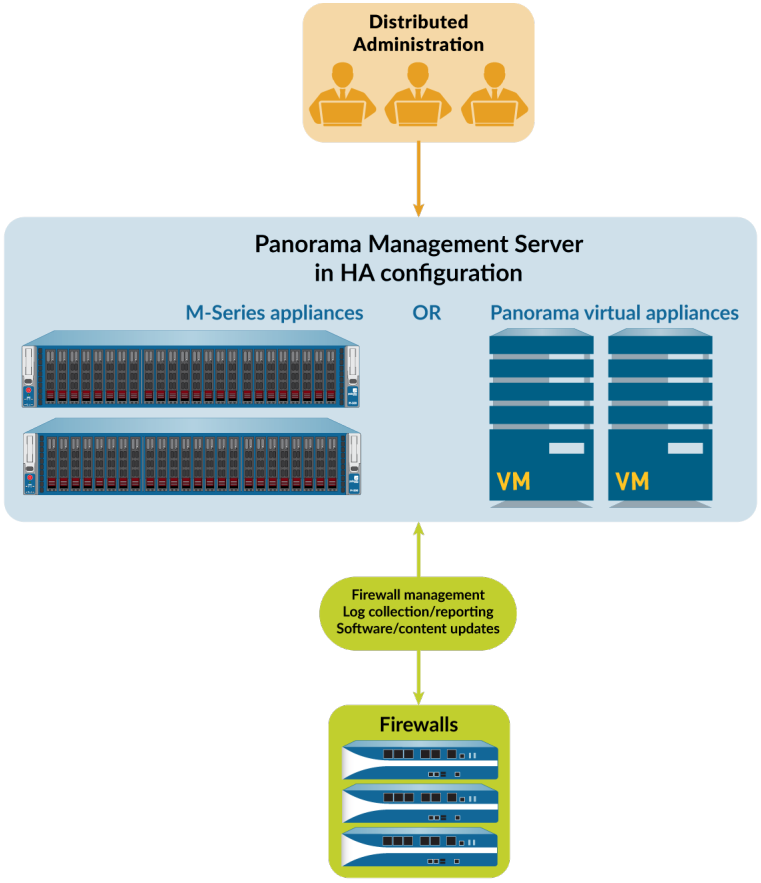


図 1 : Panorama 中央管理

© 2019 Palo Alto Networks, Inc.

Panorama モデル

Panorama は、次のいずれかの仮想アプライアンスまたは物理アプライアンスとして使用でき、最大 25 台、100 台、または 1,000 台のファイアウォールを管理できるライセンスをサポートします。さらに、M-600 アプライアンス、および同様にリソースが割り当てられた Panorama バーチャル アプライアンスは、最大 5,000 のファイアウォールを管理するライセンスもサポートしています。

- **Panorama** バーチャル アプライアンス – このモデルでは、シンプルなインストールが可能で、バーチャル管理アプライアンスを必要とするサイトのサーバ統合が容易になります。Panorama は、Amazon Web Services（AWS）、AWS GovCloud、Microsoft Azure、Google Cloud Platform（GCP）、KVM、Hyper-V、VMware ESXi サーバ、または VMware vCloud Air にインストールできます。バーチャル アプライアンスは、毎秒最大 10,000 件のログレートでファイアウォール ログをローカルに収集することができ、専用ログ コレクタを管理してロギング速度を高めることができます。バーチャル アプライアンスは、専用の管理サーバー、ローカル ログ収集機能を備えた Panorama 管理サーバー、または専用ログ コレクタとして機能することができます。サポートされているインターフェイス、ログの保存容量、ログ収集の最大速度については、Panorama バーチャル アプライアンスのセットアップ前提条件を参照してください。バーチャル アプライアンスは次のモードでデプロイできます。
  - **Panorama** モード – このモードの Panorama バーチャル アプライアンスでは、1 ~ 12 個の仮想ロギング ディスクを使用するローカル ログ コレクタがサポートされます（「ローカル ログ コレクタを使用する Panorama バーチャル アプライアンスのデプロイ」を参照）。各ロギング ディスクには 2TB のストレージ容量があり、合計は、シングル バーチャル アプライアンスで最大 24TB、高可用性（HA）ペアで 48TB です。Panorama モードのみで、既存のディスクのログを失わずに、複数の仮想ロギング ディスクを追加できます。Panorama モードには、レポート生成が速いという利点もあります。Panorama モードのバーチャル アプライアンスでは、NFS ストレージがサポートされません。

    バーチャル アプライアンスを *Panorama* モードでデプロイして、ログ ストレージとレポート生成を最適化することをお薦めします。
  - レガシー モード（ESXi および vCloud Air のみ） – このモードの Panorama バーチャル アプライアンスは、ローカル ログ コレクタを使用せずにファイアウォール ログを受信して保存します（「ローカル ログ収集を使用するレガシー モードの Panorama バーチャル アプライアンスのデプロイ」を参照）。デフォルト設定では、レガシー モードのバーチャル アプライアンスは、すべてのデータに 1 つのディスク パーティションを使用します。約 11GB のパーティションがログの保存に割り当てられます。ローカルのログ保存容量がさらに必要である場合は、ESXi 5.5 以降のバージョンまたは vCloud Air であれば、最大 8TB の仮想ディスクを追加できます。それよりも古い ESXi バージョンでは、最大 2TB の仮想ディスクをサポートしています。8TB を超える容量が必要な場合は、レガシー モードのバーチャル アプライアンスを NFS データストアにマウントできますが、これは ESXi サーバー上でのみ可能です（vCloud Air は不可）。このモードは、PAN-OS 10.0 へのアップグレード時に Panorama バーチャル アプライアンスがレガシー モードの場合にのみ使用できます。PAN-OS 9.0 以降のリリースにアップグレードすると、他のモードに変更した場合、レガシーモードは使用できなくなります。Panorama バーチャル アプライアンスをレガシー モードから使用可能なモードに変更すると、レガシー モードに戻ることができなくなります。

    レガシーモードはサポートされますが、実稼働環境には推奨されず、ラボまたはデモ環境で引き続き使用できます。
  - 管理専用モード–このモードでは、Panorama バーチャル アプライアンスは、管理対象デバイスおよび専用ログ コレクタ専用の管理アプライアンスであり、このモードでは、適切にリソースが割り当てられた Panorama バーチャル アプライアンスが、最大 5,000 のファイアウォールを管理できます。Panorama バーチャル アプライアンスには、設定ログとシステム ログ以外のログ収集機能はなく、ログを保存するには専用ログコレクタが必要です。デフォルトでは、管理専用モードのバーチャル アプライアンスには、すべてのデータ用にディスク パーティションが 1 つしかないため、

© 2019 Palo Alto Networks, Inc.

管理専用モードの Panorama バーチャル アプライアンスに転送されたすべてのログは削除されます。したがって、管理対象アプライアンスからのログデータを保存するには、管理対象デバイスからのログ データを保存するために、ログ転送を設定しなければなりません。詳細は、「デバイス管理能力要件の強化」を参照してください。

- ログ コレクタ モード —Panorama バーチャル アプライアンスは、専用ログ コレクタとして機能します。複数のファイアウォールが大量のログ データを転送する場合は、ログ コレクタ モードの Panorama バーチャル アプライアンスにより、規模を拡大し、パフォーマンスを向上させることができます。このモードの場合、アプライアンスには管理者アクセスを行うためのWeb インターフェイスがありません。コマンドライン インターフェイス (CLI) のみを使用できます。ただし、Panorama 管理サーバーの Web インターフェイスを使用してアプライアンスを管理できます。ログ コレクタ モードの Panorama バーチャル アプライアンスに CLI でアクセスする必要があるのは、初期セットアップ時およびデバッグ時のみです。設定の詳細については、専用のログ コレクタを使用する Panorama のデプロイを参照してください。

- **M-Series** アプライアンス — M-200、M-500、および M-600 アプライアンスは、大規模なデプロイを目的とした専用ハードウェア アプライアンスです。(10,000ログ/秒を超える) ロギングレートとログ保持要件の高い環境の場合、このアプリケーションを使用することで、ログ収集インフラストラクチャのスケーリングが可能になります。サポートされているインターフェイス、ログの保存容量、ログ収集の最大速度については、M-Series アプライアンス インターフェイスを参照してください。すべての M-Series モデルの共通属性は次のとおりです。

  - ファイアウォール ログを保存する RAID ドライブ、および RAID 1 ミラーリングによる、ディスク エラーからの保護
  - Panorama およびログ コレクタが生成するログを保存する SSD
  - 1Gbps のスループットをサポートする、MGT、Eth1、Eth2、Eth3 の各インターフェイス
  - 冗長、ホット スワップ可能なデュアル電源
  - 前面から背面へのエアフロー

  M-600 および M-500 アプライアンスにはさらに次の属性があり、データ センターにより適合しています。

  - 10Gbps のスループットをサポートする、Eth4 および Eth5 インターフェイス

  さらに、以下の属性により、M-600 アプライアンスは大規模なファイアウォールのデプロイメントにより適しています。

  - 管理専用モードの M-600 アプライアンスは、最大 5,000 のファイアウォールを管理できます。

  M-Series アプライアンスは次のモードでデプロイできます。

  - **Panorama** モード — アプライアンスは Panorama 管理サーバーとして機能し、ファイアウォールと専用ログ コレクタを管理します。このアプライアンスではローカル ログ コレクタもサポートされて、ファイアウォール ログが集約されます。Panorama モードがデフォルト モードです。設定の詳細については、「ローカル ログ コレクタを使用する Panorama M-Series アプライアンスのデプロイ」を参照してください。
  - 管理専用モード—Panorama アプライアンスは、管理対象デバイスおよび専用ログ コレクタ専用の管理アプライアンスです。Panorama アプライアンスには、設定ログとシステムログ以外のログ収集機能はなく、デプロイメントには、ログを保存するための専用ログ コレクタが必要です。デフォルトでは、管理専用モードの Panorama アプライアンスには、すべてのデータ用にディスク パーティションが 1 つしかないため、管理専用モードの Panorama バーチャル アプライアンスに転送されたすべてのログは削除されます。したがって、管理対象アプライアンスからのログ データを保存するには、管理対象デバイスからのログデータを保存するために、ログ転送を設定しなければなりません。
  - ログ コレクタ モード — アプライアンスは、専用ログ コレクタとして機能します。複数のファイアウォールが大量のログ データを転送する場合は、ログ コレクタ モードの M-Series アプライアンスにより、規模を拡大し、パフォーマンスを向上させることができます。このモードの場合、アプライアンスには管理者アクセスを行うためのWeb インターフェイスがありません。コマンドライン インターフェイス (CLI) のみを使用できます。ただし、Panorama 管理サーバーの Web インター

© 2019 Palo Alto Networks, Inc.

フェイスを使用してアプライアンスを管理できます。ログ コレクタ モードの M-Series アプライアンスに CLI でアクセスする必要があるのは、初期セットアップ時およびデバッグ時のみです。設定の詳細については、専用のログ コレクタを使用する Panorama のデプロイを参照してください。

M-Series アプライアンスの詳細情報と仕様についてはM-Series アプライアンスのハードウェア リファレンス ガイドをご覧ください。

© 2019 Palo Alto Networks, Inc.

ファイアウォール設定および更新の中央管理について

Panorama™ では、デバイス グループとテンプレートを使用して、類似した設定を必要とする論理セットにファイアウォールをグループ化します。デバイス グループおよびテンプレートを使用し、すべての管理対象のファイアウォールのすべての設定要素、ポリシー、オブジェクトを一元管理できます。また、Panorama ではライセンス、ソフトウェア (PAN-OS® ソフトウェア、SSL-VPN クライアント ソフトウェア、GlobalProtect™ エージェント/アプリ ソフトウェア) 、およびコンテンツ更新 (アプリケーション、脅威、WildFire®、およびアンチウイルス) を一元管理することもできます。

- ファイアウォールと Panorama 間のコンテキスト切り替え
- Panorama の合計コンフィグレーションサイズ
- テンプレートおよびテンプレート スタック
- Device Groups (デバイス グループ)

ファイアウォールと Panorama 間のコンテキスト切り替え

Panorama™ Web インターフェイスでは、各タブの左上にある **Context** (コンテキスト) ドロップダウンメニューを使用して Panorama 中心のビューとファイアウォール中心のビューを切り替えることができます。**Context** (コンテキスト) を **Panorama** に設定してファイアウォールを一元管理するか、コンテキストを特定のファイアウォールの Web インターフェイスに切り替えてローカルで設定します。Panorama およびファイアウォールの Web インターフェイスは似ているため、ファイアウォールを監視、管理するために両方を行き来しても違和感がありません。

Context (コンテキスト) ドロップダウンリストには Panorama に接続されているファイアウォールのみが表示されます。デバイス グループおよびテンプレート管理者の場合、その管理者に割り当てられているアクセスドメイン内にある接続済みのファイアウォールのみがこのドロップダウンリストに表示されます。大きなリストを検索する際はドロップダウンリストからフィルターを使用することができます。

高可用性 (HA) 構成のファイアウォールの場合、背景に色がついて HA 状態であることが分かります (次のとおり) 。ファイアウォールのコンテキストを選択する際に HA の状態が分かっていると便利です。例えば通常、アクティブ ファイアウォールでファイアウォール固有の設定変更を行います。

- 緑色–アクティブ。
- 黄色 – パッシブ、またはファイアウォールが開始中 (起動後、開始中状態が最大 60 秒継続します)。
- 赤色 – ファイアウォールが非稼働状態 (エラー状態)、サスペンド状態 (管理者がファイアウォールを無効にした)、または仮の状態 (アクティブ/アクティブ HA 設定におけるリンクまたはパスのモニタリング イベント用) である。

Panorama の合計コンフィグレーションサイズ

Panorama™ M-Series とバーチャル アプライアンスの総コンフィグレーションファイルサイズは、セキュリティ要件を満たすことを確認するために、どの M-Series アプライアンスにするか決定する、または Panorama バーチャル アプライアンス上で割り当てる必要のあるバーチャル リソースの最小量を判定する際のパフォーマンス指標となる重要な部分です。サポートされている Panorama 管理サーバーの総コンフィグレーションファイルサイズを超過すると、設定の変更、コミット、マネージドファイアウォールへのプッシュを実行する時にパフォーマンスが低下します。

Panorama モードの Panorama 管理サーバーは、すべてのテンプレート、デバイス グループ、Panorama 固有設定の 80MB の総コンフィグレーションファイルサイズをサポートします。管理専用モードの Panorama は、Panorama モデルまたは Panorama バーチャル アプライアンスに割り当てるリソースに応じて、最大で 120MB または 150MB の総コンフィグレーションファイルサイズをサポートしま

© 2019 Palo Alto Networks, Inc.

す。Panorama M-Series アプライアンス モデルまたは Panorama バーチャル アプライアンスに割り当てるリソースを基準にした、推奨される最大コンフィグレーションファイルサイズについては、以下の表を参照してください。

Panorama モデル	必須のバーチャル リソース	推奨される最大 Panorama コンフィグレーションファイル サイズ
M-200	N/A	120MB
M-500		120MB
M-600		150MB
Panorama バーチャル アプライアンス 追加のセットアップ情報については、Panorama バーチャル アプライアンスのセットアップ前提条件を参照してください。	• 16 vCPU • 128 GB メモリ	120MB
	• 56 vCPU • 256GB メモリ	150MB

テンプレートおよびテンプレート スタック

テンプレートとテンプレート スタックは、ネットワーク上でファイアウォールが動作するのに必要な設定を行うために使用します。テンプレートは、Panorama™の**Network**（ネットワーク）タブと**Device**（デバイス）タブの設定に使用する基本的な構成要素です。テンプレートを使用して、インターフェイスとゾーンの設定を定義したり、ロギングや syslog アクセス用のサーバー プロファイルを管理したり、VPN 設定を定義したりすることができます。テンプレート スタックを使用すると、複数のテンプレートをレイヤーして組み合わせた設定を作成できます。テンプレート スタックは、テンプレート スタックに接続されているすべてのデバイスに共通の基本設定を定義できるため、また、テンプレートをレイヤー化して組み合わせた設定を作成できるため、管理が簡単になります。これにより、場所または機能固有の設定でテンプレートを定義し、優先順位の降順でテンプレートをスタックすることができ、ファイアウォールはスタック内のテンプレートの順序に基づいて設定を継承します。

テンプレートとテンプレートスタックは両方とも変数に対応しています。変数を使用すると、設定ニーズに基づいてテンプレートまたはテンプレート スタックに指定された値を持つプレースホルダ オブジェクトを作成できます。設定内の IP アドレス、グループ ID、およびインターフェイスを置き換えるテンプレートまたはテンプレート スタック変数を作成します。テンプレート変数はテンプレート スタックに継承され、テンプレート スタック変数を作成するためにオーバーライドすることができます。ただし、テンプレートはテンプレート スタックで定義された変数を継承しません。変数がテンプレートまたはテンプレート スタックで定義され、ファイアウォールにプッシュされると、変数に定義された値がファイアウォールに表示されます。

固有の設定を持つファイアウォールに対応するには、テンプレートを使用してテンプレートスタック設定をオーバーライドすることができます。あるいは、より具体性の低い共通の基本設定をプッシュし、プッシュされた特定の設定を個々のファイアウォールでファイアウォール固有の値でオーバーライドすることもできます。ファイアウォール上の設定をオーバーライドする際、ファイアウォールがその設定をローカル設定に保存し、Panorama はその設定を管理しなくなります。テンプレート値をオーバーライドした後に復元するには、Panorama を使用してテンプレートまたはテンプレート スタック設定をファイアウォールに強制的に適用します。例えば、テンプレートに共通の NTP サーバーを定義し、ファイアウォールの NTP サーバーの設定をオーバーライドしてローカルのタイム ゾーンに合わせた後でも、テンプレートで定義された NTP サーバーに復元することができます。

© 2019 Palo Alto Networks, Inc.

テンプレート スタックを定義する際、ハードウェア モデルが同じであり、類似するネットワーク リソース（ゲートウェイや Syslog サーバーなど）へのアクセスを必要とするファイアウォールを割り当てることを検討してください。これにより、各々のテンプレート スタックに同じ設定を何度も追加する必要がなくなります。次の図は、アジア太平洋地域（APAC）地域のデータセンター ファイアウォールをグローバル設定のスタック、APAC 固有設定のテンプレート、データセンター固有設定のテンプレートに割り当てる例を示しています。支店固有の設定を持つテンプレートを含む別のスタックにグローバルおよび APAC 固有のテンプレートを追加することで、それらを再度使用して APAC の支店でファイアーウォールを管理することができます。スタック内のテンプレートには設定の優先順位があるため、重複した設定がある場合に Panorama が値を一つだけプッシュできるようになります。Panorama はスタック設定にリストアップされたテンプレートを上から順に（優先度が高い順に）評価していきます。次の図は、データセンターテンプレートの優先度がグローバル テンプレートよりも高いデータセンタースタックを示しています。Panoramaはデータセンターテンプレートからアイドル タイムアウトの値をプッシュし、グローバル テンプレートからの値を無視します。

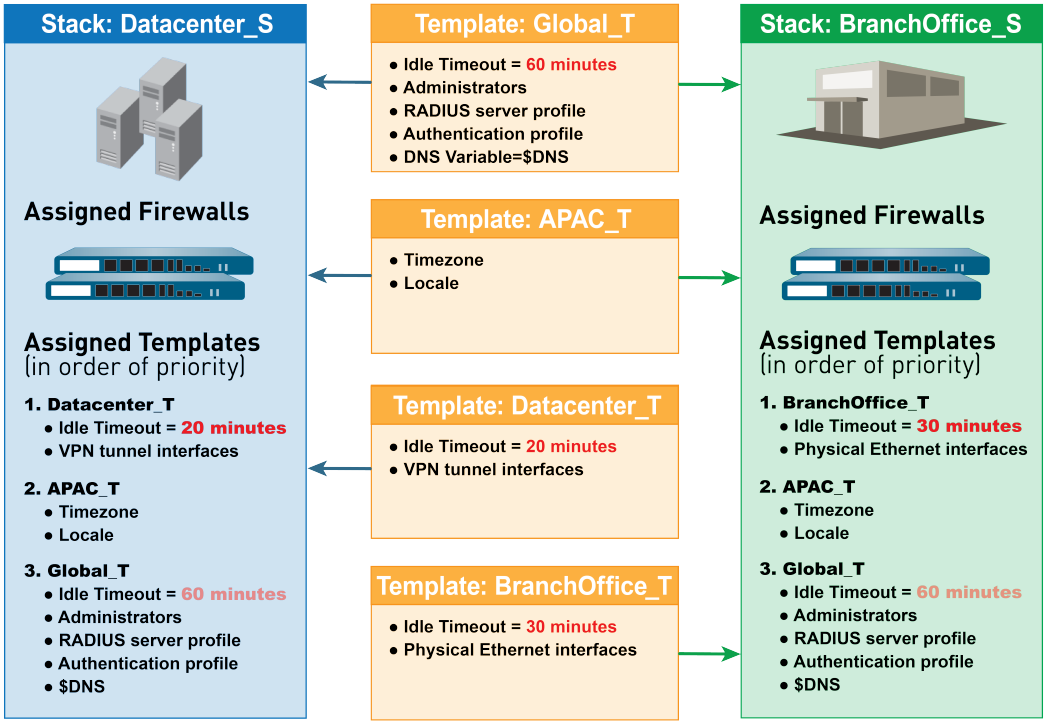


図 **2 :** テンプレート スタック

テンプレートまたはテンプレート スタックを使って次のファイアウォール モードを設定することはできません：仮想プライベートネットワーク（VPN）モード、複数の仮想システム（multi-vsys）モード、または動作モード（通常モードまたは FIPS-CC モード）。詳細については「テンプレートの機能および例外」を参照してください。しかし、非マッチング モードを持つファイアウォールを同じテンプレートあるいはスタックに割り当てることはできます。その場合、Panorama は、モード固有の設定を、そのモードをサポートするファイアウォールにのみプッシュします。例外として、テンプレート内のデフォルトの vsys の設定を、仮想システムをサポートしていないファイアウォールまたは仮想システムが設定されていないファイアウォールにプッシュするように、Panorama を設定できます。

関連作業については「テンプレートおよびテンプレートスタックの管理」を参照してください。

Device Groups（デバイス グループ）

Panorama を効果的に使用するには、ネットワーク内のファイアウォールをデバイス グループと呼ばれる論理ユニットにグループ化する必要があります。デバイスグループを使用すれば、ネットワークのセグメント化、地理的な口ケーション、組織の役割、あるいは類似のポリシー設定を必要とする各ファイア

© 2019 Palo Alto Networks, Inc.

ウォールに共通するその他の要素に基づいてグループ化を行うことができます。デバイスグループを使用し、ポリシールールやそれらが参照するオブジェクトを設定することができます。共有ルールおよびオブジェクトを最上層に、デバイスグループ固有のルールおよびオブジェクトをその配下に置くことで、デバイスグループを階層化することができます。これにより、ファイアウォールがトラフィックを扱う方法を規定する各ルールを階層化することができます。例えば、一連の共有ルールを企業の利用規定として定義することができます。次に、BitTorrent などのピアツーピア トラフィックへのアクセスを支社にのみ許可するために、Panorama がその支社だけにプッシュするデバイスグループのルールを定義することができます（あるいは共有セキュリティルールを定義し、その支社のみを対象にします）。関連作業についてはデバイス グループの管理を参照してください。デバイスグループのコンセプトやコンポーネントの詳細な説明は、以下のトピックでご確認いただけます。

- デバイス グループ階層
- デバイス グループ ポリシー
- デバイス グループ オブジェクト

デバイス グループ階層

デバイス グループの階層を作成を行えば、デバイスグループを最大 4 層から成るツリー構造に階層化し、下位のグループに上位のグループの設定（ポリシールールおよびオブジェクト）を継承させることができます。一番下のレベルのデバイス グループは、親、その親、またその親のデバイス グループ（先祖）を持つことができます。一番上のレベルのデバイス グループは、子、孫、曾孫のデバイス グループ（子孫）を持つことができます。すべてのデバイスグループは共有領域（すべてのデバイスグループで共通する設定を格納する最上位層）から設定を継承します。

デバイスグループを階層化することで、冗長な設定作業を行うこと無く、共通するポリシー要件に基づいて各ファイアウォールを組織化することができます。例えば、最上層にすべてのファイアウォールに共通するグローバルな設定を作成したり、役割固有の設定を持つデバイスグループを設定したり、その配下にロケーション固有の設定を持つデバイスグループを設定したりすることができます。階層構造を利用しなければ、Shared（共有）以下の単一の層にあるすべてのデバイスグループに対して役割固有の設定とロケーション固有の設定をどちらも行わなければならなくなります。

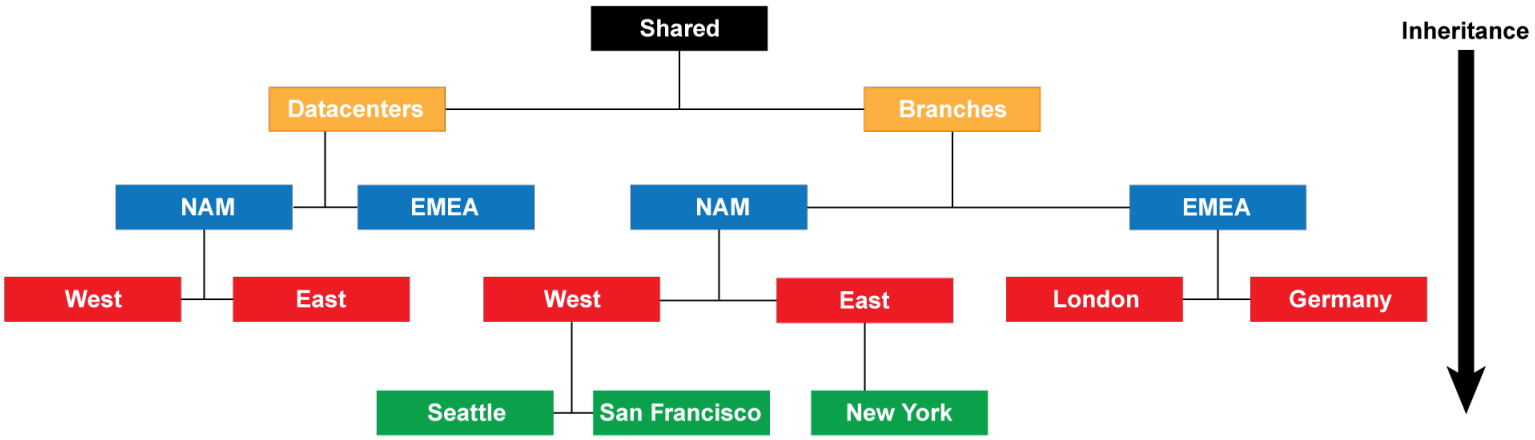


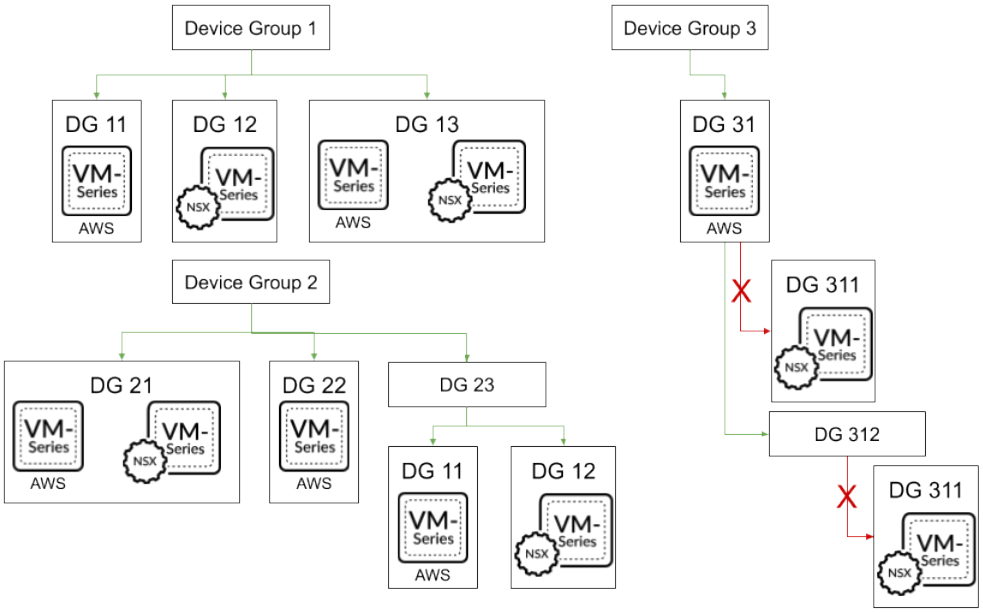
図 3：デバイス グループ階層

デバイスグループの階層構造においてファイアウォールがポリシールールを評価する順序についてはデバイス グループ ポリシーを参照してください。デバイスグループが先祖デバイスグループから継承したオブジェクトの値をオーバーライドする方法についてはデバイス グループ オブジェクトを参照してください。

複数の実行する Panorama プラグイン デプロイメントで、特定のハイパーバイザにデプロイされたファイアウォールを含むデバイス グループを、別のハイパーバイザにデプロイされたファイアウォールを含むデバイス グループの子または親にすることはできません。たとえば、Panorama が VMware NSX-V および

© 2019 Palo Alto Networks, Inc.

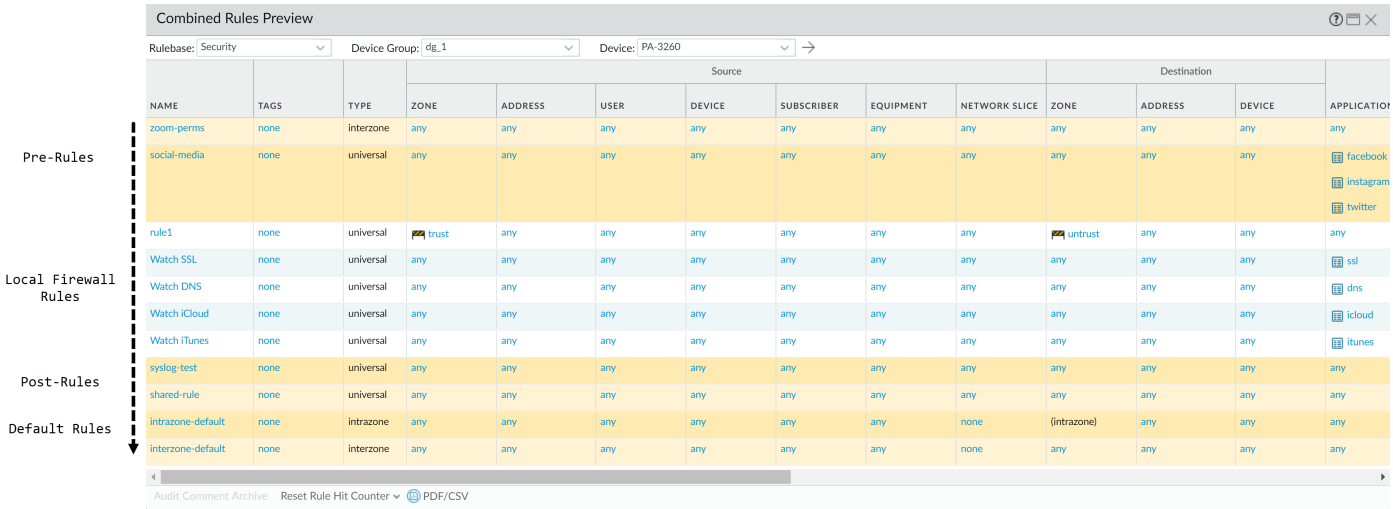
AWS から IP アドレスの更新を受信した場合、AWS VM-Series ファイアウォール デバイスグループの子である NSX-V VM-Series ファイアウォールのデバイス グループを作成することはできません。



デバイス グループ ポリシー

デバイス グループを使用すると、管理対象ファイアウォールのネットワーク全体のポリシーを管理する階層的な手段を実装できます。ファイアウォールは、層 (共有、デバイスグループ、およびローカル) ごとに、種類 (プレルール、ポストルール、およびデフォルトルール) ごとに次の順序で上から順番にポリシールールを評価します。ファイアウォールはトラフィックを受け取ると、そのトラフィックにマッチする最初に評価したルールで定義されているアクションを実行し、それ以降のルールはすべて無視します。特定の層、タイプ、ルールベース (例：共有セキュリティ プレルール) であるルールの評価順序を変える場合はルール階層の管理をご覧ください。

ルールをファイアウォールまたは Panorama のどちらで表示するかに関わらず、ルールは評価順で Web インターフェイスに表示されます。すべての共有ルール、デバイス グループ ルール、およびファイアウォールが Panorama から継承するデフォルトのルールは、オレンジ色で表示されます。ローカルのファイアウォール ルールは、プレルールとポストルールの間に表示されます。



© 2019 Palo Alto Networks, Inc.

評価順序	ルール範囲と説明	管理デバイス
共有プレ ルール デバイス グループのプレ ルール	Panorama はすべてのデバイスグループの全ファイアウォールに共有プレ ルールをプッシュします。Panorama は特定のデバイスグループおよびその子孫デバイスグループのすべてのファイアウォールにデバイスグループ固有のプレルールをプッシュします。 ファイアウォールがデバイスグループの階層構造において複数の層にあるデバイスグループからルールを継承する場合、上位から下位へとプレルールを評価します。そのため、ファイアウォールはまず共有ルールを評価し、子孫を持たないデバイスグループのルールを最後に評価することになります。 プレルールを使用すれば、組織の利用規約に対する遵守を徹底させることができます。例えば、プレルールによって特定の URL カテゴリへのアクセスをブロックしたり、すべてのユーザーの DNS（Domain Name System）トラフィックを許可したりする場合があり得ます。	これらのルールはファイアウォール上に表示されますが、管理は Panorama でしか行えません。
ローカル ファイアウォールのルール	ローカル ルールは、単体のファイアウォールあるいは仮想システム（vsys）に固有のものです。	ローカルのファイアウォール管理者またはローカル ファイアウォール コンテキストに切り替えた Panorama 管理者が、ローカル ファイアウォール ルールを編集できます。
デバイス グループのポスト ルール 共有ポスト ルール	Panorama はすべてのデバイスグループの全ファイアウォールに共有ポスト ルールをプッシュします。Panorama は特定のデバイスグループおよびその子孫デバイスグループのすべてのファイアウォールにデバイスグループ固有のポストルールをプッシュします。 ファイアウォールがデバイスグループの階層構造において複数の層にあるデバイスグループからルールを継承する場合、下位から上位へとポストルールを評価します。そのため、ファイアウォールはまず子孫を持たないデバイスグループのルールを評価し、共有ルールを最後に評価することになります。 通常、ポスト ルールには、App-ID™ のシグネチャ、User-ID™ の情報（ユーザーまたはユーザー グループ）、または	これらのルールはファイアウォール上に表示されますが、管理は Panorama でしか行えません。

© 2019 Palo Alto Networks, Inc.

評価順序	ルール範囲と説明	管理デバイス
	サービスに基づいてトラフィックへのアクセスを拒否するルールが含まれます。	
イントラゾーン デフォルト インターゾーン デフォルト	デフォルトルールはセキュリティ ルールベースにのみ適用され、Panorama（共有レベル）およびファイアウォール（各 vsys において）で事前に定義されています。これらのルールは、他のあらゆるルールにマッチしないトラフィックを PAN-OS が扱う方法を規定します。 イントラゾーン デフォルト ルールはあるゾーンにおけるすべてのトラフィックを許可します。インターゾーン デフォルト ルールはゾーン間におけるすべてのトラフィックを拒否します。 デフォルトルールをオーバーライドすると、その優先順序が下位から上位の順になります。すなわち、ファイアウォール レベルでオーバーライドされた設定は、デバイス グループ レベルの設定よりも優先されることになり、共有レベルの設定よりも優先度が高くなります。	デフォルト ルールは事前定義済みの設定の一部であるか、Panorama によってファイアウォールにプッシュされたルールであるため、最初は読み取り専用になっています。ただし、タグ、アクション、ログ記録、およびセキュリティ プロファイルのルール設定はオーバーライドできます。ルールをオーバーライドできるレベルは、コンテキストによって決まります。 • Panorama—事前に定義された設定の一部であるデフォルトルールを共有あるいはデバイス グループ レベルでオーバーライドできます。 • Firewall—ファイアウォールまたは vsys で事前に定義された設定の一部であるデフォルトルール、あるいは Panorama が共有領域あるいはデバイス グループからプッシュしたデフォルトルールをオーバーライドできます。

デバイス グループ オブジェクト

オブジェクトは、ポリシールールが参照する設定要素です。例えば、IPアドレス、URL カテゴリ、セキュリティ プロファイル、ユーザー、サービス、アプリケーションなどです。あらゆるタイプのルール（プレルール、ポストルール、デフォルトルール、ファイアウォールのローカルで定義されたルール）およびあらゆるルールベース（セキュリティ、NAT、QoS、ポリシーベースの転送、復号化、アプリケーション オーバーライド、キャプティブポータル、および DoS 保護）がオブジェクトを参照できます。デバイス グループ階層のオブジェクトと同じ範囲を持つルールであれば、いくらでもオブジェクトを再利用できます。例えばオブジェクトを共有領域に追加する場合、あらゆるデバイスグループは共有領域からオブジェクトを継承するため、階層構造中のすべてのルールがその共有オブジェクトを参照することができます。オブジェクトを特定のデバイスグループに追加する場合、そのデバイスグループおよびその子孫デバイス グループのルールだけがデバイス グループ オブジェクトを参照できます。デバイス グループのオブジェクトの値を、先祖デバイス グループから継承された値以外のものにしなければならない場合は、継承したオブジェクトの値をオーバーライドできます（継承したオブジェクトの値をオーバーライドする手順を参照）。また、いつでも継承したオブジェクトの値を復元することが可能です。共有またはデバイス グループ ポリシーで使用するオブジェクトの作成を一度行って繰り返し使用すれば、管理面のオーバーヘッドを軽減し、各ファイアウォール ポリシーの一貫性を保つことができます。

システム全体で Panorama が共有オブジェクトを処理する方法を設定できます。

- **Pushing unused objects**（未使用のオブジェクトをプッシュ）—共有あるいはデバイスグループのポリシールールがそのオブジェクトを参照しているかどうかに関わらず、Panorama はデフォルトですべての共有オブジェクトをファイアウォールにプッシュします。任意で、参照されているオブジェクトのみを Panorama がプッシュするように設定することもできます。詳細については、「未使用の共有オブジェクトの管理」を参照してください。
- **Precedence of ancestor and descendant objects**（先祖および子孫オブジェクトの優先度）—デバイス グループデフォルト設定では、階層構造における複数の階層にあるデバイスグループが同じ名前のオ

© 2019 Palo Alto Networks, Inc.

ブジェクトを持っていながら値が異なっている（例えばオーバーライドにより）場合、子孫デバイスグループのポリシールールは先祖デバイスグループあるいは共有から継承したオブジェクトの値ではなく、その子孫のオブジェクトの値を使用します。また、任意でこの優先度を逆にして、オブジェクトを含有する共有あるいはトップレベルの先祖の値をすべての子孫デバイスグループにプッシュすることもできます。詳細については、「継承したオブジェクトの優先度を管理」を参照してください。

© 2019 Palo Alto Networks, Inc.

ログとレポートの中央管理

Panorama では、すべての管理対象ファイアウォールからログを集約し、ネットワーク上のすべてのトラフィックを可視化できます。また、管理対象ファイアウォールに対して行われたすべてのポリシーおよび設定の変更に関する監査証跡も実行できます。Panorama では、ログを集約するだけでなく、SNMP トラップ、電子メール通知、Syslog メッセージ、HTTP ペイロードとしてログを外部サーバーに転送できます。

ログとレポートの集中管理については、Panorama とシームレスに動作する設計のクラウドベースの Cortex Data Lake を使用するオプションもあります。Cortex Data Lake により、管理対象ファイアウォールは、Panorama や管理対象ログ コレクタではなく、Cortex Data Lake 基盤にログを転送できるようになるため、既存の分散ログ収集のセットアップを増強でき、時間と労力をかけずに現在のロギング基盤を拡張することも可能です。

Panorama のアプリケーション コマンド センター（ACC）により、単一のペインを使用して、すべてのファイアウォールの統合されたレポートを生成できます。これにより、一元的にネットワーク アクティビティの監視を行い、トラフィックやセキュリティ インシデントを分析、調査、およびレポートできるようになります。Panorama では、ログを表示したり、Cortex Data Lake、Panorama、または管理対象ログ コレクタ（設定されている場合）に転送されるログからレポートを生成したり、管理対象ファイアウォールに直接クエリを発行したりできます。たとえば、Panorama（および管理対象コレクタ）に保存されているログに基づいて、または管理対象ファイアウォールにローカルに保存されているログにアクセスして、あるいは Cortex Data Lake において、管理対象ネットワーク内のトラフィック、脅威、および/またはユーザーアクティビティに関するレポートを生成できます。

Panorama へのログ転送の設定を行わない場合、または Cortex Data Lake を設定しない場合、管理対象ファイアウォールごとにレポートの実行スケジュールを設定して、結果を Panorama に転送することで、ユーザーアクティビティとネットワーク トラフィックの統合ビューを得られます。レポートでは、特定の情報およびアクティビティへの詳細なドリルダウンを実行することはできませんが、統合されたモニタリング アプローチは提供されます。

- 管理対象コレクタおよびコレクタ グループ
- ローカルおよび分散ログ収集
- 複数のログ コレクタを含むコレクタ グループに関する注意事項
- ログ転送オプション
- 一元的なレポート

管理対象コレクタおよびコレクタ グループ

Panorama は、ログ コレクタを使用して、管理対象ファイアウォールからのログを集約します。レポートを生成する際、Panorama は、ログ コレクタに対してクエリを実行し、ログ情報を取得します。これにより、ユーザーは、ファイアウォールが監視するすべてのネットワーク アクティビティを確認できます。ログ コレクタは Panorama を使用して設定および管理するため、ログ コレクタのことを管理対象コレクタと呼ぶこともあります。Panorama は、以下の 2 つのタイプのログ コレクタを管理できます。

- ローカル ログ コレクタ – このタイプのログ コレクタは、Panorama 管理サーバー上でローカルに実行されます。ローカル ログ コレクタをサポートするのは、Panorama モードの M-600、M-500 アプライアンス、M-200、M-100 アプライアンス、または Panorama バーチャル アプライアンスのみです。

  レガシー モードの *Panorama* バーチャル アプライアンスにログを転送する場合、ログは、ログ コレクタを使用せずにローカルに保存されます。
- 専用のログ コレクタ – これは、ログ コレクタ モードの M-600、M-500、M-200、M-100 アプライアンスまたはログ コレクタ モードのPanorama バーチャル アプライアンスです。Panorama モードの M-Series アプライアンス、または Panorama もしくは Legacy（ESXi および vCloud Air）モードの Panorama バーチャル アプライアンスを使用して、専用のログ コレクタを管理できます。Panorama

© 2019 Palo Alto Networks, Inc.

Web インターフェイスを使用して専用のログ コレクタを管理するには、専用のログ コレクタを管理対象コレクタとして追加する必要があります。そうしない場合、専用のログ コレクタへの管理アクセスは、定義済みの管理ユーザー（*admin*）アカウントを使用した CLI 経由のアクセスでのみ行うことができます。専用のログ コレクタでは、管理ユーザー アカウントを追加できません。

いずれかまたは両方のタイプのログ コレクタを使用して、ご使用の環境に最適なロギング ソリューションを構築できます（ローカルおよび分散ログ収集を参照）。

コレクタ グループは、単一の論理ログ収集ユニットとして動作する 1 から 16 個の管理対象コレクタです。コレクタ グループに専用のログ コレクタが含まれている場合、Panorama は、各ログ コレクタのすべてのディスク間およびグループ内のすべてのログ コレクタ間でログを均一に分散します。この分散により、使用可能なストレージ スペースが最適化されます。ログ コレクタでログを受信できるようにするには、ログ コレクタをコレクタ グループに追加する必要があります。複数のログ コレクタをコレクタ グループに割り当てることによってログの冗長性を有効にすることができます（複数のログ コレクタを含むコレクタ グループに関する注意事項を参照してください）。コレクタ グループ設定で、グループ内のログ コレクタにログを送信できる管理対象ファイアウォールを指定します。

ログコレクタおよびコレクタ グループを設定する方法については**ログ収集の管理**をご覧ください。

ローカルおよび分散ログ収集

Panorama への**ログ転送を設定**する前に、ローカル ログ コレクタを使用するのか、専用のログ コレクタを使用するのか、それともその両方を使用するのかを決定する必要があります。

ローカル ログ コレクタは、追加のハードウェアや仮想マシン インスタンスが不要であるため、簡単にデプロイできます。高可用性（HA）構成では、両方の Panorama ピアのローカル ログ コレクタにログを送信できます。つまり、フェイルオーバーが発生しても、パッシブ Panorama では、待ち時間なしでログ収集が開始されます。

ローカル ログ収集の場合、レガシー モードの *Panorama* バーチャル アプライアンスにログを転送することもできます。これらのログは、ログ コレクタを論理コンテナとして使用せずに保存されます。

専用のログ コレクタは、ログ コレクタ モードの M-600、M-500、M-200 または Panorama バーチャル アプライアンスです。専用のログ コレクタは、ファイアウォール管理を実行せず、ログ収集のみを実行します。そのため、ローカル ログ コレクタよりも堅牢な環境を実現できます。専用のログ コレクタには、以下の利点があります。

- Panorama 管理サーバーが、ロギングよりも管理機能により多くのリソースを使用できる。
- 専用のハードウェア アプライアンス上には大容量のログ ストレージを設置できる。
- ロギング レートをより高くすることができる。
- RAID 1 によるスケーラビリティと冗長性が得られる。
- ファイアウォールがリモートの Panorama 管理サーバーにログを送信する場合よりも、近くのログ コレクタに送信する方がより多くの帯域幅を使用できるネットワークにおいて、帯域幅のリソースを最適化できる。
- 地域の規制の要件を満たすことができる（たとえば、地域によってはログを残すことが許されない場合もあるでしょう）。

「**分散ログ収集**」は、HA 構成の Panorama ピアがファイアウォールと専用のログ コレクタの導入および設定を管理するトポロジーを示しています。

Panorama 管理サーバーは、*HA* 構成でデプロイできますが、専用のログ コレクタは、*HA* 構成でデプロイできません。

© 2019 Palo Alto Networks, Inc.

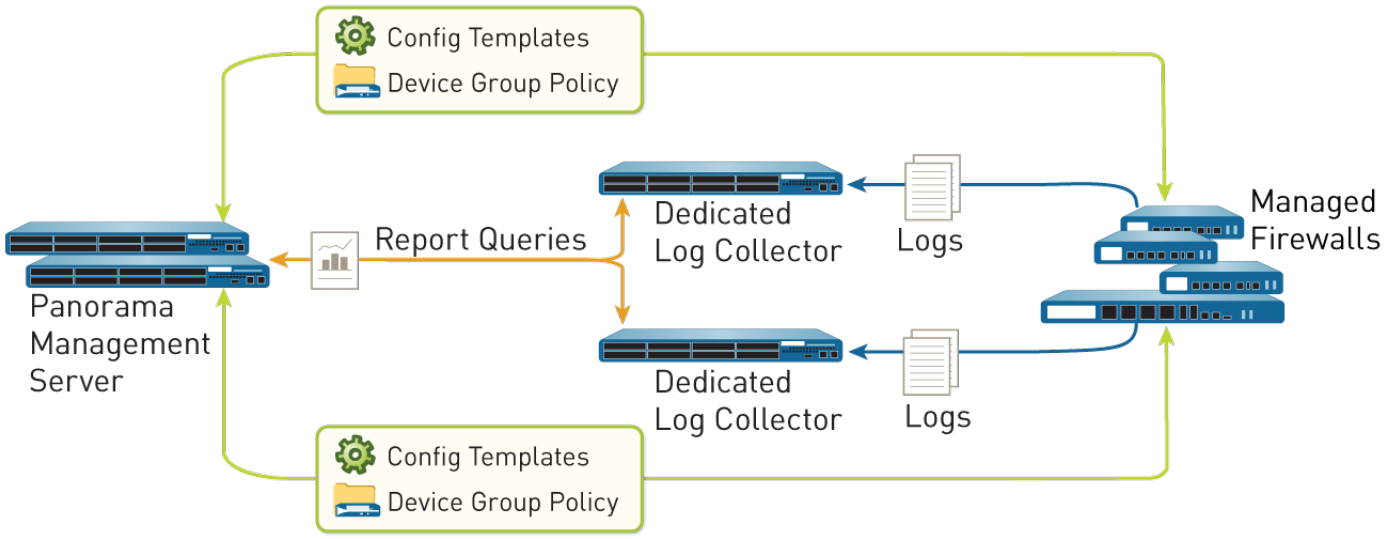


図 4 : 分散ログ収集 (DLC)

複数のログ コレクタを含むコレクタ グループに関する注意事項

複数のログ コレクタ (最大 16 個) を持つコレクタ グループの設定を行うことで、ログの冗長性を確保する、ログの保持期間を延ばす、単一のログ コレクタの能力を超えるロギング速度を達成することができます (能力については「Panorama モデル」を参照)。単一のコレクタ グループでは、すべてのログ コレクタ、すべての M-600 アプライアンス、すべての M-500 アプライアンス、すべての M-200 アプライアンス、すべての Panorama バーチャル アプライアンスは同じ Panorama モデルで動作する必要があります。たとえば、ある 1 つの管理対象ファイアウォールで 48TB のログを生成する場合、そのログを受信するコレクタ グループには少なくとも、M-200 アプライアンスである 6 つのログ コレクタ、あるいは M-500 アプライアンスまたは Panorama バーチャル アプライアンスである 2 つのログ コレクタが必要になります。

複数のログ コレクタが含まれているコレクタ グループは使用可能なストレージ スペースを単一の論理ユニットとして使用し、ログ コレクタ全体にかけてログを均等に分散します。ログの分散は、ログ コレクタのディスク容量 (「Panorama モデル」を参照) と、ログを所有してディスクに書き込むログ コレクタを動的に決定するハッシュ アルゴリズムに基づいて行われます。Panorama では、設定リストを使用して、管理対象ファイアウォールがログを転送できる各ログ コレクタの優先順位を設定しますが、ログは必ずしも設定リストで最初に指定されたログ コレクタに書き込まれるわけではありません。たとえば、以下の設定リストを考えます。

管理対象ファイアウォール	コレクタ グループで定義されているログ転送の設定リスト
FW1	L1、L2、L3
FW2	L4、L5、L6

このリストを使用すると、FW1 は、そのプライマリ ログ コレクタが使用可能である限り、L1 にログを転送します。ただし、ハッシュ アルゴリズムに基づいて、Panorama は L2 をオーナーとして選択し、ログはそのディスクに書き込まれる場合があります。L2 がアクセスできなくなった場合や、シャーシに障害が発生した場合でも、FW1 は L1 に接続できるため、その障害は FW1 に通知されません。

© 2019 Palo Alto Networks, Inc.

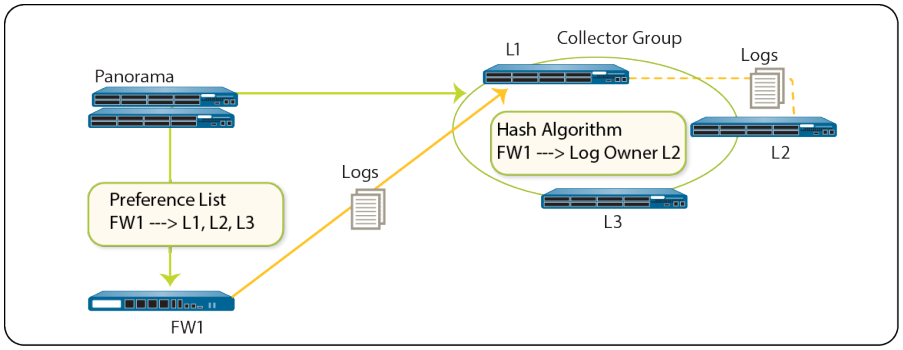


図 **5 :** 例 **-** 一般的なログ コレクタ グループの設定

コレクタ グループにログ コレクタが 1 つしかなく、ログ コレクタに障害が発生すると、ファイアウォールはその HDD/SSD にログを保存します (使用可能な保存領域はファイアウォールのモデルによって異なります) 。ログ コレクタへの接続が復元されるとすぐに、ファイアウォールは、障害発生前の転送していないログの転送を再開します。

ログ コレクタが複数あるコレクタ グループの場合、障害が発生したログ コレクタが 1 つのみであれば、ファイアウォールはログをローカル ストレージにバッファしません。L2 での障害の発生を想定した例では、FW1 は L1 にログを送信し続けて、L2 に送信されるログデータを L1 が保存します。L2 がバックアップされると、L1 は L2 向けのログデータを保存しなくなり、配信が正常に再開します。コレクタグループ内のログコレクタのいずれかがダウンした場合、ダウンしたログコレクタに書き込まれるログは優先リスト内の次のログコレクタに再分散されます。

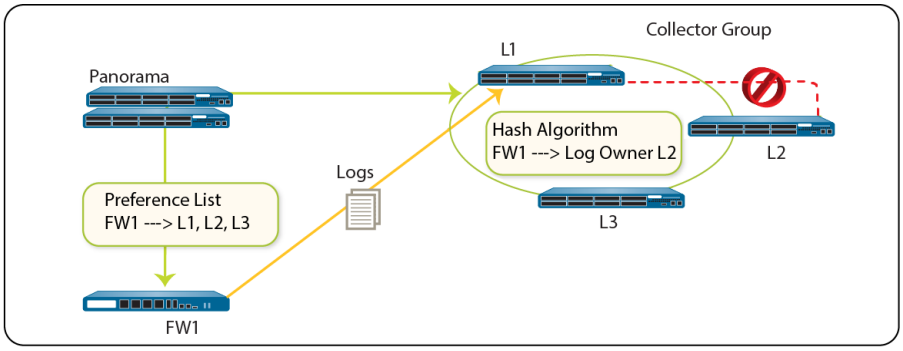


図 **6 :** 例 **-** ログ コレクタの障害

コレクタ グループ内で複数のログ コレクタを使用する場合は、以下のリスク軽減策をお勧めします。

- コレクタ グループの設定を行う際、ログ冗長化を有効にします。これにより、コレクタ グループのいずれかのログ コレクタが利用できなくなった際にログが失われなくなります。各ログのコピーが 2 つ作成され、それぞれ異なるログ コレクタに保存されます。各ログ コレクタのロギング用ディスク数が同じ場合にのみ、ログの冗長化が可能になります。

  冗長性を有効にすると、作成されるログが多くなるため、この設定には、より大きなストレージ容量が必要です。コレクタ グループの容量が不足すると、古いログが削除されます。

  冗長性を有効にすると、コレクタ グループ内のログ処理トラフィックが *2* 倍になり、最大ロギング率が半分になります。各ログ コレクタが、受信する各ログのコピーを配信する必要があるためです。
- ログ コレクタの障害が発生した場合に迅速な置換を可能するため、オンサイト スペア (OSS) を取得します。

© 2019 Palo Alto Networks, Inc.

- ログを Panorama に転送するだけでなく、バックアップ ストレージとして外部サービスへの転送を設定します。外部サービスとして、Syslog サーバー、電子メール サーバー、SNMP トラップ サーバー、HTTP サーバーがあります。

ログ転送オプション

デフォルト設定では、各ファイアウォールはすべてのログ ファイルをローカルに保存します。Panorama を使用して、ログのモニタリングおよびレポートの生成を一元的に行うには、Panorama へのログ転送の設定を行う必要があります。Panorama は、ログ コレクタ、Cortex Data Lake、またはその両方へのログの転送をサポートしています。ファイアウォールから直接、または Panorama からサービスにログを転送することにより、アーカイブ、通知、または分析を行う外部サービスを利用することもできます。外部サービスには、Syslog サーバー、電子メール ーバー、SNMP トラップ サーバー、HTTP ベースのサービスなどがあります。ファイアウォール ログの転送に加えて、Panorama 管理サーバーおよびログ コレクタが生成するログを転送できます。ログを転送する Panorama 管理サーバー、ログ コレクタ、またはファイアウォールは、ログを宛先に適した形式に変換します (Syslog メッセージ、電子メール通知、SNMP トラップ、または HTTP ペイロード) 。

Palo Alto Networks のファイアウォールおよび Panorama は、以下のログ転送オプションをサポートしています。オプションを選択する前に、 Panorama モデルのログ容量を検討して、Panorama のログ ストレージ要件を決定してください。

- ファイアウォールから Panorama、Panorama から外部サービスにログを転送する – この設定は、特にリモートと接続する場合など、ファイアウォールと外部サービス間の接続にログ率を維持できる十分な帯域幅がないデプロイ環境に最適です。この設定では、一部の処理が Panorama にオフロードされるため、ファイアウォールのパフォーマンスが向上します。

各コレクタ グループはログを異なる宛先に転送するように設定することができます。

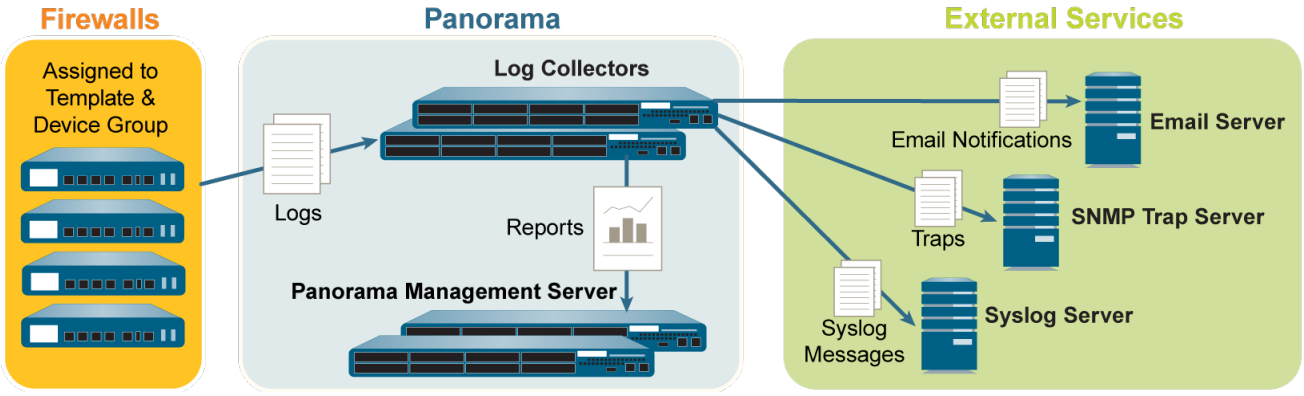


図 7 : **Panorama**、外部サービスの順にログを転送

- ファイアウォールから Panorama と外部サービスに同時にログを転送する – この設定では、Panorama と外部サービスの両方が個別のログ転送フローのエンドポイントになります。ファイアウォールは、Panorama を使用せずにログを外部サービスに転送します。この設定は、特にローカルと接続する場合など、ファイアウォールと外部サービス間の接続にログ率を維持できる十分な帯域幅があるデプロイ環境に最適です。

© 2019 Palo Alto Networks, Inc.

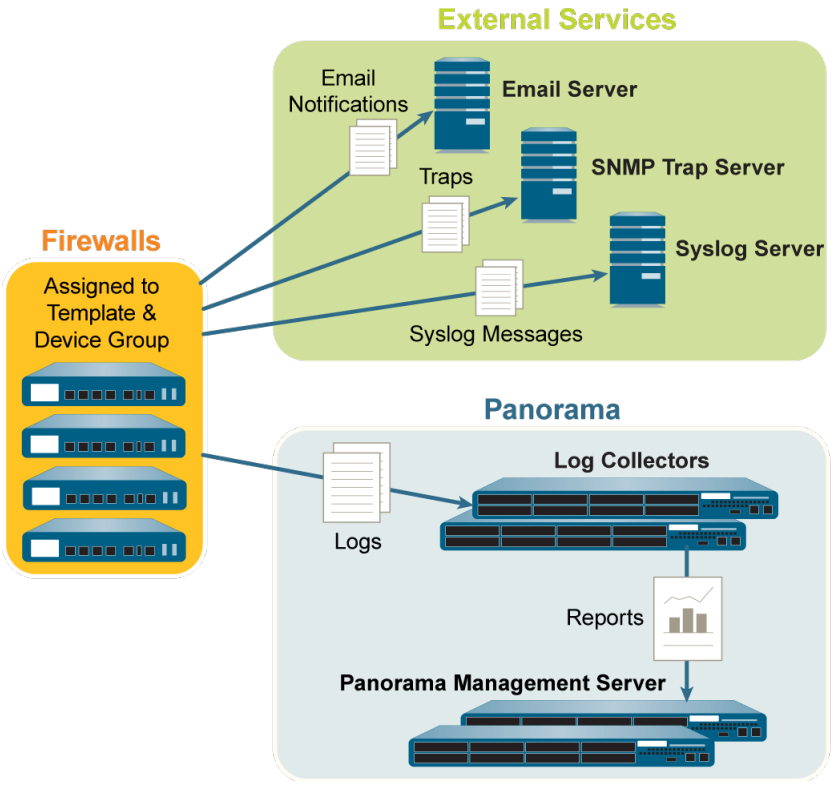


図 **8 :** 外部サービスと **Panorama** に同時にログを転送

一元的なレポート

Panorama は、すべての管理対象ファイアウォールからログを集約し、その集約データをレポートできます。これにより、ネットワーク全体のアプリケーションの使用、ユーザー アクティビティ、およびトラフィック パターンのグローバル ビューを得られます。ファイアウォールが Panorama に追加されるとすぐに、ネットワークを通過するすべてのトラフィックを ACC に表示できます。ログが有効になっている場合、ACC のログ エントリをクリックすると、アプリケーションに関する詳細に直接アクセスできます。

Panorama では、レポートを生成する際に、ローカル Panorama データベースと管理対象リモート ファイアウォールの 2 つのソースを使用します。Panorama データベースは、サマリー ログといくつかの詳細ログを保存するために割り当てられた Panorama 上のローカル ストレージを参照します。分散ログ収集デプロイ環境では、Panorama データベースに、Panorama およびすべての管理対象ログ コレクタのローカル ストレージが含まれます。Panorama では、すべての管理対象ファイアウォールから 15 分間隔で収集された情報 (トラフィック、アプリケーション、脅威) が要約されます。ローカル Panorama データベースを使用すると応答時間が短縮されますが、ログを Panorama に転送しない場合でも、Panorama はリモート ファイアウォールに直接アクセスして、管理対象ファイアウォールにローカルに保存されているデータのレポートを実行できます。

Panorama には、そのまま使用できる 40 以上の事前定義済みレポートが用意されています。また、これらのレポートを他のレポートの要素と組み合わせてカスタマイズし、保存可能なカスタム レポートおよびレポート グループを生成できます。レポートは、要求時や定期的なスケジュールで生成できます。また、電子メール配信用にスケジュール設定することもできます。これらのレポートには、ユーザーやコンテキストの情報が含まれているため、イベントを相関させたり、パターン、傾向、および関心の対象となりそうなエリアを識別したりできます。ログおよびレポートへの統合的なアプローチにより、ACC は同じイベントに関連する複数のログ エントリを相関させることができます。

詳細は、「ネットワーク アクティビティのモニター」を参照してください。

© 2019 Palo Alto Networks, Inc.

Panorama を使用したデータの再配信

データの再配信を行うことで、各送信元を 1 回設定するだけで、複数のデータ タイプを必要な数のクライアントに再配信できます。これは、ネットワークのニーズの変化に応じて送信元とクライアントを簡単に追加または削除できるように、ネットワークを拡張するのに有用です。

また、データの再配信は、指定するファイアウォールまたは Panorama 管理システムのみに該当する種類の情報を再配信することにより、よりきめ細かな設定が可能となります。サブネット、範囲、およびリージョンを使用して、ネットワーク トラフィックをさらに削減し、デバイス容量を最大化できます。

Palo Alto Networks ファイアウォールの主なメリットの 1 つは、IP アドレスの代わりにユーザー名とタグに基づいてポリシーを適用し、レポートを生成できることです。大規模ネットワークで課題となるのは、ポリシーを適用してレポートを生成するすべてのファイアウォールに、すべてのポリシー ルールに適用されるマッピングとタグがあることを確認する作業です。さらに、認証ポリシーを適用するすべてのファイアウォールに、まったく同じユーザー ベースの認証タイムスタンプの完全なセットが必要です。ユーザーがサービスやアプリケーションにアクセスするために認証する場合、必ず各ファイアウォールは関連付けられたタイムスタンプを記録しますが、一貫性を確保するために他のファイアウォールと自動的に共有するわけではありません。データ再配信は、必要なデータを再配信できるようにすることで、大規模ネットワークのこうした課題を解決しています。しかも、ファイアウォール間でデータを再配信するために追加の接続を設定する代わりに、データをマネージドファイアウォールに再配信するために Panorama インフラストラクチャを利用することができます。このインフラストラクチャには、ファイアウォールから Panorama へレイヤーのデータを再配信するために使用できる既存の接続があります。そのため、Panorama はファイアウォールに情報を再配信し、ファイアウォールはポリシーを適用してレポートを生成することができます。

各ファイアウォールまたは Panorama 管理サーバーは最大 100 の再配信ポイントからデータを受信できます。再配信ポイントは、他のファイアウォールまたは Panorama 管理サーバーにすることができます。ただし、Windows ベースの User-ID エージェントを使用してマッピングを実行し、情報をファイアウォールに再配信することもできます。ファイアウォールは、トラフィックが認証ポリシー ルールに一致する場合にのみ認証タイムスタンプを記録します。

© 2019 Palo Alto Networks, Inc.

ロールベースのアクセス制御

ロールベースのアクセス制御（RBAC）では、管理ユーザー（管理者）の権限および役割を定義できます。各管理者はロールおよび認証方法を指定するユーザーアカウントを持っていなければなりません。管理ロールPanoramaやファイアウォールが関わる特定の設定、ログ、およびレポートへのアクセスを定義します。デバイスグループおよびテンプレート管理者の場合、アクセス ドメインにロールをマッピングし、特定のデバイスグループ、テンプレート、およびファイアウォールへのアクセスを定義できます（コンテキスト切り替えによる）。各アクセスドメインを一つのロールに統合することで、組織の各部門・担当地域ごとに利用できる情報を厳密に区別することができます。例えば、データセンターのファイアウォールについてはアクティビティを監視でき、テスト ラボのファイアウォールについてはポリシーを設定できるなど、管理者に制限を与えることができます。デフォルト設定では、すべての機能領域、デバイス グループ、テンプレートおよびファイアウォールに対する読込・書込の全権限（スーパーユーザー アクセス）を与える定義済みの管理者アカウント（admin）がすべての Panorama アプライアンス（バーチャル アプライアンスあるいは M-Series アプライアンス）に備わっています。各管理者に対し、Panorama がユーザーのアクセス認証情報を検証する方法を規定する認証プロファイルを定義することができます。



デフォルトのアカウントをすべての管理者に対して使用するのではなく、*Panorama* の管理機能またはレポート機能に対するアクセス権を必要とするユーザーごとに別個の管理アカウントを作成するようお勧めします。これにより、無権限での設定変更から保護する能力を高め、*Panorama*が各管理者のアクションを特定し、ログに記録できるようになります。

- 管理ロール
- 認証プロファイルと認証シーケンス
- アクセス ドメイン
- 管理認証

管理ロール

組織内でのセキュリティ要件、ネットワークで使用している既存の認証サービス、および必要な管理ロールに応じて管理者アカウントを設定します。ロールにより、管理者が利用できるシステムへのアクセス権のタイプを定義します。組織のセキュリティ要件に応じて、アクセスを柔軟に定義および制限できます。たとえば、データセンター管理者にはすべてのデバイスおよびネットワーク設定へのアクセスを許可し、セキュリティ管理者にはセキュリティ ポリシー定義の制御のみを許可し、他の主要なユーザーには CLI または XML API アクセスを制限することができます。以下のロール タイプがあります。

- ダイナミック ロール – Panorama および管理対象のファイアウォールへのアクセス権を付与する組み込みのロール。新しい機能が追加されると、Panorama によってダイナミック ロールの定義が自動的に更新されます。ユーザーが手動で更新する必要はありません。次の表に、ダイナミック ロールに関連付けられたアクセス権限の一覧を示します。

ダイナミック ロール	権限
スーパーユーザー	Panorama に対する読み取り/書き込みのフル アクセス権
スーパーユーザー（読み取り専用）	Panorama に対する読み取り専用アクセス権
Panorama 管理者	Panorama に対するフル アクセス権。ただし、以下のアクションを除きます。 • Panorama またはファイアウォールの管理者およびロールの作成、変更、削除。

© 2019 Palo Alto Networks, Inc.

ダイナミック ロール	権限
	• **[Device]** > [セットアップ] > [操作] ページから設定をエクスポート、検証、保存、ロード、インポートする、または設定を元に戻す操作を実行する。 • **Panorama** タブで、**Scheduled Config Export** (スケジュール設定された設定のエクスポート機能を設定する。

- 管理者ロール プロファイル – Web インターフェイス、CLI、または XML API のさまざまな機能領域へのアクセスをよりきめ細かく制御するには、カスタム ロールを作成します。新しい機能が製品に追加されたら、それぞれのアクセス権限を持つロールを更新する必要があります。Panoramaが自動的に新しい機能をカスタムロール定義に追加することはありません。管理者ロール プロファイルの設定を行う際、次のプロファイル タイプのいずれかを選択します。

管理者ロール プロファイル	説明
Panorama	このロールでは、スーパーユーザー ダイナミック ロールで使用可能なすべての Panorama 機能 (ただし、Panorama 管理者および Panorama ロールの管理を除く) に対して、読み取り/書き込みアクセス権または読み取り専用アクセス権を付与できます。また、これらの機能に対するアクセス権を一切与えない (アクセス権なし) ようにすることもできます。Panorama 管理者および Panorama ロールの管理機能については、読み取り専用アクセス権を付与するか、アクセス権なしにすることはできますが、読み取り/書き込みアクセス権を付与することはできません。 Panorama ロールは、たとえば、Panorama のセキュリティ ポリシー定義、ログ、レポートにアクセスする必要があるセキュリティ管理者に割り当てます。

デバイス グループとテンプレート	そのようなロールについては、デバイス グループ、テンプレート、およびファイアウォールに関わる特定の機能領域への読み取り/書き込みアクセス権あるいは読み取り専用アクセス権を付与したり、アクセス権を一切与えないようにしたりすることも可能です。これらのロールを「アクセス ドメイン」と統合することで、組織の各部門· 担当地域ごとに利用できる情報を厳密に区別することができます。デバイス グループおよびテンプレートには次のような制限があります。
	
	• CLI または XML API に対するアクセス権は付与されない
	• 設定またはシステム ログに対するアクセス権は付与されない
	• VM 情報ソースに対するアクセス権は付与されない
	• **Panorama** タブでは、次の項目へのアクセスが制限されます。
	  • デバイス デプロイ機能 (読込· 書込、読込のみ、あるいは権限なし)
	  • 管理者アカウントで指定されたデバイス グループ (読み取り/書き込み、読み取り専用、あるいはアクセス権なし)
	  • 管理者アカウントで指定されたテンプレートおよび管理対象のファイアウォール (読み取り専用、あるいはアクセス権なし)
	
	このロールは、たとえば、特定のデバイス グループおよび (または) テンプレート用の Web インターフェイスのデバイスおよびネットワーク設定エリアにアクセスする必要のある操作担当の管理者に割り当てます。

© 2019 Palo Alto Networks, Inc.

認証プロファイルと認証シーケンス

認証プロファイルは、管理者が Panorama にログインする際の認証情報を検証する認証サービスを定義します。サービスは、ローカル認証または外部認証サービスにすることができます。一部のサービス（SAML、TACACS+、RADIUS）では、管理者アカウントの認証と認可を両方とも Panorama ではなくて外部サーバーで管理するオプションが提供されます。認証プロファイルは、認証サービスに加えて、Kerberos シングル サインオン（SSO）および SAML シングル ログアウト（SSO）などのオプションを定義します。

一部のネットワークには、異なるユーザーおよびユーザー グループを対象とした複数のデータベース（TACACS+ および LDAP など）が存在します。このような場合に管理者を認証するには、認証シーケンスを設定します。つまり、Panorama がログイン中に管理者を照合する認証プロファイルの順位を設定します。Panorama は、いずれかが管理者を正常に認証するまで、各プロファイルを順番にチェックします。シーケンスのすべてのプロファイルで認証に失敗した場合にのみ、管理者のアクセスが拒否されます。

アクセス ドメイン

アクセス ドメインでは、特定のデバイス グループとテンプレートへの管理アクセスが制御されます。また、管理対象ファイアウォールの Web インターフェイスにコンテキスト切り替える機能も制御されます。アクセス ドメインは、デバイス グループおよびテンプレート ロールを持つ管理者にのみ適用されます。アクセス ドメインに管理ロールをマッピングすると、管理者が Panorama でアクセスする情報を非常に詳細に制御できます。たとえば、データ センター内のファイアウォールのすべてのデバイス グループが含まれるアクセス ドメインを設定し、データ センター トラフィックの監視は許可されているが、ファイアウォールの設定は許可されていない管理者にそのアクセス ドメインを割り当てるとします。この場合、すべてのモニタリング権限を有効にするが、デバイス グループ設定へのアクセスは無効にするロールにアクセス ドメインをマッピングします。さらに、デバイスグループとテンプレートの管理者は、設定ログやシステム ログの表示など、アクセスドメイン内の管理対象ファイアウォールの管理タスクの実行、構成監査の実施、および再起動、テクニカルサポート ファイルの生成、統計ダンプの実行、コアファイルのエクスポートなどのファイアウォール操作への直接アクセスなどのディレクトリへのアクセスが可能です。

アクセス ドメインは、ローカルの Panorama 設定で構成してから、管理アカウントおよびロールに割り当てます。割り当ては、ローカルに実行することも、外部の SAML、TACACS+、または RADIUS サーバーを使用することもできます。外部サーバーを使用すると、Panorama で設定を再構成する代わりに、ディレクトリ サービスを介してすばやくアクセス ドメインを再割り当てできます。外部サーバーを使用するには、Panorama がサーバーにアクセスできるようにサーバー プロファイルを定義する必要があります。また、RADIUS または TACACS+ サーバーでベンダー固有属性（VSA）を定義するか、SAML IdP サーバーで SAML 属性を定義する必要もあります。

たとえば、RADIUS サーバーを使用する場合は、管理者ごとに VSA の番号と値を定義します。定義された値は、Panorama で設定したアクセス ドメインと一致する必要があります。管理者が Panorama にログインしようとすると、管理者のアクセス ドメインと属性番号が RADIUS サーバーに対してクエリされます。RADIUS サーバーからの応答に基づいて、管理者にアクセス権が認証され、アクセス ドメインに割り当てられたファイアウォール/仮想システム、デバイス グループ、テンプレートに制限されます。

関連作業については、以下を参照してください。

- アクセス ドメインの設定.
- Panorama 管理者用に RADIUS 認証を設定.
- Panorama 管理者用に TACACS+ 認証を設定.
- Panorama 管理者用に SAML 認証を設定.

管理認証

Panorama 管理者には、次のタイプの認証と認可（管理ロールとアクセス ドメイン）を設定できます。

© 2019 Palo Alto Networks, Inc.

認証方式	認可方式	説明
ローカル	ローカル	管理者アカウント認証情報と認証メカニズムが Panorama に対してローカルです。Panorama を使用して、管理ロールとアクセス ドメインをアカウントに割り当てます。アカウントの安全性を高めるには、パスワードの有効期間を定義するパスワード プロファイルを作成したり、Panorama 全体でのパスワードの複雑性設定を行ったりします。詳細は、「Panorama 管理者用にローカルあるいは外部認証を設定」を参照してください。
SSH 鍵	ローカル	管理者アカウントは Panorama に対してローカルですが、CLI への認証は SSH 鍵に基づきます。Panorama を使用して、管理ロールとアクセス ドメインをアカウントに割り当てます。詳細は、「SSH 鍵ベースで CLI への認証を行う管理者を設定」を参照してください。
証明書	ローカル	管理者アカウントは Panorama に対してローカルですが、Web インターフェイスへの認証はクライアント証明書に基づきます。Panorama を使用して、管理ロールとアクセス ドメインをアカウントに割り当てます。詳細は、「証明書ベースで Web インターフェイスへの認証を行う Panorama 管理者を設定」を参照してください。
外部サービス	ローカル	Panorama でローカルに定義する管理者アカウントは、多要素認証、SAML、Kerberos、TACACS+、RADIUS、LDAP のいずれかの外部サーバーで定義されているアカウントの参照として動作します。外部サーバーが認証を行います。Panorama を使用して、管理ロールとアクセス ドメインをアカウントに割り当てます。詳細は、「Panorama 管理者用にローカルあるいは外部認証を設定」を参照してください。
External	外部サービス	管理者アカウントは、SAML、TACACS+、RADIUS のいずれかの外部サーバーでのみ定義されます。サーバーが認証と認可を両方とも行います。TACACS+ サーバーまたは RADIUS サーバーではベンダー固有属性（VSA）、SAML サーバーでは SAML 属性を認可用に定義します。Panorama は、Panorama で定義された管理者ロールとアクセス ドメインに属性をマッピングします。詳細は、以下を参照してください。 • Panorama 管理者用に SAML 認証を設定 • Panorama 管理者用に TACACS+ 認証を設定 • Panorama 管理者用に RADIUS 認証を設定

© 2019 Palo Alto Networks, Inc.

Panorama のコミット、検証、およびプレビュー操作

Panorama で候補設定に行った変更を有効にしたり、Panorama が管理するデバイス（ファイアウォール、ログ コレクタ、WildFire アプライアンス、アプライアンス クラスタ）に変更をプッシュしたりする準備が整ったら、「設定変更のプレビュー、検証、コミット」を行うことができます。例えば、Panorama 設定にログ コレクタを追加する場合、Panorama に加えた変更をコミットし、次にそのログ コレクタを含むコレクタ グループに対して変更をプッシュするまでの間、ファイアウォールはそのログ コレクタにログを送信できません。

変更を管理者または場所でフィルタリングし、それらの変更のみをコミット、プッシュ、検証、またはプレビューできます。場所は、特定のデバイス グループ、テンプレート、コレクタ グループ、ログ コレクタ、共有設定、Panorama 管理サーバーになります。

変更をコミットすると、実行中の設定の一部になります。コミットされていない変更は、候補設定の一部になります。Panorama はコミット要求をキューで処理するので、前回のコミットの進行中に新しいコミットを追加することができます。Panorama は追加された順番でコミットを実行しますが、Panorama が追加した自動コミット（FQDN 更新など）を優先的に行います。ただし、管理者が開始したコミットがすでにキューの上限まで追加されている場合（10）、新しいコミットを行う前に、Panorama が保留中のコミットを完了するまで待つ必要があります。保留中のコミットをキャンセルする場合や、保留中、実行中、完了済み、あるいは失敗したコミットの詳細を表示する場合は、「Panorama タスク マネージャの使用」（Tasks）を使用できます。コミットによってどの変更が有効に成るか確認するには、コミット プレビューを実行します。

コミットを開始すると、変更を有効にする前にPanoramaが変更の有効性を検証します。検証結果の表示画面には、コミットをブロックする状況（エラー）、あるいは通知が必要な状況（警告）が表示されます。例えばこの検証の結果、不正なルートの宛先が見つかり、コミットを続けるためには修正が必要になる場合があります。検証プロセスを利用すると、エラーを検出、修正してからコミットできます（実行中の設定は変更されません）。固定のコミット ウィンドウがあり、エラーなしでコミットを確実に実行したい場合に便利です。

自動コミットリカバリはデフォルトで有効になっており、管理対象ファイアウォールが Panorama からプッシュされた設定をローカルでテストして、新たな変更によって Panorama と管理対象ファイアウォール間の接続が切断されないことを確認できます。コミットされた設定が Panorama と管理対象ファイアウォールの間の接続を切断した場合、ファイアウォールは自動的にコミットに失敗し、設定は以前に実行していた設定に復元され、共有ポリシーまたはテンプレート ステータス（**Panorama**（**Panorama**）> **Managed Devices**（デバイス管理）> **Summary**（概要）の順で移行）は、プッシュされた設定オブジェクトに応じて同期しなくなります。さらに、管理対象ファイアウォールは Panorama への接続を 60 分ごとにテストし、管理対象ファイアウォールが Panorama に正常に接続できなくなったことを検出した場合、設定を以前に実行していた設定に戻します。

候補設定および現在アクティブな設定の詳細は、「Panorama およびファイアウォールの設定のバックアップを管理」をご参照ください。

複数の管理者が同時セッションで設定変更を行うのを防止する方法については、「設定変更を制限するためのロックの管理」をご参照ください。

設定を管理対象ファイアウォールにプッシュする際、*Panorama* は実行中の設定をプッシュします。そのため、*Panorama* は、まず変更が *Panorama* にコミットされていないと、管理対象ファイアウォールに変更をプッシュできません。

© 2019 Palo Alto Networks, Inc.

Panorama のデプロイ計画

- 管理アプローチを決定します。Panorama を使用して、ポリシーを一元的に設定および管理したり、ソフトウェア、コンテンツ、ライセンス更新を一元管理したり、ネットワーク上の管理対象のファイアウォールのログおよびレポートを一元的に行ったりしますか?

  ネットワーク上にすでに Palo Alto Networks ファイアウォールを導入および設定している場合、ファイアウォールを中央管理に移行するかどうかを決定します。このプロセスでは、すべての設定およびポリシーをファイアウォールから Panorama に移行する必要があります。詳細については、ファイアウォールをPanorama管理に移行を参照してください。
- Panoramaおよびファイアウォールのソフトウェアバージョンを検証します。Panoramaは、Panoramaのバージョンと同じか、それ以前のバージョンのものと同じバージョンのPAN-OSを実行しているファイアウォールを管理できます。たとえば、Panorama 8.0 は、PAN-OS 8.1 を実行しているファイアウォールを管理できません。さらに、Panorama 8.1 は PAN-OS 6.0.0 から 6.0.3 を実行するファイアウォールを管理することができず、Panorama バージョンよりも後の PAN-OS バージョンを実行するファイアウォールは管理できません。
- すべての管理対象ファイアウォールで同じ URL フィルタリング データベース (BrightCloud または PAN-DB) を使用するように計画します。BrightCloud データベースを使用しているファイアウォールと、PAN-DB を使用しているファイアウォールがある場合、Panorama では、いずれかの URL フィルタリング データベースのセキュリティ ルールのみを管理できます。他のデータベースの URL フィルタリング ルールは、そのデータベースを使用しているファイアウォールでローカルに管理する必要があります。
- Panorama と管理対象デバイスおよび高可用性ピアの間の認証方法を決めます。デフォルトでは、Panorama は事前定義済み証明書を使用し、管理とデバイス間通信に使用する SSL 接続を認証します。ただし、カスタム証明書に基づく認証を設定し、Panorama、ファイアウォール、ログ コレクタ間の SSL 接続のセキュリティを強化できます。カスタム証明書を使用すると、固有の信頼チェーンを確立して、Panorama と管理対象デバイスの間で相互認証を確保できます。証明書は、会社の公開鍵基盤 (PKI) からインポートするか、Panorama で作成することができます。
- Panorama を高可用性設定で使用するように計画します。アクティブ/パッシブ高可用性ペアとして設定します。Panorama 高可用性を参照してください。
- 大規模なデプロイでは、ネットワークをセグメント化する方法およびセキュリティ要件を満たす方法を計画します。デフォルトでは、M-Series アプライアンスで動作している Panorama は、Panorama への管理アクセス、デバイス (ファイアウォール、ログ コレクタ、WildFire アプライアンス、アプライアンス クラスタ) の管理、ログの収集、コレクタ グループとの通信、デバイスへのソフトウェア更新とコンテンツ更新のデプロイに管理 (MGT) インターフェイスを使用します。ただし、セキュリティを強化してネットワークのセグメント化を可能にするため、MGT インターフェイスは管理アクセスに予約して、M-Series アプライアンスのインターフェイス (Eth1、Eth2、Eth3、Eth4、Eth5) をその他のサービスに使用できます。
- ネットワーク アクティビティに関する有益なレポートを得られるように、ログ ソリューションを計画します。

  - Panorama バーチャル アプライアンスのリソース割り当てが、AWS または Azure のログ コレクタ モードでデプロイされることを確認します。Panorama バーチャル アプライアンスは、サイズ変更された場合、ログ コレクタ モードを保持しません。この結果、ログ データが失われます。
  - セキュリティおよびコンプライアンス要件を満たすためにネットワークに必要なログ ストレージ容量を見積もります。Panorama モデルのロギング容量、ネットワーク トポロジ、ログを送信するファイアウォール数、ログ トラフィックのタイプ (たとえば、URL フィルタリング、脅威ログかトラフィック ログかなど)、ログの生成レート、Panorama にログを保存する日数などの要因を考慮する必要があります。詳細については、Panoramaのログ保持要件を決定を参照してください。
  - Panorama の他に Syslog サーバーなどの外部サービスにもログを転送する必要がありますか?ログ転送オプションを参照してください。

© 2019 Palo Alto Networks, Inc.

- ログ ストレージを自己所有または管理していますか、それとも Palo Alto Networks が提供する Cortex Data Lake の利用を検討していますか？
- 長期保管ソリューションが必要な場合、ログを転送できる Splunk や ArcSight などのセキュリティ情報およびイベント管理（SIEM）ソリューションがありますか?
- ログに冗長性が必要ですか?

  複数のログ コレクタを含むコレクタ グループを設定する場合は、冗長性を有効にして、いずれかのログ コレクタが使用不可になってもログが失われないようにすることができます（複数のログ コレクタを含むコレクタ グループに関する注意事項を参照）。

  HA 構成でレガシー モードの Panorama バーチャル アプライアンスをデプロイすると、管理対象ファイアウォールは両方の HA ピアにログを送信できるため、各ログのコピーが各ピアに存在することになります。この冗長性オプションはデフォルトで有効になっています（ログ転送とバッファのデフォルトの変更を参照）。
- ネットワーク ファイル システム（NFS）にログを記録しますか?Panorama バーチャル アプライアンスがレガシー モードであり、専用ログ コレクタを管理しない場合は、NFS ストレージが、8TB を超えてログ保存容量を増やすための唯一の選択肢です。NFS ストレージを使用できるのは、Panorama が ESXi サーバー上で動作する場合のみです。NFS ストレージを使用する場合、ファイアウォールは HA ペアのプライマリ ピアにのみログを送信できます。また、NFS にマウントして NFS に書き込むことができるのはプライマリ ピアだけです。

- ❑ 管理者が管理対象ファイアウォールと Panorama にアクセスするために必要となるロールベース アクセス権限を決めます。Panorama への管理アクセスのセットアップを参照してください。
- ❑ 必要なデバイス グループを計画します。ファイアウォールをグループ化するときの基準として、機能、セキュリティ ポリシー、地理的な場所、ネットワーク セグメンテーションのどれを使用するのかを検討します。たとえば、機能ベースのデバイスグループの例として、研究開発チームが使用するすべてのファイアウォールを含むグループが考えられます。共通点に基づいて小さなデバイス グループを作成するのか、スケーリングしやすいように大きなデバイス グループを作成するのか、あるいは管理用の各層の複雑さを軽減するためにデバイス グループ階層を作成するのかを検討してください。
- ❑ ポリシー管理の階層化方法を計画します。デバイス グループ階層においてファイアウォールがポリシールールを継承・評価する方法、およびネットワークのニーズに合った共有ルールやデバイス グループ ルール、ファイアウォール固有のルールの最適な実装方法をよく考えます。ポリシーの可視化および中央管理を実現するために、共有あるいはデバイス グループ ルールに対するファイアウォール固有の例外を作成しなければならない場合でも、Panorama を使用してルールを管理することを検討してください。必要な場合はデバイスグループ内のファイアウォールのサブセットにポリシールールをプッシュすることができます。
- ❑ テンプレートおよびテンプレートスタックからネットワーク設定を継承する方法に基づき、ファイアウォールの編成を計画します。たとえば、ハードウェア モデル、地理的な近接性、およびタイム ゾーンに関するネットワーク要件、DNS サーバー、インターフェイス設定に基づいてファイアウォールをテンプレートに割り当てる方法を検討します。

© 2019 Palo Alto Networks, Inc.

Panorama のデプロイ：タスクの概要

以下のタスク リストに、Panorama を導入する手順の概要を示します。Panorama による一元管理の例については、「「ユース ケース：Panorama を使用してファイアウォールを構成」を参照してください。

STEP 1 | （M-Series アプライアンスのみ）アプライアンスをラック マウントします。

STEP 2 | 初期設定を実行して、Panorama へのネットワーク アクセスを有効にします。「Panorama バーチャル アプライアンスのセットアップ」または「M-Series アプライアンスのセットアップ」を参照してください。

STEP 3 | Panorama の登録とライセンスのインストール.

STEP 4 | Panorama のコンテンツ更新とソフトウェア更新のインストール.

STEP 5 | （推奨）高可用性設定で Panorama をセットアップします。「Panorama の高可用性」を参照してください。

STEP 6 | 管理対象デバイスとしてのファイアウォールの追加.

STEP 7 | または「デバイス グループの追加」、「デバイス グループの階層を作成」、および（該当する場合）「テンプレートの追加」を行います。 テンプレート スタックの設定

STEP 8 | （任意）Panorama や外部のサービスへのログ転送を設定します。「ログ収集の管理」を参照してください。

STEP 9 | ネットワーク アクティビティのモニターPanorama の可視化およびレポート ツールを使用して行います。

© 2019 Palo Alto Networks, Inc.

Panorama のセットアップ

ネットワーク上のすべてのファイアウォールでレポートの一元化や包括的なポリシー管理を行うため、Panorama™ 管理サーバーをバーチャル アプライアンスまたはハードウェア アプライアンス (M-200、M-500、または M-600 アプライアンス) としてデプロイできます。

以下のトピックでは、ネットワークでの Panorama のセットアップ方法について説明します。

> Panorama のログ保持要件を決定
> Panorama バーチャル アプライアンスのセットアップ
> M-Series アプライアンスのセットアップ
> Panorama の登録とライセンスのインストール
> Panorama デバイス証明書のインストール
> Panorama のコンテンツ更新とソフトウェア更新のインストール
> 別の Panorama モデルへの移行
> Panorama 管理インターフェイスへのアクセスおよびナビゲート
> Panorama への管理アクセスのセットアップ
> カスタム証明書を使用する認証のセットアップ

Panorama のログ保持要件を決定

Panorama の導入計画を行う際、デプロイする Panorama モデルを決定する際に必要になる Panorama のログの保存容量、デフォルトの容量以上にストレージを拡大するかどうか、専用ログ コレクタをデプロイするかどうか、Panorama から外部の宛先へのログ転送を設定するかどうかを予め検討します。ログ ストレージが最大容量に達すると、Panorama は自動的に古いログを削除して新しいログ用のスペースを作ります。

次の各作業を行い、Panorama に必要となるログ保存容量を見積もります。詳細やユースケースについては、「Panorama のサイジングおよび設計ガイド」を参照してください。

STEP 1 | 組織のログ保持要件を決定します。

ログ保持要件に影響を与える要素：

- 組織の IT ポリシー
- ログの冗長性—コレクタ グループの設定行う際にログの冗長化を有効にする場合、各ログのコピーが作成されるため、ログの保存容量が 2 倍必要になります。
- クレジットカード業界のセキュリティ基準（PCI DSS）、サーベンス オクスリー法、医療保険の携行性と責任に関する法律（HIPAA）などの規制の要件。



お客様の組織で一定の期間後にログを削除する必要がある場合は、各ログ タイプに対して有効期間を設定することができます。また、ログのタイプごとに優先度を付ける必要がある場合は、各ログ タイプのストレージ割り当てを合計空き容量のうちのパーセント値で設定することもできます。詳細については、「ログおよびレポートのストレージ割り当ておよび有効期間を管理」を参照してください。

STEP 2 | 日次の平均ログギング率を決定します。

ピーク時およびピーク時以外の日に複数回検討を行い、平均値を予測します。より多くサンプルを採る方が予測の精度が上がります。

1. 現在のログ生成率をログ/秒の形で表示します。
   - Panorama がまだログを収集していない場合は、各ファイアウォールの CLI にアクセスし、次のコマンドを実行してすべてのファイアウォールの合計率を算出します。これは直近 1 秒の間に受信したログの数を表示するコマンドです。

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

   - Panorama がすでにログを収集している場合は、ログを受信する各アプライアンスの CLI で次のコマンドを実行し（Panorama 管理サーバーあるいは専用ログコレクタ）、合計率を算出します。これは直近 5 分間の平均ログギング レートを表示するコマンドです。

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



SNMP マネージャを使用して、ログ コレクタ（*panLogCollector MIB*、*OID 1.3.6.1.4.1.25461.1.1.6* を参照）およびファイアウォール（*panDeviceLogging*、*OID 1.3.6.1.4.1.25461.2.1.2.7* を参照）のログギング レートを判断することもできます。

2. サンプルとして採った率の平均値を算出します。
3. 平均ログ/秒に 86,400 を掛け、日次のログギング レートを算出します。

STEP 3 | 必要なストレージ容量を見積もります。

© 2019 Palo Alto Networks, Inc.

この計算式で得られるのは概算値に過ぎません。必要なストレージ容量は、厳密に言えば計算式の結果とは異なります。

次の計算式を使用します。

<必要な保存期間> x <ログの平均サイズ> x <ロギングの平均頻度>

ログの平均サイズは、ログの種類によって大きく異なります。ただし、おおよそのログの平均サイズとして 500 バイトを使用できます。

例えば、Panoramaがログを30日間保存する必要があり、すべてのファイアウォールの平均ロギング率の合計が21,254,400ログ/日であるとすると、必要なログの保存容量は：30 x 500 x 21,254,400 = 318,816,000,000 bytes（およそ318GB）になります。

STEP 4 | 次のステップ...

Panorama でログ ストレージ容量がさらに必要であると判断した場合:

- 「Panorama バーチャル アプライアンスでのログ ストレージ容量の拡張」
- 「M-Series アプライアンスのストレージの拡張」

© 2019 Palo Alto Networks, Inc.

Panorama バーチャル アプライアンスのセットアップ

Panorama バーチャル アプライアンスにより、既存の VMware 仮想インフラストラクチャを使用して Palo Alto Networks ファイアウォールおよび専用ログ コレクタを一元的に管理し、監視することができます。仮想アプライアンスは、ESXi サーバー、Amazon Web Services（AWS）、AWS GovCloud、Microsoft Azure、Google Cloud Platform（GCP）、KVM、Hyper-V または vCloud Air にインストールできます。専用ログ コレクタをデプロイするのに加えて、または専用ログ コレクタをデプロイする代わりに、ファイアウォール ログを直接 Panorama バーチャル アプライアンスに転送することができます。ログ ストレージ容量を増やしてレポート生成の時間を短縮するために、バーチャル アプライアンスをレガシー モードから Panorama モードに切り替えてローカル ログ コレクタを設定することもできます。Panorama バーチャル アプライアンスおよびそのモードについての詳細は、Panorama モデルを参照してください。

これらのトピックでは、バーチャル アプライアンスを作成するために必要なパブリックおよびプライベート ハイパーバイザー製品を十分理解していることを前提として話を進めていくため、関連するコンセプトや用語には触れません。

- Panorama バーチャル アプライアンスのセットアップ前提条件
- Panorama バーチャル アプライアンスのインストール
- Panorama バーチャル アプライアンスの初期設定の実行
- ログ コレクタを使用する Panorama バーチャル アプライアンスのセットアップ
- ローカル ログ コレクタを使用する Panorama バーチャル アプライアンスのセットアップ
- Panorama モードの Panorama バーチャル アプライアンスのセットアップ
- 管理専用モードの Panorama バーチャル アプライアンスのセットアップ
- Panorama バーチャル アプライアンスでのログ ストレージ容量の拡張
- Panorama バーチャル アプライアンスの CPU およびメモリを増やす
- Panorama バーチャルアプライアンスにシステムディスクを追加する
- Panorama バーチャル アプライアンスのセットアップの完了

Panorama バーチャル アプライアンスのセットアップ前提条件

Panorama バーチャル アプライアンスのインストールを行う前に、以下の作業を完了させます。

- ブラウザを使用してPalo Alto Networks カスタマー サポート Web サイトにアクセスし、Panorama の登録を行います。その際、送信済みの注文処理メールに記載されている Panorama のシリアル番号が必要になります。Panorama の登録後、Panorama ソフトウェア ダウンロード ページにアクセスできるようになります。
- サポートされている Panorama ハイパーバイザを確認し、ハイパーバイザが Panorama をデプロイするために必要なバージョンの最低要件を満たしていることを確認します。
- Panorama を VMware ESXi サーバーにインストールする場合、サーバーが「Panorama バーチャル アプライアンスのシステム要件」に記載された最低要件を満たすことを確認してください。以下の要件は、Panorama 5.1 以降のリリースに適用されます。要件は、バーチャル アプライアンスを Panorama モードで実行するか管理専用モードで実行するかによって異なります。モードの詳細は、「Panorama モデル」を参照してください。

Panorama を VMware vCloud Air にインストールする場合、インストール中にシステム設定を行います。

Amazon Web Services（AWS）、AWS GovCloud、Microsoft Azure、Google Cloud Platform（GCP）、Hyper-V、KVM、VMware ESXi 上に Panorama バーチャル アプライアンスをデプロイ

© 2019 Palo Alto Networks, Inc.

するための最低リソース要件を確認し、仮想マシンが目的のモード（Panorama、管理専用、あるいはログコレクタ）の最低リソース要件を満たしていることを確認してください。Panorama バーチャル アプライアンスの最小リソース要件は、Panorama および ログ コレクタ モードで、ログ収集の 1 秒あたりの最大ログ数（LPS）を達成できるように設計されています。仮想 ロギング ディスクを追加または削除した結果、推奨される仮想 ロギング ディスクの数（以下）未満あるいは超過する設定になると、LPS が削減されます。

Panorama バーチャル アプライアンスのインストールの際に Panorama モードの最小リソース要件を満たしていない場合、Panorama は、サポートされているすべてのパブリック (AWS、AWS GovCloud、Azure、および GCP) およびプライベート (Hyper-V、KVM、および VMware ESXi) ハイパーバイザすべてで管理専用モードをデフォルトに設定します。管理専用モードの最小リソース要件を満たしていない場合、Panorama はサポートされるすべてのパブリックハイパーバイザ、Hyper-V、および KVM をデフォルトのメンテナンスモードに変更します。VMware で Panorama をインストールの際に管理専用モードの最小リソース要件を満たしていない場合、Panorama はデフォルトのレガシーモードに変更します。



デバイス管理機能とログ収集機能の両方で、のために、*Panorama* モードで *Panorama* 管理サーバーを *Panorama* モードでデプロイすることをお勧めします。レガシーモードは引き続きサポートされますが、実稼働環境には推奨されません。また、*Panorama* をレガシーモードに切り替えることはできません。サポートされているモードの詳細については、Panorama モデルを参照してください。

表 **1 : Panorama** バーチャル アプライアンスのシステム要件

要件	管理専用モードの Panorama バーチャル アプライアンス	Panorama モードの Panorama バーチャル アプライアンス	ログコレクタ モードの Panorama バーチャル アプライアンス
仮想ハードウェア バージョン	• **VMware ESXi および vCloud Air** – 64 ビットのカーネルベースの VMware ESXi 5.5、6.0、6.5、または6.7。ESXi サーバー上の仮想ハードウェア ファミリー タイプ（VMware 仮想ハードウェア バージョンとも呼ばれる）でサポートされているバージョンは vmx-10 です。 • **Hyper-V** – Hyper-V のロールを持つ Windows Server 2016 または Hyper-V 2016 • **KVM** – Ubuntu バージョン 16.04 または CentOS7 Panorama モードでは、任意の ESXi バージョンを実行するバーチャル アプライアンスは最大 12 台の仮想ロギング ディスク（それぞれのログ ストレージは 2TB）をサポートしています。合計で、最大容量は 24TB となります。 （VMware ESXi および vCloud Air のみ）レガシーモードでは、バーチャル アプライアンスは 1 台の仮想 ロギング ディスクをサポートします。ESXi 5.5 以降のバージョンは最大 8TB のディスク 1 台をサポートしています。これよりも古い ESXi バージョンでは最大 2TB のディスク 1 台をサポートしています。		
（ESXi および vCloud Air のみ） クライアント コンピュータ	Panorama バーチャル アプライアンスをインストールしてそのリソースを管理するには、ESXi サーバーと互換性がある VMware vSphere クライアントまたは VMware Infrastructure クライアントをインストールする必要があります。		
システム ディスク	• デフォルト – 81GB • アップグレード済み – 224GB	• デフォルト – 81GB	81GB ログの保存用に、Panorama はシステム ディスクまたは

© 2019 Palo Alto Networks, Inc.

要件	管理専用モードの Panorama バーチャル アプライアンス	Panorama モードの Panorama バーチャル アプライアンス	ログコレクタ モードの Panorama バーチャル アプライアンス
		• アップグレード済み – 224GB（SD-WAN に必要） ログの保存用に、Panorama はシステム ディスクまたは NFS データストアの代わりに仮想ロギング ディスクを使用します。	NFS データストアの代わりに仮想ロギング ディスクを使用します。

CPU、メモリ、およびロギング ディスク	• 最大 500 台の管理対象デバイスの管理
	  • 16 CPU
	  • 32 GB メモリ
	  • ローカル ログ ストレージはサポートされていません
	• 最大 1,000 台の管理対象デバイスの管理
	  • 32 CPU
	  • 128 GB メモリ
	  • ローカル ログ ストレージはサポートされていません
	• 1,000 を超えるファイアウォールを管理するには、「デバイス管理能力要件の強化」を参照してください。
		• 最大 10,000 ログ/秒：
		  • 16 CPU
		  • 32 GB メモリ
		  • 4 個の 2TB ロギング ディスク
		  • 最大 500 台の管理対象デバイスの管理
		• 最大 20,000 ログ/秒
		  • 32 CPU
		  • 128 GB メモリ
		  • 8個の 2TB ロギング ディスク
		  • 最大 1,000 台の管理対象デバイスの管理
			• 最大 15,000 ログ/秒
			  • 16 CPU
			  • 32 GB メモリ
			  • 4 個の 2TB ロギング ディスク
			• 最大 25,000 ログ/秒
			  • 32 CPU
			  • 128 GB メモリ
			  • 8個の 2TB ロギング ディスク

ログ ストレージ容量	管理専用モードの Panorama では、専用ログ コレクタへのログ転送が必要です。	2TB から 24TB	2TB から 24TB

サポートされるインターフェイス

インターフェイスを使用してデバイスの管理、ログ収集、コレクタ グループ通信、ライセンスおよびソフトウェアの更新を行えます。

機能	Amazon Web Services（AWS）および AWS GovCloud	Microsoft Azure	Google Cloud Platform（	KVM	Hyper-V	VMware（ESX Air）
デバイス管理	任意のインターフェイスをサポート					
デバイス ログ収集	任意のインターフェイスをサポート					

© 2019 Palo Alto Networks, Inc.

機能	Amazon Web Services（AWS）および AWS GovCloud		Microsoft Azure	Google Cloud Platform（	KVM	Hyper-V	VMware（ESX Air）
コレクタ グループ通信	任意のインターフェイスをサポート						
ライセンスおよびソフトウェアの更新	MGT インターフェイスのみ	MGT インターフェイスのみ	MGT インターフェイスのみ	MGT インターフェイスのみ	任意のインターフェイスをサポート	任意のインターフェイスをサポート	任意のインターフェイスをサポート

Panorama バーチャル アプライアンスのインストール

インストール前に、Panorama モード、管理専用モード、ログ コレクタ モード、またはレガシー モード（VMware のみ）で仮想アプライアンスを実行するかどうかを決定します。Each mode has different resource requirements, as described in Panorama バーチャル アプライアンスのセットアップ前提条件に記載されている通り、各モードには別のリソース要件があります。前提条件を満たしてから、インストールを始める必要があります。

バーチャル アプライアンスを *Panorama* モードでインストールして、ログ ストレージとレポート生成を最適化することをお薦めします。*Panorama* モードとレガシー モードの詳細は、Panorama モデルを参照してください。

- VMware で Panorama をインストール
- AWS で Panorama をインストール
- AWS GovCloud で Panorama をインストール
- Panorama で Azure をインストール
- Panorama を Google Cloud Platform にインストールする
- KVM で Panorama をインストール
- Hyper-V で Panorama をインストール

VMware で Panorama をインストール

Panorama バーチャル アプライアンスは、ESXi および vCloud Air VMware プラットフォームにインストールできます。

- ESXi サーバーに Panorama をインストール
- vCloud Air に Panorama をインストール
- Panorama バーチャル アプライアンスにおける VMware ツールのサポート

ESXi サーバーに Panorama をインストール

VMware ESXi サーバーに新しい Panorama バーチャル アプライアンスをインストールするには、以下の手順を使用します。既存の Panorama バーチャル アプライアンスをアップグレードする場合は、「Panorama 用のコンテンツ更新およびソフトウェア更新のインストール」に進んでください。

STEP 1 | Panorama 10.0 のベース イメージ Open Virtual Appliance (OVA) ファイルをダウンロードします。

1. Palo Alto Networksソフトウェア ダウンロード サイトに移動します。（ログインできない場合は、Palo Alto Networksカスタマーサポート ウェブサイトにてサポートをご利用ください）

© 2019 Palo Alto Networks, Inc.

2. Panorama Base Images（ベース イメージ）セクションの Download（ダウンロード）列で、Panorama リリース OVA ファイルの最新バージョン（`Panorama-ESX-10.0.0.ova`）をダウンロードします。

STEP 2 | Panorama をインストールします。

1. VMware vSphere クライアントを起動し、VMware サーバーに接続します。
2. [ファイル] > [**OVF** テンプレートのデプロイ] の順に選択します。
3. Panorama OVAファイルを**Browse**（参照）して選択し、**Next**（次へ）をクリックします。
4. 製品の名前と説明がダウンロードしたバージョンと一致していることを確認し、**Next**（次へ）をクリックします。
5. Panorama バーチャル アプライアンスの分かりやすい名前を入力し、**Next**（次へ）をクリックします。
6. Panorama イメージをインストールするデータストアの場所（システム ディスク）を選択します。対応のシステム ディスク サイズについては、Panorama バーチャル アプライアンスのセットアップ前提条件 を参照してください。データストアを選択したら、**Next**（次へ）をクリックします。
7. ディスク フォーマットに **Thick Provision Lazy Zeroed**（シックプロビジョニング（**Lazy Zeroed**））を選択し、**Next**（次へ）をクリックします。
8. Panorama バーチャル アプライアンスに使用するネットワークをインベントリで指定し、**Next**（次へ）をクリックします。
9. 選択したオプションを確認し、**Finish**（終了）をクリックしてインストールを開始し、完了したら **Close**（閉じる）をクリックします。Panorama バーチャル アプライアンスにはまだ電源を入れません。

STEP 3 | Panorama バーチャル アプライアンスでリソースを設定します。

1. Panorama バーチャル アプライアンスを右クリックし、**Edit Settings**（設定変更）を選択します。
2. **Hardware**（ハードウェア）設定で、必要に応じて CPU とメモリを割り当てます。

   十分な *CPU* と *Memory*（メモリ）を割り当て、仮想ロギング用ディスクを追加すると（この手順の後半）、バーチャル アプライアンスは *Panorama* モードで起動します。その他の場合、アプライアンスは管理専用モードで起動します。モードの詳細は、「Panorama モデル」を参照してください。
3. **SCSI Controller**（**SCSI**コントローラ）を **LSI Logic Parallel**（**LSI** ロジック パラレル）に設定します。
4. 仮想ロギング用ディスクを追加します。

   この手順は、以下のシナリオで必要となります。
   - *Panorama* モードで、専用のロギング ディスクにログを保存する場合。
   - *SD-WAN* デプロイメントを管理専用モードで管理します。

   1. ディスクを **Add**（追加）してハードウェア タイプとして **Hard Disk**（ハード ディスク）を選択し、**Next**（次へ）をクリックします。
   2. **Create a new virtual disk**（新しい仮想ディスクを作成）して、**Next**（次へ）をクリックします。
   3. **Disk Size**（ディスク サイズ）を正確に 2TB に設定します。

      Panorama モードでは、後でそれぞれ *2TB* のストレージに、さらにロギング ディスクを追加（合計で *12*）できます。既に *Panorama* に追加されているロギング ディスクのサイズの拡張は、サポートされていません。
   4. 優先する **Disk Provisioning**（ディスク プロビジョニング）disk format（ディスクフォーマット）を選択します。

      Disk Provisioning disk format（ディスク プロビジョニング フォーマット）を選択する際は、ビジネスニーズを考慮してください。Disk Provisioning（ディスク プロビジョニング）のパフォー

© 2019 Palo Alto Networks, Inc.

マンスに関する考慮事項の詳細については、VMware Thick vs Thin Disks and All Flash Arrays（シックディスク対シンディスク、およびオールフラッシュアレイ）のドキュメント、またはその他の VMware ドキュメントを参照してください。



複数のロギング ディスクを追加する場合、発生する可能性のある予期しないパフォーマンスの問題を回避するために、すべてのディスクに同じ *Disk Provisioning*（ディスク プロビジョニング）フォーマットを選択することが、ベストプラクティスです。

5. 場所として **Specify a datastore or datastore structure**（データストアまたはデータストア構造を指定）を選択し、十分なストレージがあるデータストアを **Browse**（参照）によって選択し、**OK** をクリックしてから **Next**（次へ）をクリックします。
6. SCSI **Virtual Device Node**（仮想デバイス ノード）（デフォルトのセクションを使用可能）を選択して**Next**（次へ）をクリックします。



SCSI 以外の形式を選択すると、*Panorama* は起動できなくなります。

7. 設定が正しいことを確認し、**Finish**（完了）をクリックします。

5. **OK** をクリックして変更内容を保存します。

STEP 4 | Panorama バーチャル アプライアンスをパワーオンします。

1. vSphereクライアントでPanorama バーチャル アプライアンスを右クリックし、**Power** > **Power On**(電源 > 電源オン)を選択します。Panorama の起動を待ってから続行します。
2. バーチャル アプライアンスが正しいモードで動作していることを確認します。
   1. Panorama バーチャル アプライアンスを右クリックし、**Open Console**（コンソールを開く）を選択します。
   2. ログイン用のユーザー名およびパスワードを入力します（デフォルトはどちらも **admin**）。
   3. 以下のコマンドを入力してモードを表示します。

```
> show system info
```

出力の `system-mode` は、`panorama` モードか `management-only` モードになります。

STEP 5 | ESXi サーバーに Panorama のシステムディスクを追加する以下の目的で Panorama バーチャル アプライアンスを使用する場合：

- SD-WAN デプロイメントを Panorama モードで管理します。
- 大規模なファイアウォール デプロイメントを管理する場合は、ダイナミック更新のための追加のストレージ スペースが必要です。

これで、Panorama バーチャル アプライアンスの初期設定の実行を行う準備ができました。

vCloud Air に **Panorama** をインストール

VMware vCloud Airに新しい Panorama バーチャル アプライアンスをインストールするには、以下の手順を使用します。vCloud Airにデプロイされた Panorama バーチャル アプライアンスをアップグレードしている場合は、Panorama用のコンテンツ更新およびソフトウェア更新のインストールに進んでください。

STEP 1 | Panorama 10.0 のベース イメージ Open Virtual Appliance (OVA) ファイルをダウンロードします。

1. Palo Alto Networksソフトウェア ダウンロード サイトに移動します。（ログインできない場合は、Palo Alto Networksカスタマーサポート ウェブサイトにてサポートをご利用ください）
2. Panorama ベース イメージ セクションの Download（ダウンロード）列で、Panorama 10.0 リリース OVA ファイル（`Panorama-ESX-10.0.0 ova`）をダウンロードします。

© 2019 Palo Alto Networks, Inc.

STEP 2 | Panoramaイメージを vCloud Air カタログにインポートします。

このステップの詳細については、OVFツールのユーザーガイドを参照してください。

1. OVF ツールをクライアントシステムにインストールします。
2. クライアントシステムの CLI にアクセスします。
3. OVF Tool ディレクトリに移動します（例：C:\Program Files\VMware\VMware OVF Tool）。
4. OVA ファイルを OVF パッケージに変換します。

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

5. ブラウザを使ってvCloud AirのWebコンソールにアクセスし、**Virtual Private Cloud OnDemand**（仮想プライベート クラウド（オンデマンド））の場所を選択し、ブラウザのURLを控えておきます。次のステップでは、この URL 情報を使用して作業を完了させることになります。**https://<virtual#cloud#location>.vchs.vmware.com/compute/cloud/org/<vCloud#account#number>/#/catalogVAppTemplateList?catalog=<catalog#ID>**.
6. OVFパッケージをインポートし、vCloud AirのURLの情報を使って<virtual-cloud-location>、<vCloud-account-number>、<catalog-ID>の変数を埋めます。他の変数は、vCloud Airのユーザー名およびドメイン <user>@<domain>、仮想データセンター <datacenter>、およびvCloud Airテンプレート <template>です。

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

STEP 3 | Panorama をインストールします。

1. vCloud AirのWebコンソールにアクセスし、ご自身の **Virtual Private Cloud OnDemand**（仮想プライベート クラウド オンデマンド）領域を選択します。
2. Panorama 仮想マシンを作成します。このステップについては、vCloud Air ドキュメント センターのテンプレートから仮想マシンを追加を参照してください。**CPU**、**Memory**（メモリ）および**Storage**（ストレージ）を次のようにして設定します。
   - バーチャル アプライアンスのモードを基準に **CPU** と **Memory** (メモリ) を設定する方法については、Panorama バーチャル アプライアンスのセットアップ前提条件 を参照してください。
   - Panorama バーチャル アプライアンスのシステム ディスクを設定するには、**Storage** (ストレージ) を設定します。Panorama バーチャル アプライアンスに対応するディスクサイズについては、 Panorama バーチャル アプライアンスのセットアップ前提条件 を参照してください。ログおよびレポートのパフォーマンスを高めるには、**SSD-Accelerated** オプションを選択します。

     ログの保存容量を増やすには、vCloud Air の Panorama に仮想ディスクを追加する必要があります。Panorama モードのバーチャル アプライアンスでは、ログの保存にシステム ディスクが使用されません。仮想ロギング用ディスクを追加する必要があります。

STEP 4 | ゲートウェイ上で vCloud Air NAT ルールを作成し、Panorama バーチャル アプライアンスのインバウンドおよびアウトバウンド トラフィックを許可します。

詳細な流れについては vCloud Air ドキュメント センターのNATルールの追加をご覧ください。

1. Panorama がファイアウォールからトラフィックを受け取り、管理者アクセスが Panorama にアクセスできるようにする NAT ルールを追加します。
2. Panorama が Palo Alto Networks の更新サーバーからアップデートを取得し、ファイアウォールにアクセスできるようにする NAT ルールを追加します。

© 2019 Palo Alto Networks, Inc.

STEP 5 | vCloud Airファイアウォール ルールを作成し、Panorama バーチャル アプライアンス上のインバウンドトラフィックを許可します。

アウトバウンド トラフィックはデフォルトで許可されています。

詳細な流れについては vCloud Air ドキュメント センターのファイアウォール ルールの追加をご覧ください。

STEP 6 | Panorama バーチャル アプライアンスの電源が入っていない場合は電源を入れます。

vCloud AirのWeb コンソールで**Virtual Machines**（仮想マシン）タブを選択し、さらに Panorama 仮想マシンを選択して**Power On**（電源オン）をクリックします。

これで、Panorama バーチャル アプライアンスの初期設定の実行を行う準備ができました。

Panorama バーチャル アプライアンスにおける **VMware** ツールのサポート

VMware ツールは、Panorama バーチャル アプライアンス用のソフトウェアイメージ（ovf）にバンドルされています。VMware ツールをサポートすることで、vSphere 環境（vCloud ディレクターおよび vCenter サーバー）で以下の操作を行えるようになります。

- Panorama 管理インターフェイスに割り当てられた IP アドレスを確認する。
- ハードディスク、メモリ、CPU のリソース使用状況を確認する。これらの計測データを使用すれば、vCenter サーバーあるいは vCloud ディレクターでアラームやアクションを有効化できます。
- vCenter サーバーあるいは vCloud ディレクターのパワーオフ機能を使って Panorama の再起動およびグレースフルシャットダウンを行う。
- Panorama が機能していることを検証したりファイアウォールあるいは Panorama が再起動中かどうかを検証したりするための、vCenter サーバーと Panorama 間のハートビート機能を有効化する。ファイアウォールがメンテナンス モードに移る場合、vCenter サーバーがファイアウォールをシャットダウンすることがないよう、ハートビートが無効化されます。ハートビートを無効化することで、ファイアウォールがハートビートを vCenter サーバーに送信できない場合でもメンテナンス モードで起動したままにすることができます。

AWS で Panorama をインストール

Amazon Web Services（AWS）に Panorama™ と 専用ログ コレクタをデプロイできるようになりました。AWSにデプロイされた Panorama はライセンス持ち込み（BYOL）であり、すべてのデプロイ モード（Panorama、ログ コレクタ、および管理専用）をサポートし、M-Series ハードウェア アプライアンスと同じプロセスと機能を共有します。Panorama モードの詳細は、「Panorama モデル」を参照してください。

STEP 1 | AWS Web Service のコンソールにログインし、EC2 Dashboard を選択します。

- Amazon Web Services のコンソール
- AWS GovCloud Web Service のコンソール

STEP 2 | ネットワークの必要に応じて VPC をセットアップします。

Panorama バーチャル アプライアンスを既存の VPC で起動する場合でも、新しい VPC を作成する場合でも、Panorama バーチャル アプライアンスは EC2 インスタンスからのトラフィックを受信して、VPC とインターネットとの間でインバウンドおよびアウトバウンド通信を実行できなければなりません。

VPC を作成してアクセスを設定する方法については、AWS VPC のドキュメントを参照してください。

1. 新規 VPC を作成するか、既存の VPC を使用します。AWS のドキュメント「始めましょう」を参照してください。
2. ネットワーク コンポーネントとセキュリティ コンポーネントが適切に定義されていることを確認します。

© 2019 Palo Alto Networks, Inc.

- インターネットとの通信を有効化します。デフォルトの VPC にはインターネット ゲートウェイが用意されていますので、デフォルトのサブネットで Panorama バーチャル アプライアンスをインストールすれば、VPC はインターネットにはアクセスできます。
- サブネットを作成します。サブネットは、EC2 インスタンスを起動できる VPC に割り当てられた IP アドレス範囲のセグメントです。Panorama バーチャル アプライアンスがインターネットにアクセスできるように設定するには、パブリック サブネットに属している必要があります。
- EC2 インスタンス/サブネットからのインバウンド/アウトバウンド トラフィックを管理するには、必要に応じてセキュリティグループを作成します。
- プライベート サブネットのルート テーブルにルートを追加し、該当する VPC 内のセブネットおよびセキュリティグループ全体に確実にルート可能なトラフィックをルーティングできるようにします。

STEP 3 | Panorama を Amazon Web Services にデプロイします。

1. EC2 Dashboard で、**Instances**（インスタンス）> **Launch Instance**（インスタンスを起動）をクリックします。
2. **AWS Marketplace** を選択して、**`Palo Alto Networks Panorama`**を検索し、Panorama AMI を **Select**（選択）してから **Continue**（続行）します。
3. Panorama バーチャル アプライアンスに必要なリソースを割り当てるための **EC2 instance type**（**EC2** インスタンス タイプ）を選択してから **Next**（次へ）をクリックします。**Configure Instance Details**（インスタンス詳細設定）を行います。リソース要件については、Panorama バーチャル アプライアンスのセットアップ前提条件を確認してください。

   Panorama バーチャル アプライアンスを専用ログ コレクタとして使用する場合は、必ず初回のデプロイ時に必要なリソースと共にアプライアンスを構成するようにしてください。*Panorama* バーチャル アプライアンスは、仮想マシンのデプロイ後でサイズを変更するとログ コレクタ モードのままにならず、ログ データが失われます。
4. インスタンスの詳細を設定します。
   1. **Next:Configure Instance Details**（インスタンス詳細設定）を行います。
   2. 前のステップで作成した ネットワークを選択するか、AWS が提供するデフォルト VPC を使用します。条件によっては、
   3. 前のステップで作成した **Subnet**（サブネット）を選択するか、AWS が提供するデフォルト サブネットを使用します。
   4. **Auto-assign Public IP**（パブリック **IP** を自動で割り当てる）は、**Enable**（有効）を選択します。

      この IP は、Panorama を使用して管理する予定のファイアウォールからアクセスできる必要があります。これにより、Panorama バーチャル アプライアンスの管理インターフェイス用に、公開された IP アドレスを取得することができます。後で、管理インターフェイスに Elastic IP アドレスをアタッチできます。インスタンスが終了するとバーチャル アプライアンスから関連付けが解除されるパブリック IP アドレスとは異なり、Elastic IP アドレスには永続性を提供し、Panorama バーチャル アプライアンスの新しい（または置換された）インスタンスへの IP アドレスは、Panorama バーチャル アプライアンス インスタンスの電源がオフになっても常に IP アドレスを再設定する必要はありません。
   5. 必要に応じて、追加するインスタンスの詳細を設定します。
5. Panorama バーチャル アプライアンスのストレージを設定します。
   1. **Next:**ストレージを追加します。
   2. ルート システムのディスク サイズを確認し、224GB のシステム ディスクに拡張する必要があるかどうかを判断します。必要に応じて、システム ディスクの サイズを 224GB に増やします。

      大規模なデータセットをサポートするには、ダイナミック更新などのために十分なディスク領域を確保するために、224GB のシステム ディスクが大規模なファイアウォールのデプロイを管理に必要です。

© 2019 Palo Alto Networks, Inc.

（SD-WAN のみ）Panorama バーチャル アプライアンスを Panorama モードで使用して、SD-WAN デプロイメントを管理する場合は、224GB のシステム ディスクを拡張し、管理対象ファイアウォールの状態を監視およびレポートします。



224GB のシステム ディスクを備えた *Panorama* バーチャル アプライアンス インスタンスをデプロイする場合、将来より小規模なシステム ディスクに移行することはできません。

3. **Add New Volume**（新規ボリュームを追加）して、さらにログ ストレージを追加します。

   （SD-WAN のみ）SD-WAN デプロイメントを管理専用モードで管理する予定の場合は、2TB のログ ディスクを追加する必要があります。

   Panorama モードで Panorama バーチャル アプライアンスを使用する場合、または専用ログ コレクタとして使用する場合は、最初のデプロイメント時に仮想ロギング ディスクを追加します。デフォルトでは、Panorama モードのリソース要件を満たし、少なくとも 1 つの仮想ロギング ディスクを追加した場合、Panorama バーチャル アプライアンスは初期デプロイメント用の Panorama モードになります。それ以外の場合、Panorama バーチャル アプライアンスはデフォルトで管理専用モードになります。デバイスと専用ログ コレクタを管理し、ローカルにログを収集しない場合は、Panorama バーチャル アプライアンスを管理専用モードに変更します。

   AWSの Panorama バーチャル アプライアンスは 2TB ロギング ディスクのみをサポートし、合計で最大 24TB のログ ストレージをサポートします。2TB より小さいロギング ディスク、または 2TB ロギングディスク要件で割り切れないサイズのロギング ディスクを追加することはできません。Panorama バーチャル アプライアンスは、2TB を超えるディスクを 2TB のパーティションに分割します。

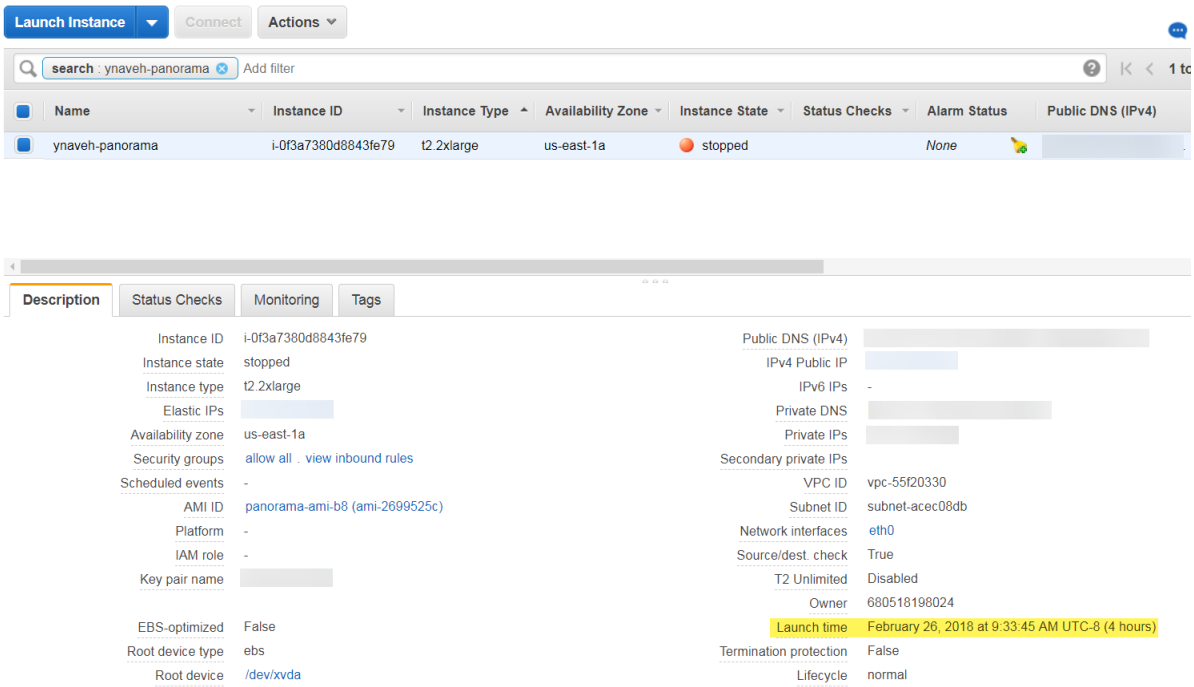
6. （任意）**Next:**（次へ）を選択：タグを追加し、メタデータとして1 つ以上のタグを追加して、Panorama バーチャル アプライアンスの識別とグループ化をします。たとえば、Panorama バーチャル アプライアンスが管理するファイアウォールを識別するための**Value**（値）を持つ**Name**（名前）タグを追加します。
7. インスタンス セキュリティ グループを設定します。
   1. **Next:**セキュリティ グループを設定します。
   2. **Security Group**（セキュリティ グループ）を新規作成するか、HTTPS と SSH が有効になっている既存のものを選択してください。このセキュリティ グループの目的は、ファイアウォールの管理インターフェイスへのアクセスを制限することです。
8. **Launch**（起動）する前に、選択内容が正確であることを確認し、Panorama バーチャル アプライアンス インスタンスを **Review and Launch**（確認して起動）します。
9. 既存のキー ペアを選択するか、または新しく作成し、要求メッセージを受け入れます。



AWS から新規のキーを作成した場合は、キーをダウンロードして安全な場所に保存します。ファイル拡張子は *.pem* です。公開鍵を PuTTYgen にロードし、 *.ppk* 形式で保存する必要があります。このキーは失うと再生成できません。

AWS で Panorama バーチャル アプライアンスを起動した後、Panorama バーチャル アプライアンスのデプロイが完了するまでに約 30 分かかります。Panorama バーチャル アプライアンスのデプロイは、インスタンスに接続されているディスクの数とサイズによって時間がかかることがあります。Panorama バーチャル アプライアンス インスタンス（ **Instances**（インスタンス））を選択して、起動時間を表示します。

© 2019 Palo Alto Networks, Inc.



Panorama バーチャル アプライアンスを専用ログ コレクタとして使用する場合は、アプライアンスに必要なリソースがあることを確認してください。*Panorama* バーチャル アプライアンスは、仮想マシンのデプロイ後でサイズを変更するとログ コレクタ モードのままにならず、ログ データが失われます。

STEP 4 | Panorama バーチャル アプライアンスをシャットダウンします。

1. EC2 Dashboard で、**Instances**（インスタンス）を選択します。
2. Panorama バーチャル アプライアンスを選択して、**Actions**（操作）> **Instance State**（インスタンスの状態）> **Stop**（停止）の順にクリックします。

STEP 5 | 管理インターフェイスに Elastic IP（EIP）アドレスを作成または割り当てます。

1. AWS コンソールで、 **Elastic IPs** と **Allocate New Address**（新規アドレスを割り当て）を選択します。
2. **Allocate**（割り当て）をクリックして新規 EIP アドレスを作成し、**Actions**（操作）をクリックして、**Associate address**（アドレスの割り当て）を行います。
3. **Instance**（インスタンス）を選択し、EIP アドレスを割り当てるPanorama バーチャル アプライアンス インスタンスを選択し、管理インターフェイスに関連付けられた **Private IP address**（プライベート **IP** アドレス）を入力し、**Associate**（関連付け）をクリックします。

STEP 6 | Panorama バーチャル アプライアンスをパワーオンします。

1. EC2 Dashboard で、**Instance**（インスタンス）を選択します。
2. リストから、Panorama バーチャル アプライアンスを選択して、**Actions**（操作）> **Instance State**（インスタンスの状態）> **Start**（開始）の順にクリックします。

STEP 7 | Panorama バーチャル アプライアンスの新しい管理者パスワードを設定します。

一意な管理者用パスワードを設定しなければ Panorama バーチャル アプライアンスのWebインターフェイスにアクセスできません。CLI にアクセスするには、Panorama バーチャル アプライアンスの起動に使用する秘密鍵が必要です。

- お使いのコンピュータに SSH サービスがインストールされている場合：

© 2019 Palo Alto Networks, Inc.

1. 以下のコマンドを入力して、Panorama バーチャル アプライアンスにログインします。

```
ssh -i <private_key.ppk> admin@<public-ip_address>
```

2. 以下のコマンドを使用し、画面上のプロンプトに従って新しいパスワードを設定します。

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

3. BYOL を有効にする必要がある場合は、Panorama バーチャル アプライアンスが Palo Alto Networks ライセンス サーバーにアクセスできるように DNS サーバーの IP アドレスを設定します。DNSサーバーのIPアドレスを設定する場合は以下のコマンドを実行してください。

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

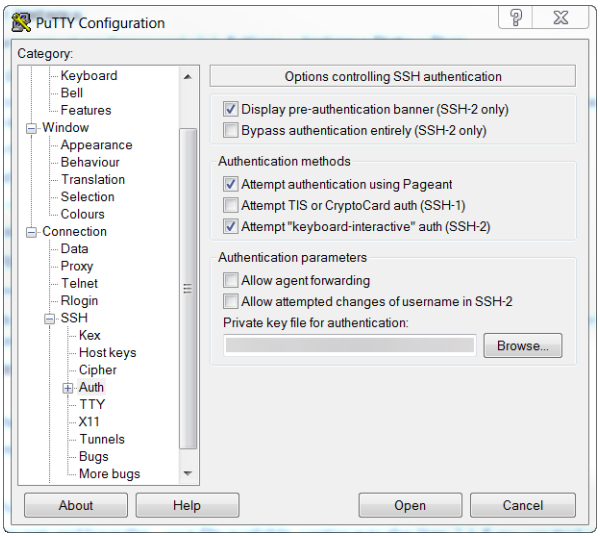
4. 以下のコマンドで変更内容をコミットします。

```
admin# commit
```

5. SSH セッションを終了します。

- Panorama バーチャル アプライアンスに PuTTY を使用して SSH を使用している場合：

1. 既存のキーペアを使用していて、.ppk ファイルを使用できる場合はステップ 7.3 を続行します。新しいキーペアを作成した場合、または既存のキーペアの .pem ファイルのみを持つ場合は、PuTTYgen を開き、 .pem ファイルを **Load**（読み込み）します。
2. ローカルのアクセス可能な宛先に **Save the private key**（秘密鍵を保存）します。
3. PuTTY を開き、select **SSH** > **Auth**を選択してから、前のステップで保存した .ppk ファイルを **Browse**（参照）します。



4. **Sessions**（セッション）を選択し、Panorama バーチャル アプライアンスのパブリック IP アドレスを入力します。**Open**（開く）をクリックし、セキュリティ プロンプトが表示されたら**Yes**（はい）をクリックします。
5. 指示に従って管理者としてログインします。
6. 以下のコマンドを使用し、画面上のプロンプトに従って新しいパスワードを設定します。

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


© 2019 Palo Alto Networks, Inc.

7. Panorama バーチャル アプライアンスが Palo Alto Networks ライセンス サーバーにアクセスできるように DNS サーバーの IP アドレスを設定します。DNSサーバーのIPアドレスを設定する場合は以下のコマンドを実行してください。

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

8. 以下のコマンドで変更内容をコミットします。

```
admin# commit
```

9. SSH セッションを終了します。

STEP 8 | Panorama バーチャル アプライアンスのデバイス管理ライセンスとサポート ライセンスを有効にします。

- Panorama バーチャル アプライアンスがインターネットに接続している時のファイアウォール管理ライセンスのアクティベーション/取得
- Panorama バーチャル アプライアンスがインターネットに接続していない時のファイアウォール管理ライセンスのアクティベーション/取得
- Panorama サポート ライセンスのアクティベーション

STEP 9 | デプロイメントのニーズに合わせて Panorama バーチャル アプライアンスの設定を完了します。

- （管理専用モード）管理専用モードの Panorama バーチャル アプライアンスのセットアップ.
- （ログ コレクタ モード）Panorama モードからログ コレクタ モードに切り替えを行うには、ステップ 6 を開始してください。

  Panorama 管理サーバーに管理コレクタとしてログ コレクタを追加すると、専用ログコレクタのパブリック *IP* アドレスを入力します。*IP address*（*IP* アドレス）、*Netmask*（ネットマスク）、または *Gateway*（ゲートウェイ）を指定することはできません。
- (Panorama および管理専用モード) 管理対象コレクタの設定 して、専用ログ コレクタを Panorama バーチャル アプライアンスに追加するようにします。管理専用モードはローカル ログ収集をサポートしておらず、管理対象デバイス ログを保存する専用ログ コレクタが必要です。

AWS GovCloud で Panorama をインストール

Amazon Web Services（AWS）GovCloudに Panorama™ と 専用ログ コレクタをデプロイできるようになりました。AWS GovCloud は、米国政府機関や顧客の規制あるいはコンプライアンス要件を満たす、AWS の独立した領域のことです。AWS GovCloud にデプロイされた Panorama はライセンス持ち込み（BYOL）であり、すべてのデプロイモード（Panorama、ログコレクタ、管理専用）をサポートしています。Panorama モードの詳細については、Panorama モデルを参照してください。

AWS GovCloud（米国）領域にある政府向けデータや公開データ、およびすべてのカテゴリーの CUI（Controlled Unclassified Information）データを含むワークロードの安全性を保つために、Panorama バーチャル アプライアンスは AWS GovCloud 上の標準的な AWS パブリック クラウドと同様のセキュリティ機能を提供します。AWS GovCloud の Panorama バーチャル アプライアンスと標準の AWS パブリック クラウドは、同じ機能・能力をサポートしています。

Panorama バーチャル アプライアンスのセットアップ前提条件をレビューし、サポートされている EC2 インスタンスのタイプを確認してください。準備ができたら、AWS で Panorama をインストールを参照して AWS GovCloud に Panorama バーチャル アプライアンスをインストールします。

次の各作業を参照し、Panorama バーチャル アプライアンスにロギング用ストレージを追加するか、CPU コアおよびメモリの割り当てを増やします：

© 2019 Palo Alto Networks, Inc.

- AWS の Panorama に仮想ディスクを追加
- AWS 上の Panorama の CPU とメモリを増やす

Panorama で *Azure* をインストール

Microsoft Azure に Panorama™ と 専用ログ コレクタをデプロイできるようになりました。Azure にデプロイされた Panorama はライセンス持ち込み（BYOL）であり、すべてのデプロイ モード（Panorama、ログ コレクタ、および管理専用）をサポートし、M-Series ハードウェア アプライアンスと同じプロセスと機能を共有します。Panorama モードの詳細は、「Panorama モデル」を参照してください。

STEP 1 | Microsoft Azure ポータルにログインします。

STEP 2 | Panorama バーチャル アプライアンスをデプロイします。

1. Azure Dashboard で、**Virtual Machines**（仮想マシン）そ選択して **Add**（追加）します。
2. Palo Alto Networks を検索して、最新の Panorama バーチャル アプライアンス イメージを選択します。
3. Panorama バーチャル アプライアンスを **Create**（作成）します。

STEP 3 | Panorama バーチャル アプライアンスを設定します。

1. 自分の Azure **Subscription**（サブスクリプション）を選択します。
2. すべての Azure インスタンス リソースを含める Azure **Resource Group**（リソース グループ）を選択します。
3. Panorama バーチャル アプライアンスの **Virtual machine name**（仮想マシン名）を入力します。
4. デプロイする Panorama バーチャル アプライアンスの**Region**（地域）を選択します。
5. （任意）**Availability options**（可用性オプション）を選択します。詳細は、 可用性セットの使用方法を参照してください。
6. Panorama 管理サーバのデプロイに使用する **Image**（イメージ）を選択します。すべてのパブリックおよびプライベートイメージを参照して、Azure マーケットプレイスで Panorama イメージから Panorama 管理サーバをデプロイします。
7. Panorama バーチャル アプライアンスのサイズを設定します。サイズ要件については Panorama バーチャル アプライアンスのセットアップ前提条件 を確認します。

   Panorama バーチャル アプライアンスを専用ログ コレクタとして使用する場合は、必ず初回のデプロイ時に必要なリソースと共にアプライアンスを構成するようにしてください。*Panorama* バーチャル アプライアンスは、仮想マシンのデプロイ後でサイズを変更するとログ コレクタ モードのままにならず、ログ データが失われます。
8. Panorama バーチャル アプライアンス管理者の **Username (ユーザー名)** を入力します。ユーザー名が安全であることを確認するため、admin は有効なエントリではありません。
9. Panorama バーチャル アプライアンスへの管理者アクセスを保護するための**Password** [パスワード]を入力するか、**SSH public key** [SSH公開鍵]をコピー＆ペーストします。

   FIPS-CC 操作モードで *Panorama* バーチャル アプライアンスのこのインスタンスを使用する場合、*SSH*キー認証を有効にする必要があります。ユーザー名とパスワードを使用して *Panorama* バーチャル アプライアンス をデプロイすることはできますが、操作モードを *FIPS-CC* に変更すると、そのユーザー名とパスワードを使用して認証できなくなります。*FIPS-CC* モードへのリセット後、*SSH* キーを使用してログインする必要があります。その後、*Panorama Web* インターフェースに後でログインするために使用できるユーザー名とパスワードを設定できます。*SSH*キー作成の詳細については、Azureのドキュメントを参照してください。
10. Panorama バーチャル アプライアンス インスタンスの ネットワーキングの設定
    1. 既存の**Virtual network**（仮想ネットワーク）を選択するか、新規の仮想ネットワークを作成します。

© 2019 Palo Alto Networks, Inc.

2. **Subnet**（サブネット）を設定します。サブネットは、前の ステップ で選択または作成した仮想ネットワークに依存します。既存の仮想ネットワークを選択した場合は、選択した仮想ネットワークのサブネットの 1 つを選択できます。
3. 既存の**Public IP address**（パブリック **IP** アドレス）を選択するか、または新しく作成します。これにより、Panorama バーチャル アプライアンスにアクセスするための管理インターフェイスが作成されます。
4. 既存の**NIC network security group**（**NIC** ネットワーク セキュリティ グループ）を選択するか、新しいセキュリティ グループを作成します。ネットワーク セキュリティ グループは、仮想マシンへのトラフィックを制御します。HTTPS と SSH がインバウンド ルールに対して許可されていることを確認してください。

11. インスタンスの **Management**（管理）設定を指定します。

1. **Auto-shutdown**（自動シャットダウン）を有効にするかどうかを選択します。自動シャットダウンを使用すると、自動シャットダウンを無効にする仮想マシンを自動的にシャットダウンする毎日の時間を設定することができ、新しいパブリック IP アドレスが仮想マシンに割り当てられたり、ログがドロップされたり、ログが破棄されたりしないようにすることができます。Panorama バーチャル アプライアンスのシャットダウン中は、ファイアウォールを監視できません。
2. ブート **Monitoring**'（監視）を有効にするかどうかを選択します。有効になっている場合は、診断ストレージ アカウントを選択します。監視は自動的に起動診断ログを Diagnostics ストレージ アカウントに送信します。詳細情報は、 Microsoft Azure の監視の概要を参照してください。
3. 必要に応じて、その他の設定を指定します。

12. 概要を確認し、利用規約およびプライバシー ポリシーに同意した後、**Create**（作成）をクリックして Panorama バーチャル アプライアンスをデプロイします。

STEP 4 | Panorama バーチャル アプライアンスが正常にデプロイされたことを確認します。

1. **Dashboard**（ダッシュボード）> **Resource Groups**（リソース グループ）を選択してから、Panorama バーチャル アプライアンスを含むリソース グループを選択します。
2. 設定で仮想マシンのデプロイメントの状態に対して **Deployments**（デプロイメント）を選択します。

Panorama バーチャル アプライアンスのデプロイには約 *30* 分かかります。*Panorama* バーチャル アプライアンスの起動は、仮想マシンに設定されているリソースによっては時間がかかることがあります。*Microsoft Azure* は、*ICMP* プロトコルが正常にデプロイされたかどうかをテストすることを許可しません。

Panorama バーチャル アプライアンスを専用ログ コレクタとして使用する場合は、アプライアンスに必要なリソースが正しく設定されていることを確認してください。*Panorama* バーチャル アプライアンスは、仮想マシンのデプロイ後でサイズを変更するとログ コレクタ モードのままにならず、ログ データが失われます。

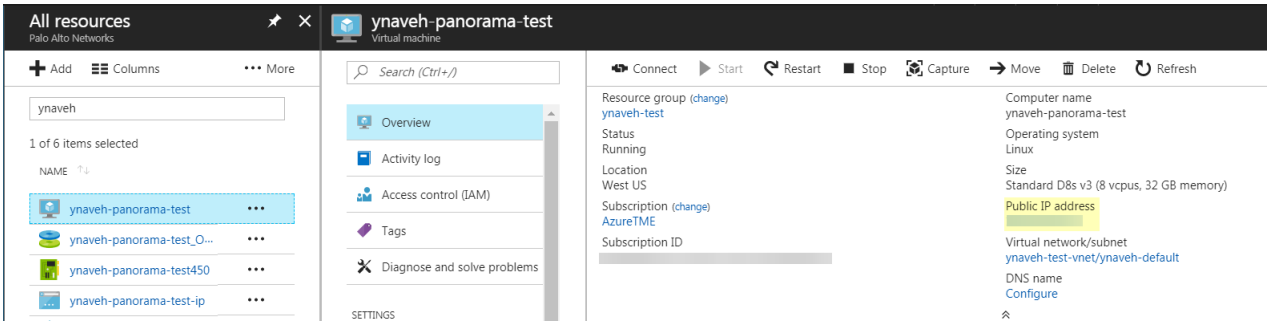
STEP 5 | 静的パブリック IP アドレスを設定します。

1. Azure ポータルで、**Virtual Machines**（仮想マシン）を選択し、Panorama バーチャル アプライアンスを選択します。
2. **Overview**（概要）を選択して **Public IP address**（パブリック **IP** アドレス）をクリックします。
3. 割り当てで、**Static**（静的）を選択して新規 IP アドレス設定を **Save**（保存）します。

STEP 6 | Panorama バーチャル アプライアンスの Web インターフェイスにログインします。

1. Azure ポータルの**All Resources**（すべてのリソース）で Panorama バーチャル アプライアンスを選択し、概要セクションにあるパブリック IP アドレスを表示します。

© 2019 Palo Alto Networks, Inc.



2. Web ブラウザからセキュア (https) 接続を使用し、パブリック IP アドレスを使用して Panorama バーチャル アプライアンスにログインします。
3. Panorama バーチャル アプライアンスのユーザー名とパスワードを入力します。証明書の警告が表示されます。証明書の警告に同意し、Web ページに進みます。

STEP 7 | Panorama バーチャル アプライアンスのデバイス管理ライセンスとサポート ライセンスを有効にします。

- Panorama バーチャル アプライアンスがインターネットに接続している時のファイアウォール管理ライセンスのアクティベーション/取得
- Panorama バーチャル アプライアンスがインターネットに接続していない時のファイアウォール管理ライセンスのアクティベーション/取得
- Panorama サポート ライセンスのアクティベーション

STEP 8 | デプロイメントのニーズに合わせて Panorama バーチャル アプライアンスの設定を完了します。

(SD-WAN のみ) SD-WAN デプロイメントを管理専用モードで管理する予定の場合は、2TB のログ ディスクを追加する必要があります。

1. Azure の Panorama に仮想ディスクを追加します。デフォルトでは、81GB のシステム ディスクが初期デプロイメント時に自動的に作成されます。

   Panorama バーチャル アプライアンスを Panorama モードまたはログ コレクタ モードに変更するには、仮想ログ ディスクを追加する必要があります。

   初回のデプロイ時、デフォルトでは、Azure の Panorama バーチャル アプライアンスは Management Only (管理専用) モードになっています。Panorama モードで Panorama バーチャル アプライアンスを使用する場合、または専用ログ コレクタとして使用する場合は、Azure に Panorama を正しくデプロイした後、仮想ログ ディスクを追加します。

   Azure の Panorama バーチャル アプライアンスは 2TB ログ ディスクのみをサポートし、合計で最大 24TB のログ ストレージをサポートします。2TB より小さいログ ディスク、または 2TB ログディスク要件で割り切れないサイズのログ ディスクを追加することはできません。Panorama バーチャル アプライアンスは、2TB を超えるディスクを 2TB のパーティションに分割します。
2. Panorama バーチャル アプライアンス モードを変更します。

   デフォルトでは、Azure の Panorama バーチャル アプライアンスは管理専用モードでデプロイされています。Panorama モードまたはログ コレクタ モードに変更するには、最初のデプロイ後に少なくとも 1 つのログ ディスクを追加する必要があります。デバイスと専用ログ コレクタを管理し、ローカルにログを収集しない場合は、Panorama バーチャル アプライアンスを管理専用モードのままにします。

   - Panorama モードの Panorama バーチャル アプライアンスのセットアップを行います。
   - (ログ コレクタ モード) Panorama モードからログ コレクタ モードに切り替えを行うには、ステップ 6 を開始してください。

© 2019 Palo Alto Networks, Inc.

Panorama 管理サーバーに管理コレクタとしてログ コレクタを追加すると、専用ログコレクタのパブリック *IP* アドレスを入力します。*IP address* (*IP* アドレス)、*Netmask* (ネットマスク)、または *Gateway* (ゲートウェイ) を指定することはできません。

3. (Panorama および管理専用モード) 管理対象コレクタを設定して、専用ログ コレクタを追加するように管理対象コレクタを設定します。管理専用モードはローカル ログ収集をサポートしておらず、管理対象デバイス ログを保存する専用ログ コレクタが必要です。

Panorama を *Google Cloud Platform* にインストールする

Google Cloud Platform (GCP) に Panorama™ と 専用ログ コレクタをデプロイできるようになりました。GCP にデプロイされた Panorama はライセンス持ち込み (BYOL) であり、すべてのデプロイ モード (Panorama、ログ コレクタ、および管理専用) をサポートし、M-Series ハードウェア アプライアンスと同じプロセスと機能を共有します。Panorama モードの詳細は、「Panorama モデル」を参照してください。

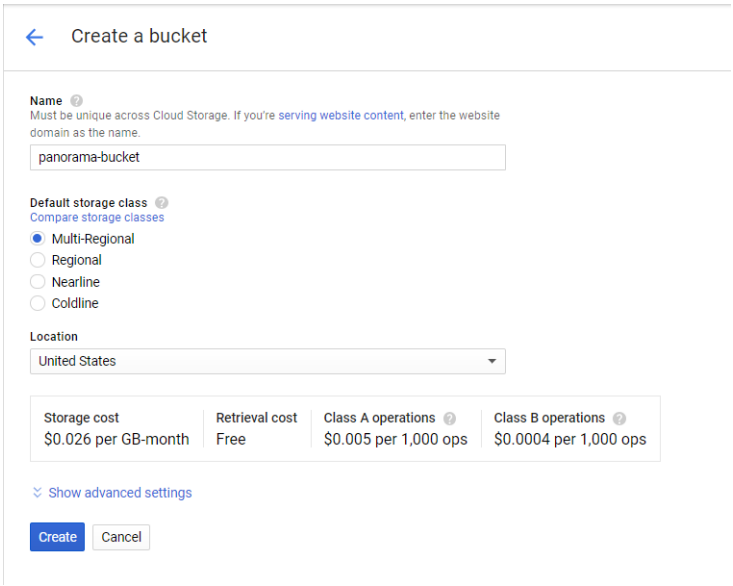
Panorama バーチャル アプライアンスを GCP にデプロイする場合、カスタム イメージをビルドする必要があります。この作業を始めるために、Palo Alto Networks カスタマーサポート ポータルから Panorama `tar.gz`をダウンロードし、それを GCP ストレージ バケットにアップロードする必要があります。その後、カスタム イメージを作成し、そのイメージを使って GCP に Panorama バーチャル アプライアンスをデプロイできるようになります。

STEP 1 | Panorama バーチャル アプライアンスのイメージをダウンロードします。

1. Palo Alto Networks サポートポータルにログインします。
2. **Updates (アップデート)** > **Software Updates (ソフトウェア アップデート)**を選択し、**Panorama Base Images (Panorama** ベースイメージ)でフィルタリングします。
3. Panorama on GCP の最新バージョンの `tar.gz` イメージをダウンロードします。

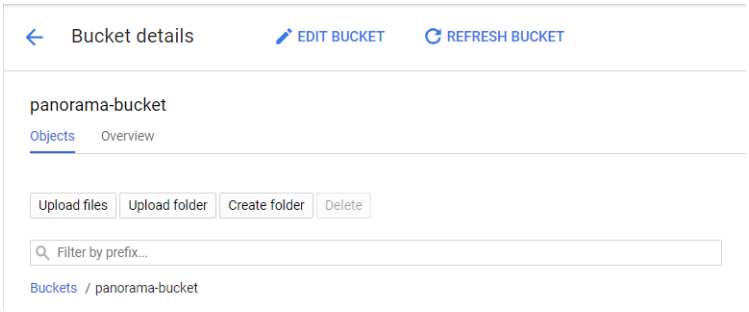
STEP 2 | Panorama バーチャル アプライアンスのイメージを Google Cloud Platform にアップロードします。

1. Google Cloud コンソールにログインします。
2. **Products and Services** (製品とサービス) メニューで**Storage (ストレージ)**を選択します。
3. **Create Bucket (バケットの作成)**をクリックし、新しいストレージ バケットを構成して**Create (作成)**をクリックします。

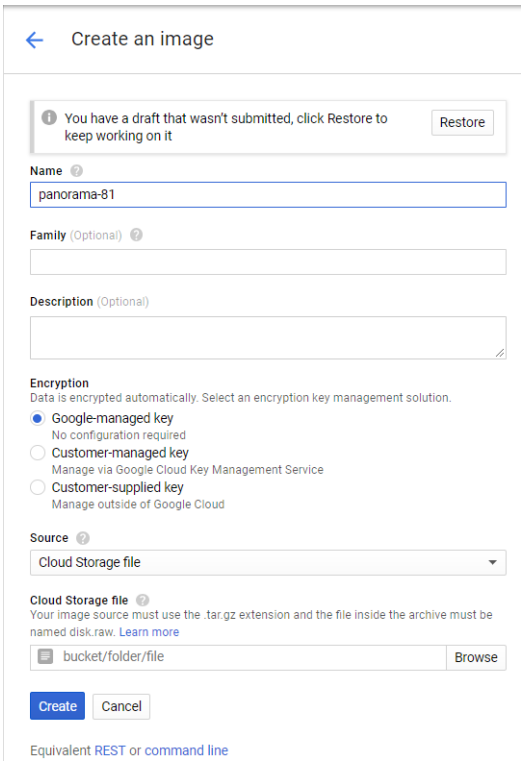


© 2019 Palo Alto Networks, Inc.

4. 前のステップで作成したストレージ バケットを選択して**Upload files** (ファイルのアップロード)をクリックし、ダウンロード済みの Panorama バーチャル アプライアンスのイメージを選択します。



5. **Products and Services** (製品とサービス)メニューで**Compute Engine** (コンピュート エンジン) > **Images** (イメージ)を選択します。
6. **Create Image** (イメージの作成)をクリックして Panorama バーチャル アプライアンスのイメージを作成します。
   1. Panorama バーチャル アプライアンスのイメージに**Name** (名前)を付けます。
   2. **Source** (ソース)フィールドで、ドロップダウンリストから**Cloud Storage file** (クラウドストレージ ファイル)を選択します。
   3. **Browse** (参照)をクリックし、Panorama バーチャル アプライアンスのイメージをアップロードしたストレージ バケットに移動し、アップロード済みのイメージを**Select** (選択)します。
   4. Panorama バーチャル アプライアンスのイメージを**Create** (作成)します。



STEP 3 | Panorama バーチャル アプライアンスを設定します。

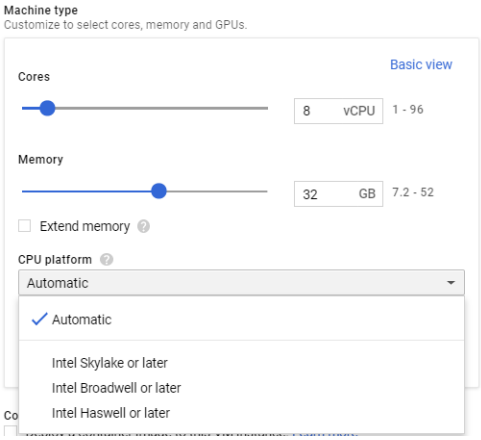
1. **Products and Services** (製品とサービス)メニューで**Compute Engine** (コンピュート エンジン)を選択します。
2. **Create Instance** (インスタンスの作成)をクリックして Panorama バーチャル アプライアンスのデプロイを開始します。

© 2019 Palo Alto Networks, Inc.

3. Panorama バーチャル アプライアンスを簡単に識別するためのわかりやすい**Name**（名前）を追加します。
4. Panorama バーチャル アプライアンスをデプロイする**Region** (リージョン)と**Zone** (ゾーン)を選択します。
5. **Machine Type** (マシンタイプ)を割り当て、CPU コア、メモリ、CPU プラットフォームを**Customize** (カスタマイズ)します。最低リソース要件については、Panorama バーチャル アプライアンスのセットアップ前提条件を確認してください。

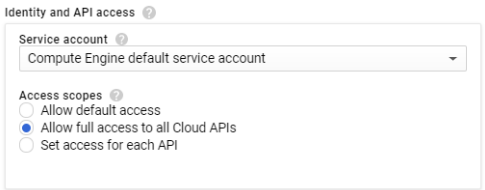
   Panorama バーチャル アプライアンスを専用ログ コレクタとして使用する場合は、必ず初回のデプロイ時に必要なリソースと共にアプライアンスを構成するようにしてください。*Panorama* バーチャル アプライアンスは、仮想マシンのデプロイ後でサイズを変更するとログ コレクタ モードのままにならず、ログ データが失われます。

   GCP のゾーン選択により、利用できる *CPU* プラットフォームが左右されます。詳細についてはリージョンおよびゾーンを参照してください。



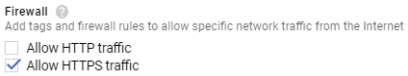
6. Panorama 起動ディスクを設定します。
   1. **Boot Disk**（起動ディスク）で、**Change** > **Custom image**（カスタム イメージの変更）をクリックして、ステップ2 でアップロードした Panorama イメージファイルを選択します。
   2. 起動ディスク サイズを設定します。デフォルトでは、システム ディスクは 81GB ですが、システム ディスクのサイズを 224GB に増やすことができます。

      （SD-WAN のみ）この Panorama バーチャル アプライアンスを Panorama モードで使用して、SD-WAN デプロイメントを管理する場合は、システム ディスクのサイズを 224GB に増やす必要があります。SD-WAN デプロイメントを管理専用モードで管理する場合は、2TB のログ ディスクを追加する必要があります。
   3. **Select**（選択）をクリックし、設定を保存します。
7. **Identity and API access**（アイデンティティと **API** アクセス）で、**Allow full access to all Cloud APIs**（クラウド **API** への完全なアクセスを許可）を選択します。



8. **Firewall**（ファイアウォール）で、**Allow HTTPS traffic**（**HTTPS** トラフィックを許可）を選択します。

© 2019 Palo Alto Networks, Inc.

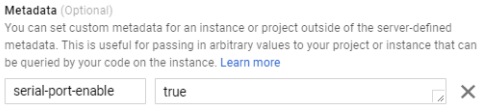


STEP 4 | **Management, security, disks, networking, sole tenancy (管理、セキュリティ、ディスク、ネットワーキング、sole tenancy)** Management, security, disks, networking, sole tenancy を拡張します。

STEP 5 | Panorama バーチャル アプライアンスを管理できるように、シリアル ポートへのアクセスを有効にします。

1. **Management**（管理）を選択します。
2. メタデータとして次の名前と値のペアを入力します。

   ```
   serial-port-enable true
   ```



STEP 6 | 管理インターフェイス用の静的 IP アドレスを予約します。

Panorama バーチャル アプライアンスが再起動する場合、IP アドレスが割り当て直される際に管理対象デバイスが Panorama バーチャル アプライアンスへの接続を失わないケースに備え、管理インターフェイス用の静的内部・外部 IP アドレスを予約します。

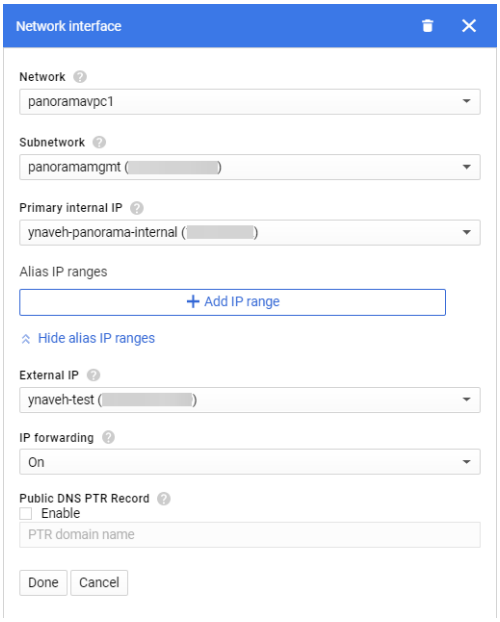
IP アドレスの 予約方法については、静的内部 IP アドレスの予約と 静的外部 IP アドレスの予約を参照してください。

1. **Networking**（ネットワーキング）を選択します。
2. ネットワーク インターフェイスを **Edit**（編集）します。



3. Panorama バーチャル アプライアンスの **Network**（ネットワーク）を選択します。
4. Panorama バーチャル アプライアンスの **Subnetwork**（サブネットワーク）を選択します。同じサブネットワーク内のインスタンスは、内部 IP アドレスを使用して相互通信します。
5. **Primary internal IP**（プライマリ内部 **IP**）アドレスを設定します。
   - **Ephemeral (Automatic)**（一時的（自動））—自動的にプライマリ内部 IP アドレスを割り当てます。
   - **Ephemeral (Custom)**（一時的（カスタム））—GCP がプライマリ内部 IP アドレスを割り当てるために使用するカスタム IP 範囲を設定します。
   - **Reserve a static internal IP address**（静的内部 **IP** アドレスを予約する）—静的プライマリ内部 IP アドレスを手動で設定します。
6. **External IP**（外部 **IP**）アドレスを設定します。
   - **Ephemeral**（一時的）—共有 IP プールから外部 IP アドレスを自動的に割り当てます。
   - 既存の予約済み外部 IP アドレスを選択します。
   - **Create IP address**（**IP** アドレスを作成）—外部 IP アドレスを予約します。
7. Panorama バーチャル アプライアンスが一致しない宛先または送信元 IP アドレスからパケットを受信できるようにするには、**IP forwarding**（**IP** 転送）を **On**（オン）に設定します。

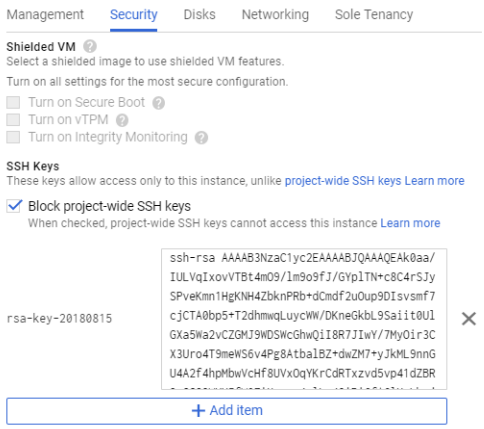
© 2019 Palo Alto Networks, Inc.



STEP 7 | SSH キーを設定します。初期デプロイ後に管理者パスワードを設定するには、Panorama バーチャル アプライアンスの CLI にアクセスするための SSH キーが必要です。

1. **Security** (セキュリティ)を選択します。
2. **Block project-wide SSH keys** (プロジェクト全体の **SSH** キーをブロック)のボックスを選択します。初回のデプロイ後に Panorama バーチャル アプライアンスにログインする際、現在使用できるのはインスタンス キーだけです。
3. コメント ボックスに SSH キーを貼り付けます。正しい SSH キーのフォーマットと GCP 用の SSH キーの生成方法については、メタデータでの SSH キーの管理を参照してください。

SSH キーを生成するときは、秘密鍵を *.ppk* 形式で保存します。秘密鍵は、管理パスワードを設定する前に、初期デプロイ後に *Panorama* バーチャル アプライアンスにログインする必要があります。



STEP 8 | (Panorama とログ コレクタ モード) ログ収集用に追加のストレージを追加します。必要に応じてこのステップを繰り返し、仮想ロギング ディスクを追加します。

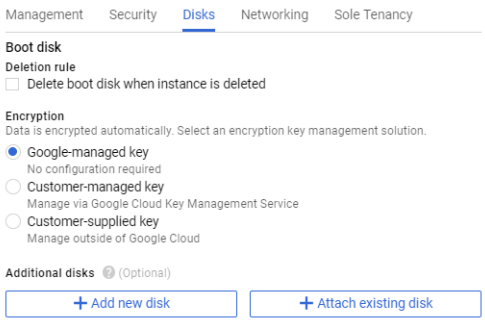
Panorama モードで Panorama バーチャル アプライアンスを使用する場合、または専用ログ コレクタとして使用する場合は、最初のデプロイメント時に仮想ロギング ディスクを追加します。デフォルトでは、Panorama モードのリソース要件を満たし、少なくとも 1 つの仮想ロギング ディスクを追加し

© 2019 Palo Alto Networks, Inc.

た場合、Panorama バーチャル アプライアンスは初期デプロイメント用の Panorama モードになります。そうでない場合、Panorama バーチャル アプライアンスはデフォルトで Management Only（管理専用）モードになり、そこでデバイスおよび専用ログコレクタを管理できますが、ログをローカルで収集できません。

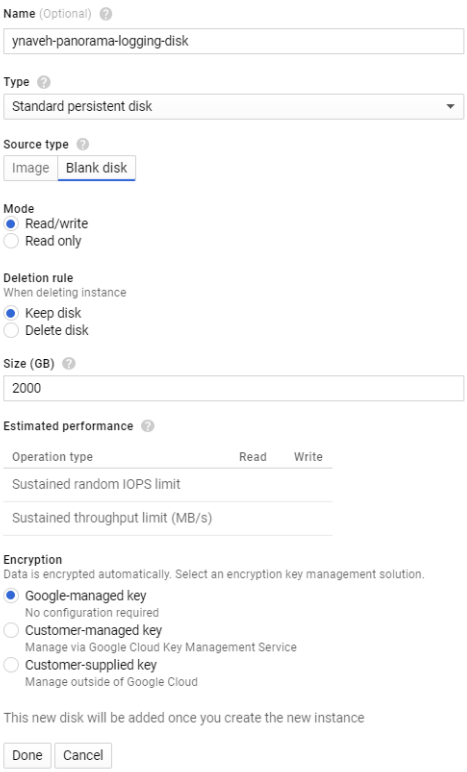
AWSの Panorama バーチャル アプライアンスは 2TB ロギング ディスクのみをサポートし、合計で最大 24TB のログ ストレージをサポートします。2TB より小さいロギング ディスク、または 2TB ロギングディスク要件で割り切れないサイズのロギング ディスクを追加することはできません。Panorama バーチャル アプライアンスは、2TB を超えるディスクを 2TB のパーティションに分割します。

1. を選択し、**Disks**（ディスク）> **Add new disk** (新しいディスクを追加)します。



2. **Name**（名前）を入力します。
3. **Type**（タイプ）ドロップダウンメニューを展開し、目的のタイプを選択します。
4. **Source type** (送信元タイプ)に対して、**Blank disk** (空のデバイス)を選択します。
5. **Mode** (モード)については**Read/write** (読込/書込)を選択します。
6. **Deletion rule** (削除ルール)を選択し、Panorama バーチャル アプライアンスのインスタンスが削除されたら仮想ロギング ディスクを削除するかどうか指定します。受信者
7. 仮想ロギングディスクの**Size (GB)**（サイズ（**GB**））を設定します。
8. 仮想ロギング ディスクのデータに対して優先的に使用する**Encryption** (暗号化)ソリューションをセットします。
9. **Done** (完了)をクリックします。

© 2019 Palo Alto Networks, Inc.



STEP 9 | Panorama バーチャル アプライアンスを **Create**（作成）します。Panorama バーチャル アプライアンスは初期デプロイ後に起動するまでに約 10 分かかります。

STEP 10 | Panorama バーチャル アプライアンスの新しい管理者パスワードを設定します。

一意な管理者用パスワードを設定しなければ Panorama バーチャル アプライアンスのWebインターフェイスにアクセスできません。CLI にアクセスするには、秘密鍵を使用して Panorama バーチャル アプライアンスを起動します。

- お使いのコンピュータに SSH サービスがインストールされている場合：

1. 以下のコマンドを入力して、Panorama バーチャル アプライアンスにログインします。

```
ssh -i <private_key.ppk> admin@<public-ip_address>
```

2. 以下のコマンドを使用し、画面上のプロンプトに従って新しいパスワードを設定します。

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

3. BYOL を有効にする必要がある場合は、Panorama バーチャル アプライアンスが Palo Alto Networks ライセンス サーバーにアクセスできるように DNS サーバーの IP アドレスを設定します。DNSサーバーのIPアドレスを設定する場合は以下のコマンドを実行してください。

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

4. 変更をコミットします：

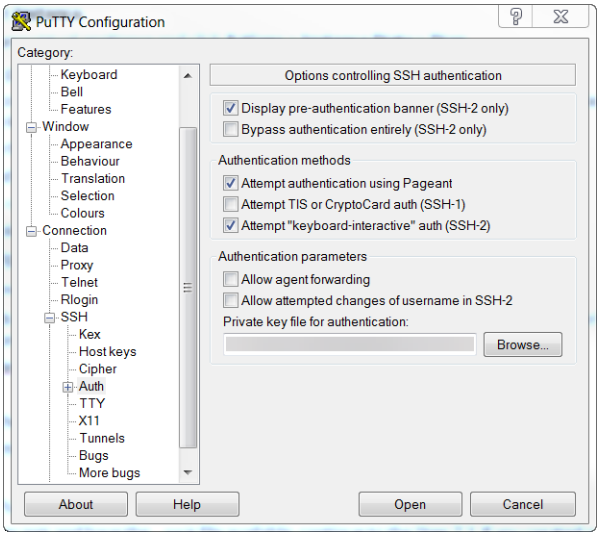
```
admin# commit
```


© 2019 Palo Alto Networks, Inc.

5. SSH セッションを終了します。

- Panorama バーチャル アプライアンスに PuTTY を使用して SSH を使用している場合：

1. 既存のキーペアを使用していて、.ppk ファイルを使用できる場合はステップ 11.3 を続行します。新しいキーペアを作成した場合、または既存のキーペアの .pem ファイルのみを持つ場合は、PuTTYgen を開き、 .pem ファイルを **Load**（読み込み）します。
2. ローカルのアクセス可能な宛先に **Save the private key**（秘密鍵を保存）します。
3. PuTTY を開き、select **SSH** > **Auth**を選択してから、前のステップで保存した .ppk ファイルを **Browse**（参照）します。



4. **Sessions**（セッション）を選択し、Panorama バーチャル アプライアンスのパブリック IP アドレスを入力します。**Open**（開く）を選択し、セキュリティ プロンプトが表示されたら**Yes**（はい）をクリックします。
5. メッセージが表示されたら管理者としてログインします。
6. 以下のコマンドを使用し、画面上のプロンプトに従って新しいパスワードを設定します。

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

7. Panorama バーチャル アプライアンスが Palo Alto Networks ライセンス サーバーにアクセスできるように DNS サーバーの IP アドレスを設定します。DNSサーバーのIPアドレスを設定する場合は以下のコマンドを実行してください。

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

8. 以下のコマンドで変更内容をコミットします。

```
admin# commit
```

9. SSH セッションを終了します。

STEP 11 | Panorama バーチャル アプライアンスのデバイス管理ライセンスとサポート ライセンスを有効にします。

- Panorama バーチャル アプライアンスがインターネットに接続している時のファイアウォール管理ライセンスのアクティベーション/取得
- Panorama バーチャル アプライアンスがインターネットに接続していない時のファイアウォール管理ライセンスのアクティベーション/取得

© 2019 Palo Alto Networks, Inc.

- Panorama サポート ライセンスのアクティベーション

STEP 12 | デプロイメントのニーズに合わせて Panorama バーチャル アプライアンスの設定を完了します。

- （管理専用モード）管理専用モードの Panorama バーチャル アプライアンスのセットアップ.
- （ログ コレクタ モード）Panorama モードからログ コレクタ モードに切り替えを行うには、ステップ 6 を開始してください。

> *Panorama* 管理サーバーに管理コレクタとしてログ コレクタを追加すると、専用ログコレクタのパブリック *IP* アドレスを入力します。*IP address*（*IP* アドレス）、*Netmask*（ネットマスク）、または *Gateway*（ゲートウェイ）を指定することはできません。

- (Panorama および管理専用モード) 管理対象コレクタの設定 して、専用ログ コレクタを Panorama バーチャル アプライアンスに追加するようにします。管理専用モードはローカル ログ収集をサポートしておらず、管理対象デバイス ログを保存する専用ログ コレクタが必要です。

KVM で Panorama をインストール

KVM に Panorama™ と 専用ログ コレクタをデプロイできるようになりました。KVM にデプロイされた Panorama はライセンス持ち込み（BYOL）であり、すべてのデプロイ モード（Panorama、ログ コレクタ、および管理専用）をサポートし、M-Series ハードウェア アプライアンスと同じプロセスと機能を共有します。Panorama モードの詳細は、「Panorama モデル」を参照してください。

STEP 1 | KVM の Panorama バーチャル アプライアンス イメージをダウンロードします。

1. Palo Alto Networks サポートポータルにログインします。
2. **Software Updates**（ソフトウェア アップデート）を選択し、KVM ベース イメージの Panorama を探します。
3. 利用可能な最新の Panorama .qcow2 ファイルをダウンロードします。

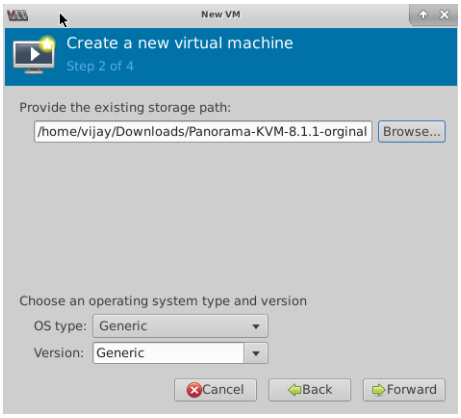
STEP 2 | 新しい仮想マシン イメージを作成し、KVM の Panorama バーチャル アプライアンスを Virtual Machine Manager に追加します。

1. Virtual Machine Manager で、**Create a new virtual machine**（新規仮想マシンを作成）を選択します。
2. **Import Existing disk image**（既存のディスク イメージをインポート）を選択して、**Forward**（転送）をクリックします。



3. Panorama バーチャル アプライアンスのイメージ ボリュームを **Browse**（参照）して、**Choose volume**（ボリュームを選択）します。
4. **Forward**（転送）をクリックします。

© 2019 Palo Alto Networks, Inc.



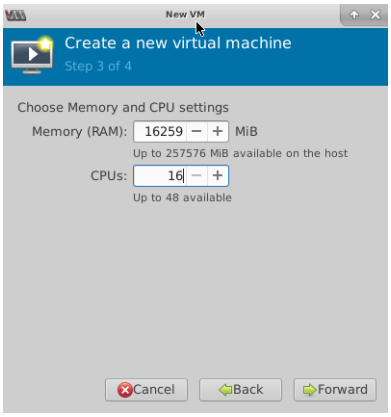
STEP 3 | メモリと CPU の設定を構成します。

最低リソース要件については、Panorama バーチャル アプライアンスのセットアップ前提条件を確認してください。

Panorama バーチャル アプライアンスを専用ログ コレクタとして使用する場合は、必ず初回のデプロイ時に必要なリソースと共にアプライアンスを構成するようにしてください。*Panorama* バーチャル アプライアンスは、仮想マシンのデプロイ後でサイズを変更するとログ コレクタ モードのままにならず、ログ データが失われます。

1. 目的の操作モードの要件に応じて**Memory (メモリ)**を設定します。

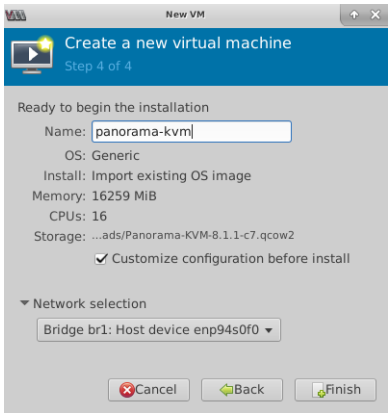
   Virtual Machine Manager は、実行しているバージョンに応じて *MiB*（メビバイト）を使用してメモリを割り当てることができます。*MiB* を使用する場合は、必要なメモリ割り当てを正しく変換して、*Panorama* バーチャル アプライアンスでプロビジョニングされないようにします。
2. 目的の操作モードの要件に応じて**CPU**を設定します。
3. **Forward**（転送）をクリックします。



STEP 4 | Panorama バーチャル アプライアンスに名前を付け、設定のカスタマイズを有効にして、管理インターフェイス ブリッジを選択します。

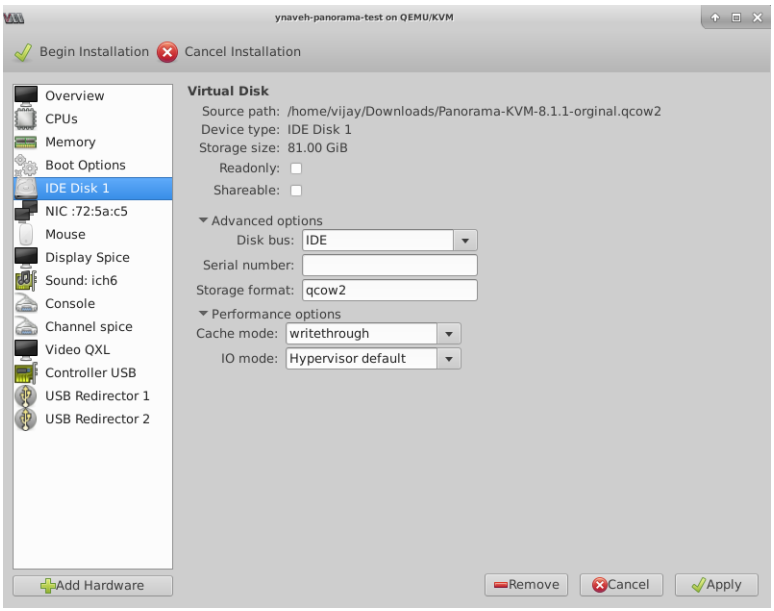
1. Panorama バーチャル アプライアンスの分かりやすい **Name (名前)** を入力します。
2. **Customize configuration before install**（インストール前に構成をカスタマイズ）を行います。
3. **Network selection**（ネットワークの選択）—管理インターフェイス用のブリッジを選択し、デフォルトの設定をそのまま受け入れます。
4. **Finish**（完了）をクリックします。

© 2019 Palo Alto Networks, Inc.



STEP 5 | 仮想システム ディスク設定を設定します。

1. **IDE Disk 1**（**IDE** ディスク **1**）に選択し、**Advanced options**（詳細オプション）に移動して、以下を選択します。
   - **Disk Bus**（ディスク バス）—設定に応じて **VirtIO** または **IDE**。
   - **Storage format**（ストレージ形式）—**qcow2**
2. **Performance options**（パフォーマンス オプション）に移動して、**Cache mode**（キャッシュ モード）を **writethrough** に設定します。この設定により、インストール所要時間が短縮され、Panorama バーチャル アプライアンスの実行速度が向上します。
3. **Apply**（適用）をクリックします。

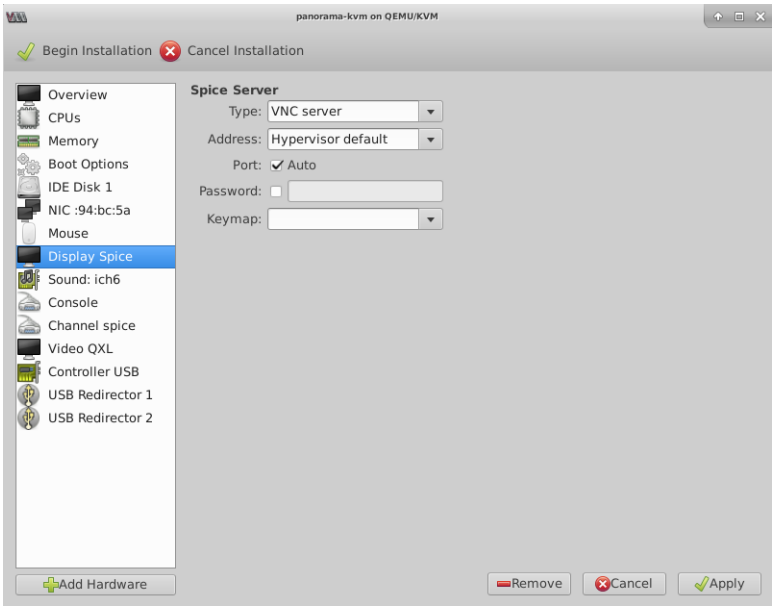


STEP 6 | 仮想マシン コンソール ディスプレイを設定して、 VNC サーバーを仮想マシンとの対話に使用します。

1. **Display Space**（ディスプレイ領域）を選択します。

   仮想マシンはすでに *VNC* サーバーを使用して表示されているため、*Display VNC*（*VNC* を表示する）がハードウェア一覧に載っている場合は、次のステップを設定します。
2. **Type**（タイプ） ドロップダウン リストで、**VNC server**（**VNC** サーバー） を選択します。
3. **Apply**（適用）をクリックします。

© 2019 Palo Alto Networks, Inc.



STEP 7 | （Panorama とログ コレクタ モード）ログ収集用に追加のストレージを追加します。必要に応じてこのステップを繰り返し、仮想ログギング ディスクを追加します。

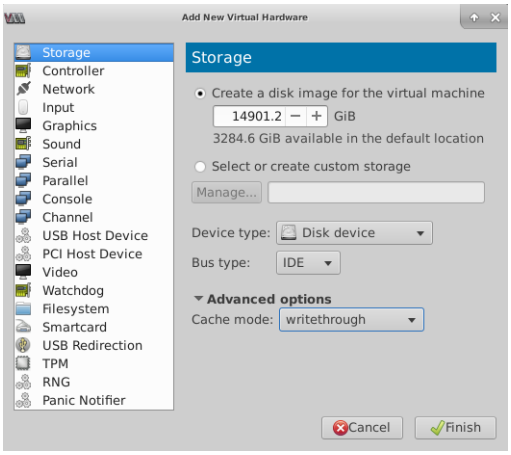
Panorama モードで Panorama バーチャル アプライアンスを使用する場合、または専用ログ コレクタとして使用する場合は、最初のデプロイメント時に仮想ログギング ディスクを追加します。デフォルトでは、Panorama モードのリソース要件を満たし、少なくとも 1 つの仮想ログギング ディスクを追加した場合、Panorama バーチャル アプライアンスは初期デプロイメント用の Panorama モードになります。それ以外の場合、Panorama バーチャル アプライアンスはデフォルトで管理専用モードになります。デバイスと専用ログ コレクタを管理し、ローカルにログを収集しない場合は、Panorama バーチャル アプライアンスを管理専用モードに変更します。

KVN の Panorama バーチャル アプライアンスは 2TB ログギング ディスクのみをサポートし、合計で最大 24TB のログ ストレージをサポートします。2TB より小さいログギング ディスク、または 2TB ログギングディスク要件で割り切れないサイズのログギング ディスクを追加することはできません。Panorama バーチャル アプライアンスは、2TB を超えるディスクを 2TB のパーティションに分割します。

1. **Add Hardware**(ハードウェアの追加)を行います。
2. 新しい **Storage**（ストレージ）ディスクを設定します：
   1. **Create a disk image for a virtual machine**（仮想マシンのディスクイメージを作成）し、仮想ディスク ストレージ容量を 14901.2 GiB（2TB 相当）に設定します。

      Virtual Machine Manager は、実行しているバージョンに応じて *GiB*（ギビバイト）を使用してメモリを割り当てることができます。*GiB* が使用される場合、仮想ログギング ディスクのプロビジョニングや *Panorama* バーチャル アプライアンスのメンテナンスモードへの移行を避けるために、必要なストレージ容量を正しく変換してください。
   2. **Device Type**（デバイス タイプ）を **Disk**（ディスク）デバイスに設定します。
   3. 設定に従い、**Bus Type**（バス タイプ）を、**VirtIO** または **IDE** に設定します。
   4. **Advanced options**（詳細オプション）に移動して、**Cache mode**（キャッシュ モード）を **writethrough** に設定します。
3. **Finish**（完了）をクリックします。

© 2019 Palo Alto Networks, Inc.



STEP 8 | **Begin Installation**（インストールの開始）（ Begin Installation ）を行います。Panorama バーチャル アプライアンスは起動するまでに約 10 分かかります。

STEP 9 | 管理インターフェイスへのネットワーク アクセス設定を行います。

1. コンソールとの接続を開きます。
2. デフォルトのユーザー名とパスワード（admin/admin）を使用してファイアウォールにログインする必要があります。
3. 以下のコマンドを入力して設定モードに切り替えます。

```
admin> configure
```

4. 以下のコマンドを使用して、管理インターフェイスを設定し、アクセスを有効にします。

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

<Panorama-IP> は管理インターフェイスに割り当てる IP アドレス、*<netmask>* はサブネット マスク、*<gateway-IP>* はネットワーク ゲートウェイの IP アドレス、*<DNS-IP>* は DNS サーバーの IP アドレスです。

```
admin# commit
```

STEP 10 | Panorama バーチャル アプライアンスのデバイス管理ライセンスとサポート ライセンスを有効にします。

- Panorama バーチャル アプライアンスがインターネットに接続している時のファイアウォール管理ライセンスのアクティベーション/取得
- Panorama バーチャル アプライアンスがインターネットに接続していない時のファイアウォール管理ライセンスのアクティベーション/取得
- Panorama サポート ライセンスのアクティベーション

STEP 11 | デプロイメントのニーズに合わせて Panorama バーチャル アプライアンスの設定を完了します。

- （管理専用モード）管理専用モードの Panorama バーチャル アプライアンスのセットアップ.

© 2019 Palo Alto Networks, Inc.

- （ログ コレクタ モード）Panorama モードからログ コレクタ モードに切り替えを行うには、ステップ 6 を開始してください。

  Panorama 管理サーバーに管理コレクタとしてログ コレクタを追加すると、専用ログコレクタのパブリック *IP* アドレスを入力します。*IP address*（*IP* アドレス）、*Netmask*（ネットマスク）、または *Gateway*（ゲートウェイ）を指定することはできません。
- (Panorama および管理専用モード) 管理対象コレクタの設定 して、専用ログ コレクタを Panorama バーチャル アプライアンスに追加するようにします。管理専用モードはローカル ログ収集をサポートしておらず、管理対象デバイス ログを保存する専用ログ コレクタが必要です。

Hyper-V で Panorama をインストール

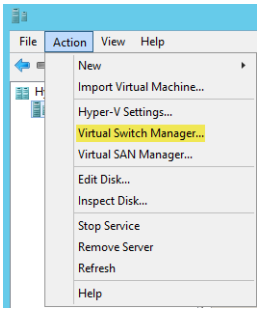
KVM に Panorama™ と 専用ログ コレクタをデプロイできるようになりました。GCP にデプロイされた Panorama はライセンス持ち込み（BYOL）であり、すべてのデプロイ モード（Panorama、ログ コレクタ、および管理専用）をサポートし、M-Series ハードウェア アプライアンスと同じプロセスと機能を共有します。Panorama モードの詳細は、「Panorama モデル」を参照してください。Panorama バーチャル アプライアンスと Hyper-V の仮想専用ログ コレクタは、PAN-OS 8.1.3 以降のリリースでのみ使用できます。

STEP 1 | VHDX ファイルをダウンロードします。

1. Palo Alto Networks サポートポータルにログインします。
2. **Updates (アップデート)** > **Software Updates (ソフトウェア アップデート)**を選択し、**Panorama Base Images (Panorama** ベースイメージ)でフィルタリングして VHDX ファイルをダウンロードします。

STEP 2 | 必要な vSwitch をすべてセットアップします。詳細については、仮想スイッチの種類を参照してください。

1. Hyper-V Manager でホストを選択し、**Action**（アクション）> **Virtual Switch Manager**（仮想スイッチ マネージャー）の順に選択して仮想スイッチ マネージャーのウィンドウを開きます。

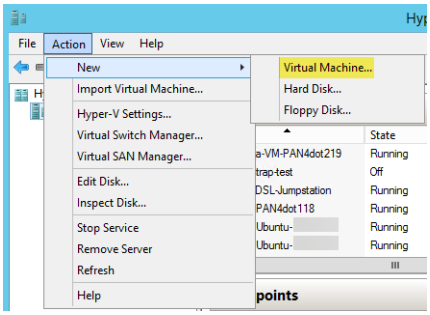


2. **Create virtual switch**（仮想スイッチの作成）で vSwitch のタイプを選択し、**Create Virtual Switch**（仮想スイッチの作成）をクリックして作成します。

STEP 3 | Panorama バーチャル アプライアンスのインストール

1. Hyper-V Manager でホストを選択し、**Action**（アクション）> **New**（新規）> **Virtual Machine**（仮想マシン）を選択します。新規仮想マシン ウィザードで次の設定を行います。

© 2019 Palo Alto Networks, Inc.



1. Panorama バーチャル アプライアンスの **Name**（名前）および**Location**（ロケーション）を選択します。Panorama バーチャル アプライアンスは指定されたロケーションに VHDX ファイルを保存します。
2. **Generation 1**（第一世代）を選択します。これがデフォルトのオプションであり、唯一サポートされているバージョンです。
3. **Startup Memory (起動メモリ)**については、目的のシステムモードに応じてメモリを割り当てます。各モードのメモリ要件については、Panorama バーチャル アプライアンスのセットアップ前提条件を参照してください。

   動的メモリは有効化しないでください。*Panorama* バーチャル アプライアンスには静的なメモリ割り当てが必要です。
4. **Networking**（ネットワーキング）を構成します。ファイアウォールの管理インターフェイスに接続する外部 vSwitch を選択します。
5. **Virtual Hard Disk**（仮想ハードディスク）に接続するには、**Use an existing virtual hard disk**（既存の仮想ハードディスクを使用）を選択し、ダウンロード済みの VHDX ファイルを参照します。
6. サマリーを確認し、**Finish**（完了）をクリックします。

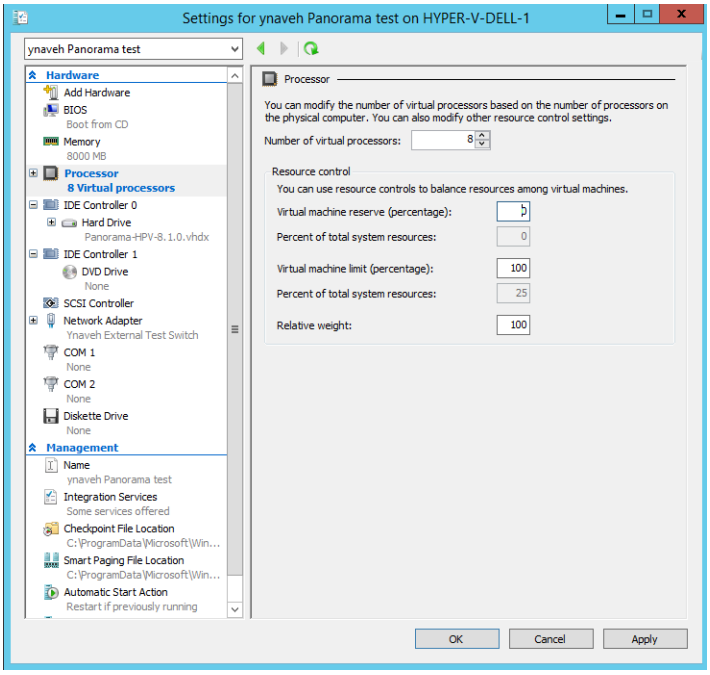
STEP 4 | Panorama バーチャル アプライアンスの CPU コアを割り当てます。

最低リソース要件については、Panorama バーチャル アプライアンスのセットアップ前提条件を確認してください。

Panorama バーチャル アプライアンスを専用ログ コレクタとして使用する場合は、必ず初回のデプロイ時に必要なリソースと共にアプライアンスを構成するようにしてください。*Panorama* バーチャル アプライアンスは、仮想マシンのデプロイ後でサイズを変更するとログ コレクタ モードのままにならず、ログ データが失われます。

1. **Hardware (ハードウェア)**のリストで**Processor (プロセッサ)**を選択します。
2. 現在割り当てられている**Number of virtual processors (仮想プロセッサの数)**を編集します。

© 2019 Palo Alto Networks, Inc.



STEP 5 | ファイアウォールのデータプレーン インターフェイス用ネットワーク アダプタに少なくとも 1 つ接続します。このステップを繰り返し、Panorama バーチャル アプライアンス上で追加のネットワークインターフェイスを作成します。

1. **Settings**（設定）> **Hardware**（ハードウェア）> **Add Hardware**（ハードウェア追加）を選択し、ネットワーク アダプタの **Hardware type**（ハードウェア タイプ）を選択します。

   レガシー ネットワーク アダプタおよび *SR-IOV* はサポートされていません。選択した場合、*VM-Series* ファイアウォールがメンテナンス モードで起動します。

2. **OK** をクリックします。

STEP 6 | （Panorama とログ コレクタ モード）ログ収集用に追加のストレージを追加します。必要に応じてこのステップを繰り返し、仮想ログ ディスクを追加します。Panorama バーチャル アプライアンスを Management Only（管理専用）モードでデプロイする場合、ステップ 6に進みます。

Panorama モードで Panorama バーチャル アプライアンスを使用する場合、または専用ログ コレクタとして使用する場合は、最初のデプロイメント時に仮想ログ ディスクを追加します。デフォルトでは、Panorama モードのリソース要件を満たし、少なくとも 1 つの仮想ログ ディスクを追加した場合、Panorama バーチャル アプライアンスは初期デプロイメント用の Panorama モードになります。それ以外の場合、Panorama バーチャル アプライアンスはデフォルトで管理専用モードになります。デバイスと専用ログ コレクタを管理し、ローカルにログを収集しない場合は、Panorama バーチャル アプライアンスを管理専用モードに変更します。

Hyper-V の Panorama バーチャル アプライアンスは 2TB ログ ディスクのみをサポートし、合計で最大 24TB のログ ストレージをサポートします。2TB より小さいログ ディスク、または 2TB ログディスク要件で割り切れないサイズのログ ディスクを追加することはできません。Panorama バーチャル アプライアンスは、2TB を超えるディスクを 2TB のパーティションに分割します。

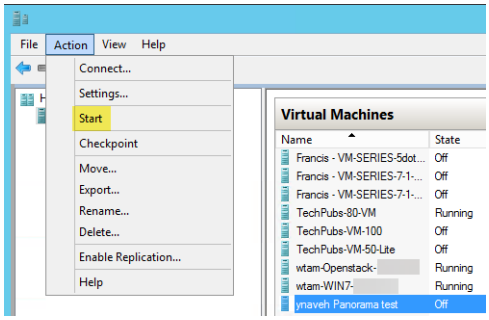
1. Hyper-V Manager でホストを選択し、**Action**（アクション）> **New**（新規）> **Hard Disk** (ハードディスク)の順に選択します。
2. Before You Begin (開始する前に) のプロンプトが表示されたら、**Next** (次へ)をクリックして仮想ログ ディスクの追加を開始します。

© 2019 Palo Alto Networks, Inc.

3. Disk Format (ディスク フォーマット) は**VHDX**を選択します。**Next** (次へ)をクリックして続行します。
4. 要件に応じて、Disk Type (ディスク タイプ) は**Fixed Size** (固定サイズ)あるいは**Dynamically Expanding** (動的に拡張)を選択します。**Next** (次へ)をクリックして続行します。
5. 仮想ロギング ディスク ファイルの**Name** (名前)および**Location** (場所)を指定します。**Next** (次へ)をクリックして続行します。
6. **Create a new virtual hard disk** (新しい仮想ハードディスクを作成)を選択してディスク容量を入力し、ディスクを構成します。**Next** (次へ)をクリックして続行します。
7. Summary (サマリー) を確認し、仮想ハード ロギング ディスクの追加を**Finish** (完了)させます。

STEP 7 | Panorama バーチャル アプライアンスをパワーオンします。

1. **Virtual Machines** (仮想マシン)のリストから Panorama バーチャル アプライアンスのインスタンスを選択します。
2. **Action** (操作) > **Start** (起動)を選択して、バーチャル アプライアンスの電源を入れます。



STEP 8 | 管理インターフェイスの IP アドレスを設定します。

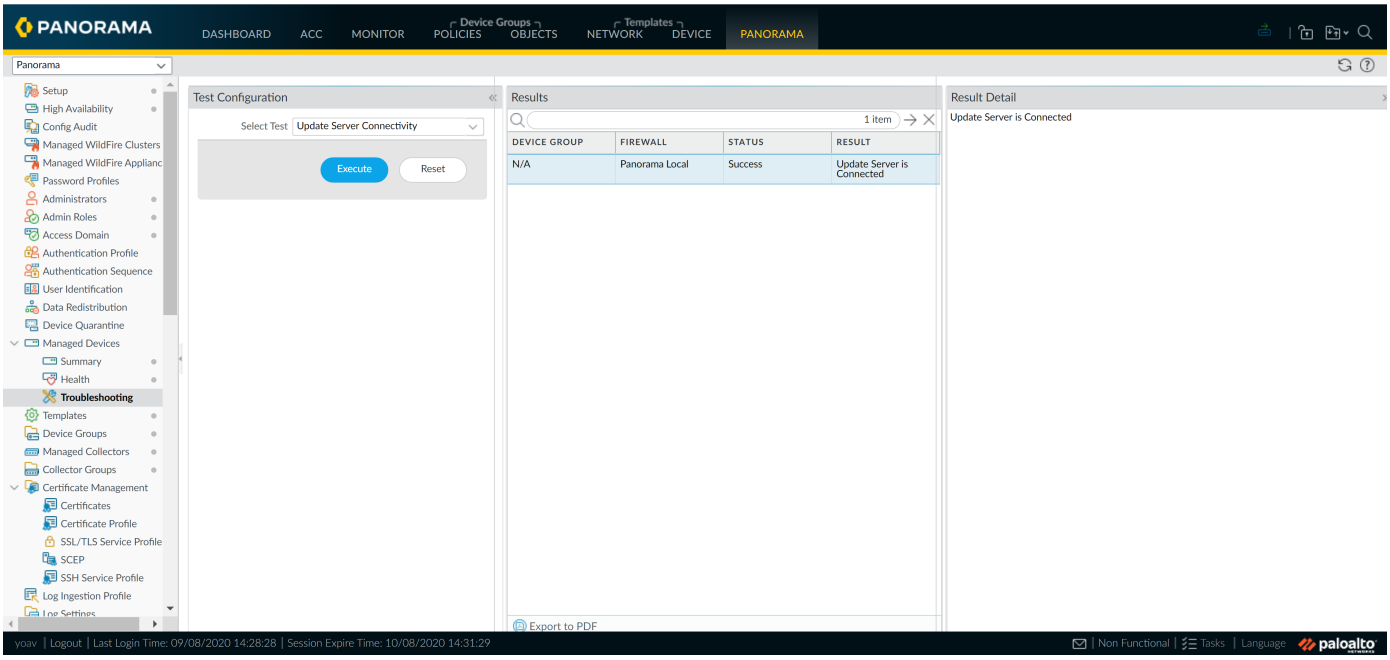
仮想スイッチ ネットワークで DHCP サービスが有効な場合、このステップをスキップできます。

1. **Virtual Machines** (仮想マシン)のリストで Panorama バーチャル アプライアンスを選択します。
2. **Actions** (操作) > **Connect** (接続)を選択し、ログイン用のユーザー名およびパスワードを入力します（デフォルトはどちらも admin）。
3. 次のコマンド（*<Panorama-IP>* は Panorama 管理インターフェイスに割り当てる IP アドレス、*<netmask>* はサブネット マスク、*<gateway-IP>* はネットワーク ゲートウェイの IP アドレス、*<DNS-IP>* は DNS サーバーの IP アドレス）を入力します。

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

4. ネットワーク リソースへの接続のトラブルシューティング次の例のようにファイアウォールの管理に必要な外部サービス (デフォルトゲートウェイ、DNS サーバー、Palo Alto Networks の更新サーバーなど) へのネットワーク アクセスを検証します。

© 2019 Palo Alto Networks, Inc.



STEP 9 | Panorama バーチャル アプライアンスのデバイス管理ライセンスとサポート ライセンスを有効にします。

- Panorama バーチャル アプライアンスがインターネットに接続している時のファイアウォール管理ライセンスのアクティベーション/取得
- Panorama バーチャル アプライアンスがインターネットに接続していない時のファイアウォール管理ライセンスのアクティベーション/取得
- Panorama サポート ライセンスのアクティベーション

STEP 10 | デプロイメントのニーズに合わせて Panorama バーチャル アプライアンスの設定を完了します。

- （管理専用モード）管理専用モードの Panorama バーチャル アプライアンスのセットアップ.
- （ログ コレクタ モード）Panorama モードからログ コレクタ モードに切り替えを行うには、ステップ 6 を開始してください。

  Panorama 管理サーバーに管理コレクタとしてログ コレクタを追加すると、専用ログコレクタのパブリック *IP* アドレスを入力します。*IP address*（*IP* アドレス）、*Netmask*（ネットマスク）、または *Gateway*（ゲートウェイ）を指定することはできません。

- (Panorama および管理専用モード) 管理対象コレクタの設定 して、専用ログ コレクタを Panorama バーチャル アプライアンスに追加するようにします。管理専用モードはローカル ログ収集をサポートしておらず、管理対象デバイス ログを保存する専用ログ コレクタが必要です。

Panorama バーチャル アプライアンスの初期設定の実行

Panorama モデルに基づいて、AWS、Azure、または GCP Web インターフェイス、KVM Virtual Machine Manager、Hyper-V Manager、VMware vSphere Client、またはvCloud Air Web コンソールを使用して Panorama バーチャル アプライアンスへのネットワーク アクセスをセットアップします。デフォルトでは、Panorama バーチャル アプライアンスは Panorama モードでデプロイされます。統合されたレポート作成を行うには、すべての管理対象のファイアウォールおよびログコレクタと Panorama のタイム ゾーンに対して同じGMT（Greenwich Mean Time）またはUTC（Coordinated Universal Time）を使用することを考慮してください。

© 2019 Palo Alto Networks, Inc.

STEP 1 | ネットワーク管理者から必要な情報を入手します。

管理（MGT）インターフェイスの次の情報を集めます。

- 管理（MGT）インターフェイスの IP アドレス
- ネットマスク
- デフォルト ゲートウェイ
- DNS サーバーの IP アドレス

MGT インターフェイスの設定を完了するには、*IP* アドレス、ネットマスク（*IPv4* の場合）、プレフィックス長（*IPv6* の場合）のいずれかと、デフォルト ゲートウェイを指定する必要があります。設定が省略された場合（デフォルト ゲートウェイなど）、以降の設定変更ではコンソール ポート経由でしか *Panorama* にアクセスできなくなります。必ず、完全な *MGT* インターフェイス設定をコミットすることをお薦めします。

STEP 2 | Panorama バーチャル アプライアンスのコンソールにアクセスします。

1. コンソールにアクセスします。

   ESXiサーバー上：

   1. VMware vSphereクライアントを立ち上げます。
   2. Panorama バーチャル アプライアンスの **Console**（コンソール）タブを選択し、Enterを押してログイン画面を表示します。

   vCloud Air上：

   1. vCloud AirのWebコンソールにアクセスし、ご自身の **Virtual Private Cloud OnDemand**（仮想プライベート クラウド オンデマンド）領域を選択します。
   2. **Virtual Machines**（仮想マシン）タブを選択し、Panorama仮想マシンを右クリックして **Open In Console**（コンソールで開く）を選択します。
2. ログイン用のユーザー名およびパスワードを入力します（デフォルトはどちらも admin）。

   AWS、Azure、GCP、KVM、および Hyper-V の場合：

   - Panorama CLI へのログインを行います。

STEP 3 | デフォルトの管理者用パスワードを変更します。

PAN-OS 9.0.4 で開始するときは、事前定義済みのデフォルトの管理者パスワード（*admin / admin*）は、デバイスへの初回のログイン時に変更しなければなりません。新しいパスワードは *8* 文字以上で、*1* 文字以上の小文字と *1* 文字以上の大文字、および数字または特殊文字 *1* 字を含める必要があります。

パスワードの強度を高めるために、必ずパスワード強度のベスト プラクティスに従い、パスワードの複雑性の設定を確認してください。

管理インターフェイスを確実に保護するために、パスワード複雑性設定を設定します（*Panorama* > *Setup*（セットアップ）> *Management*（管理））。

1. Webインターフェイスのフッター領域の左側にある **admin** リンクをクリックします。
2. **Old Password**（現在のパスワード）と**New Password**（新しいパスワード）を入力し、新しいパスワードを安全な場所に記録します。
3. **OK** をクリックします。

STEP 4 | MGT インターフェイスのネットワーク アクセス設定を行います。

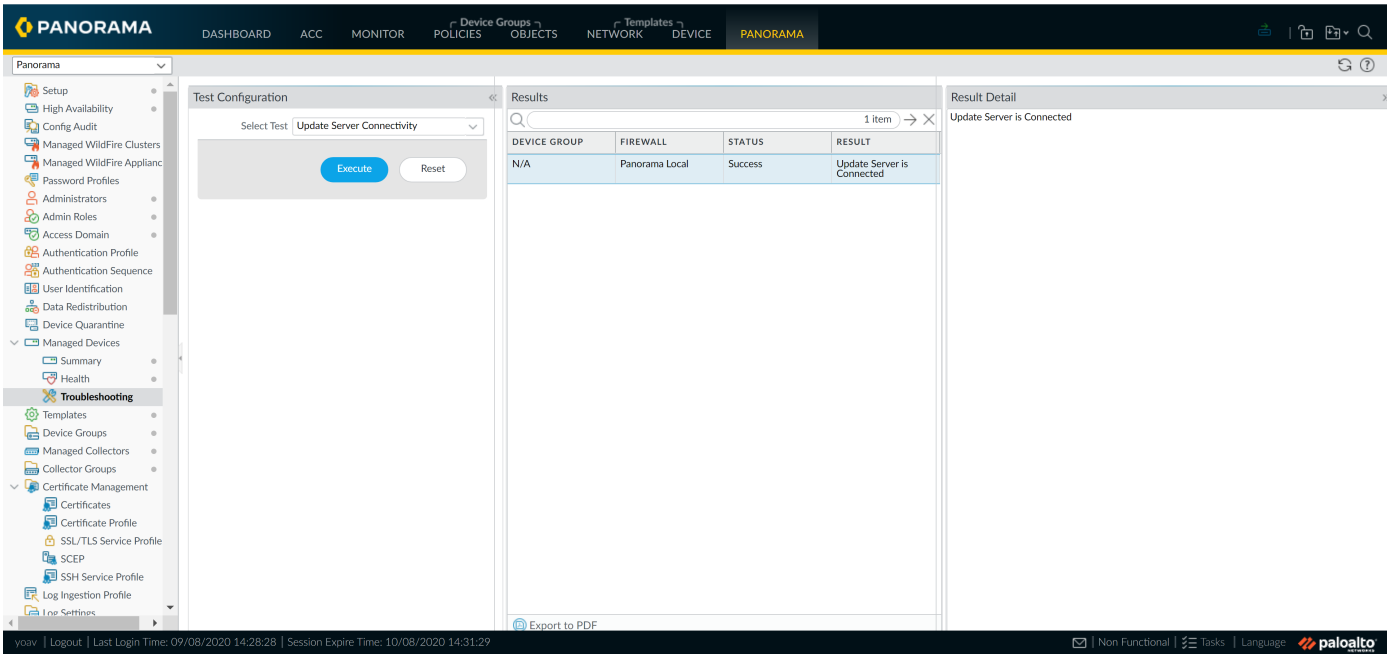
© 2019 Palo Alto Networks, Inc.

Panoramaは、管理トラフィック、高可用性の同期、ログ収集、コレクタ グループ内での通信のためにMGTインターフェイスを使用します。

1. 次のコマンド（*<Panorama-IP>* は Panorama 管理インターフェイスに割り当てる IP アドレス、*<netmask>* はサブネット マスク、*<gateway-IP>* はネットワーク ゲートウェイの IP アドレス、*<DNS-IP>* は DNS サーバーの IP アドレス）を入力します。

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

2. ネットワーク リソースへの接続のトラブルシューティング次の例のようにファイアウォールの管理に必要な外部サービス (デフォルトゲートウェイ、DNS サーバー、Palo Alto Networks の更新サーバーなど) へのネットワーク アクセスを検証します。



STEP 5 | 一般設定の設定を行います。

1. Web ブラウザから安全な接続（HTTPS）を使用し、管理インターフェイスに割り当てられた IP アドレスとパスワードを使用してPanorama Webインターフェイスにログインします（https://<IP address>）。
2. **[Panorama]** > **[セットアップ]** > **[管理]** の順に選択し、[一般設定] を編集します。
3. サーバーの **Hostname**（ホスト名）を入力し、ネットワークの **Domain**（ドメイン）名を入力します。ドメイン名は単なるラベルであり、ドメインに参加するために Panorama で使用されることはありません。
4. Panorama と管理対象ファイアウォールのクロックを、同じタイム ゾーン（**GMT** または **UTC** など）を使用するように合わせます。Cortex Data Lake を使用する予定の場合、NTP を設定して、Panorama が Cortex Data Lake との同期を維持できるようにします。

   Panoramaがログを受信し、管理対象のファイアウォールがログを作成する際、タイムスタンプが記録されます。Panorama とファイアウォールの両方でタイム ゾーンを合わせることにより、タイムスタンプが確実に同期され、Panorama でのログのクエリとレポートの生成プロセスで調和が保たれるようにします。

© 2019 Palo Alto Networks, Inc.

5. **Latitude**（経度）と **Longitude**（緯度）を入力し、Panorama 管理サーバーが世界地図上の正確な場所に配置されるようにします。
6. 注文処理メールで受け取った **Serial Number**（シリアル番号）を入力します。
7. **OK** をクリックして変更内容を保存します。

STEP 6 | （任意）管理インターフェイス設定を変更します。

1. **Panorama** > **Setup**（セットアップ）> **Interfaces**（インターフェイス）の順に選択し、**Management**（管理）をクリックします。
2. ファイアウォールがプライベート IP アドレス（NAT）に変換されるパブリック IP アドレスを使って Panorama 管理サーバーに接続する場合、**Public IP Address (パブリック IP アドレス)**フィールドにパブリック IP を、**IP Address (IP アドレス)**フィールドにプライベート IP を入力し、両方のアドレスをファイアウォールにプッシュします。
3. どのネットワーク接続サービスをインターフェイスで許可するかを選択します（**SSH** アクセスなど）。

   Telnet または *HTTP* は選択しないでください。これらのサービスはプレーンテキストを使用するため、他のサービスに比べて安全性に劣ります。
4. **OK** をクリックして、インターフェイスに対する変更を保存します。

STEP 7 | 設定の変更をコミットします。

Commit（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

STEP 8 | 次のステップ...

1. 必要に応じて、Panorama バーチャル アプライアンスでのログ ストレージ容量の拡張を行います。
2. （推奨）管理（MGT）インターフェイス全体の HTTPS トラフィックを保護するために、Panorama が使用するデフォルトの証明書を交換します。
3. Panorama サポート ライセンスのアクティベーションを行います。
4. Panorama バーチャル アプライアンスがインターネットに接続している時のファイアウォール管理ライセンスのアクティベーション/取得。
5. Panorama のコンテンツ更新とソフトウェア更新のインストールを行います。
6. Panorama への管理アクセスのセットアップ

ログ コレクタを使用する Panorama バーチャル アプライアンスのセットアップ

ログ収集専用の仮想アプライアンスが必要な場合は、ESXi、AWS、AWS GovCloud、Azure、Google Cloud Platform、KVM、Hyper-V のいずれかの Panorama バーチャル アプライアンスをログ コレクタ モードで設定します。そのためにはまず、Panorama モードで仮想アプライアンスの初期設定を行います。これには、ライセンシング、ソフトウェアおよびコンテンツ更新のインストール、管理（MGT）インターフェイスの設定といった作業が伴います。その後で Panorama バーチャル アプライアンスをログ コレクタ モードに切り替え、ログ コレクタの設定を完了させます。さらに、ログ収集やコレクタ グループ通信に MGT インターフェイスの代わりに専用の M-Series アプライアンス インターフェイス（推奨）を使用する場合、まずは Panorama 管理サーバー用のインターフェイスを設定し、次にそれに対してログ コレクタ用の設定を行い、さらに Panorama のコミットを実行した後でコレクタ グループのコミットを行う必要があります。

新しい バーチャル アプライアンスをログ コレクタとしてセットアップする、あるいはすでに Panorama 管理サーバーとしてデプロイされている既存の バーチャル アプライアンスを切り替える場合は、以下の作業を行います。

© 2019 Palo Alto Networks, Inc.



バーチャル アプライアンスを *Panorama* モードからログ コレクタ モードに切り替えると、アプライアンスが再起動し、ローカル ログ コレクタが削除され、管理アクセス設定を除くすべての設定と既存のログ データが削除されます。また、モードを変えることによりライセンス、ソフトウェア更新、コンテンツ更新が削除されることはありません。

STEP 1 | まだ作業を行っていない場合は、ログ コレクタを管理する Panorama バーチャル アプライアンス管理サーバーをセットアップします。

以下のいずれかの作業を行います。

- Panorama バーチャル アプライアンスのセットアップ
- M-Series アプライアンスのセットアップ

STEP 2 | Panorama 管理サーバーの管理 IP アドレスを控えておきます。

Panorama を高可用性（HA）設定でデプロイしている場合、それぞれの HA ピアの IP アドレスが必要になります。

1. Panorama 管理サーバーの Web インターフェイスにログインします。
2. **Panorama** > **Setup**（セットアップ）> **Management**（管理）を選択し、管理インターフェイスの設定を確認して単独（非 HA）あるいはアクティブ（HA）Panorama の **IP Address**（**IP** アドレス）を控えておきます。
3. HA デプロイメントの場合は、**Panorama** > **High Availability**（高可用性）の順に選択して Setup（セットアップ）セクションを確認し、パッシブ Panorama の **Peer HA IP Address**（ピア **HA IP** アドレス）を控えておきます。

STEP 3 | 専用のログ コレクタとして機能する Panorama バーチャル アプライアンスをセットアップします。

すでにこのアプライアンスを Panorama 管理サーバーとしてデプロイしている場合は、MGT インターフェイスがすでに設定されており、ライセンスおよび更新ファイルがすでにインストールされているため、このステップを飛ばして構いません。

ログ コレクタ モードの Panorama バーチャル アプライアンスには設定タスクを行うための Web インターフェイスが備わっておらず、CLI しかありません。そのため、Panorama バーチャル アプライアンスでモードを変更する前に、Panorama モードで Web インターフェイスを使用して次の作業を行います。

1. 次のいずれかのサポートされているハイパーバイザで Panorama バーチャル アプライアンスを設定します。
   - ESXi サーバーに Panorama をインストール
   - AWS で Panorama をインストールする。
   - AWS GovCloud で Panorama をインストール
   - Panorama で Azure をインストールする。
   - Panorama を Google Cloud Platform にインストールする。
   - Hyper-V で Panorama をインストール
2. Panorama バーチャル アプライアンスの初期設定の実行を行います。
3. Panorama の登録とライセンスのインストールを行います。
4. Panorama のコンテンツ更新とソフトウェア更新のインストールを行います。

STEP 4 | （ Azure 上の Pandora のみ ）管理者パスワードを変更します。

専用ログ コレクタは、ログ コレクタモードに変更するために admin 管理者ユーザーのみをサポートします。管理者パスワードを変更して、admin 管理者ユーザーを使用してログインできるようにします。

1. Panorama Web インターフェイスへのログイン。
2. **Panorama** > **Administrators**（管理者）の順に選択し、**admin** を選択します。

© 2019 Palo Alto Networks, Inc.

3. **Password**（パスワード）、**Confirm Password**（確認用パスワード）を入力し、**OK** をクリックします。
4. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

STEP 5 | （AWS と Azure 上の Panorama のみ）管理ユーザー以外のすべてのユーザーを削除します。

1. admin として Panorama Web インターフェイスへログインします。
2. **Panorama** > **Administrators** [管理者]
3. admin を除く既存の管理者を選択し、**Delete**（削除）します。
4. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

STEP 6 | Panorama CLI へのログインを行います。

STEP 7 | Panorama モードからログ コレクタ モードに切り替えます。

1. 次のコマンドを入力して、ログ コレクタ モードに切り替えます。

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

2. **Y**を入力して、モード変更を確定します。バーチャル アプライアンスが再起動します。再起動処理によってターミナル エミュレーション ソフトウェアのセッションが終了した場合は、バーチャル アプライアンスに再接続し、Panorama のログイン画面を表示します。

   CMS Login *(CMS*ログイン*)*画面が表示された場合は、ログコレクタが再起動をまだ完了させていないということです。入力を指示されたら、ユーザー名やパスワードは入力せずに *Enter* キーを押します。

3. CLI に再度ログインします。
4. ログ コレクタ モードへの切り替えが正しく完了したことを、次のコマンドで確認します。

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

モード変更が正しく完了した場合、出力は次のようになります。

```
system-mode: logger
```

STEP 8 | ログ コレクタおよび Panorama 管理サーバー間の接続を有効にします。

ログコレクタのCLIで次のコマンド（適宜、*<IPaddress1>*は単独（非HA）あるいはアクティブ（HA）PanoramaのMGTインターフェイスのもの、*<IPaddress2>*はパッシブ（HA）PanoramaのMGTインターフェイスのもの）を入力します。

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

STEP 9 | ログ コレクタのシリアル番号を控えておきます。

Panorama 管理サーバーでログ コレクタを管理対象のコレクタとして追加する際、このシリアル番号が必要になります。

1. ログ コレクタの CLI で以下のコマンドを入力し、シリアル番号を表示します。

© 2019 Palo Alto Networks, Inc.

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

2. シリアル番号を控えておきます。

STEP 10 | ログ コレクタを管理対象のコレクタとして Panorama 管理サーバーに追加します。

1. **Panorama** > **Managed Collectors**(Panorama > 管理対象コレクタ) の順に選択し、管理対象コレクタを**Add** (追加)します。
2. **General**（全般）設定で、ログ コレクタについて記録したシリアル番号（**Collector S/N**（コレクタ シリアル番号））を入力します。
3. **Panorama Server IP**（**Panorama** サーバー **IP**）フィールドに、単独（非 HA）あるいはアクティブ（HA）Panorama の IP アドレスまたは FQDN を入力します。HA デプロイメントの場合、**Panorama Server IP 2**（**Panorama** サーバー **IP 2**）フィールドに、パッシブ Panorama ピアの IP アドレスあるいは FQDN を入力します。

   これらの IP アドレスは、**Device Management and Device Log Collection**（デバイス管理およびデバイス ログ収集）サービスを有効にした Panorama インターフェイスを指定する必要があります。デフォルトでは、これらのサービスは MGT インターフェイスでのみ有効です。ただし、Panorama 管理サーバーである M-Series アプライアンスのセットアップを実行したときに他のインターフェイスでこれらのサービスを有効にしている場合もあります。
4. **Interfaces (インターフェイス)**を選択して、**Management**（管理）をクリックし、専用ログ コレクタの **Public IP address**（パブリック **IP** アドレス）を入力します。
5. **OK** を 2 回クリックして、ログ コレクタに対する変更を保存します。
6. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、Panorama 設定に対して、変更内容を **Commit**（コミット）します。
7. **Panorama** > **Managed Collectors**（管理対象コレクタ）で、追加したログ コレクタが表示されていることを確認します。Connected（接続済み）列には、ログ コレクタが Panorama に接続されていることを示すチェック マークが表示されます。更新された接続ステータスがページに表示されるまで、数分かかる場合があります。

   この時点では、*Configuration Status*（設定ステータス）列には *Out of Sync*（非同期）、*Run Time Status*（ランタイム ステータス）列には *disconnected*（未接続）が表示されます。コレクタ グループを設定すると、このステータスは *In Sync*（同期）および *connected*（接続済み）に変わります。

STEP 11 | ロギング用ディスクを有効にします。

1. **Panorama** > **Managed Collectors**(Panorama > 管理対象コレクタ) の順に選択し、ログ コレクタを編集します。
2. **Disks**（ディスク）を選択し、各ディスクを **Add**（追加）します。
3. **OK** をクリックして変更内容を保存します。
4. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、Panorama 設定に対して、変更内容を **Commit**（コミット）します。

STEP 12 | （推奨）Panorama 管理サーバーおよびログ コレクタが **Device Log Collection**（デバイス ログ収集）（ファイアウォールからのログの受信）および **Collector Group Communication**（コレクタ グループ通信）に使用する場合は、**Ethernet1**、**Ethernet2**、**Ethernet3**、**Ethernet4**、**Ethernet5** インターフェイスを設定します。

以前に Panorama 管理サーバーとしてログ コレクタをデプロイし、そのインターフェイスを設定している場合、ログ コレクタ モードに切り替えたときに、管理アクセス設定を除くすべての設定が削除されているため、設定し直す必要があります。

© 2019 Palo Alto Networks, Inc.

1. まだ設定していない場合は、Panorama 管理サーバーで各インターフェイスを設定します（MGT インターフェイスを除く）。
   1. **Panorama** > **Setup**（セットアップ）> **Interfaces**（インターフェイス）を選択し、インターフェイス名をクリックします。
   2. *<interface-name>* を選択してインターフェイスを有効化します。
   3. ネットワークの IP プロトコルに合わせて、以下のいずれか、あるいは両方のフィールドを入力します。
      - ESXi の場合
        - IPv4 — **Public IP address**（パブリック **IP** アドレス）、 **IP address**（**IP** アドレス）、**Netmask**（ネットマスク）、および **Default Gateway**（デフォルト ゲートウェイ）

          IPv6 — **IPv6 Address/Prefix Length**（**IPv6** アドレス/プレフィックス長）および **Default IPv6 Gateway**（デフォルト **IPv6** ゲートウェイ）
      - AWS、Azure、Google™ Cloud Platform の場合
        - パブリック**IP**アドレス
   4. インターフェイスでサポートされるデバイス管理サービスを選択します。

      Device Management and Device Log Collection（デバイス管理およびデバイス ログ収集）— 1 つ以上のインターフェイスを割り当てることができます。

      Collector Group Communication（コレクタ グループ通信）— インターフェイスを 1 つのみ割り当てることができます。

      Device Deployment（デバイスのデプロイ）（ソフトウェア更新とコンテンツ更新）— インターフェイスを 1 つのみ割り当てることができます。
   5. **OK** をクリックして変更内容を保存します。
2. ログ コレクタで各インターフェイスを設定します（MGT インターフェイスを除く）。
   1. **Panorama** > **Managed Collectors**(Panorama > 管理対象コレクタ) の順に選択し、ログ コレクタを編集します。
   2. **Interfaces**（インターフェイス）を選択してインターフェイスの名前をクリックします。
   3. *<interface-name>* を選択してインターフェイスを有効化します。
   4. ネットワークの IP プロトコルに合わせて、以下のいずれか、あるいは両方のフィールドを入力します。
      - ESXi の場合
        - IPv4 — **Public IP address**（パブリック **IP** アドレス）、 **IP address**（**IP** アドレス）、**Netmask**（ネットマスク）、および **Default Gateway**（デフォルト ゲートウェイ）

          IPv6 — **IPv6 Address/Prefix Length**（**IPv6** アドレス/プレフィックス長）および **Default IPv6 Gateway**（デフォルト **IPv6** ゲートウェイ）
      - AWS および Azure 場合
        - パブリック**IP**アドレス
   5. インターフェイスでサポートされるデバイス管理サービスを選択します。

      Device Log Collection（デバイス ログ収集）— インターフェイスを 1 つ以上割り当てることができます。

      Collector Group Communication（コレクタ グループ通信）— インターフェイスを 1 つのみ割り当てることができます。
   6. **OK** をクリックして、インターフェイスに対する変更を保存します。
3. **OK** をクリックして、ログ コレクタに対する変更を保存します。
4. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、Panorama 設定に対して、変更内容を **Commit**（コミット）します。

© 2019 Palo Alto Networks, Inc.

STEP 13 | （任意）デプロイメントで Panorama と管理対象デバイス間の認証にカスタム証明書を使用している場合、カスタム クライアント デバイス証明書をデプロイします。詳細は、「カスタム証明書を使用する認証のセットアップ」を参照してください。

1. **Panorama** > **Certificate Management**（証明書の管理）> **Certificate Profile**（証明書プロファイル）の順に選択し、ドロップダウンから証明書プロファイルを選択するか、**New Certificate Profile**（新しい証明書プロファイル）をクリックして作成します。
2. ログ コレクタの **Panorama** > **Managed Collectors**（管理対象コレクタ）> **Add**（追加）> **Communication**（通信）を選択します。
3. **Secure Client Communication**（保護されたクライアント通信）チェック ボックスをオンにします。
4. Type（タイプ）ドロップダウンからデバイス証明書のタイプを選択します。
   - ローカル デバイス証明書を使用している場合、それぞれのドロップダウン リストから **Certificate**（証明書）および **Certificate Profile**（証明書プロファイル）を選択します。
   - デバイス証明書として SCEP を使用している場合、それぞれのドロップダウンから **SCEP Profile**（**SCEP** プロファイル）および **Certificate Profile**（証明書プロファイル）を選択します。
5. **OK** をクリックします。

STEP 14 | （任意）ログ コレクタで Secure Server Communication（保護されたサーバー通信）を設定します。詳細は、「カスタム証明書を使用する認証のセットアップ」を参照してください。

1. **[Panorama]** > **[管理対象コレクタ]** > **[追加]** > の順に選択します。**Communication**.
2. **Custom Certificate Only**（カスタム証明書のみ）チェック ボックスがオフになっていることを確認します。これにより、カスタム証明書への移行中もすべてのデバイスの管理を続行できます。

   Custom Certificate Only（カスタム証明書のみ）チェック ボックスをオンにしていると、ログ コレクタは事前定義済みの証明書を使用したデバイスからのログを認証せず、受信することができません。
3. **SSL/TLS Service Profile**（**SSL/TLS** サービス プロファイル）ドロップダウンから SSL/TLS サービス プロファイルを選択します。この SSL/TLS サービス プロファイルは、ログ コレクタとログを送信するデバイス間のすべての SSL 接続に適用されます。
4. **Certificate Profile**（証明書プロファイル）ドロップダウンから証明書プロファイルを選択します。
5. **Authorize Client Based on Serial Number**（シリアル番号に基づいてクライアントを承認）を選択し、サーバーが管理対象デバイスのシリアル番号と照合してクライアントをチェックするようにします。クライアント証明書では、シリアル番号に基づいて認証するために CN として特殊なキーワード $UDID を設定する必要があります。
6. **Disconnect Wait Time (min)** (切断待機時間 (分)) に、Panorama が管理対象デバイスとの接続を切断して再開するまで待機する分数を入力します。このフィールドはデフォルトで空白であり、範囲は 0 ~ 44,640 分です。

   切断待機時間は、新しい設定をコミットするまでカウント ダウンを開始しません。
7. （任意）認証リストを設定します。
   1. Authorization List（承認リスト）で **Add**（追加）をクリックします。
   2. 識別子タイプとして **Subject**（サブジェクト）または **Subject Alt Name**（サブジェクト代替名）を選択します。
   3. 選択したタイプの識別子を入力します。
   4. **OK** をクリックします。
   5. **Check Authorization List**（承認リストのチェック）を選択して認証リストを適用します。
8. **OK** をクリックします。
9. **Commit**（コミット）> **Commit to Panorama**（**Panorama** にコミット）を選択します。

STEP 15 | コレクタ グループにログ コレクタを割り当てます。

© 2019 Palo Alto Networks, Inc.

1. コレクタ グループの設定ログ コレクタの設定を Panorama と同期し、Eth1、Eth2、Eth3、Eth4、および Eth5 インターフェイス（これらを設定している場合）がログ コレクタ上で稼働できる状態にするには、Panorama のコミットを行い、次にコレクタ グループのコミットを行う必要があります。

   単一のコレクタ グループでは、すべてのログ コレクタ、すべての *M-600* アプライアンス、すべての *M-500* アプライアンス、すべての *M-200* アプライアンス、すべての *Panorama* バーチャル アプライアンスは同じ *Panorama* モデルで動作する必要があります。

   推奨としては、複数のログ コレクタを *1* つのコレクタ グループに追加する場合、*Enable log redundancy across collectors*（コレクタ間のログ冗長性の有効化）します。このオプションでは、各ログ コレクタのロギング用ディスクの数が同じでなければなりません。
2. **Panorama** > **Managed Collectors** (Panorama > 管理対象コレクタ)を選択し、ログコレクタの構成がPanoramaと同期していることを確認します。

   Configuration Status（設定ステータス）列には In Sync（同期）、Run Time Status（ランタイム ステータス）列には connected（接続済み）が表示されている必要があります。
3. ログ コレクタの CLI にアクセスして次のコマンドを入力し、そのインターフェイスが稼働できる状態になっていることを確認します。

   ```
   > show interface all
   ```

   各インターフェイスが稼働できる状態である場合、`state` が `up` であると出力されます。
4. コレクタ グループにログ コレクタが複数ある場合は、ネットワーク リソースへの接続のトラブルシューティングしてそのログ コレクタが使用する各インターフェイスに対して Ping 接続性テストを実行し、ログ コレクタ同士が通信できることを確認します。`source` IP アドレスについては、いずれかのインターフェイスのログ コレクタを指定します。`host` IP address（ホスト IP アドレス）は、同じコレクタ グループに所属する別のログ コレクタの、対応するインターフェイスを指定します。

STEP 16 | 次のステップ...

ログ コレクタがファイアウォール ログを受信できるようにするには：

1. Panorama へのログ転送の設定
2. Panorama へのログ転送の確認

ローカル ログ コレクタを使用する Panorama バーチャル アプライアンスのセットアップ

Panorama 8.0 以前のリリースから Panorama 8.1（またはそれ以降）のリリースにアップグレードした後に Panorama バーチャル アプライアンスがレガシー モードになっている場合は、ローカル ログ コレクタを作成するために Panorama モードに切り替え、既存のログを失うことなく複数のログディスクを追加します。最大 24TBのログストレージを増設し、レポートの生成を高速化できます。

レガシーモードから *Panorama* モードに変更すると、レガシーモードは使用できなくなります。

Panorama 8.1 にアップグレードした後で、最初にバーチャル アプライアンスのシステム リソースを Panorama モードの最小必要量まで増加します。リソースを増加すると Panorama が再起動するため、この手順は保守期間中に実行してください。より大きなシステム ディスク（81GB）をインストールして、ログ ストレージ容量に基づいて CPU とメモリを増加し、仮想ロギング ディスクを追加する必要がありま

© 2019 Palo Alto Networks, Inc.

す。新しいロギング ディスクには、最低でも現在レガシー モードで使用しているアプライアンスと同じ容量が必要であり、2TB 未満であってはいけません。仮想ディスクを追加すると、既存のログをログ コレクタに追加し、ログ コレクタで新しいログを保存できるようになります。

Panorama が HA 設定でデプロイされている場合、最初にセカンダリ ピアで、次にプライマリ ピアで次のステップを実行します。

STEP 1 | バーチャル アプライアンスを Panorama モードで稼働する前に増加する必要があるシステム リソースを決定します。

すでに *Panorama* に十分なリソースがあると判断した場合でも、このステップで指定したコマンドは実行する必要があります。

1. Panorama CLI にアクセスします。
   1. Panorama MGT インターフェイス用に指定した IP アドレスに対して SSH セッションを開くには、PuTTY などの端末エミュレーション ソフトウェアを使用します。
   2. 指示に従って CLI にログインします。
2. 以下のコマンドを実行して、増加する必要があるリソースを確認します。

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

続行を促されたら、「**y**」と入力します。出力によって、増加する必要があるリソースが指定されます。以下に例を示します。

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

STEP 2 | CPU とメモリを増加し、システム ディスクをより大きいディスクに交換します。

1. VMware ESXi vSphere クライアントにアクセスし、**Virtual Machines**（仮想マシン）を選択して Panorama バーチャル アプライアンスを右クリックし、**Power**（電源）> **Power Off**（電源オフ）の順に選択します。
2. Panorama バーチャル アプライアンスを右クリックし、**Edit Settings**（設定変更）を選択します。
3. **Memory**（メモリ）を選択し、**Memory Size**（メモリ サイズ）に新しい値を入力します。
4. **CPUs** を選択し、CPU の数（**Number of virtual sockets**（仮想ソケット数）x **Number of cores per socket**（ソケット毎のコア数））を指定します。
5. 仮想ディスクを追加します。

   このディスクを使用して既存のシステム ディスクを交換します。

   1. **Hardware**（ハードウェア）設定でディスクを **Add**（追加）し、ハードウェア タイプとして **Hard Disk**（ハード ディスク）を選択し、**Next**（次へ）をクリックします。
   2. **Create a new virtual disk**（新しい仮想ディスクを作成）して、**Next**（次へ）をクリックします。
   3. **Disk Size**（ディスク サイズ）を正確に 81GB に設定し、**Thick Provision Lazy Zeroed**（シック プロビジョニング（**Lazy Zeroed**））ディスク フォーマットを選択します。
   4. 場所として **Specify a datastore or datastore structure**（データストアまたはデータストア構造を指定）を選択し、81GB 以上のデータストアを **Browse**（参照）して **OK** をクリックし、**Next**（次へ）をクリックします。

© 2019 Palo Alto Networks, Inc.

5. SCSI **Virtual Device Node**（仮想デバイス ノード）（デフォルトのセクションを使用可能）を選択して**Next**（次へ）をクリックします。

   SCSI 以外の形式を選択すると、*Panorama* は起動できなくなります。

6. 設定が正しいことを確認してから、**Finish**（完了）、**OK** の順にクリックします。

6. Panorama バーチャル アプライアンスを右クリックし、**Power**（電源）> **Power On**（電源オン）を選択します。Panorama が再起動するのを待ってから続行します。
7. Panorama CLI に戻って元のシステム ディスクから新しいシステム ディスクにデータをコピーします。

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

   続行を促されたら、「**y**」と入力します。

   コピーにはおよそ 20～25 分かかり、その間に Panorama は再起動します。コピーが完了したら、Panorama をシャットダウンするよう出力で指示されます。
8. vSphere クライアント コンソールに戻り、Panorama バーチャル アプライアンスを右クリックして **Power**（電源）> **Power Off**（電源オフ）の順に選択します。
9. Panorama バーチャル アプライアンスを右クリックし、**Edit Settings**（設定変更）を選択します。
10. 元のシステム ディスクを選択し、**Remove**（除去）をクリックして **Remove from virtual machine**（仮想マシンから除去）を選択し、**OK** をクリックします。
11. Panorama バーチャル アプライアンスを右クリックし、**Edit Settings**（設定変更）を選択します。
12. 新しいシステム ディスクを選択し、**Virtual Device Node**（仮想デバイス ノード）を **SCSI (0:0)** に設定し、**OK** をクリックします。
13. Panorama バーチャル アプライアンスを右クリックし、**Power**（電源）> **Power On**（電源オン）を選択します。続行する前に、新しいシステム ディスクで Panorama が再起動するのを待ちます（約 15 分）。

STEP 3 | 仮想ログ用ディスクを追加します。

これが、既存のログを移行するディスクになります。

1. VMware ESXi vSphere クライアントで Panorama バーチャル アプライアンスを右クリックし、**Power**（電源）> **Power Off**（電源オフ）の順に選択します。
2. Panorama バーチャル アプライアンスを右クリックし、**Edit Settings**（設定変更）を選択します。
3. 仮想ディスクを追加するステップを繰り返します。必要なログ ストレージの量に基づいて **Disk Size**（ディスク サイズ）を 2TB の倍数に設定します。容量は、最低でも既存の仮想ディスク、または Panorama が現在ログに使用している NFS ストレージと同じである必要があります。ディスク容量は 2TB の倍数である必要があり、最大 24TB です。たとえば、既存のディスクに 5TB のログ ストレージがある場合、6TB 以上の新しいディスクを追加する必要があります。

   Panorama モードに切り替えると、Panorama は自動的に新しいディスクを 2TB のパーティションに分割し、各パーティションが個別の仮想ディスクとして機能します。
4. Panorama バーチャル アプライアンスを右クリックし、**Power**（電源）> **Power On**（電源オン）を選択します。Panorama が再起動するのを待ってから続行します。

STEP 4 | レガシー モードから Panorama モードに切り替えます。

モードを切り替えると、アプライアンスは再び再起動し、自動的にローカル ログ コレクタおよびコレクタ グループを作成します。既存のログは、この手順の後半で移行するまで、クエリやレポートに使用できなくなります。

1. Panorama CLI に戻り、以下のコマンドを実行します。

© 2019 Palo Alto Networks, Inc.

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

続行を促されたら、「**y**」と入力します。再起動後、Panorama は自動的にローカル ログ コレクタ（名前は Panorama）を作成し、ローカル ログ コレクタを含めるコレクタ グループ（名前はデフォルト）を作成します。Panorama は、追加した仮想ロギング ディスクの設定も行い、2TB ずつのディスクに分割します。このプロセスが完了し、Panorama が再起動するのを待ってから（約 5 分）続行します。

2. Panorama Web インターフェイスにログインします。
3. **Dashboard**（ダッシュボード）の **General Information**（一般情報）設定で、現在の **Mode**（モード）が **panorama** であることを確認します。

   HA デプロイで、セカンダリ ピアはこの時点でサスペンド状態になっています。これは、そのモード（Panorama）がプライマリ ピア（レガシー）のモードと一致しないためです。この手順の後半でプライマリ ピアを Panorama モードに切り替えた後でセカンダリ ピアのサスペンド状態を解除します。
4. **Panorama** > **Collector Groups** (コレクタ グループ)を選択し、**default** (デフォルト)のコレクタ グループが作成されていることと、デフォルトのコレクタ グループにローカル ログコレクタが含まれていることを確認します。
5. 設定を管理対象のデバイスにプッシュします。
   - 保留中の変更がない場合：
     1. **Commit**（コミット）> **Push to Devices**（デバイスへのプッシュ）の順に選択し、**Edit Selections**（選択内容の編集）を行います。
     2. **Collector Group** (コレクタ グループ)を選択し、**default** (デフォルト)のコレクタ グループが選択されていることを確認します。
     3. **OK**、**Push**（プッシュ）の順にクリックします。
   - 保留中の変更がある場合：
     1. **Commit** (コミット) > **Commit and Push** (コミットしてプッシュ) を選択して **Edit Selections** (選択内容の編集) します。
     2. **Device Group** (デバイスグループ)の各デバイスと、**Templates** (テンプレート)が含まれていることを確認します。
     3. **Collector Group** (コレクタ グループ)を選択し、**default** (デフォルト)のコレクタ グループが選択されていることを確認します。
     4. **OK**および**Commit and Push** (コミットしてプッシュ)をクリックします。
6. **Panorama** > **Managed Collectors**（管理対象コレクタ）の順に選択し、列でローカル ログ コレクタの以下の情報が表示されていることを確認します。
   - コレクタ名 — このデフォルトは Panorama ホスト名です。これは、**default**（デフォルト）コレクタ グループの下に表示さます。
   - 接続済み — チェック マーク
   - 設定ステータス — 同期中
   - ランタイム ステータス — 接続済み

STEP 5 | （HA のみ）プライマリ Panorama をレガシー モードから Panorama モードに切り替えます。



このステップにより、フェイルオーバーがトリガーされます。

1. プライマリ Panorama でステップ 1 ~ ステップ 4 を実行します。

   プライマリ Panorama が再起動し、アクティブ HA 状態に戻るのを待ちます。プリエンプションが有効でない場合、手動でフェイルバックする必要があります。**Panorama** > **High Availability**（高可

© 2019 Palo Alto Networks, Inc.

用性）の順に選択し、Operational Commands（操作コマンド）セクションで **Make local Panorama functional**（ローカル **Panorama** を稼働状態にする）操作を実行します。
2. プライマリ Panorama で **Dashboard**（ダッシュボード）を選択し、High Availability（高可用性）セクションで **Sync to peer**（ピアと同期）して **Yes**（はい）をクリックし、**Running Config**（実行中の設定）で **Synchronized**（同期済み）ステータスが表示されるのを待ちます。
3. セカンダリ Panorama で **Panorama** > **High Availability**（高可用性）の順に選択し、Operational Commands（操作コマンド）セクションで **Make local Panorama functional**（ローカル **Panorama** を稼働状態にする）操作を実行します。

   このステップは、セカンダリ Panorama をサスペンド HA 状態から回復させるために必要です。

STEP 6 | 既存のログを新しい仮想ロギング ディスクに移行します。

Panorama を HA 設定でデプロイした場合、この手順はプライマリ ピアでのみ実行します。

1. Panorama CLI に戻ります。
2. ログの移行を開始します。

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

このプロセスにかかる時間は、移行するログ データの量によって異なります。移行の状況を確認するには、以下のコマンドを実行します。

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

移行が完了すると、出力が表示されます：`migration has been done.`

3. 既存のログが使用できることを確認します。
   1. Panorama Web インターフェイスにログインします。
   2. **Panorama** > **Monitor**（監視）の順に選択し、既存のログと一致することが分かっているログ タイプを選択（たとえば、**Panorama** > **Monitor**（監視）> **System**（システム））して、ログが表示されることを確認します。

STEP 7 | 次のステップ...

ログ コレクタがファイアウォールから新しいログを受信するように、Panorama へのログ転送を設定します。

Panorama モードの Panorama バーチャル アプライアンスのセットアップ

Panorama モードでは、Panorama™ バーチャル アプライアンスは、ローカル ログ収集機能を持つ Panorama 管理サーバーとして動作することができます。デフォルトでは、Panorama バーチャル アプライアンスは、初期デプロイ時に Amazon Web Services（AWS）、AWS GovCloud、Azure、Google Cloud Platform、KVM、Hyper-V、ESXi、または vCloud Air 上の Panorama バーチャル アプライアンスに少なくとも 1 つの仮想ロギング ディスクが接続されている場合、Panorama モードでデプロイされます。

引き続きサポートされますが、*50GB* ロギング ディスクのレガシー モードから *Panorama* モードへの切り替えは、実稼働環境では推奨されません。*50GB* ロギング ディスクの *Panorama* モードに切り替える場合、追加のロギング ディスクに追加することはできません。

STEP 1 | Panorama CLI へのログインを行います。

© 2019 Palo Alto Networks, Inc.

STEP 2 | Panorama モードに切り替えます。

1. Panorama モードに変更します。

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

2. **y**を入力して、モード変更を確定します。Panorama バーチャル アプライアンスが再起動します。再起動処理によってターミナル エミュレーション ソフトウェアのセッションが終了した場合は、Panorama バーチャル アプライアンスに再接続し、Panorama のログイン画面を表示します。

   CMS Login (CMSログイン)画面が表示された場合は、Panorama バーチャル アプライアンスが再起動をまだ完了させていないということです。入力を指示されたら、ユーザー名やパスワードは入力せずに Enter キーを押します。

STEP 3 | Panorama モードへの切り替えが正しく完了したことを、次のコマンドで確認します。

1. CLI に再度ログインします。
2. Panorama モードへの切り替えが正しく完了したことを、次のコマンドで確認します。

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

モード変更が正しく完了した場合、出力は次のようになります。

```
> system mode:panorama
```

管理専用モードの Panorama バーチャル アプライアンスのセットアップ

管理専用モードでは、Panorama バーチャル アプライアンスは、ローカル ログ収集機能を持たない Panorama 管理サーバーとして厳密に動作することができます。デフォルトでは、Panorama バーチャル アプライアンスは Panorama モードで初期デプロイメント用になっています。管理専用モードに変更すると、管理専用モードの Panorama バーチャル アプライアンスはログ収集をサポートしないため、Panorama 管理アプライアンスに転送されるログがないことが必須のため、最初のデプロイ直後に Panorama バーチャル アプライアンスを管理専用に変更することをお勧めします。管理専用モードに変更すると、Panorama バーチャル アプライアンスに保存されている既存のログ データにアクセスできなくなり、ACC およびレポート機能は Panorama バーチャル アプライアンス保存されているログを照会できなくなります。

STEP 1 | Panorama CLI へのログインを行います。

STEP 2 | 管理専用モードに切り替えます。

1. 管理専用モードに変更します。

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

2. **y**を入力して、モード変更を確定します。Panorama バーチャル アプライアンスが再起動します。再起動処理によってターミナル エミュレーション ソフトウェアのセッションが終了した場合は、Panorama バーチャル アプライアンスに再接続し、Panorama のログイン画面を表示します。

   CMS Login (CMSログイン)画面が表示された場合は、Panorama バーチャル アプライアンスが再起動をまだ完了させていないということです。入力を指示されたら、ユーザー名やパスワードは入力せずに Enter キーを押します。

STEP 3 | 管理専用モードへの切り替えが正しく完了したことを、次のコマンドで確認します。

© 2019 Palo Alto Networks, Inc.

1. CLI に再度ログインします。
2. 管理専用モードへの切り替えが正しく完了したことを、次のコマンドで確認します。

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

モード変更が正しく完了した場合、出力は次のようになります。

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

Panorama バーチャル アプライアンスでのログ ストレージ容量の拡張

Panorama バーチャル アプライアンスの初期設定の実行後、使用可能なログ ストレージ容量とその拡張オプションは、仮想プラットフォーム（VMware ESXi、vCloud Air、AWS、AWS GovCloud、Azure、Google Cloud Platform、KVM、または Hyper-V）とモード（Legacy、Panorama、またはログ コレクタ モード）によって異なります。詳細は、Panorama モデルを参照してください。

Panorama バーチャル アプライアンスでログ ストレージ容量を拡張するには、追加のロギング ディスクを追加しなければなりません。既存のロギング ディスクのログ ストレージ容量の拡張はサポートされておらず、Panorama は追加のストレージ容量を認識しません。例えば、2TB のロギング ディスクを追加して、その既存のロギング ディスクを 4TB に拡張した場合、Panorama はロギング ディスクを 2TB のストレージ容量として認識し続け、追加の 2TB のストレージ容量を無視します。

さらにログ保存容量を増やす場合、ファイアウォール ログを専用ログコレクタに転送する（管理対象コレクタの設定を参照）か、Panorama から外部の宛先へのログ転送を設定することもできます。

Panorama のログの保存容量を拡張する前に、Panoramaのログ保持要件を決定してください。

- レガシー モードの Panorama バーチャル アプライアンスにストレージを追加するときに既存のログを保持
- ESXi サーバー上の Panorama に仮想ディスクを追加
- vCloud Air の Panorama に仮想ディスクを追加
- AWS の Panorama に仮想ディスクを追加
- Azure の Panorama に仮想ディスクを追加
- Google Cloud Platform 上の Panorama に仮想ディスクを追加
- KVM の Panorama に仮想ディスクを追加
- Hyper-V の Panorama に仮想ディスクを追加
- NFS データストアに Panorama ESXi サーバーをマウント

レガシー モードの *Panorama* バーチャル アプライアンスにストレージを追加するときに既存のログを保持

レガシー モードの Panorama バーチャル アプライアンスは、仮想ディスクを 1 つだけ使用してロギングを行います。そのため、ロギング専用の仮想ディスクを追加すると、Panorama はシステム ディスクにあるデフォルトの 11GB のログ ストレージを使用するのを止め、既存のログをすべて新しいロギング ディスクに自動でコピーします。（ログ以外のデータに関しては、Panorama はシステム ディスクを使用し続けます）

2TBのストレージ容量を持つ既存のロギング専用ディスクを最大8TBのディスクと交換すると、既存のディスクにあるログは失われます。次のいずれかを行えば、ログを保持できます。

© 2019 Palo Alto Networks, Inc.

- 仮想ディスクを交換する前に、外部の宛先へのログ転送を設定します。

- 新しい8TBのディスク用にPanorama バーチャル アプライアンスを新たにセットアップし、その口グが必要な間、古いディスクを含んだPanoramaにアクセスできる状態を保つことができます。ファイアウォール ログを新しい Panorama バーチャル アプライアンスに転送する方法の一つは、ファイアウォールが新しい Panorama の IP アドレスに接続するよう設定し（ **Device**（デバイス）> **Setup**（セットアップ）> **Management**（管理）の順に選択し、Panorama Settings（Panorama 設定）を編集）、新しい Panorama に管理対象のデバイスとしてファイアウォールを追加し、「Panorama への口グ転送の設定」を行います。もう一つの方法として、新しいPanoramaで古いPanoramaのIPアドレスを再利用する場合は、古いPanoramaの設定をエクスポートし、新しいPanoramaに対する設定のインポート、読み込みを行います。

- 古いディスクのログを新しいディスクにコピーします。このコピーは、現在ディスクに保存されている口グの数によっては数時間かかる場合があり、また処理を行っている間、Panoramaは口グを収集できなくなります。Palo Alto Networksカスタマーサポートに説明をお求めください。

ESXi サーバー上の *Panorama* に仮想ディスクを追加

Panorama バーチャル アプライアンスでログ ストレージ容量を拡張するには、仮想口ギング ディスクを追加します。アプライアンスが Panorama モードの場合は、それぞれが 2TB の仮想 口ギング ディスクまたは 1 台で 24TB の仮想 口ギング ディスクを 1 台から 12 台、つまり最大で合計 24TB まで追加できます。アプライアンスがレガシー モードの場合、ESXi 5.5 以降のバージョンでは、最大 8TB の仮想口ギング ディスクを 1 台追加できます。また、これより前のバージョンの ESXi では、最大 2TB のディスクを 1 台追加できます。さらに、プロビジョニングフォーマットが異なる複数のディスクを使用する場合に予期しないパフォーマンス低下が発生する可能性を避けるため、口ギング ディスクの追加は、同じディスクのプロビジョニングフォーマットで行うことが推奨されます。

Panorama が新しい仮想ディスクへの接続を失うと、障害期間中の口グを *Panorama* が損失する可能性があります。

冗長性を許可するには、*RAID* 設定の仮想ディスクを使用します。*RAID10* では、口ギングを大量に行うアプリケーションで最適な書き込みパフォーマンスが得られます。

必要な場合はESXi サーバーの仮想ディスクを交換することができます。

STEP 1 | 別のディスクを Panorama に追加します。

どのモードでも、別のディスクを追加するには、*Panorama VM* の最初の口ギング ディスクが *2TB* 以上でなければなりません。最初の口ギング用ディスクが *2TB* 未満の場合は、別のディスク スペースを追加することはできません。

1. VMware vSphere クライアントにアクセスして**Virtual Machines**（仮想マシン）を選択します。
2. Panorama バーチャル アプライアンスを右クリックし、**Power**（電源）> **Power Off**（電源オフ）を選択します。
3. Panorama バーチャル アプライアンスを右クリックし、**Edit Settings**（設定変更）を選択します。
4. **Hardware**（ハードウェア）タブで **Add**（追加）をクリックして、Add Hardware（ハードウェア追加）ウィザードを開きます。
5. ハードウェア タイプとして **Hard Disk**（ハードディスク）を選択し、**Next**（次へ）をクリックします。
6. **Create a new virtual disk**（新しい仮想ディスクを作成）して、**Next**（次へ）をクリックします。

© 2019 Palo Alto Networks, Inc.

7. **Disk Size**（ディスク サイズ）を設定します。Panorama バーチャル アプライアンスが Panorama モードの場合は、サイズを 2TB 以上に設定します。アプライアンスがレガシー モードの場合は、サイズは 8TB まで設定できます。

   Panorama モードの場合は、*2TB* より大きいサイズのディスクを追加できます。この場合、*Panorama* は、*2TB* のパーティションを可能な数だけ自動的に作成します。たとえば、ディスク *sdc* が *24TB* であれば、*2TB* のパーティションを *12* 個作成します。これらのディスクには、*sdc1 ~ 12* の名前が付けられます。
8. **Disk Provisioning**（ディスク プロビジョニング）フォーマットを選択し、**Next**（次へ）をクリックします。
9. **Specify a datastore or datastore structure**（データストアまたはデータストア構造を指定）します。次に、指定した **Disk Size**（ディスク サイズ）に対して十分なスペースを持つデータストアを **Browse**（参照）し、**OK** をクリックして **Next**（次へ）をクリックします。
10. SCSI **Virtual Device Node**（仮想デバイス ノード）（デフォルトのセクションを使用可能）を選択して **Next**（次へ）をクリックします。

    選択したノードは *SCSI* フォーマットでなければなりません。別のフォーマットを選択した場合は *Panorama* の再起動が失敗します。
11. 設定が正しいことを確認してから、**Finish**（完了）、**OK** の順にクリックします。

    新しく追加したディスクが、バーチャル アプライアンスのデバイス一覧に表示されます。
12. Panorama バーチャル アプライアンスにさらにディスクを追加する必要がある場合は、ステップ 4 からステップ 11 を繰り返します。
13. Panorama バーチャル アプライアンスを右クリックし、**Power**（電源）> **Power On**（電源オン）を選択します。初回使用のために仮想ディスクが初期化されます。初期化にかかる時間は新しいディスクのサイズによります。

STEP 2 | 各ディスクを設定します。

以下の例では、sdc 仮想ディスクを使用します。

1. Panorama CLI へのログインを行います。
2. 以下のコマンドを入力して、Panorama バーチャル アプライアンスのディスクを表示します。

   `show system disk details`

   以下の応答が表示されます。

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

3. 以下のコマンドを入力し、応答が `Reason :` であるすべてのディスクについて、確認を促されたら、要求を確認します。`Admin disabled` 応答:

   `request system disk add sdc`

   Management Only（管理専用）モードはログ記録をサポートしていないため、このモードの *Panorama* 管理サーバでは ***`request system disk add`*** コマンドを使用できません。コマンドが見つからない場合はPanorama モードの Panorama バーチャ

© 2019 Palo Alto Networks, Inc.

ル アプライアンスのセットアップを行ってロギング ディスクを有効化してください。一旦 *Panorama* モードでPanorama CLI にログインし、ステップ 4に進んでディスクの追加を確認します。

4. **show system disk details** コマンドを入力して、ディスクの追加に関するステータスを検証します。新しく追加したすべてのディスクの応答として次の内容が表示されたら、ステップ 3 に進みます。 `Reason :Adminenabled.`

STEP 3 | ディスクのロギングを有効にします。

1. Panorama Web インターフェイスにログインします。
2. **Panorama** > **Managed Collectors**(Panorama > 管理対象コレクタ) の順に選択し、ログ コレクタを編集します。
3. **Disks** (ディスク) を選択し、新しく追加された各ディスクを Add (追加) します。
4. **OK** をクリックします。
5. **Commit** (コミット) > **Commit and Push** (コミットしてプッシュ) の順に選択し、変更内容を **Commit and Push** (コミットしてプッシュ) します。

STEP 4 | ログを受信するように Panorama を設定します。

このステップは、Panorama モードの新しい Panorama を導入するために実行します。既存の Panorama バーチャル アプライアンスにロギング ディスクを追加する場合は、ステップ 5 に進みます。

1. 管理対象コレクタの設定
2. コレクタ グループの設定
3. Panorama へのログ転送の設定

STEP 5 | Panorama ログ ストレージ容量が増加していることを確認します。

1. Panorama Web インターフェイスにログインします。
2. **Panorama** > **Collector Groups** (コレクタ グループ) の順に選択し、Panorama バーチャル アプライアンスが属しているコレクタ グループを選択します。
3. **Log Storage** (ログ ストレージ) 容量にディスク容量が正確に表示されていることを確認します。

vCloud Air の Panorama に仮想ディスクを追加

仮想ロギング ディスクを追加して、Panorama™バーチャル アプライアンスのログ ストレージ容量を拡張できます。アプライアンスが Panorama モードの場合は、それぞれが 2TB の仮想 ロギング ディスクまたは 1 台で 24TB の仮想 ロギング ディスクを 1 台から 12 台、つまり最大で合計 24TB まで追加できます。アプライアンスがレガシー モードの場合は、最大 8TB の仮想ロギング ディスクを 1 台追加できます。

Panorama が新しい仮想ディスクへの接続を失うと、障害期間中のログを *Panorama* が損失する可能性があります。

必要な場合は、vCloud Air サーバーの仮想ディスクを交換できます。

STEP 1 | Panorama に別のディスクを追加します。

どのモードでも、別のディスクを追加するには、*Panorama VM* の最初のロギング ディスクが *2TB* 以上でなければなりません。最初のロギング ディスクが *2TB* 未満の場合は、別のディスク スペースを追加することはできません。

1. vCloud Air Web コンソールにアクセスし、**Virtual Private Cloud On Demand** (仮想プライベート クラウド オンデマンド) 領域を選択します。
2. **Virtual Machines** (仮想マシン) タブで Panorama バーチャル アプライアンスを選択します。
3. 別のディスクを追加します (**Actions** (操作) > **Edit Resources** (リソース編集))。

© 2019 Palo Alto Networks, Inc.

4. **Storage**（ストレージ）のサイズを設定します。Panorama バーチャル アプライアンスが Panorama モードの場合は、サイズを 2TB 以上に設定します。アプライアンスがレガシー モードの場合は、サイズは 8TB まで設定できます。

   Panorama モードの場合は、*2TB* より大きいサイズのディスクを追加できます。この場合、*Panorama* は、*2TB* のパーティションを可能な数だけ自動的に作成します。たとえば、ディスク *sdc* が *24TB* であれば、*Panorama* は *2TB* のパーティションを *12* 個作成します。これらのディスクには、*sdc1 ~ 12* の名前が付けられます。
5. ストレージ層を **Standard**（標準）または **SSD-Accelerated**（**SSD** アクセラレート）に設定します。
6. 前の ステップ を繰り返して、必要に応じて追加のディスクを Panorama バーチャル アプライアンスに追加します。
7. 変更を**Save**（保存）します。

STEP 2 | 各ディスクを設定します。

以下の例では、sdc 仮想ディスクを使用します。

1. Panorama CLI へのログインを行います。
2. 以下のコマンドを入力して、Panorama バーチャル アプライアンスのディスクを表示します。

   `show system disk details`

   以下の応答が表示されます。

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

3. 以下のコマンドを入力し、応答が `Reason :`であるすべてのディスクについて、確認を促されたら、要求を確認します。`Admindisabled` 応答：

   `request system disk add sdc`

   Management Only（管理専用）モードはログ記録をサポートしていないため、このモードの *Panorama* 管理サーバでは ***`requestsystem disk add`*** コマンドを使用できません。コマンドが見つからない場合はPanorama モードの Panorama バーチャル アプライアンスのセットアップを行ってロギング ディスクを有効化してください。一旦 *Panorama* モードでPanorama CLI にログインし、ステップ 4に進んでディスクの追加を確認します。
4. **`show system disk details`** コマンドを入力して、ディスクの追加に関するステータスを検証します。新しく追加したすべてのディスクの応答として `Reason :`が表示されたら、次のステップに進みます。`Adminenabled`.

STEP 3 | ディスクのロギングを有効にします。

1. Panorama Web インターフェイスにログインします。
2. **Panorama** > **Managed Collectors**(Panorama > 管理対象コレクタ) の順に選択し、ログ コレクタを編集します。
3. **Disks**（ディスク）を選択し、新しい各ディスクを **Add**（追加）します。
4. **OK** をクリックします。

© 2019 Palo Alto Networks, Inc.

5. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択し、変更内容を **Commit and Push**（コミットしてプッシュ）します。

STEP 4 | ログを受信するように Panorama を設定します。

このステップは、Panorama モードの新しい Panorama を導入するために実行します。既存の Panorama バーチャル アプライアンスにロギング用ディスクを追加する場合は、次のステップに進みます。

1. 管理対象コレクタの設定
2. コレクタ グループの設定
3. Panorama へのログ転送の設定

STEP 5 | Panorama ログ ストレージ容量が増加していることを確認します。

1. Panorama Web インターフェイスにログインします。
2. **Panorama** > **Collector Groups**（コレクタ グループ）の順に選択し、Panorama バーチャル アプライアンスが属しているコレクタ グループを選択します。
3. **Log Storage**（ログ ストレージ）容量に新しいディスク容量が正確に表示されていることを確認します。

AWS の Panorama に仮想ディスクを追加

AWS に Panorama をインストールあるいはAWS GovCloud で Panorama をインストールした後に、仮想ロギング ディスクを Panorama™ バーチャル アプライアンス インスタンスに追加し、管理対象ファイアウォールによって生成されたログのストレージを提供します。Panorama モードまたは専用ログ コレクタ用の Panorama バーチャル アプライアンスのローカル ログ コレクタに仮想ディスクを追加できます。仮想ディスクを追加するには、Amazon Web サービスコンソール、Panorama コマンドライン インターフェイス（CLI）、および Panorama Web インターフェイスにアクセスできる必要があります。

AWS の Panorama バーチャル アプライアンスは 2TB ロギング ディスクのみをサポートし、合計で最大 24TB のログ ストレージをサポートします。容量が 2TB より小さいロギング ディスク、または 2TB で均等に割り切れないサイズのロギング ディスクを追加することはできません。これは、Panorama バーチャル アプライアンスがロギング ディスクを 2TB パーティションに分割するためです。たとえば、4TB ロギング ディスクを接続すると、Panorama は 2TB パーティションを 2 つ作成します。ただし、5TB ロギング ディスクの追加は、残った 1TB はパーティションとしてサポートされていないため、不可能です。

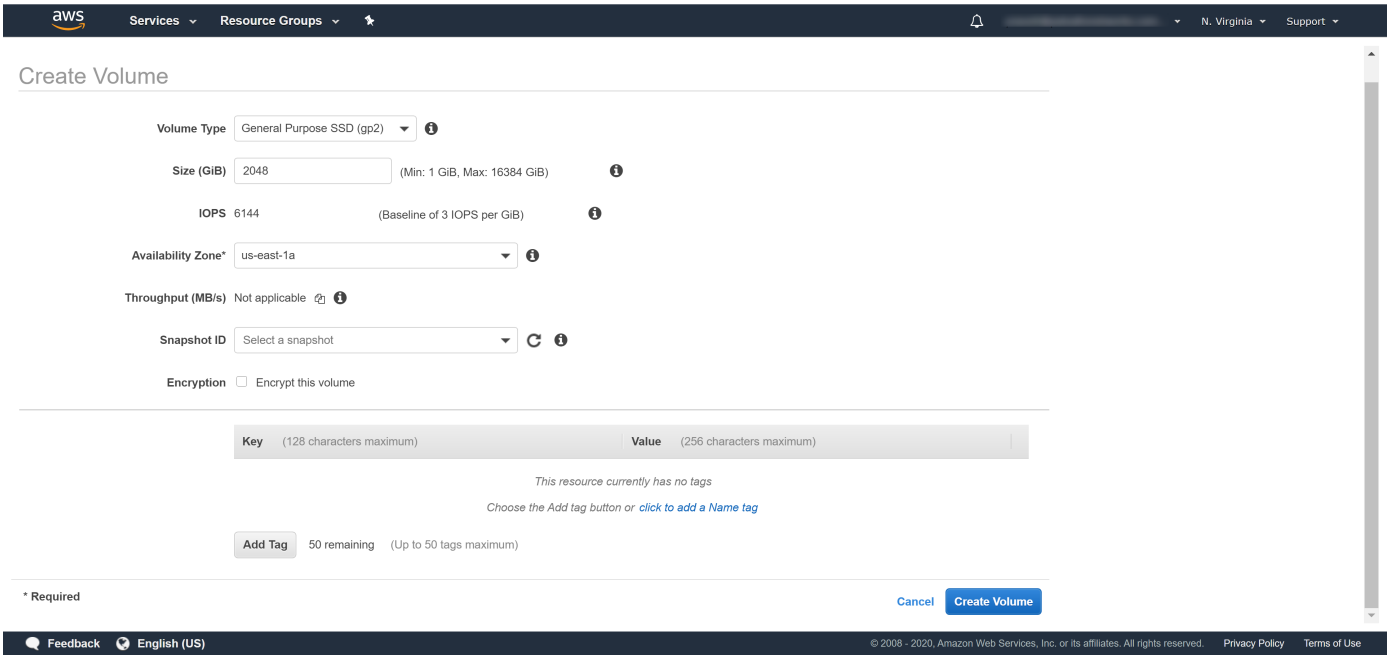
STEP 1 | AWS Web Service のコンソールにログインし、EC2 Dashboard を選択します。

- Amazon Web Services のコンソール
- AWS GovCloud Web Service のコンソール

STEP 2 | 仮想ロギング用ディスクを Panorama に追加します。

1. EC2 Dashboard で、**Volumes**（ボリューム）を選択して**Create Volume**（ボリューム作成）を選択します：
   - 設定するボリューム タイプを選択します。汎用目的の場合は、 **General Purpose SSD (GP2)**（汎用 **SSD**（**GP2**））を選択します。
   - ボリュームの **Size (**サイズ**)** を 2048 GiB に設定します。
   - Panorama バーチャル アプライアンス インスタンスが配置されているのと同じ可用性ゾーンを選択します。
   - （任意）ボリュームを暗号化します。
   - （任意）ボリュームにタグを追加します。
2. **Create Volume**（ボリュームを作成）をクリックします。

© 2019 Palo Alto Networks, Inc.



3. ボリューム ページで、ボリュームを選択し、**Actions**（操作）> **Attach Volume**（ボリュームをアタッチする）を選択します。
4. Panorama バーチャル アプライアンス インスタンスをアタッチします。

STEP 3 | 各ディスクを設定します。

以下の例では、sdc 仮想ディスクを使用します。

1. Panorama CLI へのログインを行います。
2. 以下のコマンドを入力して、Panorama バーチャル アプライアンスのディスクを表示します。

   `show system disk details`

   以下の応答が表示されます。

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

3. 以下のコマンドを入力し、応答が `Reason :`であるすべてのディスクについて、確認を促されたら、要求を確認します。`Admin disabled` 応答:

   `request system disk add sdc`

   Management Only（管理専用）モードはログ記録をサポートしていないため、このモードの *Panorama* 管理サーバでは ***`request system disk add`*** コマンドを使用できません。コマンドが見つからない場合はPanorama モードの Panorama バーチャル アプライアンスのセットアップを行ってロギング ディスクを有効化してくださ

© 2019 Palo Alto Networks, Inc.

い。一旦 *Panorama* モードでPanorama CLI にログインし、ステップ 4に進んでディスクの追加を確認します。

4. **`show system disk details`** コマンドを入力して、ディスクの追加に関するステータスを検証します。新しく追加したすべてのディスクの応答として `Reason :` が表示されたら、次のステップに進みます。`Adminenabled`.

STEP 4 | ディスクのロギングを有効にします。

1. Panorama Web インターフェイスにログインします。
2. ログ コレクタを編集します（**Panorama** > **Managed Collectors**（管理対象のコレクタ））
3. **Disks**（ディスク）を選択し、新しく追加された各ディスクを **Add**（追加）します。
4. **OK** をクリックします。
5. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択し、変更内容を **Commit and Push**（コミットしてプッシュ）します。

STEP 5 | （Panorama モードでの新規 Panorama デプロイメントのみ）ログを受信するために Panorama を設定します。

既存の Panorama バーチャル アプライアンスにロギング ディスクを追加する場合は、ステップ 6 をスキップしてください。

1. コレクタ グループの設定
2. Panorama へのログ転送の設定

STEP 6 | Panorama ログ ストレージ容量が増加することを確認します。

1. Panorama Web インターフェイスにログインします。
2. Panorama バーチャル アプライアンスが属するコレクタ グループを選択します（**Panorama** > **Collector Groups**（コレクタ グループ））。
3. **Log Storage**（ログ ストレージ）容量にディスク容量が正確に表示されていることを確認します。

Azure の Panorama に仮想ディスクを追加

Azure に Panorama をインストールした後に、仮想ロギング ディスクを Panorama™ バーチャル アプライアンス インスタンスに追加し、管理対象ファイアウォールによって生成されたログのストレージを提供します。Panorama モードまたは専用ログ コレクタ用の Panorama バーチャル アプライアンスのローカル ログ コレクタに仮想ディスクを追加できます。仮想ディスクを追加するには、Microsoft Azure ポータル、Panorama コマンドライン インターフェイス（CLI）、および Panorama Web インターフェイスにアクセスできる必要があります。

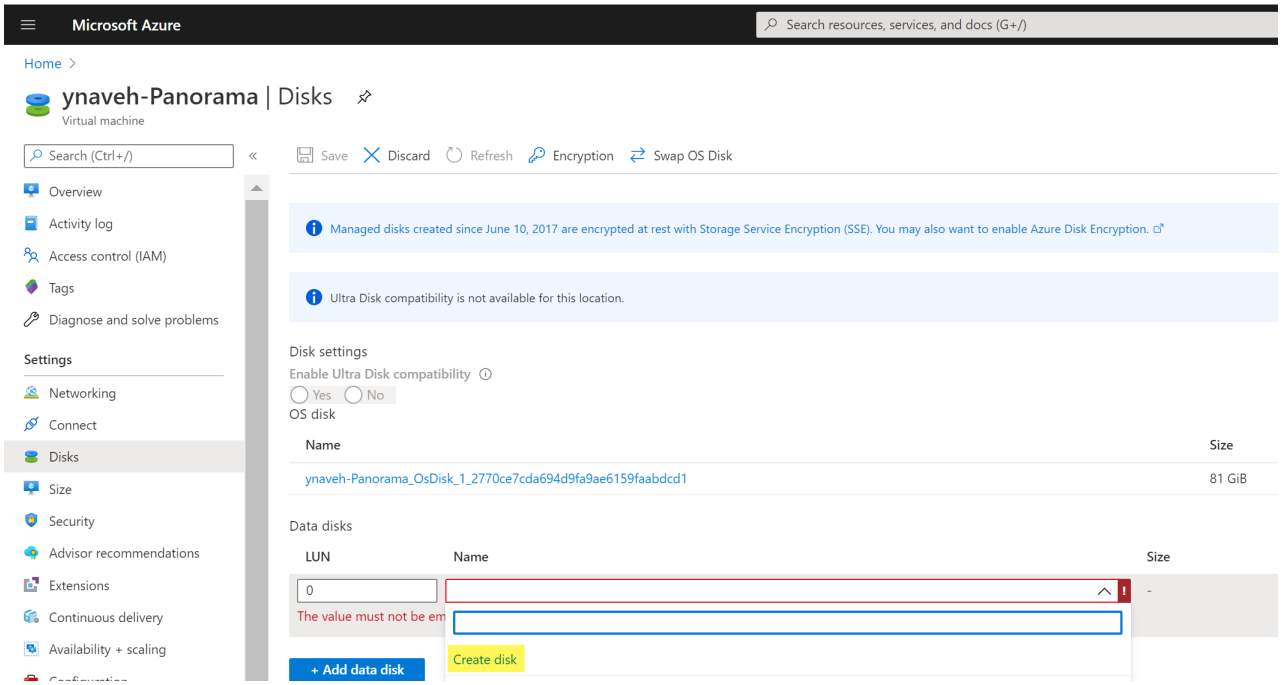
Azureの Panorama バーチャル アプライアンスは 2TB ロギング ディスクのみをサポートし、合計で最大 24TB のログ ストレージをサポートします。容量が 2TB より小さいロギング ディスク、または 2TB で均等に割り切れないサイズのロギング ディスクを追加することはできません。これは、Panorama バーチャル アプライアンスがロギング ディスクを 2TB パーティションに分割するためです。たとえば、4TB ロギング ディスクを接続すると、Panorama は 2TB パーティションを 2 つ作成します。ただし、5TB ロギング ディスクの追加は、残った 1TB はパーティションとしてサポートされていないため、不可能です。

STEP 1 | Microsoft Azure ポータルにログインします。

STEP 2 | 仮想ロギング用ディスクを Panorama に追加します。

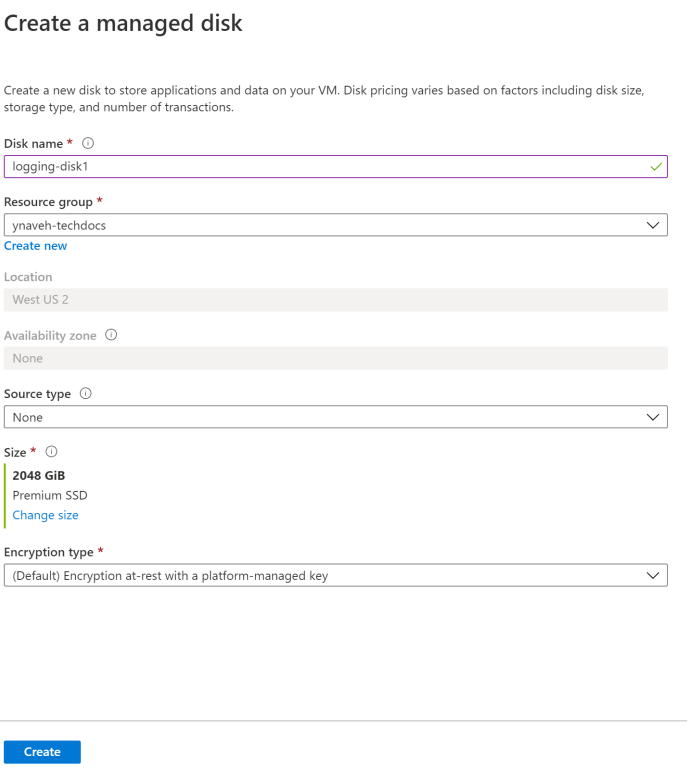
1. Azure ダッシュボードで、ロギング ディスクを追加する Panorama **Virtual Machines**（仮想マシン）を選択します。
2. **Disks**（ディスク）を選択します。
3. **+Add data disk**（データ ディスクを追加）を実行します。
4. 新しいディスクのドロップダウンで、**Create disk**（ディスクの作成）を実行します。

© 2019 Palo Alto Networks, Inc.

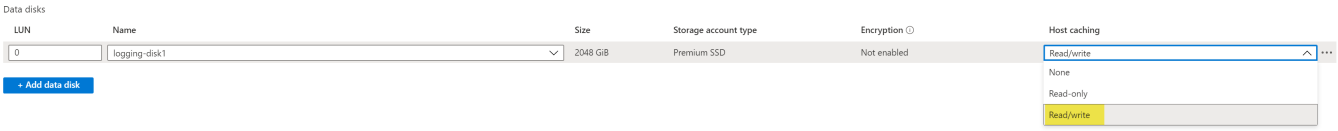


5. ロギング用ディスクを設定します。
    1. ディスクの**Name**（名前）を入力します。
    2. リソース グループを選択します。リソース グループを **Create new**（新規作成）する場合は、グループ名を入力します。
    3. **Account type**（アカウント タイプ）を確認します（このフィールドは自動的に入力されます）。
    4. **Source type**（送信元タイプ）のドロップダウンで、**None**（なし）を選択します。
    5. **Change Size (サイズ変更)** を選択し、 2048 GiB ロギング ディスクを選択します。
    6. 新しいロギング ディスクを **Create (作成)** します。

© 2019 Palo Alto Networks, Inc.



7. **Host caching (ホスト キャッシング)については、Read/write (読み取り/書き込み) を選択します。**



STEP 3 | 各ディスクを有効にします。

以下の例では、sdc 仮想ディスクを使用します。

1. Panorama CLI へのログインを行います。
2. 以下のコマンドを入力して、Panorama バーチャル アプライアンスのディスクを表示します。

   `show system disk details`

   以下の応答が表示されます。

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

3. 以下のコマンドを入力し、応答が `Reason :`であるすべてのディスクについて、確認を促されたら、要求を確認します。`Admin disabled` 応答:

© 2019 Palo Alto Networks, Inc.

```
request system disk add sdc
```



Management Only（管理専用）モードはログ記録をサポートしていないため、このモードの *Panorama* 管理サーバでは ***request system disk add*** コマンドを使用できません。コマンドが見つからない場合はPanorama モードの Panorama バーチャル アプライアンスのセットアップを行ってロギング ディスクを有効化してください。一旦 *Panorama* モードでPanorama CLI にログインし、ステップ 4に進んでディスクの追加を確認します。

4. **show system disk details** コマンドを入力して、ディスクの追加に関するステータスを検証します。新しく追加したすべてのディスクの応答として `Reason :`が表示されたら、次のステップに進みます。`Adminenabled`.

STEP 4 | ディスクのロギングを有効にします。

1. Panorama Web インターフェイスにログインします。
2. ログ コレクタを編集します（**Panorama** > **Managed Collectors**（管理対象のコレクタ））
3. **Disks**（ディスク）を選択し、新しく追加された各ディスクを **Add**（追加）します。
4. **OK** をクリックします。
5. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択し、変更内容を **Commit and Push**（コミットしてプッシュ）します。

STEP 5 | （Panorama モードでの新規 Panorama デプロイメントのみ）ログを受信するために Panorama を設定します。

既存の Panorama バーチャル アプライアンスにロギング ディスクを追加する場合は、ステップ 6 をスキップしてください。

1. コレクタ グループの設定
2. Panorama へのログ転送の設定

STEP 6 | Panorama ログ ストレージ容量が増加することを確認します。

1. Panorama Web インターフェイスにログインします。
2. Panorama バーチャル アプライアンスが属するコレクタ グループを選択します（**Panorama** > **Collector Groups**（コレクタ グループ））。
3. **Log Storage**（ログ ストレージ）容量にディスク容量が正確に表示されていることを確認します。

Google Cloud Platform 上の Panorama に仮想ディスクを追加

Google Cloud Platform に Panorama をインストールした後に、仮想ロギング ディスクを Panorama™ バーチャル アプライアンス インスタンスに追加し、管理対象ファイアウォールによって生成されたログのストレージを提供します。Panorama モードまたは専用ログ コレクタ用の Panorama バーチャル アプライアンスのローカル ログ コレクタに仮想ディスクを追加できます。Google Cloud Platform の Panorama バーチャル アプライアンスは 2TB ロギング ディスクのみをサポートし、合計で最大 24TB のログ ストレージをサポートします。容量が 2TB より小さいロギング ディスク、または 2TB で均等に割り切れないサイズのロギング ディスクを追加することはできません。これは、Panorama バーチャル アプライアンスがロギング ディスクを 2TB パーティションに分割するためです。たとえば、4TB ロギング ディスクを接続すると、Panorama は 2TB パーティションを 2 つ作成します。ただし、5TB ロギング ディスクの追加は、残った 1TB はパーティションとしてサポートされていないため、不可能です。

STEP 1 | Google Cloud コンソールにログインします。

STEP 2 | 仮想ロギング ディスクを追加します。

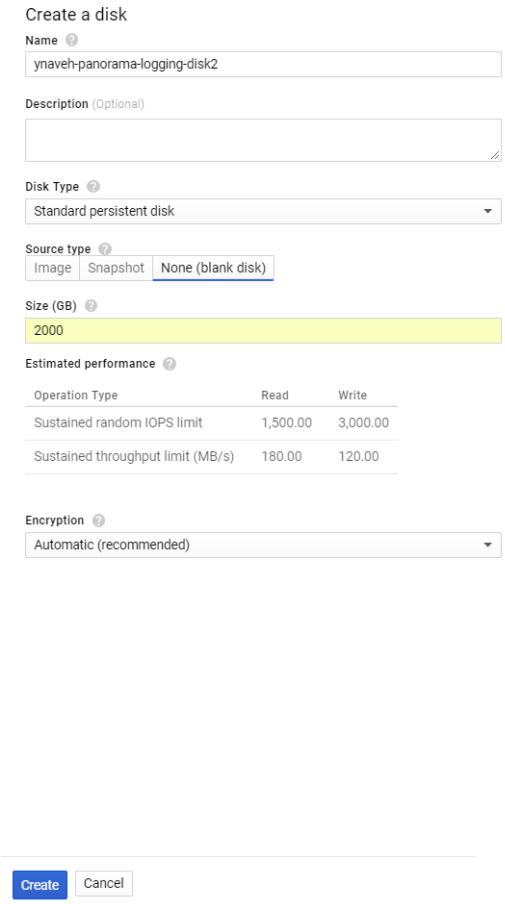
1. Products & Services (製品およびサービス) メニューで、バーチャル アプライアンスの設定を**Edit**（編集）します（**Compute Engine** > **VM Instances**（VM インスタンス））。

© 2019 Palo Alto Networks, Inc.

2. その他のディスク セクションで、 **Add Item**（項目の追加）を行います。
3. **Create disk**（ディスクの作成）（**Name**（名前）ドロップダウン）。

STEP 3 | 仮想ロギング ディスクを設定します。

1. **Name**（名前）を入力します。
2. **Disk Type**（ディスク タイプ）ドロップダウンメニューを展開し、目的のタイプを選択します。
3. **Source type**（送信元タイプ）に対して、**None (empty disk)**（なし（空のディスク））を選択します。
4. 仮想ロギングディスクの**Size (GB)**（サイズ（**GB**））を設定します。
5. **Create**（作成）をクリックします。



6. 変更を **Save**（保存）して、Panorama バーチャル アプライアンスのインスタンスを更新します。

STEP 4 | 各ディスクを設定します。

以下の例では、sdc 仮想ディスクを使用します。

1. Panorama CLI へのログインを行います。
2. 以下のコマンドを入力して、Panorama バーチャル アプライアンスのディスクを表示します。

   `show system disk details`

   以下の応答が表示されます。

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


© 2019 Palo Alto Networks, Inc.

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

3. 以下のコマンドを入力し、応答が `Reason :` であるすべてのディスクについて、確認を促されたら、要求を確認します。`Admin disabled` 応答：

   `request system disk add sdc`

   Management Only (管理専用) モードはログ記録をサポートしていないため、このモードの *Panorama* 管理サーバーでは ***`request system disk add`*** コマンドを使用できません。コマンドが見つからない場合は Panorama モードの Panorama バーチャル アプライアンスのセットアップを行ってロギング ディスクを有効化してください。一旦 *Panorama* モードで Panorama CLI にログインし、ステップ 4 に進んでディスクの追加を確認します。

4. **`show system disk details`** コマンドを入力して、ディスクの追加に関するステータスを検証します。新しく追加したすべてのディスクの応答として `Reason :` が表示されたら、次のステップに進みます。`Admin enabled`。

STEP 5 | ディスクのロギングを有効にします。

1. Panorama Web インターフェイスにログインします。
2. ログ コレクタを編集します（**Panorama** > **Managed Collectors**（管理対象のコレクタ））
3. **Disks**（ディスク）を選択し、新しく追加された各ディスクを **Add**（追加）します。
4. **OK** をクリックします。
5. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択し、変更内容を **Commit and Push**（コミットしてプッシュ）します。

STEP 6 | （Panorama モードでの新規 Panorama デプロイメントのみ）ログを受信するために Panorama を設定します。

既存の Panorama バーチャル アプライアンスにロギング ディスクを追加する場合は、ステップ 7 をスキップしてください。

1. コレクタ グループの設定
2. Panorama へのログ転送の設定

STEP 7 | Panorama ログ ストレージ容量が増加することを確認します。

1. Panorama Web インターフェイスにログインします。
2. Panorama バーチャル アプライアンスが属するコレクタ グループを選択します（**Panorama** > **Collector Groups**（コレクタ グループ））。
3. **Log Storage**（ログ ストレージ）容量にディスク容量が正確に表示されていることを確認します。

KVM の Panorama に仮想ディスクを追加

KVM に Panorama をインストールした後に、仮想ロギング ディスクを Panorama™ バーチャル アプライアンス インスタンスに追加し、管理対象ファイアウォールによって生成されたログのストレージを提供します。Panorama モードまたは専用ログ コレクタ用の Panorama バーチャル アプライアンスのローカル ログ コレクタに仮想ディスクを追加できます。KVM の Panorama バーチャル アプライアンスは 2TB ロギング ディスクのみをサポートし、合計で最大 24TB のログ ストレージをサポートします。容量が 2TB より小さいロギング ディスク、または 2TB で均等に割り切れないサイズのロギング ディスクを追加することはできません。これは、Panorama バーチャル アプライアンスがロギング ディスクを 2TB パーティショ

© 2019 Palo Alto Networks, Inc.

ンに分割するためです。たとえば、4TB ロギング ディスクを接続すると、Panorama は 2TB パーティションを 2 つ作成します。ただし、5TB ロギング ディスクの追加は、残った 1TB はパーティションとしてサポートされていないため、不可能です。

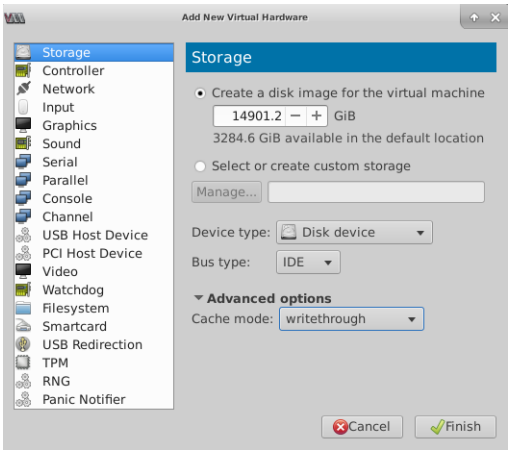
STEP 1 | Virtual Machine Manager 上の Panorama バーチャル アプライアンスを **Shutdown**（シャットダウン）します。

STEP 2 | Virtual Machine Manager 上の Panorama バーチャル アプライアンスのインスタンスをダブルクリックして、**Show virtual hardware details**（バーチャル ハードウェアの詳細を表示）をします。

STEP 3 | 仮想ロギング ディスクを追加します。さらに追加する必要がある場合はこのステップを繰り返します。

1. **Create a disk image for a virtual image**（仮想イメージのディスク イメージを作成する）（**Add Hardware**（ハードウェアの追加）> **Storage**（ストレージ））を実行し、 使用する Virtual Machine Manager に応じて 、仮想ディスクストレージ容量を適切な2TB 値（2000GB または 14901.2GiB）に設定します。

   バージョンによっては、一部の *Virtual Machine Manager* は *GiB*（*gibibyte*）を使用してメモリを割り当てます。仮想ロギング ディスクのプロビジョニングや *Panorama* バーチャル アプライアンスのメンテナンスモードへの移行を避けるために、必要なストレージ容量を正しく変換してください。
2. **Device Type**（デバイス タイプ）ドロップダウン リストで、**Disk device**（ディスク デバイス）を選択します。
3. **Bus Type**（バス タイプ）ドロップダウン リストで、設定に従い **VirtIO** または **IDE** を選択します。
4. **Advanced options**（詳細オプション）を展開して、**Cache modeCache mode**（キャッシュ モード）ドロップダウン リストで、**writethrough** を選択します。
5. **Finish**（完了）をクリックします。



STEP 4 | Panorama バーチャル アプライアンスを **Power on**（パワーオン）します。

STEP 5 | 各ディスクを設定します。

以下の例では、sdc 仮想ディスクを使用します。

1. Panorama CLI へのログインを行います。
2. 以下のコマンドを入力して、Panorama バーチャル アプライアンスのディスクを表示します。

   ```
   show system disk details
   ```

   以下の応答が表示されます。

© 2019 Palo Alto Networks, Inc.

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

3. 以下のコマンドを入力し、応答が `Reason :` であるすべてのディスクについて、確認を促されたら、要求を確認します。`Admin disabled` 応答：

   `request system disk add sdc`

   *Management Only (*管理専用*)* モードはログ記録をサポートしていないため、このモードの *Panorama* 管理サーバーでは***`request system disk add`***コマンドを使用できません。コマンドが見つからない場合はPanorama モードの Panorama バーチャル アプライアンスのセットアップを行ってロギング ディスクを有効化してください。一旦 *Panorama* モードでPanorama CLI にログインし、ステップ 4に進んでディスクの追加を確認します。

4. **`show system disk details`** コマンドを入力して、ディスクの追加に関するステータスを検証します。新しく追加したすべてのディスクの応答として `Reason :` が表示されたら、次のステップに進みます。`Admin enabled`。

STEP 6 | ディスクのロギングを有効にします。

1. Panorama Web インターフェイスにログインします。
2. ログ コレクタを編集します（**Panorama** > **Managed Collectors**（管理対象のコレクタ））
3. **Disks**（ディスク）を選択し、新しく追加された各ディスクを **Add**（追加）します。
4. **OK** をクリックします。
5. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択し、変更内容を **Commit and Push**（コミットしてプッシュ）します。

STEP 7 | （Panorama モードでの新規 Panorama デプロイメントのみ）ログを受信するために Panorama を設定します。

既存の Panorama バーチャル アプライアンスにロギング ディスクを追加する場合は、ステップ 8 をスキップしてください。

1. コレクタ グループの設定
2. Panorama へのログ転送の設定

STEP 8 | Panorama ログ ストレージ容量が増加することを確認します。

1. Panorama Web インターフェイスにログインします。
2. Panorama バーチャル アプライアンスが属するコレクタ グループを選択します（**Panorama** > **Collector Groups**（コレクタ グループ））。
3. **Log Storage**（ログ ストレージ）容量にディスク容量が正確に表示されていることを確認します。

Hyper-V の Panorama に仮想ディスクを追加

Hyper-V で Panorama をインストールを行った後に、仮想ロギング ディスクを Panorama™ バーチャル アプライアンス インスタンスに追加し、管理対象ファイアウォールによって生成されたログのストレージを提供します。Panorama モードまたは専用ログ コレクタ用の Panorama バーチャル アプライアンスのロー

© 2019 Palo Alto Networks, Inc.

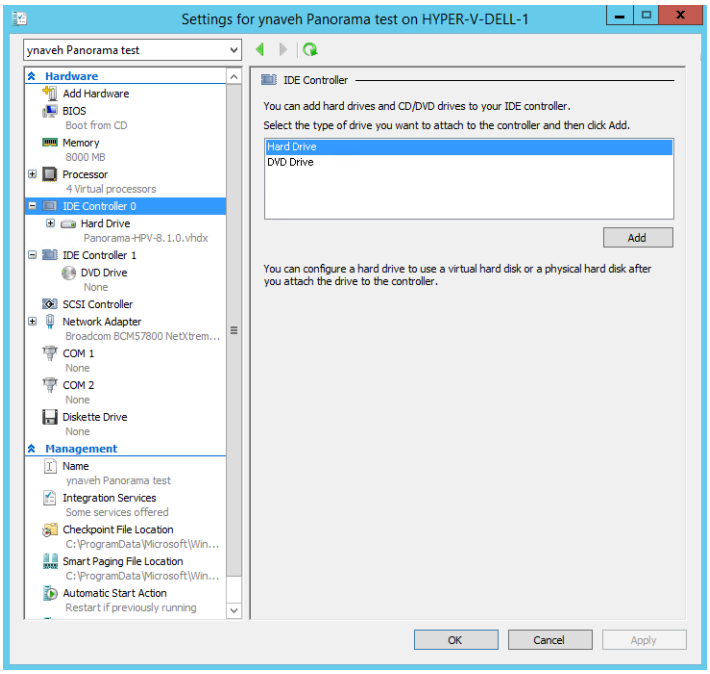
カル ログ コレクタに仮想ディスクを追加できます。Hyper-V の Panorama バーチャル アプライアンスは 2TB ロギング ディスクのみをサポートし、合計で最大 24TB のログ ストレージをサポートします。容量が 2TB より小さいロギング ディスク、または 2TB で均等に割り切れないサイズのロギング ディスクを追加することはできません。これは、Panorama バーチャル アプライアンスがロギング ディスクを 2TB パーティションに分割するためです。たとえば、4TB ロギング ディスクを接続すると、Panorama は 2TB パーティションを 2 つ作成します。ただし、5TB ロギング ディスクの追加は、残った 1TB はパーティションとしてサポートされていないため、不可能です。

STEP 1 | Panorama バーチャル アプライアンスをパワーオフします。

1. Hyper-V Manager で、**Virtual Machines** (仮想マシン)のリストから Panorama バーチャル アプライアンスのインスタンスを選択します。
2. **Action** (操作) > **Turn Off** (電源オフ)を選択して、バーチャル アプライアンスの電源を切ります。

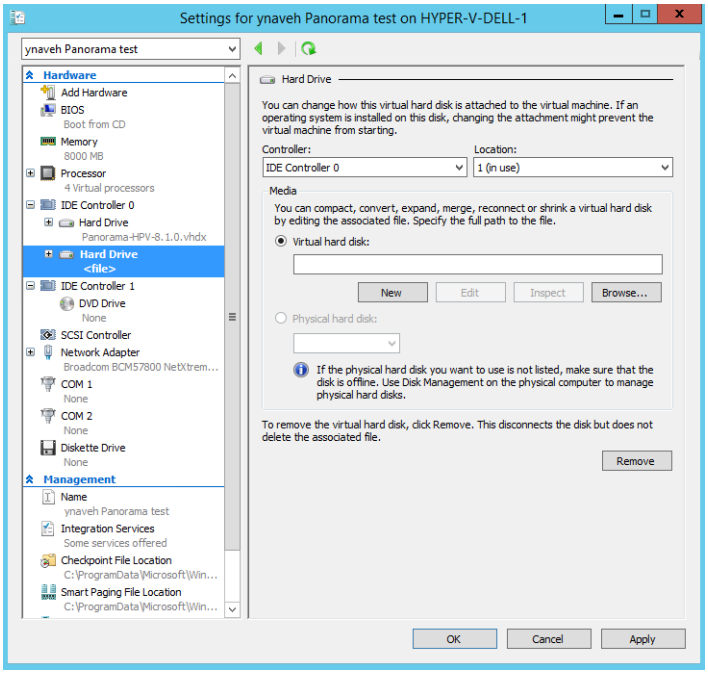
STEP 2 | 仮想ロギング ディスクを追加します。さらに追加する必要がある場合はこのステップを繰り返します。

1. **Virtual Machines** (仮想マシン)のリストで Panorama バーチャル アプライアンスを選択し、さらに**Action** (操作) > **Settings** (設定)を選択します。
2. **Hardware** (ハードウェア)のリストで**IDE Controller 0** (IDE コントローラ 0)を選択します。
3. **IDE Controller** (IDE コントローラ)ドライブのリストで**Hard Drive** (ハードドライブ)を選択し、新しい仮想ロギング ディスクを**Add** (追加)します。



4. **IDE Controller 0** (IDE コントローラ 0)のところで、作成済みの**Hard Drive** (ハードドライブ)を選択します。
5. **Media** (メディア)のところで**New** (新規)ハードディスクを追加します。

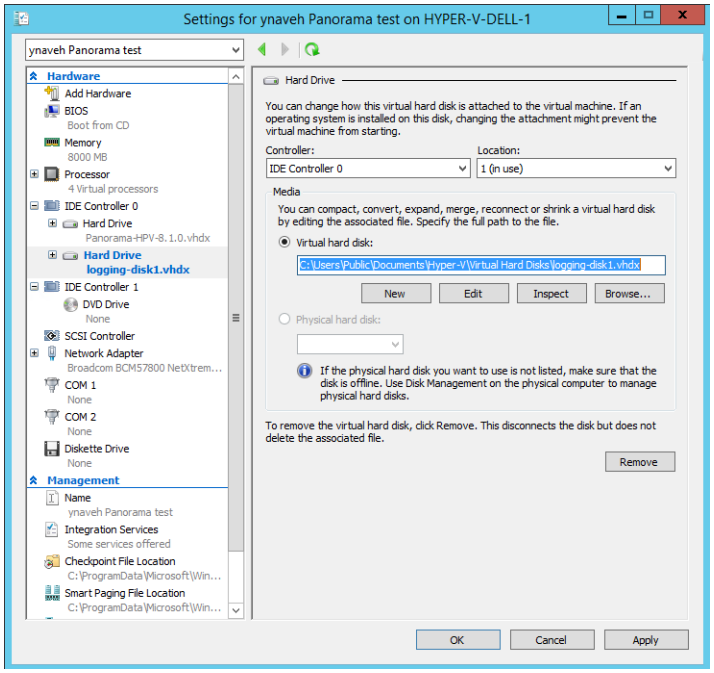
© 2019 Palo Alto Networks, Inc.



STEP 3 | 新しい仮想ロギング ディスクを設定します。

1. Before You Begin (開始する前に) のプロンプトが表示されたら、**Next** (次へ)をクリックして仮想ロギング ディスクの追加を開始します。
2. Disk Format (ディスク フォーマット) は**VHDX**を選択します。**Next** (次へ)をクリックして続行します
3. 要件に応じて、Disk Type (ディスク タイプ) は**Fixed Size** (固定サイズ)あるいは**Dynamically Expanding** (動的に拡張)を選択します。**Next** (次へ)をクリックして続行します。
4. 仮想ロギング ディスク ファイルの**Name** (名前)および**Location** (場所)を指定します。**Next** (次へ)をクリックして続行します。
5. **Create a new virtual hard disk** (新しい仮想ハードディスクを作成)を選択してディスク容量を入力し、ディスクを構成します。**Next** (次へ)をクリックして続行します。
6. Summary (サマリー) を確認し、仮想ハード ロギング ディスクの追加を**Finish** (完了)させます。
7. 新たに追加したハードディスクを**Apply** (適用)します。

© 2019 Palo Alto Networks, Inc.



STEP 4 | Panorama バーチャル アプライアンスをパワーオンします。

1. **Virtual Machines** (仮想マシン)のリストから Panorama バーチャル アプライアンスのインスタンスを選択します。
2. **Action** (操作) > **Start** (起動)を選択して、バーチャル アプライアンスの電源を入れます。

STEP 5 | 各ディスクを設定します。

以下の例では、sdc 仮想ディスクを使用します。

1. Panorama CLI へのログインを行います。
2. 以下のコマンドを入力して、Panorama バーチャル アプライアンスのディスクを表示します。

   `show system disk details`

   以下の応答が表示されます。

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

3. 以下のコマンドを入力し、応答が `Reason :` であるすべてのディスクについて、確認を促されたら、要求を確認します。`Admin disabled` 応答：

   `request system disk add sdc`

Management Only (管理専用) モードはログ記録をサポートしていないため、このモードの *Panorama* 管理サーバーでは***`request system disk add`***コマンドを使用できません。コマンドが見つからない場合はPanorama モードの Panorama バーチャ

© 2019 Palo Alto Networks, Inc.

ル アプライアンスのセットアップを行ってロギング ディスクを有効化してください。一旦 *Panorama* モードでPanorama CLI にログインし、ステップ 4に進んでディスクの追加を確認します。

4. **show system disk details** コマンドを入力して、ディスクの追加に関するステータスを検証します。新しく追加したすべてのディスクの応答として `Reason :` が表示されたら、次のステップに進みます。`Admin enabled`。

STEP 6 | ディスクのロギングを有効にします。

1. Panorama Web インターフェイスにログインします。
2. ログ コレクタを編集します（**Panorama** > **Managed Collectors**（管理対象のコレクタ））
3. **Disks**（ディスク）を選択し、新しく追加された各ディスクを **Add**（追加）します。
4. **OK** をクリックします。
5. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択し、変更内容を **Commit and Push**（コミットしてプッシュ）します。

STEP 7 | （Panorama モードでの新規 Panorama デプロイメントのみ）ログを受信するために Panorama を設定します。

既存の Panorama バーチャル アプライアンスにロギング ディスクを追加する場合は、ステップ 8 をスキップしてください。

1. コレクタ グループの設定
2. Panorama へのログ転送の設定

STEP 8 | Panorama ログ ストレージ容量が増加することを確認します。

1. Panorama Web インターフェイスにログインします。
2. Panorama バーチャル アプライアンスが属するコレクタ グループを選択します（**Panorama** > **Collector Groups**（コレクタ グループ））。
3. **Log Storage**（ログ ストレージ）容量にディスク容量が正確に表示されていることを確認します。

NFS データストアに *Panorama ESXi* サーバーをマウント

レガシー モードの Panorama バーチャル アプライアンスが ESXi サーバー上で実行されている場合は、Network File System（NFS）データストアにマウントすることで、中央の場所へ一元的にロギングを行うことや、ログの保存容量を仮想ディスクがサポートしている容量を超えて拡張することが可能になります。（ESXi 5.5以降のバージョンは最大8TBの仮想ディスクをサポートできます。それよりも古いESXiバージョンでは最大2TBの仮想ディスクをサポートしています）Panorama 高可用性（HA）設定で NFS データストアをセットアップする前に、「Panorama HA でのロギングに関する考慮事項」を参照してください。

Panorama モードの *Panorama* バーチャル アプライアンスでは、*NFS* がサポートされません。

STEP 1 | **Panorama** > **Setup** > **Operations** (Panorama > セットアップ > 操作)の順に選択し、Miscellaneous (その他)セクションで、**Storage Partition Setup** (ストレージ パーティションの設定)をクリックします。

STEP 2 | **Storage Partition**（ストレージ パーティション）のタイプを**NFS V3**に設定します。

STEP 3 | **Server**（サーバー）に NFS サーバーの IP アドレスを入力します。

STEP 4 | ログ ファイルを保存する**Log Directory**（ログのディレクトリ）パスを入力します。たとえば、「export/panorama」のように入力します。

© 2019 Palo Alto Networks, Inc.

STEP 5 | **Protocol**（プロトコル）については**TCP**あるいは**UDP**を選択し、 NFS サーバーのアクセスに使用する**Port**（ポート）を入力します。

NFS over TCP を使用するには、*NFS* サーバーでサポートされている必要があります。一般的な *NFS* ポートは、*UDP/TCP 111*（*RPC* の場合）および *UDP/TCP 2049*（*NFS* の場合）です。

STEP 6 | NFS パフォーマンスを最適にするには、**Read Size**（読み取りサイズ）および **Write Size**（書き込みサイズ）フィールドで、クライアントとサーバー間でやり取りするデータ チャンクの最大サイズを指定します。読み取り/書き込みサイズを定義すると、Panorama と NFS データストア間でやり取りするデータ ボリュームおよび転送速度が最適化されます。

STEP 7 | （任意）**Copy On Setup**（セットアップ時にコピー）を選択し、Panorama に保存された既存のログを NFS ボリュームにコピーします。Panoramaにログが大量に存在する場合は、このオプションによって大量のデータ転送が開始される場合があります。

STEP 8 | **Test Logging Partition**（ロギング パーティションのテスト）をクリックし、Panorama がNFS **Server**（サーバー）および **Log Directory**（ログ ディレクトリ）にアクセスできることを確認します。

STEP 9 | **OK** をクリックして変更内容を保存します。

STEP 10 | **Commit**（コミット） > **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。再起動を行うまでの間、Panorama バーチャル アプライアンスはログをローカル ストレージ ディスクに書き込みます。

STEP 11 | **Panorama** > **Setup** > **Operations**(Panorama > セットアップ > 操作) の順に選択し、Device Operations (デバイスの操作) セクションの**Reboot Panorama** (Panorama を再起動) を選択します。再起動後、Panoramaはログを NFSデータストアに書き込むようになります。

Panorama バーチャル アプライアンスの CPU およびメモリを増やす

「Panorama バーチャル アプライアンスの初期設定の実行」時は、アプライアンスが Panorama モードであるか管理専用モードであるかに基づいて、またログの保存領域または管理対象ファイアウォールの数に基づいて、メモリおよび CPU の数を指定します。後で保存容量や管理対象ファイアウォールを追加する場合は、メモリと CPU も増やす必要があります。ログ コレクタモードの Panorama 仮想アプライアンスはシステム要件を満たしている必要があり、CPU とメモリの最低要件を超えて増やす必要はありません。各 Panorama モードの CPU とメモリの要件については、Panorama バーチャル アプライアンスのセットアップ前提条件を確認してください。

- ESXi サーバー上の Panorama の CPU とメモリを増やす
- vCloud Air 上の Panorama の CPU とメモリを増やす
- AWS 上の Panorama の CPU とメモリを増やす
- Azure 上の Panorama の CPU とメモリを増やす
- Google Cloud Platform 上の Panorama の CPU とメモリを増やす
- KVM 上の Panorama の CPU とメモリを増やす
- Hyper-V 上の Panorama の CPU とメモリを増やす

© 2019 Palo Alto Networks, Inc.

ESXi サーバー上の Panorama の CPU とメモリを増やす

Panorama で必要となる最低の CPU とメモリについては、「Panorama バーチャル アプライアンスの CPU およびメモリを増やす」を参照してください。

STEP 1 | VMware vSphere クライアントにアクセスして**Virtual Machines**（仮想マシン）を選択します。

STEP 2 | Panorama バーチャル アプライアンスを右クリックし、**Power**（電源）> **Power Off**（電源オフ）を選択します。

STEP 3 | Panorama バーチャル アプライアンスを右クリックし、**Edit Settings**（設定変更）を選択します。

STEP 4 | **Memory**（メモリ）を選択し、**Memory Size**（メモリ サイズ）に新しい値を入力します。

STEP 5 | **CPUs** を選択し、CPU の数（**Number of virtual sockets**（仮想ソケット数）x **Number of cores per socket**（ソケット毎のコア数））を指定します。

STEP 6 | **OK** をクリックして変更内容を保存します。

STEP 7 | Panorama バーチャル アプライアンスを右クリックし、**Power**（電源）> **Power On**（電源オン）を選択します。

vCloud Air 上の Panorama の CPU とメモリを増やす

Panorama で必要となる最低の CPU とメモリについては、「Panorama バーチャル アプライアンスの CPU およびメモリを増やす」を参照してください。

STEP 1 | vCloud AirのWebコンソールにアクセスし、ご自身の **Virtual Private Cloud OnDemand**（仮想プライベート クラウド オンデマンド）領域を選択します。

STEP 2 | **Virtual Machines**（仮想マシン）タブで Panorama 仮想マシンおよび **Power Off**（電源オフ）を選択します。

STEP 3 | **Actions** > **Edit Resources** (アクション > リソース編集)を選択します。

STEP 4 | **CPU** と **Memory**（メモリ）を設定します。

STEP 5 | 変更を**Save**（保存）します。

STEP 6 | Panorama 仮想マシンおよび **Power On**（電源オン）を選択します。

AWS 上の Panorama の CPU とメモリを増やす

Panorama™ の CPU およびメモリ最低要件は、 Panorama バーチャル アプライアンスの CPU およびメモリを増やすを参照してください。

ログ コレクタ モードの *Panorama* バーチャル アプライアンスは、仮想マシンのデプロイ後でサイズを変更するとログ コレクタ モードのままにならず、ログ データが失われる可能性があります。

STEP 1 | AWS Web Service のコンソールにログインし、EC2 Dashboard を選択します。

- Amazon Web Services のコンソール

© 2019 Palo Alto Networks, Inc.

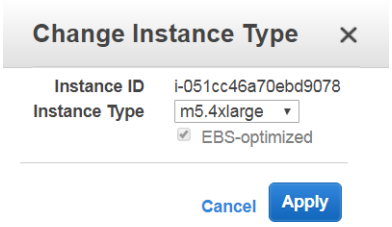
- AWS GovCloud Web Service のコンソール

STEP 2 | EC2 Dashboard で、**Instances**（インスタンス）を選択して、Panorama バーチャル アプライアンス インスタンスを選択します。

STEP 3 | **Actions**（操作）> **Instance State**（インスタンスの状態）> **Stop**（停止）を選択して、バーチャル アプライアンス インスタンスの電源を切ります。

STEP 4 | Select **Actions**（操作）> **Instance Settings**（インスタンスの設定）> **Change Instance Type**（インスタンスの状態の変更）を選択して、Panorama バーチャル アプライアンスのインスタンスのタイプを変更します。

STEP 5 | アップグレードする **Instance Type**（インスタンスのタイプ）を選択し、 **Apply**（適用）します。



STEP 6 | **Actions**（操作）> **Instance State**（インスタンスの状態）> **Start**（開始）を選択して、バーチャル アプライアンス インスタンスの電源をオンにします。

Azure 上の Panorama の CPU とメモリを増やす

Panorama™ の CPU およびメモリ最低要件は、 Panorama バーチャル アプライアンスの CPU およびメモリを増やすを参照してください。

ログ コレクタ モードの *Panorama* バーチャル アプライアンスは、仮想マシンのデプロイ後でサイズを変更するとログ コレクタ モードのままにならず、ログ データが失われる可能性があります。

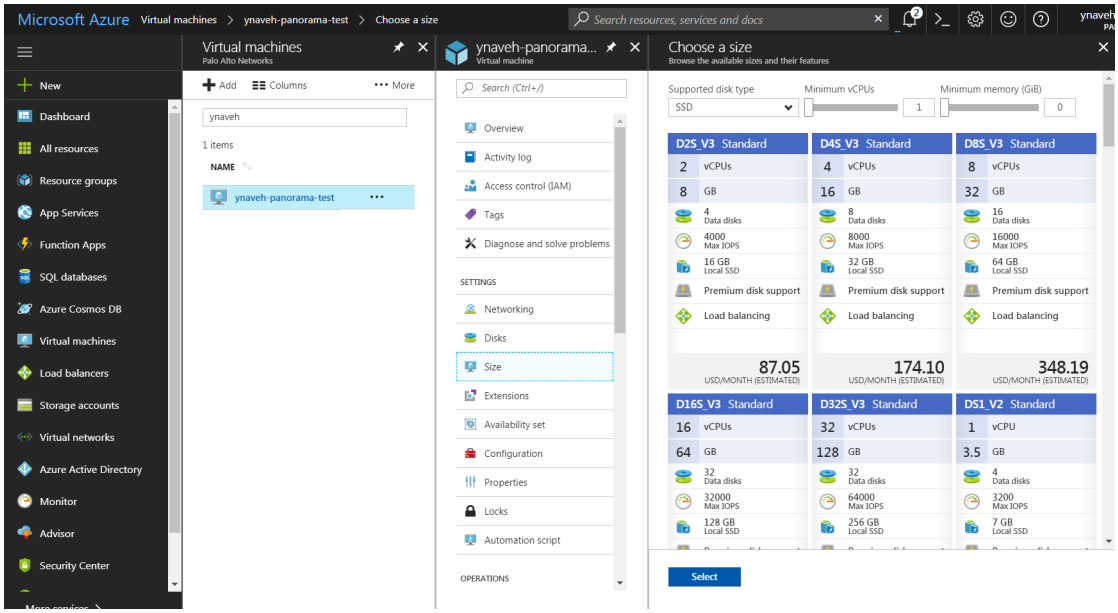
STEP 1 | Microsoft Azure ポータルにログインします。

STEP 2 | Azure Dashboard の、**Virtual Machines**（仮想マシン）で、Panorama バーチャル アプライアンスを選択します。

STEP 3 | **Overview**（概要）を選択して、Panorama バーチャル アプライアンスを **Stop**（停止）します。

STEP 4 | 新しい仮想マシンの **Size**（サイズ）を選択してから、そのサイズを **Select**（選択）します。

© 2019 Palo Alto Networks, Inc.



STEP 5 | **Overview**（概要）を選択して、Panorama バーチャル アプライアンスを **Start**（開始）します。

Google Cloud Platform 上の Panorama の CPU とメモリを増やす

Panorama™ の CPU およびメモリ最低要件は、 Panorama バーチャル アプライアンスの CPU およびメモリを増やすを参照してください。

ログ コレクタ モードの *Panorama* バーチャル アプライアンスは、仮想マシンのデプロイ後でサイズを変更するとログ コレクタ モードのままにならず、ログ データが失われる可能性があります。

STEP 1 | Google Cloud コンソールにログインします。

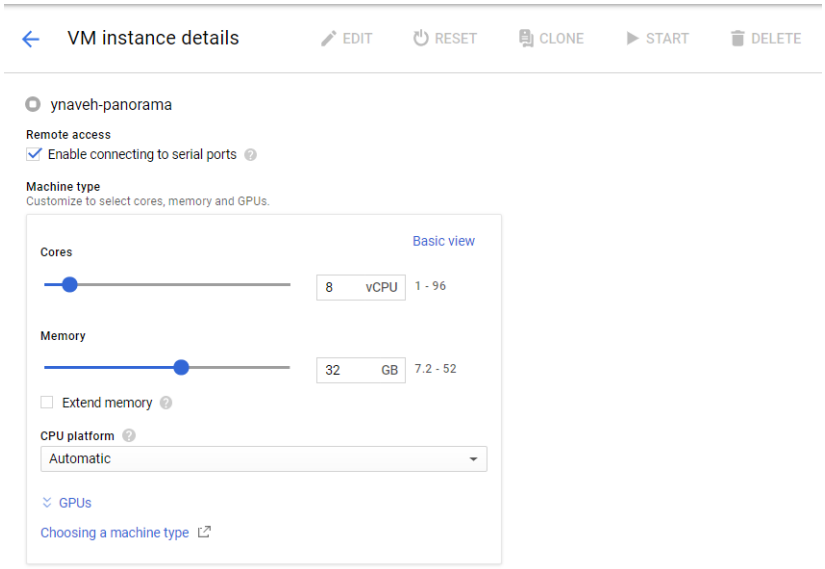
STEP 2 | Panorama バーチャル アプライアンス インスタンスを停止します。

1. Products & Services (製品およびサービス) メニューを選択します（**Compute Engine** > **VM Instances**（**VM** インスタンス））。
2. Panorama バーチャル アプライアンス インスタンスを **Stop**（停止）します。Panorama バーチャル アプライアンスの完全なシャットダウンには 2–3 分かかります。

STEP 3 | Panorama バーチャル アプライアンスのリソースを再設定します。

1. Panorama バーチャル アプライアンス インスタンスを **Edit**（編集）します。
2. マシン タイプで、Panorama バーチャル アプライアンスの CPU コアとメモリを **Customize**（カスタマイズ）します。

© 2019 Palo Alto Networks, Inc.



STEP 4 | 変更を **Save**（保存）して、Panorama バーチャル アプライアンスのインスタンスを更新します。

STEP 5 | Panorama バーチャル アプライアンスを **Start**（開始）します。

KVM 上の Panorama の CPU とメモリを増やす

Panorama™ の CPU およびメモリ最低要件は、 Panorama バーチャル アプライアンスの CPU およびメモリを増やすを参照してください。

ログ コレクタ モードの *Panorama* バーチャル アプライアンスは、仮想マシンのデプロイ後でサイズを変更するとログ コレクタ モードのままにならず、ログ データが失われる可能性があります。

STEP 1 | Virtual Machine Manager 上の Panorama バーチャル アプライアンスを **Shutdown**（シャットダウン）します。

STEP 2 | Virtual Machine Manager 上の Panorama バーチャル アプライアンスのインスタンスをダブルクリックして、**Show virtual hardware details**（バーチャル ハードウェアの詳細を表示）をします。

STEP 3 | 割り当てられた Panorama バーチャル アプライアンスの CPU コアを編集します。

1. 現在割り当てられている **CPU** を編集します。
2. 再設定された CPU コア割り当てを **Apply**（適用）します。

STEP 4 | 割り当てられた Panorama バーチャル アプライアンスのメモリを編集します。

1. 現在割り当てられている **Memory**（メモリ）を編集します。
2. 再設定されたメモリ割り当てを **Apply**（適用）します。

STEP 5 | Panorama バーチャル アプライアンスを **Power on**（パワーオン）します。

© 2019 Palo Alto Networks, Inc.

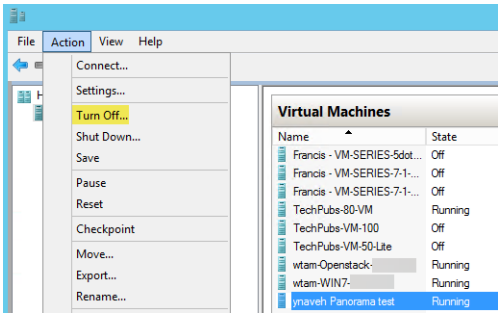
Hyper-V 上の Panorama の CPU とメモリを増やす

Panorama™ の CPU およびメモリ最低要件は、 Panorama バーチャル アプライアンスの CPU およびメモリを増やすを参照してください。

ログ コレクタ モードの *Panorama* バーチャル アプライアンスは、仮想マシンのデプロイ後でサイズを変更するとログ コレクタ モードのままにならず、ログ データが失われる可能性があります。

STEP 1 | Panorama バーチャル アプライアンスをパワーオフします。

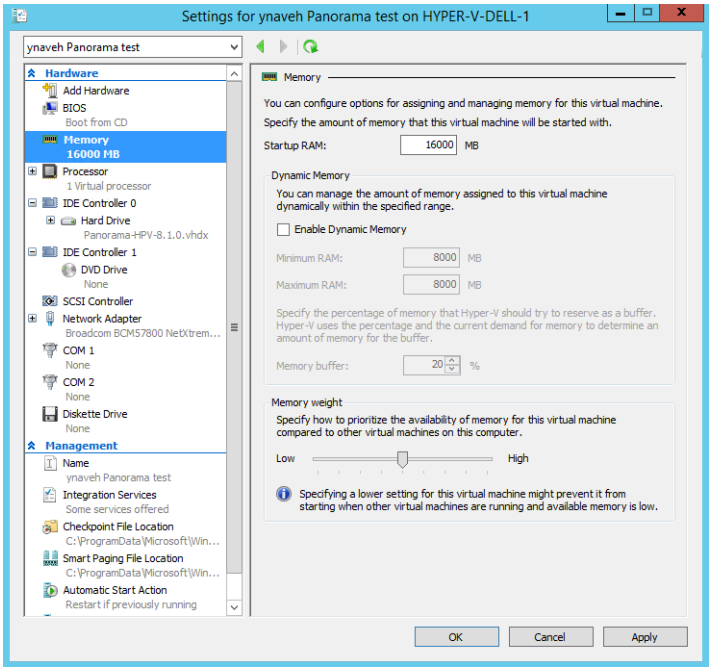
1. Hyper-V Manager で、**Virtual Machines** (仮想マシン)のリストから Panorama バーチャル アプライアンスのインスタンスを選択します。
2. **Action** (操作) > **Turn Off** (電源オフ)を選択して、バーチャル アプライアンスの電源を切ります。



STEP 2 | Hyper-V Manager で、**Virtual Machines** (仮想マシン)のリストから Panorama バーチャル アプライアンスのインスタンスを選択し、さらに**Action** (操作) > **Settings** (設定)を選択して Panorama バーチャル アプライアンスのリソースを編集します。

STEP 3 | 割り当てられた Panorama バーチャル アプライアンスのメモリを編集します。

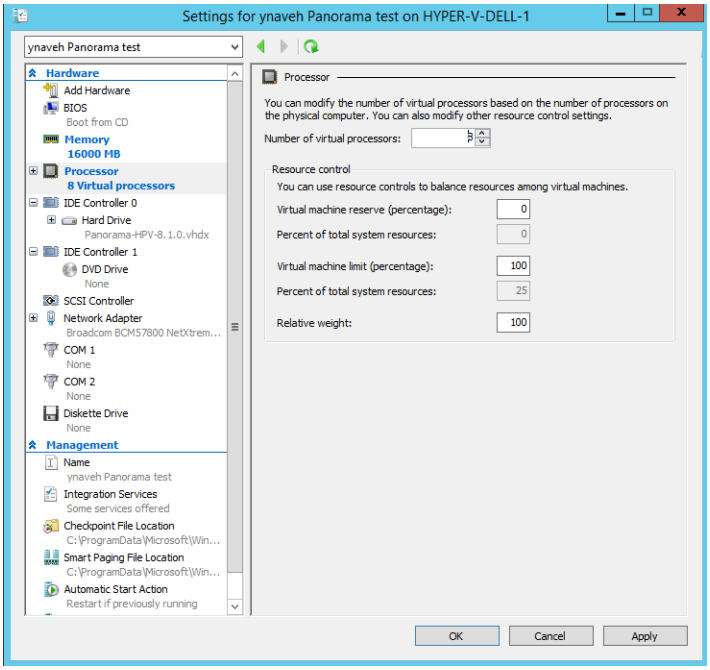
1. **Hardware** (ハードウェア)のリストで**Memory** (メモリ)を選択します。
2. 現在割り当てられている**Startup RAM** (スタートアップ RAM)を編集します。



© 2019 Palo Alto Networks, Inc.

STEP 4 | 割り当てられた Panorama バーチャル アプライアンスの CPU コアを編集します。

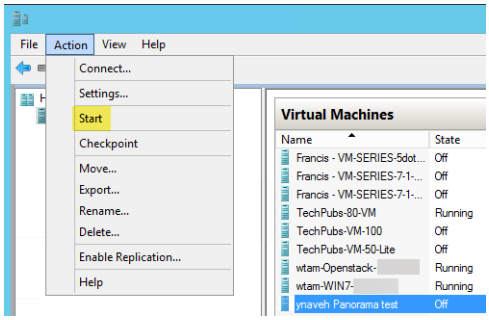
1. **Hardware** (ハードウェア)のリストで**Processor** (プロセッサ)を選択します。
2. 現在割り当てられている**Number of virtual processors** (仮想プロセッサの数)を編集します。



STEP 5 | 割り当て直したメモリおよび CPU コアを**Apply** (適用)します。

STEP 6 | Panorama バーチャル アプライアンスをパワーオンします。

1. **Virtual Machines** (仮想マシン)のリストから Panorama バーチャル アプライアンスのインスタンスを選択します。
2. **Action** (操作) > **Start** (起動)を選択して、バーチャル アプライアンスの電源を入れます。



Panorama バーチャルアプライアンスにシステムディスクを追加する

Panorama バーチャル アプライアンスが、システムのディスク容量を 224GB に拡張し、大規模なデータセットをサポートして、大規模なファイアウォールのデプロイを管理ダイナミック更新などに十分なディスク容量を確保できるようにします。さらに、Panorama バーチャル アプライアンスを Panorama モードで使用して、SD-WAN デプロイメントを管理する場合は、224GB のシステム ディスクにより、管理対象ファイアウォールの状態を監視およびレポートするためのストレージが拡張されます。

- ESXi サーバーに Panorama のシステムディスクを追加する
- Google Cloud Platform 上の Panorama のシステムディスクを追加する

© 2019 Palo Alto Networks, Inc.

ESXi サーバーに *Panorama* のシステムディスクを追加する

224GB のシステムディスクを追加して、デフォルトの 81GB のシステム ディスクを置き換えます。Panorama バーチャル アプライアンスの最小リソース要件については、Panorama バーチャル アプライアンスのセットアップ前提条件を参照してください。

Panorama バーチャル アプライアンス システム ディスクを *81GB* に減らすことはサポートされていません。

STEP 1 | （ベスト プラクティス）Panorama およびファイアウォールの設定の保存およびエクスポート。

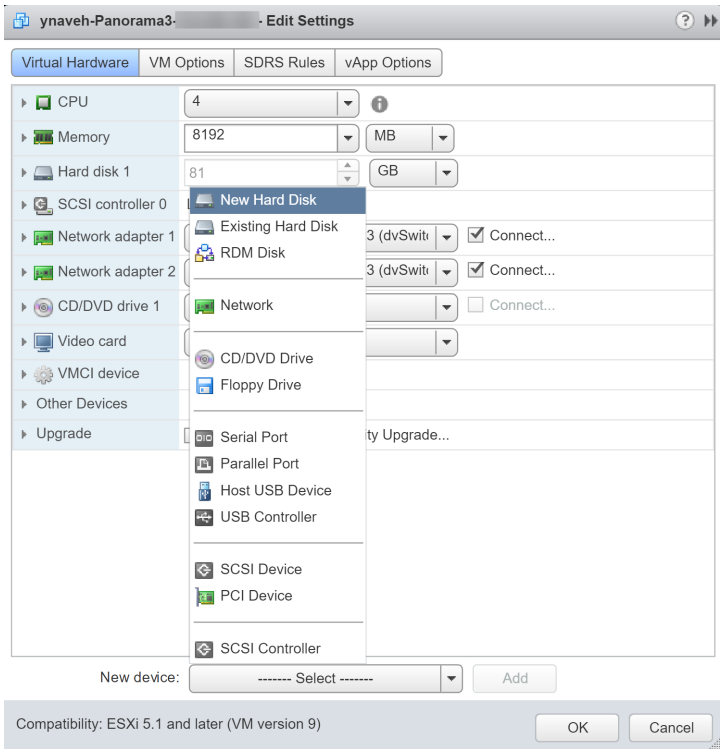
Panorama とファイアウォールの設定を保存してエクスポートし、問題が発生した場合に Panorama を復元できるようにします。

STEP 2 | VMware vSphere Client にアクセスして、Panorama バーチャル アプライアンスに移動します。

STEP 3 | Panorama バーチャル アプライアンスを右クリックし、**Power**（電源）> **Power Off**（電源オフ）を選択します。

STEP 4 | 224GB の新しいシステム ディスクを追加します。

1. Panorama バーチャル アプライアンスを右クリックし、**Edit Settings**（設定変更）を選択します。
2. **New Device**（新規デバイス）に **New Hard Disk**（新規ハードディスク）を選択し、新規デバイスを**Add**（追加）します。
3. 224GB の新規ハードディスクを設定し、 **OK** をクリックします。



STEP 5 | Panorama バーチャル アプライアンスを右クリックし、**Power**（電源）> **Power On**（電源オン）を選択します。

© 2019 Palo Alto Networks, Inc.

Panorama が新規システム ディスクを初期化するのに、最大 *30* 分かかる場合があります。この間、*Panorama Web* インターフェースと *CLI* は使用できません。

STEP 6 | 古いシステム ディスクから新しいシステム ディスクにディスクデータを移行します。

この例では、新規に追加された sdb というラベルの付いたシステム ディスクに移行しています。

1. Panorama CLI へのログイン.
2. 以下のコマンドを入力して、移行に使用できるシステム ディスクを表示します。

```
admin> request system clone-system-disk target ?
```

3. 以下のコマンドを使用して、ディスク データを新しいシステム ディスクに移行します。

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

ディスクの移行を開始するように求められたら、 **y** と入力します。

移行を開始すると、*Panorama* が再起動し、ディスクの移行が完了するまで少なくとも *20* 分かかります。この間、*Panorama Web* インターフェースと *CLI* は使用できません。

4. Web コンソールからディスクの移行を監視します。Panorama が以下のメッセージを表示して、ディスクの移行が完了したことを確認してから、以下の手順に進みます。

```
==================================
Disk Cloning Utility (Version 1.0)
==================================
SOURCE - Disk sda (82944 MB)
TARGET - Disk sdb (229376 MB)

Gathering disks info
Finished gathering disks info

Preparing disks
Finished preparing disks

Copying data
Finished copying data

Making disk bootable
Finished making disk bootable

Disk cloning procedure completed. Please shutdown the sytem and switch disks..._
```

STEP 7 | 古いシステム ディスクを削除します。

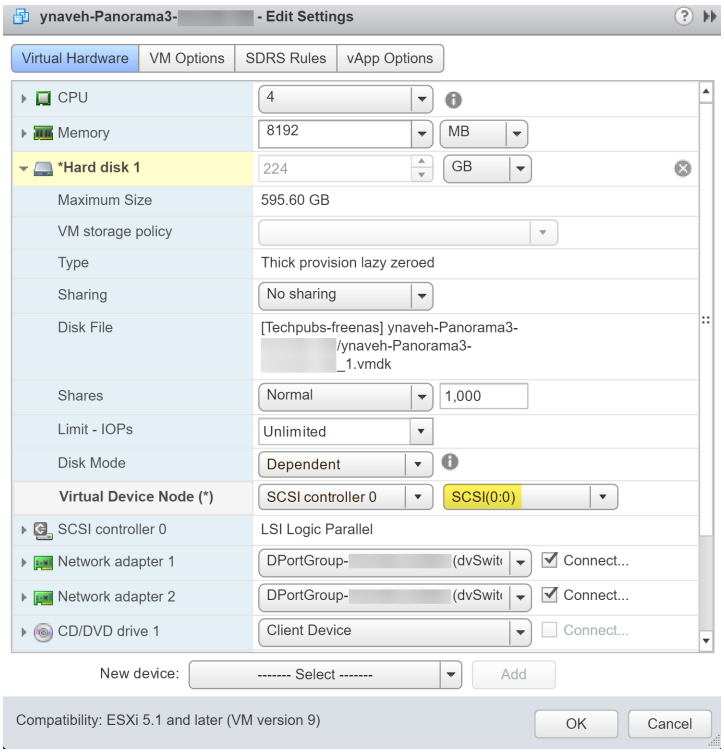
1. VMware vSphere Client にアクセスして、Panorama バーチャル アプライアンスに移動します。
2. Panorama バーチャル アプライアンスを右クリックし、**Power**（電源）> **Power Off**（電源オフ）を選択します。
3. Panorama バーチャル アプライアンスを右クリックし、**Edit Settings**（設定変更）を選択します。
4. 81GB の古いシステム ディスクを削除し、 **OK** をクリックします。

STEP 8 | 新規システム ディスクの仮想デバイス ノードを変更します。

1. 新規システム ディスクの設定オプションを展開します。

© 2019 Palo Alto Networks, Inc.

2. **Virtual Device Node**（仮想デバイス ノード）として **SCSI**（**0**：**0**）を選択します。
3. **OK** をクリックして、設定の変更を保存します。



STEP 9 | Panorama バーチャル アプライアンスを右クリックし、**Power**（電源）> **Power On**（電源オン）を選択します。

STEP 10 | 新規システムディスクへの以降が正常に完了したことを確認します。

1. Panorama CLI へのログイン.
2. 以下のコマンドを入力して、システム ディスクのパーティションを表示します。

   ディスク サイズが増加したことを確認するには、`/dev/root`、`/dev/sda5`、`/dev/sda6`、および`/dev/sda8` のパーティションを追加しなければなりません。

```
admin> show system disk-space
```

```
admin@Panorama-Ynaveh> show system disk-space

Filesystem      Size  Used Avail Use% Mounted on
/dev/root        16G  3.4G   12G  23% /
none            4.0G   60K  4.0G   1% /dev
/dev/sda5        76G  1.8G   71G   3% /opt/pancfg
/dev/sda6        23G  5.0G   17G  24% /opt/panrepo
tmpfs           4.0G  110M  3.8G   3% /dev/shm
cgroup_root     4.0G     0  4.0G   0% /cgroup
/dev/sda8        92G   52G   35G  60% /opt/panlogs
/dev/loop0       50G  7.4G   40G  16% /opt/mongobuffer
tmpfs            12M     0   12M   0% /opt/pancfg/mgmt/ssl/private
```

Google Cloud Platform 上の Panorama のシステムディスクを追加する

224GB のシステムディスクを追加して、デフォルトの 81GB のシステム ディスクを置き換えます。Panorama バーチャル アプライアンスの最小リソース要件については、Panorama バーチャル アプライアンスのセットアップ前提条件を参照してください。

© 2019 Palo Alto Networks, Inc.

STEP 1 | （ベスト プラクティス）Panorama およびファイアウォールの設定の保存およびエクスポート。

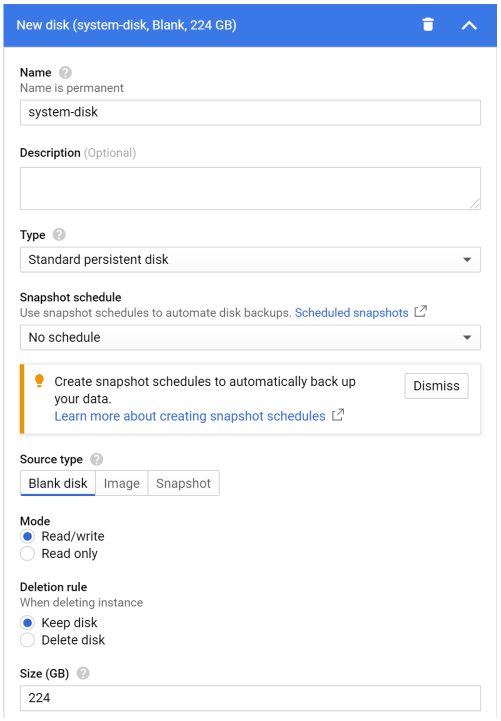
Panorama とファイアウォールの設定を保存してエクスポートし、問題が発生した場合に Panorama を復元できるようにします。

STEP 2 | Google Cloud コンソールにログインします。

STEP 3 | **VM** インスタンスで、Panorama VM インスタンスを **Stop**（停止）します。

STEP 4 | 224GB の新しいシステム ディスクを追加します。

1. Panorama VM インスタンスを選択し、**Edit**（編集）を選択します。
2. **Additional disks**（追加ディスク）のセクションで、**Add new disk**（新規ディスクの追加）を実行します。
3. 224GB の新規ハードディスクを設定し、 **OK** をクリックします。



STEP 5 | **VM** インスタンスで、Panorama VM インスタンスを **Start**（開始）します。

STEP 6 | 古いシステム ディスクから新しいシステム ディスクにディスクデータを移行します。

この例では、新規に追加された sdb というラベルの付いたシステム ディスクに移行しています。

1. Panorama CLI へのログイン.
2. 以下のコマンドを入力して、移行に使用できるシステム ディスクを表示します。

```
admin> request system clone-system-disk target ?
```

3. 以下のコマンドを使用して、ディスク データを新しいシステム ディスクに移行します。

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

ディスクの移行を開始するように求められたら、 **y** と入力します。

© 2019 Palo Alto Networks, Inc.

移行を開始すると、*Panorama* が再起動し、ディスクの移行が完了するまで少なくとも *20* 分かかります。この間、*Panorama Web* インターフェースと *CLI* は使用できません。

4. Panorama CLI にログインを試みて、ディスクの移行を監視します。システム ディスクの移行が完了すると、Panorama 管理サーバはメンテナンス モードになり、メンテナン スモード中に Panorama CLI にログインできるようになります。

STEP 7 | 224GB の新規システム ディスクをアタッチします。

1. **VM** インスタンスで、Panorama VM インスタンスを **Stop**（停止）します。
2. Panorama VM インスタンスを選択し、**Edit**（編集）を選択します。
3. **Additional disks**（追加ディスク）のセクションで、224GB の新規システム ディスクをデタッチします。
4. **Boot Disk**（ブートディスク）のセクションで、81GB の古いシステム ディスクをデタッチします。
5. **Boot Disk**（ブートディスク）のセクションで、**Add item**（アイテムの追加）を実行し、224GB の新規システム ディスクを選択します。
6. 設定の変更を**Save**（保存）します。

STEP 8 | **VM** インスタンスで、Panorama VM インスタンスを **Start**（開始）します。

STEP 9 | 新規システムディスクへの以降が正常に完了したことを確認します。

1. Panorama CLI への口グイン.
2. 以下のコマンドを入力して、システム ディスクのパーティションを表示します。

   ディスク サイズが増加したことを確認するには、`/dev/root`、`/dev/sda5`、`/dev/sda6`、および`/dev/sda8` のパーティションを追加しなければなりません。

```
admin> show system disk-space
```

```
admin@Panorama-Ynaveh> show system disk-space

Filesystem      Size  Used Avail Use% Mounted on
/dev/root        16G  3.4G   12G  23% /
none            4.0G   60K  4.0G   1% /dev
/dev/sda5        76G  1.8G   71G   3% /opt/pancfg
/dev/sda6        23G  5.0G   17G  24% /opt/panrepo
tmpfs           4.0G  110M  3.8G   3% /dev/shm
cgroup_root     4.0G     0  4.0G   0% /cgroup
/dev/sda8        92G   52G   35G  60% /opt/panlogs
/dev/loop0       50G  7.4G   40G  16% /opt/mongobuffer
tmpfs            12M     0   12M   0% /opt/pancfg/mgmt/ssl/private
```

Panorama バーチャル アプライアンスのセットアップの完了

「Panorama バーチャル アプライアンスの初期設定の実行」が完了した後、追加設定を行うために以下のタスクを続けて行います。

- Panorama サポート ライセンスのアクティベーション
- Panorama バーチャル アプライアンスがインターネットに接続している時のファイアウォール管理ライセンスのアクティベーション/取得
- Panorama のコンテンツ更新とソフトウェア更新のインストール
- Panorama 管理インターフェイスへのアクセスおよびナビゲート
- Panorama への管理アクセスのセットアップ
- ファイアウォールの管理

© 2019 Palo Alto Networks, Inc.

M-Series アプライアンスのセットアップ

M-600、M-500、M-200 アプライアンスは、管理専用モード (ローカル ログ収集のない Panorama 管理サーバー) 、Panorama モード (Panorama 管理サーバーとしてローカル ログ収集) またはログ コレクタ モード (専用ログ コレクタとして) で実行できる高性能ハードウェアアプライアンスです。これらのアプライアンスには複数のインターフェイスがあり、ファイアウォール管理や ログ収集など、さまざまな Panorama サービスに割り当てることができます。アプライアンスをセットアップする前に、セキュリティを最適化し、ネットワーク セグメンテーション (大規模デプロイ環境) を実現して、Panorama サービスのトラフィックを負荷分散するようにインターフェイスを設定する方法を検討してください。

- M-Series アプライアンス インターフェイス
- M-Series アプライアンスの初期設定
- M-Series のセットアップの概要
- M-Series アプライアンスをログ コレクタとしてセットアップ
- M-Series アプライアンスのストレージの拡張
- 複数のインターフェイスを使用するように Panorama を設定

M-Series アプライアンス インターフェイス

Panorama M-600、M-500、M-200、 M-100 アプライアンスには、管理対象ファイアウォールや Panorama 管理者のクライアント システムなど、その他のシステムと通信するためのインターフェイスがあります。Panorama はこれらのシステムと通信して、デバイス (ファイアウォール、ログ コレクタ、WildFire アプライアンスとアプライアンス クラスタ) の管理、ログの収集、コレクタ グループとの通信、デバイスへのソフトウェア更新とコンテンツ更新のデプロイ、Panorama への管理アクセスの提供など、さまざまなサービスを実行します。Panorama はデフォルトで、これらすべてのサービスに管理 (MGT) インターフェイスを使用します。ただし、MGT インターフェイスを管理アクセスに予約し、別個のインターフェイスをその他のサービス専用にして、セキュリティを高めることができます。複数のサブネットワークがあってログ トラフィックが多い大規模ネットワークでは、デバイス管理と ログ収集に複数のインターフェイスを使用すると、ネットワークのセグメント化と負荷分散も可能になります (数のインターフェイスを使用するように Panorama を設定するを参照) 。

Panorama サービスをさまざまなインターフェイスに割り当てるときには、MGT インターフェイスのみによって Panorama への管理アクセスが可能になり、設定タスクや監視タスクができるようになることに注意してください。アプライアンスの初期設定を実行する時に任意のインターフェイスをその他のサービスに割り当てることができます。これらのインターフェイスのケーブル取り付け箇所については、M-Series アプライアンス ハードウェアのリファレンス ガイドに記載があります。M-100 アプライアンスでは、次のすべてのインターフェイスで 1Gbps のスループットがサポートされます : MGT、Eth1、Eth2、および Eth3。M-500 アプライアンスでは、これらのインターフェイスに加えて、Eth4 と Eth5 のインターフェイスで 10Gbps のスループットがサポートされます。

M-Series アプライアンスは、インターフェイスを集約するための *LACP* (*Link Aggregation Control Protocol*) をサポートしていません。

サポートされるインターフェイス

インターフェイスを使用してデバイスの管理、ログ収集、コレクタ グループ通信、ライセンスおよびソフトウェアの更新を行えます。ネットワークのセグメント化の詳細については、複数のインターフェイスを使用するように Panorama を設定を参照してください。

© 2019 Palo Alto Networks, Inc.

インターフェイス	最高速度	M-600 アプライアンス	M-500アプライアンス	M-200アプライアンス
管理（MGT）	1Gbps	✓	✓	✓
Ethernet 1 (Eth1)	1Gbps	✓	✓	✓
Ethernet 2（eth2）	1Gbps	✓	✓	✓
Ethernet 3（eth3）	1Gbps	✓	✓	✓
Ethernet 4（eth4）	10Gbps	✓	✓	—
Ethernet 5（eth5）	10Gbps	✓	✓	—

ロギング レート

すべての M-Series アプライアンス モデルのロギング レートを確認します。以下にリストされたロギング レートを達成するには、M-Series アプライアンスがコレクタ グループ内の単一のログコレクタである必要があり、M-Series モデルのすべてのロギング ディスクをインストールする必要があります。例えば、M-500 アプライアンスで 30,000 ログ/秒を達成するには、1TB または 2TB のディスクで 12 のロギング ディスクすべてをインストールする必要があります。

モデルの能力および機能	M-600 アプライアンス	M-500アプライアンス	M-200アプライアンス
管理専用モードでの Panorama の最大ロギング レート	ローカル ログ ストレージはサポートされていません		
Panorama モードでの Panorama の最大ロギング レート	25,000 ログ/秒	20,000 ログ/秒	10,000 ログ/秒
ログ コレクタ モードでの Panorama の最大ロギング レート	50,000 ログ/秒	30,000 ログ/秒	28,000 ログ/秒
アプライアンス上の最大ログ保存容量	48TB（12 個の 8TB RAID ディスク）	• 24TB（24 個の 2TB RAID ディスク） • 12TB（24 個の 1TB RAID ディスク）	16TB（4 個の 8TB RAID ディスク）
アプライアンス上のデフォルト ログ保存容量	16TB（4 個の 8TB RAID ディスク）	4TB（4 個の 2TB RAID ディスク）	16TB（4 個の 8TB RAID ディスク）
アプライアンス上の SSD 容量（M-Series アプライ	240GB	240GB	240GB

© 2019 Palo Alto Networks, Inc.

モデルの能力および機能	M-600 アプライアンス	M-500アプライアンス	M-200アプライアンス
アンスが生成するログに使用）			
NFSを伴うログ ストレージ	利用不可		

M-Series アプライアンスの初期設定

Panorama のデフォルトの IP アドレスは 192.168.1.1、ユーザー名/パスワードは admin/admin です。セキュリティの理由により、他の設定タスクを続行する前に、これらの設定を変更する必要があります。これらの初期設定タスクは、管理（MGT）インターフェイスから実行するか、 M-600、M-500、または M-200 アプライアンスのコンソール ポートに直接接続して実行する必要があります。

10GB インターフェースのログ コレクタ モードで *M-Series* アプライアンスを設定中の場合、*10GB* インターフェースを `Up` として表示するには、この設定手順全体を完了する必要があります。

STEP 1 | ネットワーク管理者から、インターフェイスとサーバーに関する必要な情報を入手します。

- 構成を予定している各インターフェイス（MGT、Eth1、Eth2、Eth3、Eth4、Eth5）について、IP アドレス、ネットマスク（IPv4 の場合）あるいはプレフィックス長（IPv6 の場合）、およびデフォルト ゲートウェイを収集します。必須は、MGT インターフェイスのみです。

  MGT インターフェイスでは、これらすべての設定を指定することをお薦めします。これらの設定の一部の値が省略された場合（デフォルト ゲートウェイなど）、以降の設定変更ではコンソール ポート経由でしか *Panorama* にアクセスできなくなります。これらの設定すべてを指定するまで、他のインターフェイスの設定はコミットできません。

  Panorama 管理サーバーとしてアプライアンスを使用する予定である場合は、Panorama の管理のみに MGT インターフェイスを使用し、デバイスの管理、ログの収集、コレクタ グループとの通信、デバイスへの更新のデプロイにはその他のインターフェイスを使用することをお薦めします（「M-Series アプライアンスのインターフェイス」を参照）。
- DNS サーバーの IP アドレスを収集します。

STEP 2 | コンピュータからM-Seriesアプライアンスにアクセスします。

1. 以下のいずれかの方法で M-Series アプライアンスに接続します。
   - コンピュータからM-Seriesアプライアンスのコンソール ポートにシリアル ケーブルを接続し、ターミナル エミュレーション ソフトウェア（9600-8-N-1）を使用して接続します。
   - コンピュータからM-Seriesアプライアンスの MGT ポートに RJ-45 Ethernet ケーブルを接続します。ブラウザで、https://192.168.1.1 に移動します。この URL にアクセスできるようにするには、コンピュータの IP アドレスを、192.168.1.0 ネットワークでのアドレス（192.168.1.2 など）に変更しなければならない場合があります。
2. 指示された場合、デフォルトのユーザー名とパスワード（admin/admin）を使用してアプライアンスにログインする必要があります。アプライアンスが初期化を開始します。

STEP 3 | デフォルトの管理パスワードを変更します。

PAN-OS 9.0.4 で開始するときは、事前定義済みのデフォルトの管理者パスワード（*admin / admin*）は、デバイスへの初回のログイン時に変更しなければなりません。新しいパスワードは *8* 文字以上で、*1* 文字以上の小文字と *1* 文字以上の大文字、および数字または特殊文字 *1* 字を含める必要があります。

© 2019 Palo Alto Networks, Inc.

パスワードの強度を高めるために、必ずパスワード強度のベスト プラクティスに従い、パスワードの複雑性の設定を確認してください。

1. Web インターフェイスの左下にある **admin**（管理者）リンクをクリックします。
2. **Old Password**（以前のパスワード）、**New Password**（新しいパスワード）、および **Confirm New Password**（新しいパスワードの確認）を入力して**OK**をクリックします。新しいパスワードを安全な場所に保存します。



*MGT*インターフェイスの安全性を維持するには、*Minimum Password Complexity*（パスワード複雑性）を設定（*Panorama* > *Setup*（セットアップ）> *Management*（管理）を選択）し、管理者がパスワードを変更する必要がある間隔を指定します。

STEP 4 | Panorama の管理、デバイスの管理、ログの収集、コレクタ グループとの通信、デバイスへの更新のデプロイに使用するインターフェイスごとに、ネットワーク アクセス設定を構成します。

1. **Panorama** > **Setup**（セットアップ）> **Interfaces**（インターフェイス）を選択し、インターフェイス名をクリックします。
2. （MGT 以外のインターフェイスのみ）インターフェイスを **Enable**（有効化）します。
3. Panorama が使用するインターフェイスごとに、ネットワーク アクセス設定を編集します。MGT インターフェイスのみ必須になります。Eth1、Eth2、Eth3、Eth4、Eth5 インターフェイスは任意項目であり、M-Series アプライアンスを Panorama 管理サーバーとして使用する予定である場合のみ使用します。
   1. ネットワークの IP プロトコルに合わせて、以下のいずれか、あるいは両方のフィールドを入力します。

      IPv4 — **Public IP address**（パブリック **IP** アドレス）、 **IP address**（**IP** アドレス）、**Netmask**（ネットマスク）、および **Default Gateway**（デフォルト ゲートウェイ）

      ファイアウォールがプライベート *IP* アドレス（*NAT*）に変換されるパブリック *IP* アドレスを使って *Panorama* 管理サーバーに接続する場合、*Public IP Address (*パブリック *IP* アドレス*)*フィールドにパブリック *IP* を、*IP Address (IP* アドレス*)*フィールドにプライベート *IP* を入力し、両方のアドレスをファイアウォールにプッシュします。

      IPv6 — **IPv6 Address/Prefix Length**（**IPv6** アドレス/プレフィックス長）および **Default IPv6 Gateway**（デフォルト **IPv6** ゲートウェイ）
   2. インターフェイスでサポートされるデバイス管理サービスを選択します。

      Device Management and Device Log Collection（デバイス管理およびデバイス ログ収集）— 1 つ以上のインターフェイスを割り当てることができます。

      Collector Group Communication（コレクタ グループ通信）— インターフェイスを 1 つのみ割り当てることができます。

      Device Deployment（デバイスのデプロイ）（ソフトウェア更新とコンテンツ更新）— インターフェイスを 1 つのみ割り当てることができます。
   3. （任意）インターフェイスでサポートされるネットワーク接続サービスを選択します。

      （*MGT* インターフェイスのみ）*Telnet* と *HTTP* を無効にします。これらのサービスはプレーンテキストを使用するため、他のサービスに比べて安全性に劣ります。
   4. **OK** をクリックして変更内容を保存します。

STEP 5 | ホスト名、タイム ゾーン、および一般設定を設定します。

© 2019 Palo Alto Networks, Inc.

1. **[Panorama]** > **[セットアップ]** > **[管理]** の順に選択し、**[一般設定]** を編集します。
2. Panorama と管理対象ファイアウォールのクロックを、同じタイム ゾーン（**GMT** または **UTC** など）を使用するように合わせます。Cortex Data Lake を使用する予定の場合、NTP を設定して、Panorama が Cortex Data Lake との同期を維持できるようにします。

   ファイアウォールはログを生成する際に、Panoramaはログを受信する際に、タイムスタンプを記録します。タイム ゾーンを合わせることにより、タイムスタンプが確実に同期され、Panorama でのログのクエリとレポートの生成プロセスで調和が保たれるようにします。
3. サーバーの**Hostname**（ホスト名）を入力します。Panorama では、これをアプライアンスの表示名/ラベルとして使用します。たとえば、CLI プロンプトにこの名前が表示されます。また、**[Panorama]** > **[管理対象コレクタ]** ページでアプライアンスを管理対象コレクタとして追加する場合に、**[コレクタ名]** フィールドに表示されます。
4. （任意）**Latitude**（経度）と **Longitude**（緯度）を入力し、その M-Series アプライアンスが世界地図上の正確な場所に配置されるようにします。これらの値は、 **App Scope** > **Traffic Maps**(アプリケーション スコープ > トラフィック マップ) および **App Scope** > **Threat Maps**(アプリケーション スコープ > 脅威マップ) で使用されます。
5. **OK** をクリックして、入力項目を保存します。

STEP 6 | DNSサーバーおよびPalo Alto Networks更新サーバーを構成します。

1. **[Panorama]** > **[セットアップ]** > **[サービス]** の順に選択し、設定を編集します。
2. **Primary DNS Server**（プライマリ **DNS** サーバー）および（任意で）**Secondary DNS Server**（セカンダリ **DNS** サーバー）の IP アドレスを入力します。
3. **Update Server**（更新サーバー）のURL or static address（URL または固定アドレス）を入力します（デフォルト設定では updates.paloaltonetworks.com）。

   Panorama がソフトウェアまたはコンテンツ パッケージをダウンロードする *Update Server*（更新サーバー）に信頼できる認証局によって署名された *SSL* 証明書があることを、*Panorama* によって検証する場合は、*Verify Update Server Identity*（更新サーバー *ID* の確認）を選択します。このオプションを有効にすると、*Panorama* 管理サーバーと*Update Server (*更新サーバー*)*の間の通信におけるセキュリティ レベルが向上します。
4. **OK** をクリックして、入力項目を保存します。

STEP 7 | 設定の変更をコミットします。

Commit（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

アプライアンスを *Panorama* 管理サーバーとして使用する予定であり、*MGT* 以外のインターフェイスを構成している場合、管理対象コレクタの設定を行う際にそれらのインターフェイスを *Device Log Collection*（デバイス ログ収集）あるいは *Collector Group Communication*（コレクタ グループ通信）機能に割り当てる必要があります。その後、インターフェイスを稼働できるようにするためには、その管理対象コレクタ用のコレクタ グループの設定を行い、コレクタ グループのコミットを実行する必要があります。

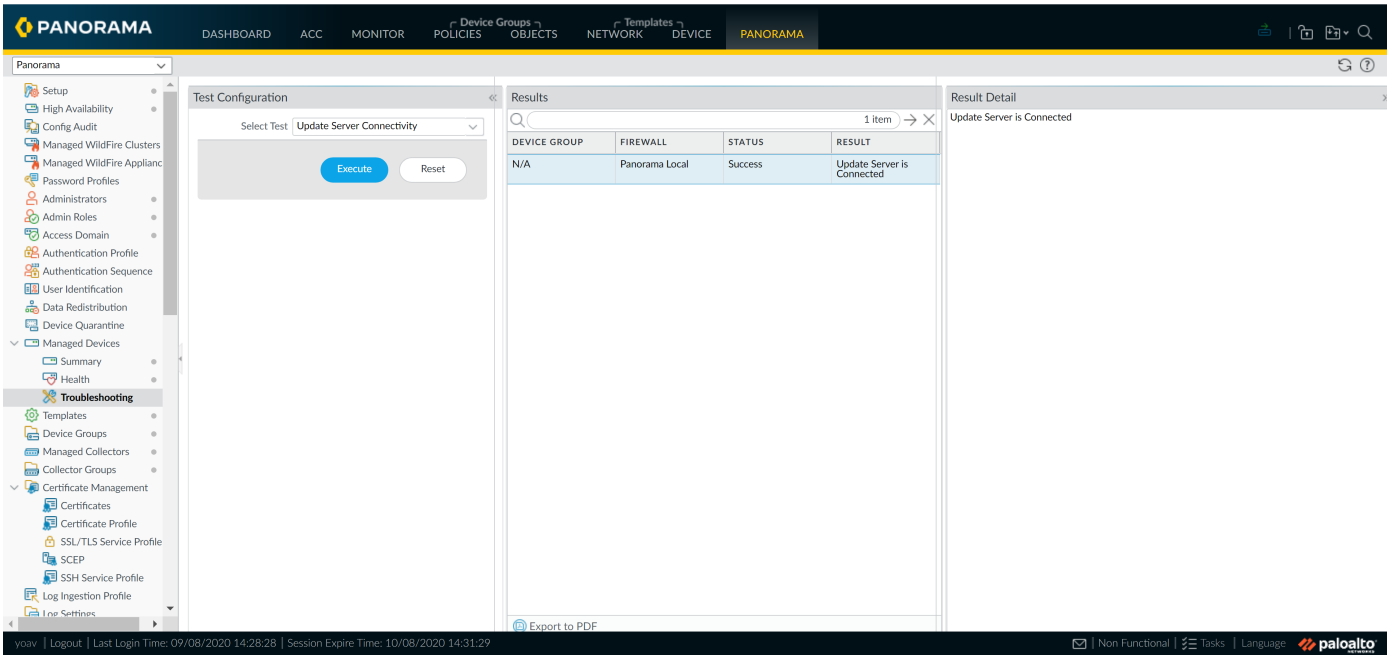
STEP 8 | Palo Alto Networks 更新サーバーなどの、Panorama管理に必要な外部サービスへのネットワーク アクセスを確認します。

1. 以下のいずれかの方法で M-Series アプライアンスに接続します。
   - お使いのパソコンから M-Series アプライアンスのコンソール ポートにシリアル ケーブルを接続します。次に、ターミナル エミュレーション ソフトウェア（9600-8-N-1）を使って接続を行います。

© 2019 Palo Alto Networks, Inc.

- PuTTY などの端末エミュレーション ソフトウェアを使用して、初期設定時に M-Series アプライアンスの MGT インターフェイス用に指定した IP アドレスに対して SSH セッションを開きます。

2. 指示に従って CLI にログインします。初期設定時に指定したパスワードとデフォルトの admin アカウントを使用します。
3. 以下の例に示すように、更新サーバー接続性テストを使用して、Palo Alto Networks 更新サーバーへのネットワーク接続を検証します。
    1. **Panorama** > **Managed Devices** (管理対象デバイス) > **Troubleshooting** (トラブルシューティング) を選択し、Select Test (テストを選択) ドロップダウンから **Updates Server Connectivity** (サーバー接続の更新) を選択します。
    2. 更新サーバー接続性テストを **Execute** (実行) します。



4. 以下のCLI コマンドを実行して、更新サーバーからPanoramaのサポート資格に関する情報を取得します。

```
admin> request support check
```

接続されている場合、更新サーバーはPanoramaのサポート ステータスを伴うレスポンスを返します。Panoramaが登録されていないため、更新サーバーは次のメッセージを返します。

```
Contact Us
https://www.paloaltonetworks.com/company/contact-us.html
Support Home
https://www.paloaltonetworks.com/support/tabs/overview.html
Device not found on this update server
```

STEP 9 | 次のステップ...

1. Panorama の登録とライセンスのインストールを行います。
2. Panorama のコンテンツ更新とソフトウェア更新のインストールを行います。

*MGTインターフェイス全体のHTTPSトラフィックを保護するために、Panoramaが使用する*デフォルトの証明書を交換*することが推奨されます。*

© 2019 Palo Alto Networks, Inc.

M-Series のセットアップの概要

M-Series アプライアンスのセットアップでは、以下の手順に従います。

- 管理専用モードの M-Series アプライアンスのセットアップ
- Panorama モードの M-Series アプライアンスのセットアップ
- ログ コレクタ モードの M-Series アプライアンスのセットアップ

管理専用モードの *M-Series* アプライアンスのセットアップ

STEP 1 | M-Series アプライアンスをラック マウントします。方法については、M-Series アプライアンスのハードウェア リファレンス ガイドを参照してください。

STEP 2 | M-Series アプライアンスの初期設定

STEP 3 | Panorama の登録とライセンスのインストール

STEP 4 | Panorama のコンテンツ更新とソフトウェア更新のインストール

STEP 5 | 管理専用モードに変更します。

1. Panorama CLI へのログインを行います。
2. Panorama モードから管理専用モードに切り替えます。

   request system system-mode management-only
3. **y**を入力して、モード変更を確定します。Panorama 管理サーバーが再起動します。再起動処理によってターミナル エミュレーション ソフトウェアのセッションが終了した場合は、Panorama 管理サーバーに再接続し、Panorama のログイン画面を表示します。

   CMS Login（CMSログイン）画面が表示された場合は、Panorama 管理サーバーが再起動をまだ完了させていないということです。入力を指示されたら、ユーザー名やパスワードは入力せずに Enter キーを押します。
4. CLI に再度ログインします。
5. 管理専用モードへの切り替えが正しく完了したことを、次のコマンドで確認します。

   show system info | match system-mode

   モード変更が正しく完了した場合、出力は次のようになります。

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

STEP 6 | Panorama への管理アクセスのセットアップ

STEP 7 | ファイアウォールの管理

STEP 8 | ログ収集の管理

Panorama モードの *M-Series* アプライアンスのセットアップ

STEP 1 | M-Series アプライアンスをラック マウントします。方法については、M-Series アプライアンスのハードウェア リファレンス ガイドを参照してください。

STEP 2 | M-Series アプライアンスの初期設定を行います。

STEP 3 | Panorama の登録とライセンスのインストールを行います。

STEP 4 | Panorama のコンテンツ更新とソフトウェア更新のインストールを行います。

© 2019 Palo Alto Networks, Inc.

STEP 5 | 各アレイを設定します。RAID ディスクをロギングに使用できるようにするには、この作業が必要になります。必要に応じて、ディスクを追加して、M-Series アプライアンスのストレージの拡張を行えます。

STEP 6 | Panorama への管理アクセスをセットアップします。

STEP 7 | ファイアウォールを管理します。

STEP 8 | ログ収集を管理します。

ログ コレクタ モードの *M-Series* アプライアンスのセットアップ

STEP 1 | M-Series アプライアンスをラック マウントします。方法については、M-Series アプライアンスのハードウェア リファレンス ガイドを参照してください。

STEP 2 | M-Series アプライアンスの初期設定

STEP 3 | Panorama の登録とライセンスのインストール

STEP 4 | Panorama のコンテンツ更新とソフトウェア更新のインストール

STEP 5 | ステップ 各アレイの設定を参照してください。RAID ディスクをロギングに使用できるようにするには、この作業が必要になります。必要に応じて、ディスクを追加して、M-Series アプライアンスのストレージの拡張を行えます。

STEP 6 | M-Series アプライアンスをログ コレクタとしてセットアップ

STEP 7 | ログ収集の管理

M-Series アプライアンスをログ コレクタとしてセットアップ

ログ収集を行う専用のアプライアンスが必要な場合は、M-200、M-500、または M-600 アプライアンスをログ コレクタ モードで設定します。そのためにはまず、Panorama モードでアプライアンスの初期設定を行います。これには、ライセンシング、ソフトウェアおよびコンテンツ更新のインストール、管理（MGT）インターフェイスの設定といった作業が伴います。その後で M-Series アプライアンスをログ コレクタ モードに切り替え、ログ コレクタの設定を完了させます。さらに、ログ収集やコレクタ グループ通信に MGT インターフェイスの代わりに専用の M-Series アプライアンス インターフェイス（推奨）を使用する場合、まずは Panorama 管理サーバー用のインターフェイスを設定し、次にそれに対してログ コレクタ用の設定を行い、さらに Panorama のコミットを実行した後でコレクタ グループのコミットを行う必要があります。

新しい M-Series アプライアンスをログ コレクタとしてセットアップする、あるいはすでに Panorama 管理サーバーとしてデプロイされている既存の M-Series アプライアンスを切り替える場合は、以下の作業を行います。

10GB インターフェースのログ コレクタ モードで *M-Series* アプライアンスを設定中の場合、*10GB* インターフェースを *Up* として表示するには、この設定手順全体を完了する必要があります。

M-Series アプライアンスを *Panorama* モードからログ コレクタ モードに切り替えると、アプライアンスが再起動し、ローカル ログ コレクタが削除され、管理アクセス設定を除くすべての設定と既存のログ データが削除されます。また、モードを変えることによりライセンス、ソフトウェア更新、コンテンツ更新が削除されることはありません。

© 2019 Palo Alto Networks, Inc.

STEP 1 | まだ作業を行っていない場合は、ログ コレクタを管理する Panorama 管理サーバーをセットアップします。

以下のいずれかの作業を行います。

- Panorama バーチャル アプライアンスのセットアップ
- M-Series アプライアンスのセットアップ

STEP 2 | Panorama 管理サーバーの管理 IP アドレスを控えておきます。

Panorama を高可用性（HA）設定でデプロイしている場合、それぞれの HA ピアの IP アドレスが必要になります。

1. Panorama 管理サーバーの Web インターフェイスにログインします。
2. **Panorama** > **Setup**（セットアップ）> **Management**（管理）を選択し、管理インターフェイスの設定を確認して単独（非 HA）あるいはアクティブ（HA）Panorama の **IP Address**（**IP** アドレス）を控えておきます。
3. HA デプロイメントの場合は、**Panorama** > **High Availability**（高可用性）の順に選択して Setup（セットアップ）セクションを確認し、パッシブ Panorama の **Peer HA IP Address**（ピア **HA IP** アドレス）を控えておきます。

STEP 3 | 専用のログ コレクタとして機能する M-Series アプライアンスをセットアップします。

すでにこのアプライアンスを Panorama 管理サーバーとしてデプロイしている場合は、MGT インターフェイスがすでに設定されており、ライセンスおよび更新ファイルがすでにインストールされているため、このステップを飛ばして構いません。

ログ コレクタ モードの M-Series アプライアンスには設定タスクを行うための Web インターフェイスが備わっておらず、CLI しかありません。そのため、M-Series アプライアンスでモードを変更する前に、Panorama モードで Web インターフェイスを使用して次の作業を行います。

1. M-Series アプライアンスの初期設定を行います。
2. Panorama の登録とライセンスのインストールを行います。
3. Panorama のコンテンツ更新とソフトウェア更新のインストールを行います。

STEP 4 | M-Series アプライアンスの CLI にアクセスします。

1. 以下のいずれかの方法で M-Series アプライアンスに接続します。
   - お使いのパソコンから M-Series アプライアンスのコンソール ポートにシリアル ケーブルを接続します。次に、ターミナル エミュレーション ソフトウェア（9600-8-N-1）を使って接続を行います。
   - PuTTY などの端末エミュレーション ソフトウェアを使用して、初期設定時に M-Series アプライアンスの MGT インターフェイス用に指定した IP アドレスに対して SSH セッションを開きます。
2. 指示に従って CLI にログインします。初期設定時に指定したパスワードとデフォルトの admin アカウントを使用します。

STEP 5 | Panorama モードからログ コレクタ モードに切り替えます。

1. 次のコマンドを入力して、ログ コレクタ モードに切り替えます。

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

2. **Y**を入力して、モード変更を確定します。M-Series アプライアンスが再起動します。再起動処理によってターミナル エミュレーション ソフトウェアのセッションが終了した場合は、M-Series アプライアンスに再接続し、Panorama のログイン画面を表示します。

© 2019 Palo Alto Networks, Inc.



CMS Login *(CMS*ログイン*)*画面が表示された場合は、ログコレクタが再起動をまだ完了させていないということです。入力を指示されたら、ユーザー名やパスワードは入力せずに *Enter* キーを押します。

3. CLI に再度ログインします。
4. ログ コレクタ モードへの切り替えが正しく完了したことを、次のコマンドで確認します。

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

モード変更が正しく完了した場合、出力は次のようになります。

```
system-mode: logger
```

STEP 6 | ロギング用ディスクを RAID1 ペアとして設定します。

すでにこのアプライアンスを Panorama 管理サーバーとしてデプロイしている場合は、ディスク ペアの設定が終了して利用できる状態になっているため、このステップを飛ばして構いません。



ドライブの設定には、ドライブのデータ量に応じて数分から *2*、*3* 時間かかります。

1. どのディスク ペアが設定時に M-Series アプライアンスの RAID ペアとして存在しているのかを確認します。

```
> show system raid detail
```

残りの各ステップを実行し、`present` 状態のディスクを持つそれぞれのディスク ペアを設定します。この例ではディスク ペア A1/A2 を使用します。

2. ペアに最初のディスクを追加するには、次のコマンドを入力し、さらにリクエストの確認を促されたら**y**を入力します。

```
> request system raid add A1
```

次のディスクをペアに追加する前に、処理が完了するのを待ちます。RAID 設定の進行状況をモニターするには、次のコマンドを再び入力します。

```
> show system raid detail
```

最初のディスクの処理が完了したら、ディスク ペアのステータスが `Available` かつ `degraded` であると出力されます。

3. ペアに 2 つ目のディスクを追加します。

```
> request system raid add A2
```

4. ディスクのセットアップが完了したことを確認します。

```
> show system raid detail
```

2 つ目のディスクの処理が完了したら、ディスク ペアのステータスが `Available` かつ `clean` であると出力されます。

© 2019 Palo Alto Networks, Inc.

```
Disk Pair A      Available
Status        clean
```

STEP 7 | ログ コレクタおよび Panorama 管理サーバー間の接続を有効にします。

ログコレクタのCLIで次のコマンド（適宜、*<IPaddress1>*は単独（非HA）あるいはアクティブ（HA）PanoramaのMGTインターフェイスのもの、*<IPaddress2>*はパッシブ（HA）PanoramaのMGTインターフェイスのもの）を入力します。

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

STEP 8 | ログ コレクタのシリアル番号を控えておきます。

Panorama 管理サーバーでログ コレクタを管理対象のコレクタとして追加する際、このシリアル番号が必要になります。

1. ログ コレクタの CLI で以下のコマンドを入力し、シリアル番号を表示します。

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

2. シリアル番号を控えておきます。

STEP 9 | ログ コレクタを管理対象のコレクタとして Panorama 管理サーバーに追加します。

1. **Panorama** > **Managed Collectors**(Panorama > 管理対象コレクタ) の順に選択し、管理対象コレクタを**Add** (追加)します。
2. **General**（全般）設定で、ログ コレクタについて記録したシリアル番号（**Collector S/N**（コレクタ シリアル番号））を入力します。
3. **Panorama Server IP**（**Panorama** サーバー **IP**）フィールドに、単独（非 HA）あるいはアクティブ（HA）Panorama の IP アドレスまたは FQDN を入力します。HA デプロイメントの場合、**Panorama Server IP 2**（**Panorama** サーバー **IP 2**）フィールドに、パッシブ Panorama ピアの IP アドレスあるいは FQDN を入力します。

   これらの IP アドレスは、**Device Management and Device Log Collection**（デバイス管理およびデバイス ログ収集）サービスを有効にした Panorama インターフェイスを指定する必要があります。デフォルトでは、これらのサービスは MGT インターフェイスでのみ有効です。ただし、Panorama 管理サーバーである M-Series アプライアンスのセットアップを実行したときに他のインターフェイスでこれらのサービスを有効にしている場合もあります。
4. **Interfaces**（インターフェイス）を選択し、**Management**（管理）をクリックした後、ネットワークの IP プロトコルに応じて MGT インターフェイス用に次のフィールドのセットのうちいずれか、あるいは両方の設定を行います。
   - IPv4 — **IP Address**（**IP** アドレス）、**Netmask**（ネットマスク）、および **Default Gateway**（デフォルト ゲートウェイ）
   - IPv6 — **IPv6 Address/Prefix Length**（**IPv6** アドレス/プレフィックス長）および **Default IPv6 Gateway**（デフォルト **IPv6** ゲートウェイ）
5. **OK** を 2 回クリックして、ログ コレクタに対する変更を保存します。
6. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、Panorama 設定に対して、変更内容を **Commit**（コミット）します。

   このステップを事前に行わなければ、ロギング用ディスクを有効にすることができません。

© 2019 Palo Alto Networks, Inc.

7. **Panorama** > **Managed Collectors**（管理対象コレクタ）で、追加したログ コレクタが表示されていることを確認します。Connected（接続済み）列には、ログ コレクタが Panorama に接続されていることを示すチェック マークが表示されます。更新された接続ステータスがページに表示されるまで、数分かかる場合があります。



この時点では、*Configuration Status*（設定ステータス）列には *Out of Sync*（非同期）、*Run Time Status*（ランタイム ステータス）列には *disconnected*（未接続）が表示されます。コレクタ グループを設定した後で（「コレクタ グループにログ コレクタを割り当てる」ステップを参照）、ステータスが *In Sync*（同期中）および接続済みに変更されます。

STEP 10 | ロギング用ディスクを有効にします。

1. **Panorama** > **Managed Collectors**(Panorama > 管理対象コレクタ) の順に選択し、ログ コレクタを編集します。
2. **Disks**（ディスク）を選択し、各 RAID ディスク ペアを **Add**（追加）します。
3. **OK** をクリックして変更内容を保存します。
4. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、Panorama 設定に対して、変更内容を **Commit**（コミット）します。

STEP 11 | （推奨）Panorama 管理サーバーおよびログ コレクタが **Device Log Collection**（デバイス ログ収集）（ファイアウォールからのログの受信）および **Collector Group Communication**（コレクタ グループ通信）に使用する場合は、**Ethernet1**、**Ethernet2**、**Ethernet3**、**Ethernet4**、**Ethernet5** インターフェイスを設定します。

以前に Panorama 管理サーバーとしてログ コレクタをデプロイし、そのインターフェイスを設定している場合、ログ コレクタ モードに切り替えた（Panorama モードからログ コレクタ モードに切り替えた）ときに、管理アクセス設定を除くすべての設定が削除されているため、設定し直す必要があります。

1. まだ設定していない場合は、Panorama 管理サーバーで各インターフェイスを設定します（MGT インターフェイスを除く）。
   1. **Panorama** > **Setup**（セットアップ）> **Interfaces**（インターフェイス）を選択し、インターフェイス名をクリックします。
   2. *<interface-name>* を選択してインターフェイスを有効化します。
   3. ネットワークの IP プロトコルに合わせて、以下のいずれか、あるいは両方のフィールドを入力します。

      IPv4 — **IP Address**（**IP** アドレス）、**Netmask**（ネットマスク）、および **Default Gateway**（デフォルト ゲートウェイ）

      IPv6 — **IPv6 Address/Prefix Length**（**IPv6** アドレス/プレフィックス長）および **Default IPv6 Gateway**（デフォルト **IPv6** ゲートウェイ）
   4. インターフェイスでサポートされるデバイス管理サービスを選択します。

      Device Management and Device Log Collection（デバイス管理およびデバイス ログ収集）— 1 つ以上のインターフェイスを割り当てることができます。

      Collector Group Communication（コレクタ グループ通信）— インターフェイスを 1 つのみ割り当てることができます。

      Device Deployment（デバイスのデプロイ）（ソフトウェア更新とコンテンツ更新）— インターフェイスを 1 つのみ割り当てることができます。
   5. **OK** をクリックして変更内容を保存します。
2. ログ コレクタで各インターフェイスを設定します（MGT インターフェイスを除く）。

© 2019 Palo Alto Networks, Inc.

1. **Panorama** > **Managed Collectors**(Panorama > 管理対象コレクタ) の順に選択し、ログ コレクタを編集します。
2. **Interfaces**（インターフェイス）を選択してインターフェイスの名前をクリックします。
3. *<interface-name>* を選択してインターフェイスを有効化します。
4. ネットワークの IP プロトコルに合わせて、以下のいずれか、あるいは両方のフィールドを入力します。

   IPv4 — **IP Address**（**IP** アドレス）、**Netmask**（ネットマスク）、および **Default Gateway**（デフォルト ゲートウェイ）

   IPv6 — **IPv6 Address/Prefix Length**（**IPv6** アドレス/プレフィックス長）および **Default IPv6 Gateway**（デフォルト **IPv6** ゲートウェイ）
5. インターフェイスでサポートされるデバイス管理サービスを選択します。

   Device Log Collection（デバイス ログ収集）— インターフェイスを 1 つ以上割り当てることができます。

   Collector Group Communication（コレクタ グループ通信）— インターフェイスを 1 つのみ割り当てることができます。
6. **OK** をクリックして、インターフェイスに対する変更を保存します。

3. **OK** をクリックして、ログ コレクタに対する変更を保存します。
4. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、Panorama 設定に対して、変更内容を **Commit**（コミット）します。

STEP 12 | （任意）デプロイメントで Panorama と管理対象デバイス間の認証にカスタム証明書を使用している場合、カスタム クライアント デバイス証明書をデプロイします。詳細は、「カスタム証明書を使用する認証のセットアップ」を参照してください。

1. **Panorama** > **Certificate Management**（証明書の管理）> **Certificate Profile**（証明書プロファイル）の順に選択し、ドロップダウンから証明書プロファイルを選択するか、**New Certificate Profile**（新しい証明書プロファイル）をクリックして作成します。
2. ログ コレクタの **Panorama** > **Managed Collectors**（管理対象コレクタ）> **Add**（追加）> **Communication**（通信）を選択します。
3. **Secure Client Communication**（保護されたクライアント通信）チェック ボックスをオンにします。
4. Type（タイプ）ドロップダウンからデバイス証明書のタイプを選択します。
   - ローカル デバイス証明書を使用している場合、それぞれのドロップダウン リストから **Certificate**（証明書）および **Certificate Profile**（証明書プロファイル）を選択します。
   - デバイス証明書として SCEP を使用している場合、それぞれのドロップダウンから **SCEP Profile**（**SCEP** プロファイル）および **Certificate Profile**（証明書プロファイル）を選択します。
5. **OK** をクリックします。

STEP 13 | （任意）ログ コレクタで Secure Server Communication（保護されたサーバー通信）を設定します。詳細は、「カスタム証明書を使用する認証のセットアップ」を参照してください。

1. **[Panorama]** > **[管理対象コレクタ]** > **[追加]** > の順に選択します。**Communication**.
2. **Custom Certificate Only**（カスタム証明書のみ）チェック ボックスがオフになっていることを確認します。これにより、カスタム証明書への移行中もすべてのデバイスの管理を続行できます。

   Custom Certificate Only（カスタム証明書のみ）チェック ボックスをオンにしていると、ログ コレクタは事前定義済みの証明書を使用したデバイスからのログを認証せず、受信することができません。
3. **SSL/TLS Service Profile**（**SSL/TLS** サービス プロファイル）ドロップダウンから SSL/TLS サービス プロファイルを選択します。この SSL/TLS サービス プロファイルは、ログ コレクタとログを送信するデバイス間のすべての SSL 接続に適用されます。
4. **Certificate Profile**（証明書プロファイル）ドロップダウンから証明書プロファイルを選択します。

© 2019 Palo Alto Networks, Inc.

5. **Authorize Client Based on Serial Number**（シリアル番号に基づいてクライアントを承認）を選択し、サーバーが管理対象デバイスのシリアル番号と照合してクライアントをチェックするようにします。クライアント証明書では、シリアル番号に基づいて認証するために CN として特殊なキーワード $UDID を設定する必要があります。
6. **Disconnect Wait Time (min)** (切断待機時間 (分)) に、Panorama が管理対象デバイスとの接続を切断して再開するまで待機する分数を入力します。このフィールドはデフォルトで空白であり、範囲は 0 ~ 44,640 分です。

   
   切断待機時間は、新しい設定をコミットするまでカウント ダウンを開始しません。
7. （任意）認証リストを設定します。
   1. Authorization List（承認リスト）で **Add**（追加）をクリックします。
   2. 識別子タイプとして **Subject**（サブジェクト）または **Subject Alt Name**（サブジェクト代替名）を選択します。
   3. 選択したタイプの識別子を入力します。
   4. **OK** をクリックします。
   5. **Check Authorization List**（承認リストのチェック）を選択して認証リストを適用します。
8. **OK** をクリックします。
9. **Commit**（コミット）> **Commit to Panorama**（**Panorama** にコミット）を選択します。

STEP 14 | コレクタ グループにログ コレクタを割り当てます。

1. コレクタ グループの設定ログ コレクタの設定を Panorama と同期し、Eth1、Eth2、Eth3、Eth4、および Eth5 インターフェイス（これらを設定している場合）がログ コレクタ上で稼働できる状態にするには、Panorama のコミットを行い、次にコレクタ グループのコミットを行う必要があります。

   
   単一のコレクタ グループでは、すべてのログ コレクタ、すべての *M-600* アプライアンス、すべての *M-500* アプライアンス、すべての *M-200* アプライアンス、すべての *Panorama* バーチャル アプライアンスは同じ *Panorama* モデルで動作する必要があります。

   
   推奨としては、複数のログ コレクタを *1* つのコレクタ グループに追加する場合、*Enable log redundancy across collectors*（コレクタ間のログ冗長性の有効化）します。このオプションでは、各ログ コレクタのロギング用ディスクの数が同じでなければなりません。
2. **Panorama** > **Managed Collectors** (Panorama > 管理対象コレクタ)を選択し、ログコレクタの構成がPanoramaと同期していることを確認します。

   Configuration Status（設定ステータス）列には In Sync（同期）、Run Time Status（ランタイム ステータス）列には connected（接続済み）が表示されている必要があります。
3. ログ コレクタの CLI にアクセスして次のコマンドを入力し、そのインターフェイスが稼働できる状態になっていることを確認します。

   ```
   > show interface all
   ```

   各インターフェイスが稼働できる状態である場合、`state` が `up` であると出力されます。
4. コレクタ グループにログ コレクタが複数ある場合は、ネットワーク リソースへの接続のトラブルシューティングしてそのログ コレクタが使用する各インターフェイスに対して Ping 接続性テストを実行し、ログ コレクタ同士が通信できることを確認します。`source` IP アドレスについては、いずれかのインターフェイスのログ コレクタを指定します。`host` IP address（ホスト IP アドレス）は、同じコレクタ グループに所属する別のログ コレクタの、対応するインターフェイスを指定します。

© 2019 Palo Alto Networks, Inc.

STEP 15 | 次のステップ...

ログ コレクタがファイアウォール ログを受信できるようにするには：

1. Panorama へのログ転送の設定
2. Panorama へのログ転送の確認

M-Series アプライアンスのストレージの拡張

M-Series アプライアンスの初期設定を行った後、既存のドライブ ペアを容量の大きいドライブにアップグレードするか、ドライブ ペアを空のドライブ ベイに追加することで、ログの保存容量を増やすことができます。例えば、M-500 アプライアンスで既存の 1TB のドライブを 2TB のものにアップグレードするか、空のドライブ ベイ（B1 ~ D2）に 2TB のドライブを追加することができます。

M-Series アプライアンスでは、ディスクで障害が発生した場合のデータ冗長性のために *RAID 1* を活用します。このため、*RAID 1* アレイのドライブのペアは同一にする必要があります。ただし、別々の *RAID 1* アレイでは、ドライブの容量を自由に混在させることができます。例えば、*A1/A2 RAID 1* アレイのドライブは *1TB* ドライブに、*B1/B2 RAID 1* アレイのドライブは *2TB* ドライブにすることができます。

次の表には、M-Series アプライアンスでサポートされるドライブ ベイの最大数およびドライブ容量を示します。

各ドライブ ペア（例えば *A1/A2*）は *RAID 1* アレイなので、合計ストレージ容量は、取り付けたドライブ合計の半分です。例えば、*M-500* アプライアンスのドライブ ベイ *A1/A2* と *B1/B2* に *2TB* ドライブを取り付けた場合、*A1/A2* アレイは合計 *2TB* のストレージを提供して *B1/B2* アレイは *2TB* をさらに提供し、合計で *4TB* になります。

アプライアンス	サポートされるドライブ ベイの数	サポートされるドライブ容量
M-200アプライアンス	4	8TB
M-500アプライアンス	24	1TB または 2TB
M-600 アプライアンス	12	8TB

ログの保存容量を穂保前に、Panoramaのログ保持要件を決定してください。M-Series アプライアンスがサポートするログストレージよりも多く必要な場合、専用ログコレクタを追加するか（Panorama から外部の宛先へのログ転送を設定するを参照）、Panorama から外部の宛先へのログ転送を設定することができます。

構成済みの *M-Series* アプライアンスにドライブを追加する際、ストレージを拡張するために *M-Series* アプライアンスをオフラインにする必要はありません。追加のドライブが構成可能・使用可能になると、*M-Series*アプライアンスは使用可能なそれらすべてのドライブにログを再配信します。このログの再配信処理はバックグラウンドで行われ、*M-Series* アプライアンスのアップタイムおよび可用性には影響しません。しかし、このプロセスは最大ロギング率を低下させます。*Redistribution State* (再配信状態)列（*Panorama* > *Collector Groups*(*Panorama* > コレクタ グループ)）に、処理の進捗状況の割合が表示されます。

- M-Series アプライアンスにドライブを追加

© 2019 Palo Alto Networks, Inc.

- Panorama 7.0.8 以降のバージョンを実行中の M-Series アプライアンスでドライブをアップグレード
- Panorama 7.0.7 以前のバージョンを実行中の M-Series アプライアンスでドライブをアップグレード

M-Series アプライアンスにドライブを追加

STEP 1 | 新しいドライブを適切なドライブ ベイに取り付けます。

ドライブは、次に空いているディスク ベイに順々に追加してください。たとえば、ドライブを B1 と B2 に追加してから、C1 と C2 に追加します。

STEP 2 | M-Series アプライアンスでコマンド ライン インターフェイス (CLI) にアクセスします。

以下のいずれかの方法で M-Series アプライアンスに接続します。

- コンピュータからコンソール ポートにシリアル ケーブルを接続し、ターミナル エミュレーション ソフトウェア (9600-8-N-1) を使用して M-Series アプライアンスに接続します。
- M-Series アプライアンスの IP アドレスに対して SSH (Secure Shell) セッションを開くには、PuTTY などの端末エミュレーション ソフトウェアを使用します。

STEP 3 | ログインを促されたら、アプライアンスにログインします。

デフォルトの管理者アカウントと割り当て済みのパスワードを使用します。

STEP 4 | 各アレイを設定します。

ドライブ上のデータのミラーリングには、ドライブのデータ量に応じて数分から数時間かかります。

以下の例では、ベイ B1 および B2 のドライブを使用しています。

1. 以下のコマンドを入力し、確認を促されたら要求を確認します。

```
> request system raid add B1
> request system raid add B2
```

2. RAID 設定の進行状況をモニターするには、以下のコマンドを使用します。

```
> show system raid detail
```

RAID のセットアップが完了すると、以下の応答が表示されます。

```
Disk Pair A       Available
   Status         clean
   Disk id A1     Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : active sync
   Disk id A2     Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : active sync
Disk Pair B        Available
   Status          clean
   Disk id B1      Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : active sync
```


© 2019 Palo Alto Networks, Inc.

```
   Disk id B2     Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : active sync
```

STEP 5 | アレイのロギングを有効にします。

アレイのロギングを有効にするには、最初に Panorama でアプライアンスを管理対象コレクタとして追加する必要があります。まだ追加していない場合は、管理対象コレクタの設定を参照してください。

1. このログ コレクタを管理している Panorama 管理サーバーの Web インターフェイスにログインします。
2. **Panorama** > **Managed Collectors**(Panorama > 管理対象コレクタ) の順に選択し、ログ コレクタを編集します。
3. **Disks**（ディスク）を選択し、各アレイを **Add**（追加）します。
4. **OK** をクリックして変更内容を保存します。
5. **Commit**（コミット） > **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。
6. **Commit (コミット)** > **Push to Devices (デバイスにプッシュ)**を選択し、さらに Collector Group (コレクタ グループ) を選択して変更内容を**Push (プッシュ)**します。

Panorama 7.0.8 以降のバージョンを実行中の M-Series アプライアンスでドライブをアップグレード

STEP 1 | M-Series アプライアンスでコマンド ライン インターフェイス（CLI）にアクセスします。

以下のいずれかの方法で M-Series アプライアンスに接続します。

- コンピュータからコンソール ポートにシリアル ケーブルを接続し、ターミナル エミュレーション ソフトウェア（9600-8-N-1）を使用して M-Series アプライアンスに接続します。
- M-Series アプライアンスの IP アドレスに対して SSH（Secure Shell）セッションを開くには、PuTTY などの端末エミュレーション ソフトウェアを使用します。

STEP 2 | ログインを促されたら、アプライアンスにログインします。

デフォルトの管理者アカウントと割り当て済みのパスワードを使用します。

STEP 3 | 設置されているドライブの RAID 1 のステータスとして、機能している RAID 1 のアレイが 2 つ以上表示されていることを確認します。アップグレードを行う際に同時にアップグレードできる RAID 1 のアレイは 1 つだけであり、アプライアンスが利用できる RAID 1 のアレイが他に 1 つ以上なければなりません。唯一機能しているアレイを設定から取り除こうとすると、アプライアンスに中止エラーが表示されます。

RAID ステータスを表示するには、以下のコマンドを入力します。

```
> show system raid detail
```

以下は、利用できるアレイが 2 つ（ディスク ペア A およびディスク ペア B）ある M-500 アプライアンスの出力の例です。利用できるアレイが 1 つしかない場合、ドライブをアップグレードする前に、「M-Series アプライアンスにドライブを追加」の説明に従って 2 つ目を追加する必要があります。

```
Disk Pair A                              Available
   Status                                    clean
   Disk id A1                              Present
```


© 2019 Palo Alto Networks, Inc.

```
        model          : ST91000640NS
        size           : 953869 MB
        status         : active sync
    Disk id A2                              Present
        model          : ST91000640NS
        size           : 953869 MB
        status         : active sync
Disk Pair B                              Available
    Status                                   clean
    Disk id B1                             Present
        model          : ST91000640NS
        size           : 953869 MB
        status         : active sync
    Disk id B2                             Present
        model          : ST91000640NS
        size           : 953869 MB
        status         : active sync
```

STEP 4 | 最初に 1TB のドライブを取り外し、2TB のドライブに交換します。

1. RAID 1構成から最初のドライブを取り外すには (この例ではA1)、以下のコマンドを入力し、さらにリクエストの確認を促されたら**y**を入力します。

```
> request system raid remove A1
```

2. ドライブ ベイから最初のドライブを物理的に取り外します。ドライブ ベイ A1 内のドライブ キャリアにある排出ボタンを押し、排出ハンドルを解除します。次にハンドルを手前に倒し、ドライブをスライドさせてアプライアンスから出します。
3. 2TB のドライブをパッケージから出し、先ほど取り外したドライブの隣にある台の上に乗せます。2TB のドライブも同じキャリアに取り付けることになるので、ドライブがどのようにキャリアに取り付けられているのか確認しておきます。
4. 1TB のドライブをキャリアに固定している 4 本のねじを取り外し、ドライブをキャリアから外します。
5. 1TB のドライブから外したのと同じ 4 本のねじを使用して 2TB のドライブをキャリアに取り付け、2TB のドライブと共にキャリアをドライブ ベイ A1 に挿入し直します。
6. 2TB のドライブが認識されることを確認するには、以下のコマンドを入力します。

```
show system raid detail
```

A1 ディスクで正しいモデルとサイズ (約 2TB) が表示されることを確認します。モデルとサイズが正しくない場合、正しいモデルとサイズが表示されるまで、上記のコマンドを再び実行します。

誤ったモデルとサイズがいつまでも表示される場合、以下のコマンドを入力します。

```
request system raid remove A1
```

一度上記のコマンドを実行したら 30 秒待ち、ディスクを取り外して再度取り付け、再び **show system raid detail** コマンドを入力してサイズとモデルを確認します。

STEP 5 | RAID 1 のアレイに取り付けられたままの 1TB のドライブにあるデータを、そのアレイに新たに取り付けた 2TB のドライブにコピーします。

データのコピーには、ドライブのデータ量に応じて数分から数時間かかります。

© 2019 Palo Alto Networks, Inc.

1. ドライブ ベイA2内にある1TBのドライブのデータを、新たにドライブ ベイA1に取り付けた2TBのドライブにコピーするには、以下のコマンドを入力し、さらに指示に従って**y**を入力します。

```
> request system raid copy from A2 to A1
```

2. コピーの進行状況についての状態を表示するには、以下のコマンドを実行します。

```
> show system raid detail
```

RAID の詳細を出力するには、アレイ (この例では A1/A2) が `Available` (利用可能) であると表示されるまでの間、このコマンドを実行し続けます。

ドライブの容量が異なっているため、この時点では *A2* が *`not in use`* (未使用) であると表示されます。

STEP 6 | RAID 1 のアレイの 2 つ目のドライブを 2TB のものにアップグレードします。

1. RAID 1 のアレイ設定から 2 つ目の 1TB のドライブを取り外します (現在の例の場合はドライブ ベイ A2 から)。

```
> request system raid remove A2
```

2. 新たに 2TB のドライブを取り付けたキャリアをドライブ ベイ A2 に挿入し、RAID 1 のアレイ設定に追加します。

```
> request system raid add A2
```

システムによって A2 のデータが A1 にコピーされ、ドライブのミラーリングが行われます。

3. コピーの進行状況についての状態を表示するには、以下のコマンドを実行します。

```
> show system raid detail
```

アレイ (この例では A1/A2) で `Available` (利用可能) と表示され、両方のディスクで `active sync` (アクティブ同期) と表示されるまでの間これを続行し、RAID の詳細を出力します。

```
Disk Pair A       Available
   Status         clean
   Disk id A1     Present
       model        : ST2000NX0253
       size         : 1907138 MB
       status       : active sync
Disk id A2     Present
       model        : ST2000NX0253
       size         : 1907138 MB
       status       : active sync
```

STEP 7 | 必要に応じて、追加の RAID 1 アレイのドライブをアップグレードします。

さらに他の RAID 1 のアレイを 2TB のドライブにアップグレードするには、この作業を繰り返し、必要に応じてドライブ指定文字を交換します。たとえば、B1/B2 RAID 1 アレイのドライブをアップグレードする場合は A1 を B1 に、A2 を B2 に切り替えます。

© 2019 Palo Alto Networks, Inc.

Panorama 7.0.7 以前のバージョンを実行中の *M-Series* アプライアンスでドライブをアップグレード

Panorama 7.0.7 以前のバージョンで動作している *M-Series* アプライアンスをアップグレードした後は、*1TB* のドライブのログを利用できなくなります。それを許容できる場合でも、このアップグレードはメンテナンス中に行うことが推奨されます。

ログを保持する必要がある場合は、*Panorama 7.0.8* 以降のバージョンにアップグレードした後、「Panorama 7.0.8 以降のバージョンを実行中の M-Series アプライアンスでドライブをアップグレード」の手順を実行する必要があります。

STEP 1 | M-Series アプライアンスでコマンド ライン インターフェイス (CLI) にアクセスします。

以下のいずれかの方法で M-Series アプライアンスに接続します。

- コンピュータからコンソール ポートにシリアル ケーブルを接続し、ターミナル エミュレーション ソフトウェア (9600-8-N-1) を使用して M-Series アプライアンスに接続します。
- M-Series アプライアンスの IP アドレスに対して SSH (Secure Shell) セッションを開くには、PuTTY などの端末エミュレーション ソフトウェアを使用します。

STEP 2 | ログインを促されたら、アプライアンスにログインします。

デフォルトの管理者アカウントと割り当て済みのパスワードを使用します。

STEP 3 | 設置されているドライブの RAID 1 のステータスとして、機能している RAID 1 のアレイが 2 つ以上表示されていることを確認します。アップグレードを行う際に同時にアップグレードできる RAID 1 のアレイは 1 つだけであり、アプライアンスが利用できる RAID 1 のアレイが他に 1 つ以上なければなりません。唯一機能しているアレイを設定から取り除こうとすると、アプライアンスに中止エラーが表示されます。

RAID ステータスを表示するには、以下のコマンドを入力します。

```
> show system raid detail
```

以下は、利用できるアレイが 2 つ (ディスク ペア A およびディスク ペア B) ある M-500 アプライアンスの出力の例です。利用できるアレイが 1 つしかない場合、ドライブをアップグレードする前に、「M-Series アプライアンスにドライブを追加」の説明に従って 2 つ目を追加する必要があります。

```
Disk Pair A                              Available
   Status                                    clean
   Disk id A1                              Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : active sync
   Disk id A2                              Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : active sync
Disk Pair B                              Available
   Status                                    clean
   Disk id B1                              Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : active sync
   Disk id B2                              Present
       model        : ST91000640NS
       size         : 953869 MB
```


© 2019 Palo Alto Networks, Inc.

```
        status        : active sync
```

STEP 4 | 最初の RAID 1 アレイ設定から初めの 2 つの 1TB のドライブを取り外し、次にドライブを物理的に取り外します。

1. RAID 1 設定からドライブを取り外すには (この例では A1 および A2)、以下のコマンドを入力し、さらに各リクエストの確認を促されたら「**y**」と入力します。

```
> request system raid remove A1
> request system raid remove A2
```

2. ドライブ ベイからドライブを物理的に取り外します。各ドライブキャリアにある排出ボタンを押し、排出ハンドルを解除します。次にハンドルを手前に倒し、ドライブをスライドさせてアプライアンスから出します。
3. 2TB のドライブを 2 つパッケージから出し、先ほど取り外したドライブの隣にある台の上に乗せます。2TB のドライブも同じキャリアに取り付けることになるので、ドライブがどのようにキャリアに取り付けられているのか確認しておきます。
4. 各ドライブをキャリアに固定している 4 本のねじを取り外し、ドライブをキャリアから外します。
5. 先ほどドライブから外したのと同じ 4 本のねじを使用して 2TB のドライブをキャリアに取り付け、新たに 2TB のドライブを取り付けたキャリアをドライブ ベイ (この例では A1 および A2) に挿入します。

STEP 5 | 取り付けた 2TB のドライブ用の RAID 1 アレイを新たに設定し、両方のドライブが新しいアレイにあることを確認します。

1. ドライブ ベイ A1 にあるドライブを含むアレイを新たに設定するには、以下のコマンドを入力します。

```
> request system raid add A1
```

2. 新しい RAID 1 のアレイ設定のステータスを表示して確定するには、以下のコマンドを実行します。

```
> show system raid detail
```

以下のように出力されると、`Disk Pair A` (ディスク ペア A) のアレイが `Available` (利用可能) な状態であることが分かります。



この時点ではドライブ *A2* が *`not in use`* (未使用) であると表示されます。

```
Disk Pair A       Available
   Status         clean, degraded
   Disk id A1     Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : active sync
   Disk id A2       Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : not in use
```

3. 新しいアレイに 2 つ目のディスクを追加します。この例では A2 を追加することになります。

```
> request system raid add A2
```


© 2019 Palo Alto Networks, Inc.

4. ディスク ペアのステータスが`clean` (クリーン)になり、さらに両方のディスクが`active sync` (アクティブ同期)の状態になるまで、**`show system raid detail`**コマンドを実行したままにしてRAID出力を確認します。

STEP 6 | 必要に応じて、追加の RAID 1 アレイのドライブをアップグレードします。

さらに他の RAID 1 のアレイを 2TB のドライブにアップグレードするには、この作業を繰り返し、必要に応じてドライブ指定文字を交換します。たとえば、B1/B2 RAID 1 アレイのドライブをアップグレードする場合は A1 を B1 に、A2 を B2 に切り替えます。

複数のインターフェイスを使用するように Panorama を設定

大規模なネットワークでは、ネットワーク セグメンテーションを実装することでセキュリティを高め、輻輳を緩和できます。ネットワーク セグメンテーションを実現するには、リソース使用量、ユーザー ロール、セキュリティ要件に基づいてサブネットワークを分離します。Panorama では、デバイス (ファイアウォール、ログ コレクタ、WildFire アプライアンス、アプライアンス クラスタ) の管理やログの収集に複数の「M-Series アプライアンス インターフェイス」を使用できるようにすることでネットワーク セグメンテーションをサポートしています。個別のインターフェイスを個別のサブネットワークのデバイスに割り当てることができます。

ログの収集に複数のインターフェイスを使用することで、負荷分散を実現できるというメリットも得られます。これは特に、ファイアウォールが高速でログ コレクタにログを転送する環境で有効です。コレクタ グループ[ログ転送設定リスト]ですべてのログ コレクタに転送設定を有効にすると、設定されたすべての構成済みインターフェースにログが送信されます。それ以外の場合、ログは単一のインターフェースを介して転送され、そのインターフェースがダウンした場合、ログ転送は次に設定されたインターフェースを介して続行されます。例えば、ログ転送に Eth1/1、Eth1/2、および Eth1/3 を設定するとします。Eth1/1 インターフェースがダウンする場合、ログ転送は Eth1/2 上で続行します。

管理者は MGT インターフェイスを介して Panorama にアクセスして管理するため、そのインターフェイスを保護することは特に重要です。MGT インターフェイスのセキュリティを高める方法の 1 つとして、Panorama サービスを他のインターフェイスにオフロードする方法があります。デバイス管理やログ収集に加えて、コレクタ グループ通信とソフトウェアおよびコンテンツ更新のデプロイをファイアウォール、ログ コレクタ、WildFire アプライアンス、アプライアンス クラスタにオフロードすることもできます。こうしたサービスをオフロードすることで、MGT インターフェイスを管理トラフィック用に予約し、ファイアウォール、ログ コレクタ、WildFire アプライアンス、アプライアンス クラスタが存在するサブネットワークから分離されたセキュアなサブネットワークに割り当てることができます。

- 複数のインターフェイスを使用してネットワーク セグメンテーションを行う例
- ネットワーク セグメンテーションを行うように Panorama を設定

複数のインターフェイスを使用してネットワーク セグメンテーションを行う例

図 10 : 複数の Panorama インターフェイスPanorama モードとログ コレクタ モードの M-500 アプライアンスで複数のインターフェイスを使用するデプロイ環境を示しています。この例では、インターフェイスにより、次のようにネットワークのセグメント化がサポートされています。

- **Panorama** 管理ネットワーク – Panorama Web インターフェイス、CLI、XML API を不正なアクセスから保護するため、管理者のみがアクセスできるサブネットワークに Panorama の MGT インターフェイスを接続します。
- インターネット – Panorama は MGT インターフェイスを使用して、Palo Alto Networks 更新サーバーなどの外部サービスと通信します。
- 境界ゲートウェイおよびデータ センター – Panorama は、インターフェイスの別個のペアを使用して、ファイアウォールとログ コレクタを各サブネットワークで管理します。一般的にファイアウォールの管理で発生するトラフィックは、レポート情報を取得するためのログ コレクタの問い合わせで発生するトラフィックよりも少なくなります。このため、Panorama は 1Gbps インターフェイス (Eth1

© 2019 Palo Alto Networks, Inc.

と Eth2) をファイアウォールの管理に、10Gbps インターフェイス (Eth4 と Eth5) をログ コレクタの問い合わせと管理に使用します。各ログ コレクタは MGT インターフェイスを使用して問い合わせに応答しますが、ファイアウォールからのログ収集に関連する、多大なトラフィックには Eth4 と Eth5 のインターフェイスを使用します。

- ソフトウェア更新とコンテンツ更新 – サブネットワークのファイアウォールとログ コレクタは、Panorama の Eth3 インターフェイスでソフトウェア更新とコンテンツ更新を取得します。

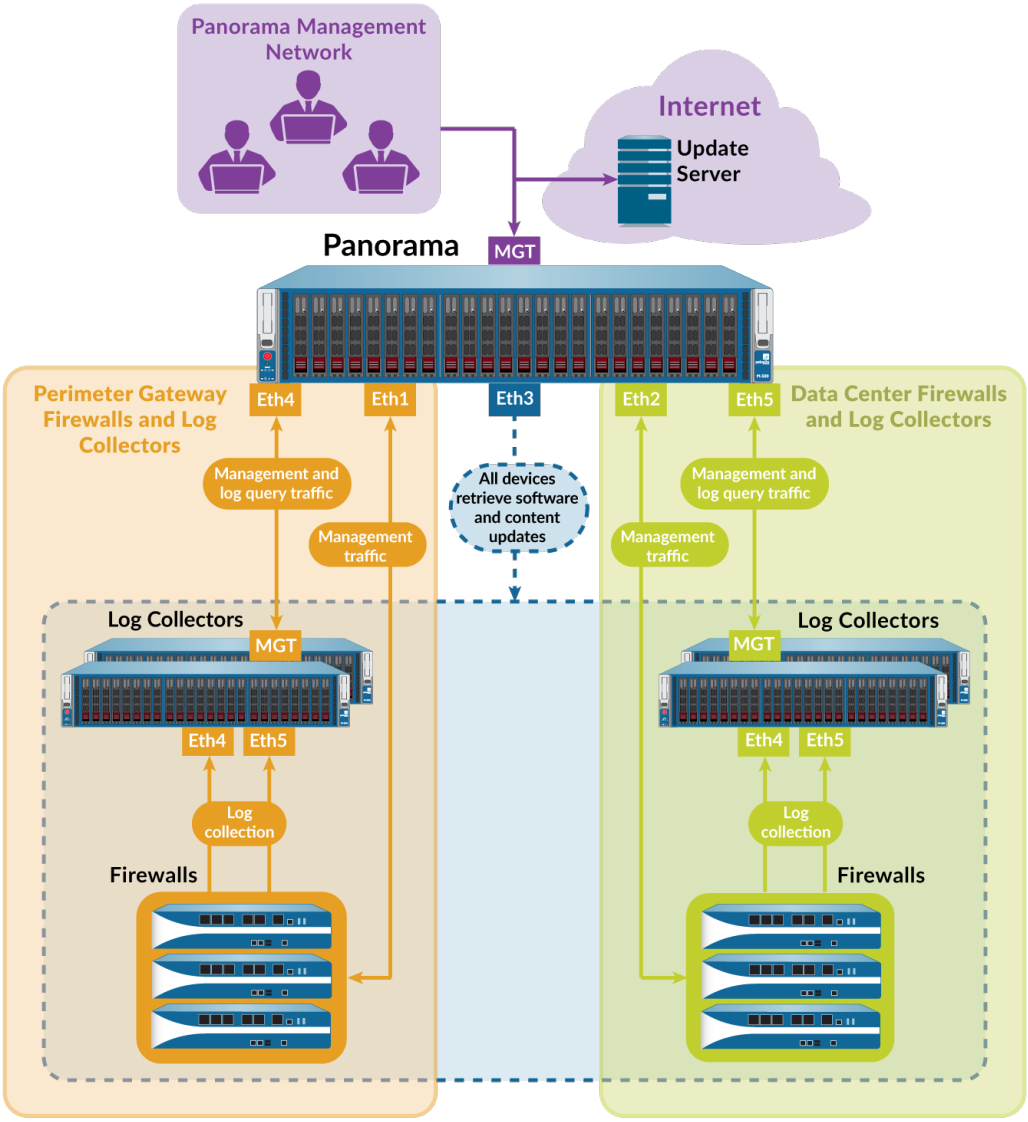


図 **10 :** 複数の **Panorama** インターフェイス

ネットワーク セグメンテーションを行うように *Panorama* を設定

Panorama サービスを MGT インターフェイスから他のインターフェイスにオフロードするには、最初に Panorama 管理サーバーでインターフェイスを設定します。ネットワークのログ トラフィックが重い場合、M-500 および M-600 アプライアンスの Eth4 および Eth5 インターフェイスは他のインターフェイス (1Gbps) よりも高いスループット (10Gbps) をサポートしていることに注意してください。次に、Panorama の特定のインターフェイスと接続するように各サブネットワークのログ コレクタを設定します。各ログ コレクタについて、コレクタ グループ通信用のインターフェイスと、ファイアウォールからログを収集するための 1 つ以上のインターフェイスも選択します。最後に、Panorama のインターフェイスと接続するように各サブネットワークのファイアウォールを設定します。

© 2019 Palo Alto Networks, Inc.

10GB インターフェースのログ コレクタ モードで *M-Series* アプライアンスを設定中の場合、*10GB* インターフェースを *Up* として表示するには、この設定手順全体を完了する必要があります。

MGT インターフェイスの *IP* アドレス、ネットマスク（*IPv4* の場合）またはプレフィックス長（*IPv6* の場合）、およびデフォルト ゲートウェイを指定することをお勧めします。これらの設定のいずれか（たとえば、デフォルト ゲートウェイ）を省略した場合、今後の設定変更で *M-Series* アプライアンスにアクセスできるのは、コンソール ポートからのみになります。

複数のインターフェイスを使用するように Panorama および専用ログ コレクタを設定するには、以下の手順を実行します。

STEP 1 | Panorama アプライアンスおよびファイアウォールが複数のインターフェイスに対応し、前提条件のソフトウェア バージョンおよび設定があることを確認します。

- 更新のデプロイに個別のインターフェイスを使用し、デバイス管理およびログ収集に複数のインターフェイスを使用するために、M-Series アプライアンスでは Panorama 8.0 以降が実行されている必要があること。M-200 および M-600 アプライアンスは、Panorama 8.1 以降を実行する必要があります。ESXi、vCloud、Air、Hyper-V、KVM にデプロイされた Panorama アプライアンスでは、Panorama 8.1 以降を実行する必要があります。
- Panorama またはログコレクタをバーチャルアプライアンスとして展開した場合は、Supported Interfaces for the Panorama Virtual Appliance（Panorama バーチャルアプライアンスでサポートされるインターフェース）を確認します。
- ログ収集またはコレクタ グループ通信に個別のインターフェイスを使用するために、M-Series アプライアンスでは Panorama 6.1 以降が実行されている必要があること。
- 各 Panorama 管理サーバーの初期設定が完了していること。これには MGT インターフェイスの設定が含まれます。
- ログ コレクタおよびコレクタ グループが設定されていること。これにはログ コレクタの MGT インターフェイスの設定が含まれます。
- ファイアウォールの初期設定が完了し、管理対象デバイスとしてファイアウォールを Panorama に追加しており、各サブネットワークのファイアウォールが個別のテンプレートに割り当てられていること。
- WildFire アプライアンスの初期設定が完了し、管理対象デバイスとして WildFire アプライアンスを Panorama に追加していること。

STEP 2 | 単独（非 HA）またはアクティブ（HA）Panorama 管理サーバーでインターフェイスを設定します。

MGT インターフェイスは *Panorama* の初期設定中に設定されているため、再び設定する必要はありません。

インターフェイスごとに以下の手順を実行します。

1. Panorama Web インターフェイスへのログイン（単独（非 HA）またはアクティブ（HA）Panorama 管理サーバーの）。
2. **[Panorama]** > [セットアップ] > [管理] の順に選択します。
3. Interface Name（インターフェイス名）をクリックしてインターフェイスを編集します。
4. <*interface-name*> を選択してインターフェイスを有効化します。
5. ネットワークの IP プロトコルに基づいてこれらのフィールド セットのいずれか、または両方を設定します。
   - IPv4 — **IP Address**（IP アドレス）、**Netmask**（ネットマスク）、および **Default Gateway**（デフォルト ゲートウェイ）

© 2019 Palo Alto Networks, Inc.

- IPv6 — **IPv6 Address/Prefix Length**（**IPv6** アドレス/プレフィックス長）および **Default IPv6 Gateway**（デフォルト **IPv6** ゲートウェイ）

6. インターフェイスでサポートされるサービスを選択します。
   - **Device Management and Device Log Collection**（デバイス管理およびデバイス ログ収集）— ファイアウォール、ログ コレクタ、WildFire アプライアンスおよびアプライアンス クラスタを管理し、ログ コレクタが生成するログを収集し、ログ コレクタにレポート情報を照会します。セグメント化されたネットワークをサポートするために、複数のインターフェイスでこれらのサービスを有効化できます。
   - **Collector Group Communication**（コレクタ グループ通信）— すべてのサブネットワークで Panorama が管理するコレクタ グループと通信します。
   - **Device Deployment**（デバイスのデプロイ）— ソフトウェアおよびコンテンツ更新をすべてのサブネットワークの管理対象ファイアウォール、ログ コレクタ、WildFire アプライアンス、およびアプライアンス クラスタにデプロイします。
7. **OK** をクリックして、インターフェイスに対する変更を保存します。
8. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順にクリックし、変更を **Commit**（コミット）します。
9. **Commit (コミット)** > **Push to Devices (デバイスへプッシュ)** をクリックして、変更したログ コレクタを含むコレクタ グループに変更をプッシュします。

STEP 3 | （HA のみ）パッシブ Panorama 管理サーバー上のインターフェイスを構成します。

1. Panorama Web インターフェイスへのログイン（アクティブ Panorama 管理サーバーの）。
2. **Panorama** > **Managed Collectors**（管理対象コレクタ）の順に選択し、パッシブ HA ピアを選択します。
3. **Interfaces (インターフェイス)**を選択し、編集するインターフェイスをクリックします。
4. **Enable Interface (インターフェイスの有効化)**ボックスにチェックを入れてインターフェイスを有効化します。
5. ネットワークの IP プロトコルに基づいてこれらのフィールド セットのいずれか、または両方を設定します。
   - IPv4 — **IP Address**（**IP** アドレス）、**Netmask**（ネットマスク）、および **Default Gateway**（デフォルト ゲートウェイ）
   - IPv6 — **IPv6 Address/Prefix Length**（**IPv6** アドレス/プレフィックス長）および **Default IPv6 Gateway**（デフォルト **IPv6** ゲートウェイ）
6. インターフェイスでサポートされるサービスを選択します。
   - **Device Management and Device Log Collection**（デバイス管理およびデバイス ログ収集）— ファイアウォール、ログ コレクタ、WildFire アプライアンスおよびアプライアンス クラスタを管理し、ログ コレクタが生成するログを収集し、ログ コレクタにレポート情報を照会します。セグメント化されたネットワークをサポートするために、複数のインターフェイスでこれらのサービスを有効化できます。
   - **Collector Group Communication**（コレクタ グループ通信）— すべてのサブネットワークで Panorama が管理するコレクタ グループと通信します。
   - **Device Deployment**（デバイスのデプロイ）— ソフトウェアおよびコンテンツ更新をすべてのサブネットワークの管理対象ファイアウォール、ログ コレクタ、WildFire アプライアンス、およびアプライアンス クラスタにデプロイします。
7. **OK** をクリックして、インターフェイスに対する変更を保存します。
8. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択し、Panorama に対する変更をコミットし、変更したパッシブ HA ピアが含まれるコレクタ グループに変更をプッシュします。

STEP 4 | Panorama インターフェイスと接続するように各ログ コレクタを設定します。

© 2019 Palo Alto Networks, Inc.

セグメント化されたネットワークをサポートするために、各サブネットワークのログ コレクタを個別の Panorama インターフェイスに接続できます。前の手順で説明しているように、インターフェイスで **Device Management and Device Log Collection**（デバイス管理およびデバイス ログ収集）を有効にする必要があります。

1. Panorama Web インターフェイスへのログイン（単独（非 HA）またはアクティブ（HA）Panorama 管理サーバーの）。
2. **Panorama** > **Managed Collectors**(Panorama > 管理対象コレクタ) の順に選択し、ログ コレクタを編集します。
3. **Panorama Server IP**（**Panorama** サーバー **IP**）フィールドに、単独（非 HA）あるいはアクティブ（HA）Panorama のインターフェイスの IP アドレスを入力します。
4. （HA のみ）**Panorama Server IP 2**（**Panorama** サーバー **IP 2**）フィールドに、アクティブ Panorama でフェイルオーバーが発生した場合に **Device Management and Device Log Collection**（デバイス管理およびデバイス ログ収集）をサポートするパッシブ Panorama のインターフェイスの IP アドレスを入力します。
5. **OK** をクリックして変更内容を保存します。
6. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択し、Panorama に対する変更をコミットし、変更したログ コレクタが含まれるコレクタ グループに変更をプッシュします。
7. 各専用ログ コレクタで以下の手順を実行します。
   1. PuTTY などのエミュレーション ソフトウェアを使用してログ コレクタ CLI にアクセスし、MGT インターフェイスの IP アドレスを使用するログ コレクタへの SSH セッションを開きます。ログインを促されたら、Panorama 管理者の認証情報を使用してログインします。
   2. 次のコマンドを実行します。ここで、*<IPaddress1>* は単独（非 HA）またはアクティブ（HA）Panorama、*<IPaddress2>* はパッシブ Panorama（該当する場合）です。

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

STEP 5 | （HA のみ）アクティブ Panorama がフェイルオーバーした場合に更新をデプロイするように、パッシブ Panorama 管理サーバーでインターフェイスを設定します。

1. Panorama Web インターフェイスへのログイン（パッシブ Panorama 管理サーバーの）。
2. **[Panorama]** > **[セットアップ]** > **[管理]** の順に選択します。
3. Interface Name（インターフェイス名）をクリックしてインターフェイスを編集します。
4. *<interface-name>* を選択してインターフェイスを有効化します。
5. ネットワークの IP プロトコルに基づいてこれらのフィールド セットのいずれか、または両方を設定します。
   - IPv4 — **IP Address**（**IP** アドレス）、**Netmask**（ネットマスク）、および **Default Gateway**（デフォルト ゲートウェイ）
   - IPv6 — **IPv6 Address/Prefix Length**（**IPv6** アドレス/プレフィックス長）および **Default IPv6 Gateway**（デフォルト **IPv6** ゲートウェイ）
6. **Device Deployment**（デバイスのデプロイ）を選択します。
7. **OK** をクリックして変更内容を保存します。
8. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順にクリックし、変更を **Commit**（コミット）します。

STEP 6 | ファイアウォールからログを収集して他のログ コレクタと通信するためにログ コレクタが使用するインターフェイスを設定します。

© 2019 Palo Alto Networks, Inc.

MGT インターフェイスはログ コレクタの初期設定中に設定されているため、再び設定する必要はありません。

1. Panorama Web インターフェイスへのログイン（単独（非 HA）またはアクティブ（HA）Panorama 管理サーバーの）。
2. **Panorama** > **Managed Collectors**(Panorama > 管理対象コレクタ) の順に選択し、ログ コレクタを編集します。
3. **Interfaces**（インターフェイス）を選択してインターフェイスごとに以下の手順を実行します。
   1. インターフェイス名をクリックしてそのインターフェイスを編集します。
   2. *<interface-name>* を選択してインターフェイスを有効化します。
   3. ネットワークの IP プロトコルに基づいて、以下のいずれか、あるいは両方のフィールドを設定します。

      Pv4 – **IP Address**（**IP** アドレス）、**Netmask**（ネットマスク）、および **Default Gateway**（デフォルト ゲートウェイ）

      IPv6 – **IPv6 Address/Prefix Length**（**IPv6** アドレス/プレフィックス長）および **Default IPv6 Gateway**（デフォルト **IPv6** ゲートウェイ）
   4. インターフェイスでサポートされる機能を選択します。

      Device Log Collection（デバイス ログ収集）– ファイアウォールからログを収集します。複数のインターフェイスでこの機能を実行できるようにすることで、ロギング トラフィックを負荷分散できます。

      Collector Group Communication（コレクタ グループ通信）– コレクタ グループ内の他のログ コレクタと通信します。
   5. **OK** をクリックして、インターフェイスに対する変更を保存します。
4. **OK** をクリックして、ログ コレクタに対する変更を保存します。
5. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択し、Panorama に対する変更をコミットし、変更したログ コレクタが含まれるコレクタ グループに変更をプッシュします。
6. **Panorama** > **Managed Collectors**（管理対象コレクタ）の順に選択し、ログ コレクタが Panorama と接続され、同期されていることを確認します。

   Configuration Status (設定ステータス) 列には`InSync`（同期）、Run Time Status (ランタイム ステータス) 列には`connected`（接続済み）が表示されている必要があります。

STEP 7 | Panorama インターフェイスと接続するようにファイアウォールを設定します。

セグメント化されたネットワークをサポートするために、各サブネットワークのファイアウォールを個別の Panorama インターフェイスに接続できます。インターフェイスで **Device Management and Device Log Collection**（デバイス管理およびデバイス ログ収集）を有効にする必要があります。この手順では、個別のテンプレートを使用して個別のサブネットワークのファイアウォールを設定することを前提としています。

この例のデプロイでは、*Panorama* はこれらのインターフェイスを使用してファイアウォールを管理しますが、ファイアウォール ログは収集しません。コレクタ グループを設定するときにファイアウォール ログを収集する専用ログ コレクタを指定します。

1. Panorama Web インターフェイスへのログイン（単独（非 HA）またはアクティブ（HA）Panorama 管理サーバーの）。
2. Panorama で **Device**（デバイス）> **Setup**（セットアップ）> **Management**（管理）の順に選択し、**Template**（テンプレート）を選択して Panorama Settings（Panorama 設定）を編集します。

© 2019 Palo Alto Networks, Inc.

3. 最初の **Panorama Servers**（**Panorama** サーバー）フィールドに、単独（非 HA）あるいはアクティブ（HA）Panorama のインターフェイスの IP アドレスを入力します。
4. （HA のみ）2 番目の **Panorama Servers**（**Panorama** サーバー）フィールドに、フェイルオーバーが発生した場合にデバイス管理をサポートするパッシブ Panorama のインターフェイスの IP アドレスを入力します。
5. **OK** をクリックして変更内容を保存します。
6. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択し、Panorama に対する変更をコミットして、テンプレートの変更をファイアウォールにプッシュします。
7. **Panorama** > **Managed Devices**（管理対象デバイス）の順に選択し、ファイアウォールが Panorama と接続され、同期されていることを確認します。

   Device State（デバイス状態）列に `Connected`（接続済み）と表示されます。Shared Policy（共有ポリシー）列と Template（テンプレート）列に `InSync`（同期中）と表示されます。

© 2019 Palo Alto Networks, Inc.

Panorama の登録とライセンスのインストール

中央管理、ロギング、およびレポート作成で Panorama を使用できるようにするには、まず、Panorama デバイス管理ライセンスおよびサポートライセンスを、登録、アクティベーション、および取得する必要があります。Panorama のすべてのインスタンスには、ファイアウォールを管理し、サポートを受ける資格を与える有効なライセンスが必要です。ファイアウォール 出刃押し管理ライセンスの種類により、Panorama で管理できるファイアウォールの最大数が決まります。このライセンスはファイアウォール上の仮想システムの数ではなくファイアウォール数(シリアル番号)が基準になっています。サポート ライセンスにより、（例えば最新のアプリケーションおよび脅威シグネチャを入手するための）Panorama のソフトウェア更新およびダイナミック コンテンツ更新が有効になります。さらに、AWS と Azure の Panorama バーチャル アプライアンスは、Palo Alto Networks から購入する必要があり、AWS または Azure マーケットプレイスでは購入できません。

Panorama バーチャル アプライアンスを PAN-OS 8.1 にアップグレードした後、容量ライセンスが正常にインストールされなかった場合、または Panorama で管理されているファイアウォールの総数がデバイス管理ライセンスを超過した場合は、プロンプトが表示されます。ライセンスがインストールされていない場合、アップグレード日から 180 日以内に有効なデバイス管理ライセンスをインストールしてください。管理されたファイアウォールの数がデバイス管理ライセンスを超えている場合は、デバイス管理ライセンスの要件を満たすためにファイアウォールを削除するか、180 日以内にデバイス管理ライセンスをアップグレードしてください。アップグレード後 180 日以内に、有効なデバイス管理ライセンスがインストールされていないか、既存のデバイス管理ライセンスの制限に達していない場合、すべてのコミットが失敗します。ライセンスを購入するには、Palo Alto Networks のセールスエンジニアまたは取り扱い小売店にお問い合わせください。

クラウドベースの Cortex Data Lake を使用する場合は、ファイアウォール管理ライセンスとプレミアム サポート ライセンスに加えて、Cortex Data Lake ライセンスも必要です。ライセンスを購入する際は、Palo Alto Networks のシステム エンジニアまたはリセラーまで問い合わせください。

Panorama バーチャル アプライアンスがインターネットに接続しており、ファイアウォール管理の評価版ライセンスを実行しており、購入した *Panorama* ライセンスを適用する場合は、Panoramaの登録およびPanorama バーチャル アプライアンスでのファイアウォール管理ライセンスのアクティベーション/取得のタスクを実行します。

- Panorama の登録
- Panorama サポート ライセンスのアクティベーション
- Panorama バーチャル アプライアンスがインターネットに接続している時のファイアウォール管理ライセンスのアクティベーション/取得
- Panorama バーチャル アプライアンスがインターネットに接続していない時のファイアウォール管理ライセンスのアクティベーション/取得
- M-Series アプライアンスにおけるファイアウォール管理ライセンスのアクティベーション/取得

Panorama の登録

STEP 1 | Panorama のシリアル番号または認証コードを記録し、販売注文番号またはカスタマー ID を記録します。

認証コード、販売受注番号、またはカスタマー ID は、Panorama の注文時に Palo Alto Networks カスタマー サポートから送信されてきた受注完了電子メールに記載されています。

シリアル番号を確認できる場所は、モデルによって異なります。

© 2019 Palo Alto Networks, Inc.

- M-Series アプライアンス—Panorama Webインターフェイスにログインし、**Dashboard**（ダッシュボード）タブ、General Information（一般情報）セクションの**Serial #**（シリアル番号）欄の値を記録します。
- Panorama バーチャル アプライアンス – 受注完了電子メールを参照してください。

STEP 2 | Panorama を登録します。手順は、サポート サイトにすでにログイン情報が登録されているかどうかに応じて異なります。

- 初めて登録する Palo Alto Networks アプライアンスである場合は、まだログイン情報は登録されていません。
  1. Palo Alto Networks カスタマーサポート ウェブサイトを訪問します。
  2. ページ下部にある **Register**（登録）をクリックし（**Overview**（概要）> **Get Help**（サポート）> **Register**（登録））、自分の **Email Address**（メール アドレス）を入力し、さらにページに表示されるコードを入力して **Submit**（送信）をクリックします。
  3. **Create Contact Details**（**Create Contact Details**）セクションのフィールドに情報を入力します。
  4. **Display Name**（表示名）、**Confirm Email Address**（確認用メール）、および **Password/Confirm Password**（パスワード/確認用パスワード）を入力します。
  5. Panorama の **Device Serial Number**（デバイスのシリアル番号）または **Auth Code**（認証コード）を入力します。
  6. **Sales Order Number**（販売受注番号）または **Customer ID**（顧客 ID) を入力します。
  7. **Submit**（送信）をクリックします。
- すでにサポート アカウントを持っている場合は、以下の手順に従います。
  1. Palo Alto Networks カスタマーサポート Web サイトにログインします。
  2. **Assets**（アセット）> **Devices**（デバイス）> **Register New Device**（新規デバイス登録）をクリックします。
  3. **Register device using Serial Number or Authorization Code**（シリアル番号または認証コードを使用してデバイスを登録）を選択し、**Submit**（送信）をクリックします。
  4. Panorama 管理サーバーがインターネットに接続されていない場合は、**Device will be used offline**（デバイスをオフラインで使用）にチェックボックスを選択して、**OS Release**（OS リリース）バージョンを選択します。
  5. Panorama の **Serial Number**（シリアル番号）を入力します。
  6. 4 時間の RMA を購入した場合は、必要な口ケーション情報（アスタリスクで示される）を入力します。
  7. EULA に**Agree and Submit**（同意して送信）してください。

     登録完了のメッセージが表示されたら、デバイス登録ダイアログを閉じます。

Panorama サポート ライセンスのアクティベーション

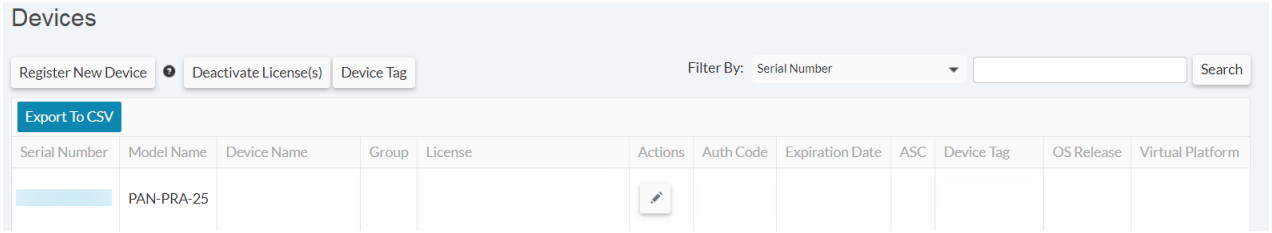
Panorama M-Series アプライアンスまたは Panorama バーチャル アプライアンスで Panorama のサポート ライセンスをアクティベートする前に、Panorama の登録を行う必要があります。

サポート ライセンスの有効期限が切れても *Panorama* はまだファイアウォールおよびログ コレクタを管理できますが、ソフトウェアおよびコンテンツ更新を利用できなくなります。*Panorama* のソフトウェアおよびコンテンツ バージョンは、管理対象のファイアウォールのバージョンと同じかそれより新しいものでなければなりません。そうでなければエラーが発生します。詳細は、「Panorama、ログ コレクタ、ファイアウォール、および WildFire のバージョン互換性」を参照してください。

© 2019 Palo Alto Networks, Inc.

STEP 1 | Palo Alto Networks のカスタマー サポート ポータルにログインして、認証コードをアクティベートします。

1. **Assets (アセット)** > **Devices (デバイス)**を選択し、Panorama のシリアル番号を入力して、**Serial Number**（シリアル番号）でフィルタリングを実行します。



2. Action（アクション）列にある鉛筆アイコンを選択し、**Activate Auth-Code**（認証コードのアクティベーション）を選択します。次に、サポート ライセンスの **Authorization Code**（認証コード）を入力し、**Agree and Submit**（同意して送信）をクリックします。

STEP 2 | Panorama Web インターフェイスにログインし、**Panorama** > **Support**（サポート） > **Activate feature using authorization code**（認証コードを使用した機能のアクティベーション）を選択します。

STEP 3 | **Authorization Code**（認証コード）を入力し、**OK** をクリックします。

STEP 4 | サブスクリプションがアクティベートされていることを確認します。ページの Support（サポート）セクションで詳細（**Expiry Date**（有効期限）、サポートの **Level**（レベル）、**Description**（説明）など）を確認します。

Panorama バーチャル アプライアンスがインターネットに接続している時のファイアウォール管理ライセンスのアクティベーション/取得

Panorama でデバイスを管理するには、PAN-OS により生成されたファイアウォール管理ライセンスをアクティベートする必要があります。アクティベートするデバイス管理ライセンスによって、Panorama が管理できるデバイスの数が決まります。ログ コレクタと WildFire アプライアンスは、管理対象デバイスとして扱われません。そのため、デバイス管理ライセンスで割り当てられるデバイスの数には含まれません。

Panorama バーチャル アプライアンスでファイアウォール管理ライセンスのアクティベーションおよび取得を実行する前に、Panorama の登録を行う必要があります。評価版ライセンスを実行しており、購入したライセンスを適用する場合は、購入したライセンスを登録し、アクティベーション/取得する必要があります。さらに、Panorama のシリアル番号を評価用シリアル番号から本番用シリアル番号に変更する必要があります。

STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | **[Panorama]** > **[セットアップ]** > **[管理]** の順に選択し、[一般設定] を編集します。

STEP 3 | Panorama の **Serial Number**（シリアル番号）（受注完了電子メールに記載）を入力し、**OK** をクリックします。

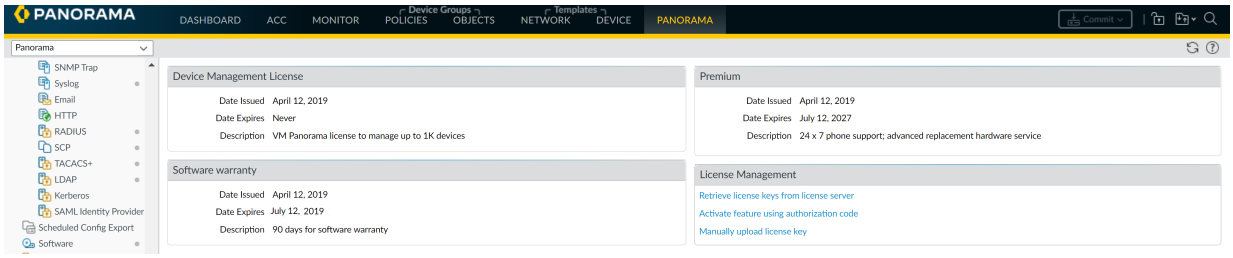
STEP 4 | **Panorama** > **Licenses (ライセンス)** を選択して、ファイアウォール管理ライセンスをアクティブ化または取得します。

© 2019 Palo Alto Networks, Inc.

- **Retrieve license keys from license server** (ライセンス サーバーからライセンス キーを取得)–Panorama は、Panorama 更新サーバーからファイアウォール管理ライセンスを自動的に取得してアクティブ化します。
- **Activate feature using authorization code** (認証コードを使用した機能のアクティベーション)-ファイアウォール管理ライセンス認証コードを入力し、**OK** をクリックしてライセンスをアクティブにします。認証コードは、受注完了電子メール、または Palo Alto Networks カスタマー サポート Web サイト にログインして Panorama 管理サーバーを検索することで取得できます。
- **Manually upload license key** (ライセンス キーの手動アップロード)-Palo Alto Networks カスタマー サポート Web サイトにログインし、Panorama 管理サーバーを検索してファイアウォール管理ライセンス キーをローカルデバイスにダウンロードします。ライセンス キーのダウンロードが終了した後、**Choose File** (ファイルの選択) をクリックしてライセンス キーを選択し、**OK** をクリックします。

STEP 5 | ファイアウォール管理ライセンスがアクティブ化されていることを確認します。

デバイス管理ライセンスセクションが表示され、ライセンスの発行日、ライセンスの有効期限、およびファイアウォール管理ライセンスの説明が表示されます。



Panorama バーチャル アプライアンスがインターネットに接続していない時のファイアウォール管理ライセンスのアクティベーション/取得

Panorama バーチャル アプライアンスでファイアウォール管理ライセンスのアクティベーションおよび取得を実行する前に、Panorama の登録を行う必要があります。Panorama でデバイスを管理するには、デバイス管理ライセンスをアクティベートする必要があります。アクティベートするデバイス管理ライセンスによって、Panorama が管理できるデバイスの数が決まります。ログ コレクタと WildFire アプライアンスは、管理対象デバイスとして扱われません。そのため、デバイス管理ライセンスで割り当てられるデバイスの数には含まれません。評価版ライセンスを実行しており、購入したライセンスを適用する場合は、購入したライセンスを登録し、アクティベーション/取得する必要があります。

PAN-OS 8.1 にアップグレードした後、Panorama の再起動が完了したときに初めて Panorama Web インターフェイスにログインするときに、有効な Panorama 管理ライセンスを取得するように求められます。Panorama バーチャル アプライアンスがオフラインまたは Palo Alto Networks アップデート サーバーにアクセスできない場合、アクティブな管理ライセンスをアクティブ化または取得するには、Panorama バーチャル アプライアンスの関連するアプライアンス情報を取得してカスタマーサポート Web サイトにアップロードする必要があります。

STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | （初期デプロイメントのみ）Panorama **Serial Number**（シリアル番号）を入力します。

1. **[Panorama]** > [セットアップ] > [管理] の順に選択し、[一般設定] を編集します。
2. Panorama の **Serial Number**（シリアル番号）（受注完了電子メールに記載）を入力し、**OK** をクリックします。

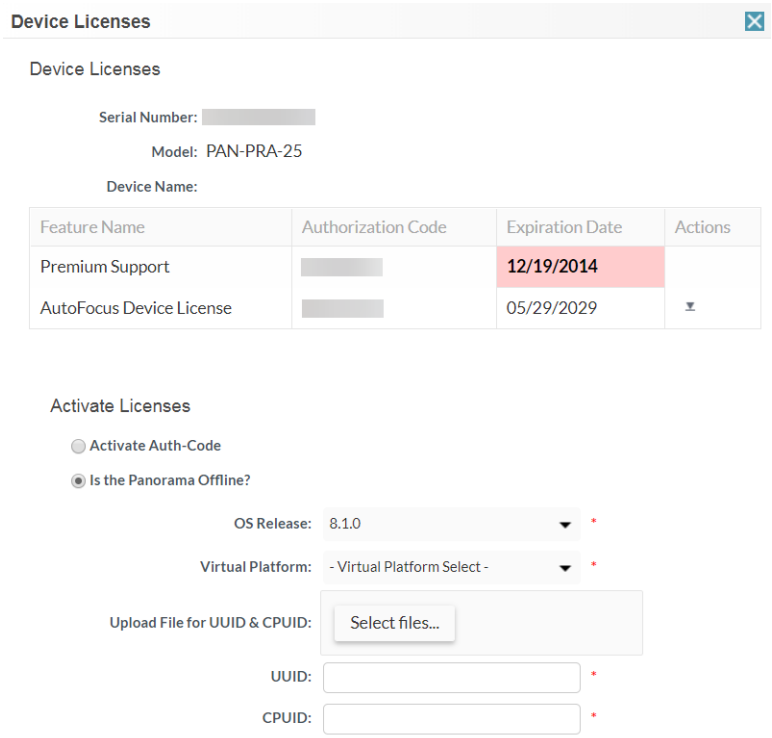
© 2019 Palo Alto Networks, Inc.

3. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

STEP 3 | Panorama バーチャル アプライアンスの情報をカスタマーサポートの Web サイトにアップロードします。

1. 管理ライセンスの取得ダイアログで、**here**（こちら）のリンクをクリックして、UUID、CPUID、Panorama バージョン、およびバーチャル プラットフォームの情報を収集します。**Download Link**（ダウンロード リンク）をクリックして、カスタマサポートポータル（CSP）にアップロードできる必要な Panorama 情報の XML ファイルをダウンロードします。

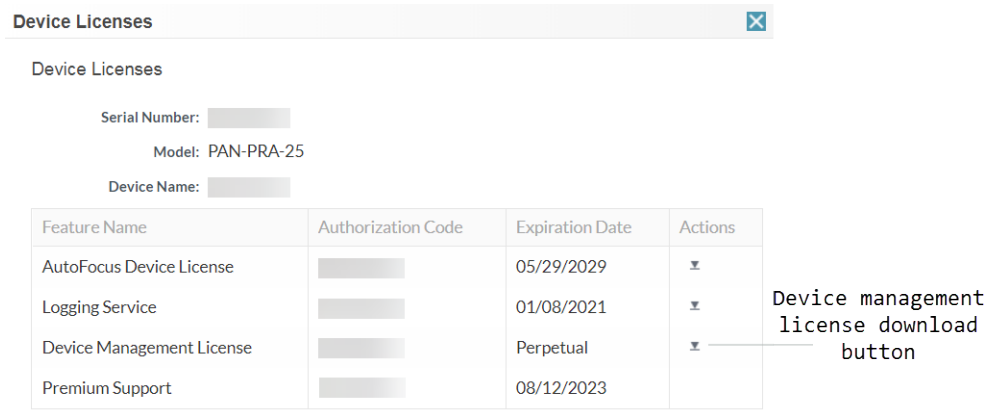
   最初のデプロイ時には、ログアウトして Web インターフェイスに戻ってダイアログを表示する必要があります。
2. Palo Alto Networks カスタマーサポート Web サイトにログインします。
3. 右上隅の**Get Support**（サポートを受ける）をクリックします。
4. **Assets (アセット)** > **Devices (デバイス)**タブを選択し、Panorama バーチャル アプライアンスを探し、Action (アクション) 列で編集アイコン（ ）をクリックします。
5. **Is the Panorama Offline?**（**Panorama** はオフラインですか？）を選択し、ステップ 2 で収集した Panorama 情報を入力するか、**Select files...**（ファイルを選択...）をクリックしてダウンロードした XML ファイルをアップロードします。
6. EULA に**Agree and Submit**（同意して送信）してください。



STEP 4 | デバイス管理ライセンスのインストールを行います。

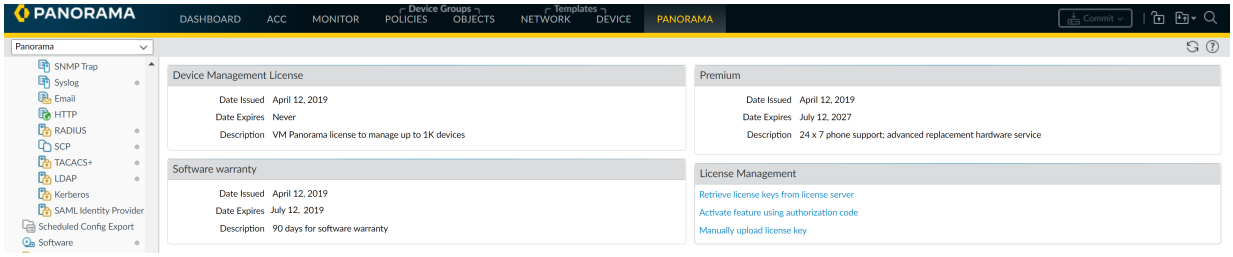
1. Actions（アクション）列で、デバイス管理ライセンスをダウンロードします。

© 2019 Palo Alto Networks, Inc.



2. Panorama Web インターフェイスで、**Panorama** > **Licenses**（ライセンス）の順にクリックし、**Manually upload license key**（ライセンス キーの手動アップロード）を行います。
3. **Choose file**（ファイルの選択）をクリックし、デバイス管理ライセンス キーを見つけたら、**OK**をクリックします。

STEP 5 | デバイス管理ライセンスが正常にアップロードされたことを確認するには、デバイス管理ライセンスがライセンス情報とともに表示されることを確認します。



M-Series アプライアンスにおけるファイアウォール管理ライセンスのアクティベーション/取得

Panorama でデバイスを管理するには、キャパシティ ライセンスをアクティベートする必要があります。キャパシティ ライセンスによって、Panorama が管理できるデバイスの数が決まります。ログ コレクタと WildFire アプライアンスは、管理対象デバイスとして扱われません。そのため、キャパシティ ライセンスで割り当てられるデバイスの数には含まれません。

M-Series アプライアンスで Panorama ファイアウォール管理ライセンスのアクティベーションおよび取得を行う前に：

- Panorama を登録します。
- 購入した製品/サブスクリプションの認証コードを準備します。注文時に、Palo Alto Networks カスタマー サービスから、購入に関連する認証コードを記載した電子メールが送信されます。この電子メールが見つからない場合は、Palo Alto Networks カスタマー サポートに連絡して認証コードを入手し、それから次に進んでください。

ライセンスをアクティベーションして取得すると、**Panorama** > **Licenses**(Panorama > ライセンス) ページに、関連する発行日、有効期限日、およびそのライセンスにより Panorama で管理できるファイアウォールの数が表示されます。

以下の方法でライセンスをアクティベートして取得できます。

- Web インターフェイスを使用して、ライセンスをアクティベートおよび取得します。

© 2019 Palo Alto Networks, Inc.

この方法は、Panorama で Palo Alto Networks の更新サーバーに接続する準備ができているが（M-Series アプライアンスの初期設定のタスクが完了している）、Palo Alto Networks カスタマー サポート Web サイトでライセンスをアクティベートしていない場合に選択します。

1. **[Panorama]** > [ライセンス] の順に選択し、[認証コードを使用した機能のアクティベーション] をオンにします。
2. **Authorization Code**（認証コード）を入力し、**OK** をクリックします。Panorama がライセンスを取得してアクティベートします。

- ライセンス サーバーからライセンス キーを取得します。

  Panorama で更新サーバーに接続する準備ができていない場合（たとえば、M-Series アプライアンスの初期設定を完了していない場合）は、サポート Web サイトでライセンスをアクティベートして、Panorama での接続準備ができてから、Web インターフェイスを使用してアクティベートされたライセンスを取得できます。アクティベートされたライセンスを取得するプロセスは、取得とアクティベーションの両方のプロセスよりも短い時間で処理されます。

  1. Palo Alto Networks カスタマー サポート Web サイトでライセンスをアクティベートします。
     1. インターネットにアクセスできるホストで、Web ブラウザから Palo Alto Networks のカスタマー サポート Web サイトにアクセスし、ログインします。
     2. **Assets (アセット)** > **Devices (デバイス)**タブを選択し、M-Series アプライアンスを探し、Action (アクション) 列で編集アイコン（）をクリックします。
     3. **Activate Auth-Code (認証コードのアクティベート)**を選択し、**Authorization Code (認証コード)**を入力して**Agree and Submit (同意して送信)**をクリックし、ライセンスをアクティベートします。
  2. 更新サーバーに接続するように Panorama を設定します。「M-Series アプライアンスの初期設定」を参照してください。
  3. **[Panorama]** > [ライセンス] の順に選択し、[ライセンス サーバーからライセンス キーを取得] を選択します。Panorama がアクティベートされたライセンスを取得します。

- ホストから Panorama にライセンスを手動でアップロードします。Panorama がそのホストにアクセスできる必要があります。

  Panorama をセットアップ済み（M-Series アプライアンスの初期設定作業を完了している場合）でも、更新サーバーと接続されていない場合は、サポート Web サイトでライセンスをアクティベートし、更新サーバーに接続することができるホストにそのライセンスをダウンロードして、ライセンスを Panorama にアップロードします。

  1. Palo Alto Networks カスタマー サポート Web サイトでライセンスをアクティベートおよびダウンロードします。
     1. インターネットにアクセスできるホストで、Web ブラウザから Palo Alto Networks のカスタマー サポート Web サイトにアクセスし、ログインします。
     2. **Assets (アセット)** > **Devices (デバイス)**タブを選択し、M-Series アプライアンスを探し、Action (アクション) 列で編集アイコン（）をクリックします。
     3. **Activate Auth-Code (認証コードのアクティベート)**を選択し、**Authorization Code (認証コード)**を入力して**Agree and Submit (同意して送信)**をクリックし、ライセンスをアクティベートします。
     4. Action（アクション）列で、ダウンロード アイコンをクリックし、ライセンス キー ファイルをホストに保存します。
  2. Panorama Web インターフェイスで、**Panorama** > **Licenses**（ライセンス）の順に選択し、**Manually upload license key**（ライセンス キーの手動アップロード）をクリックして、**Browse**（参照）をクリックします。
  3. ホストにダウンロードしたキー ファイルを選択し、**Open**（開く）をクリックします。

© 2019 Palo Alto Networks, Inc.

4. **OK** をクリックして、アクティベートされたライセンス キーをアップロードします。

© 2019 Palo Alto Networks, Inc.

Panorama デバイス証明書のインストール

PAN-OS 9.1.3 以降のリリースでは、Palo Alto Networks のカスタマーサポートポータル（CSP）で Panorama が正常に認証され、ゼロタッチプロビジョニング（ZTP）、デバイス テレメトリ、IoT、およびエンタープライズ データ漏洩防止 (DLP) などのクラウド サービスを利用するには、Panorama™ 管理サーバにデバイス証明書をインストールする必要があります。デバイス証明書を正常にインストールするには、Panorama からインターネットにアクセス可能であることが必要です。

クラウド サービス プラグインを利用している場合に*Panorama* デバイス証明書を正常にインストールするには、クラウド サービス プラグイン 1.5 以降のリリース が必要です。

STEP 1 | Palo Alto Networks カスタマー サポート ポータル（CSP）を含むPanorama の登録。

STEP 2 | Network Time Protocol（NTP）サーバーを設定します。

NTP サーバは、デバイス証明書の有効期限を検証し、デバイス証明書が早期に期限切れになったり、無効になっていないことを確認します。

1. Panorama Web インターフェイスへのログイン.
2. **Panorama** > **Setup** > **Services**の順に選択します。
3. **NTP** を選択し、ホスト名 `pool.ntp.org` を **Primary NTP Server**（プライマリ **NTP** サーバー）として入力するか、プライマリ NTP サーバーの IP アドレスを入力します。
4. （任意）**Secondary NTP Server** [セカンダリ NTP サーバー]のアドレスを入力します。
5. （任意）NTP サーバーからの時間の更新を認証するには、各サーバーの **Authentication Type**（認証タイプ）で以下のいずれかを選択します。
   - **None**（なし）（デフォルト）– NTP 認証を無効にします。
   - **Symmetric Key** [対称キー] – ファイアウォールで対象キー交換（共有のシークレット）を使用して時間の更新を認証します。
     - **Key ID** – Key ID（1 ~ 65534）を入力します。
     - **Algorithm**（アルゴリズム）– NTP 認証に使用するアルゴリズムを選択します（**MD5** または **SHA1**）。
6. **OK** をクリックして、設定の変更を保存します。
7. **Commit (コミット)** および **Commit to Panorama (Panorama** へのコミット**)** をクリックします。

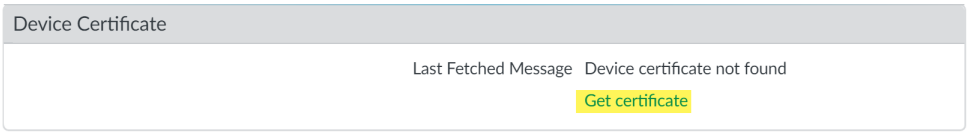
STEP 3 | ワンタイム パスワード（OTP）を生成します。

1. カスタマーサポート ポータルにログインします。
2. **Assets** > **Device Certificates**（デバイス証明書）および **Generate OTP**（**OTP**の生成）を選択します。
3. **Device Type**（デバイス タイプ）で、**Panorama** の **OTP** の生成および**OTP** の生成 の順で選択します。
4. **Panorama Device**（**Panorama** デバイス）のシリアル番号を選択します。
5. **OTP** を生成して、OTP をコピーします。

STEP 4 | 管理ユーザーとしてPanorama Web インターフェイスへのログイン。

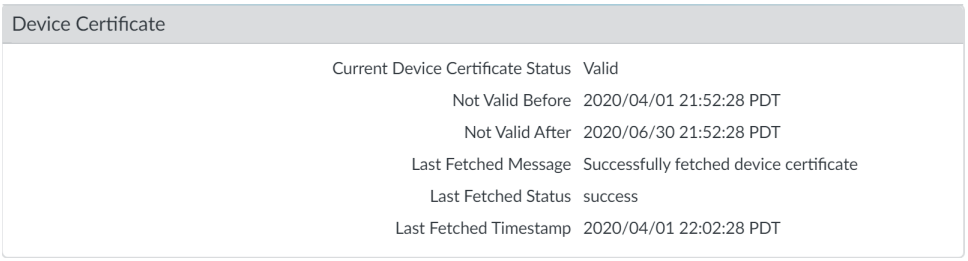
STEP 5 | **Panorama** > **Setup** > **Management** > **Device Certificate Settings**（デバイス証明書設定）そして **Get certificate**（証明書の取得）の順に選択します。

© 2019 Palo Alto Networks, Inc.



STEP 6 | 生成した **One-time Password**（ワンタイム パスワード）を入力して、 **OK** をクリックします。

STEP 7 | Panorama は証明書を正常に取得してインストールします。



© 2019 Palo Alto Networks, Inc.

Panorama のコンテンツ更新とソフトウェア更新のインストール

有効なサポート サブスクリプションにより、Panorama のソフトウェア イメージとリリース ノートにアクセスすることができます。最新の修正およびセキュリティ強化を利用するため、リセラーまたは Palo Alto Networks のシステム エンジニアがデプロイ環境に推奨する、最新のソフトウェアとコンテンツ更新へアップグレードしてください。ソフトウェア更新とコンテンツ更新をインストールする手順は、Panorama からインターネットに直接接続できるかどうか、および高可用性 (HA) 構成かどうかによって異なります。

- Panorama、ログ コレクタ、ファイアウォール、および WildFire のバージョン互換性
- HA 設定の Panorama に更新をインストール
- Panorama からインターネットに接続できる場合の更新のインストール
- Panorama からインターネットに接続できない場合の更新のインストール
- インターネットに接続せずにPanoramaのアップデートを自動的にインストールする
- Panorama ログの新しいログ形式への移行

Panorama、ログ コレクタ、ファイアウォール、および WildFire のバージョン互換性

Panorama™ の互換性に関する、次のガイドラインに従うことをお薦めします。

- Panorama 管理サーバーと専用ログ コレクタの両方に、同じ Panorama リリースをインストールします。
- Panorama は、管理するファイアウォールと同じまたはそれ以降の PAN-OS バージョンで動作している必要があります。ファイアウォールを PAN-OS 10.0 にアップグレードする前に、まず Panorama を 10.0 にアップグレードする必要があります。

  Panorama 6.1 以降のバージョンでは、*PAN-OS 6.0.0 ~ PAN-OS 6.0.3* を実行しているファイアウォールに設定をプッシュできません。
- PAN-OS 10.0 を実行する Panorama では、PAN-OS 10.0 リリース以前を実行している WildFire® アプライアンスと WildFire アプライアンス クラスタを管理できます。Panorama 管理サーバー、WildFire アプライアンス、WildFire アプライアンス クラスタに同じ PAN-OS リリースを実行させることが推奨されます。
- Panorama 管理サーバー上のコンテンツ バージョンは、専用ログ コレクタまたは管理対象ファイアウォール上のコンテンツ バージョンと同じかそれ以前のものでなければなりません。

  Panorama と専用ログ コレクタおよびファイアウォールに同じバージョンのアプリケーション データベースをインストールすることをお勧めします。

  サブスクリプションにアプリケーション データベース、あるいはアプリケーション データベースと脅威データベースが含まれているかどうかに関わらず、Panorama はアプリケーション データベースのみをインストールします。Panorama および専用ログ コレクタはポリシー ルールを強制しないため、脅威データベースから得られる脅威シグネチャを必要としません。アプリケーション データベースには、管理対象のファイアウォールにプッシュ送信するポリシールールを定義する際や、ログおよびレポートに含まれる脅威情報を解析する際にPanoramaと専用ログコレクタが使用する、脅威についてのメタデータ (脅威IDや名称など) が含まれています。ただし、ログに記録されている ID を対応する脅威、URL、またはアプリケーション名と照合する際、ファイアウォールは完全なアプリケーション データベースおよび脅威データベースを求めます。Panorama のリリースに必要な最低コンテンツ リリース バージョンについては、リリース ノートをご覧ください。

© 2019 Palo Alto Networks, Inc.

HA 設定の Panorama に更新をインストール

シームレスなフェイルオーバーを行うには、高可用性（HA）構成の Panorama ソフトウェアを更新するとき、アクティブとパッシブの Panorama ピアで同じ Panorama リリースを実行し、アプリケーション データベース バージョンを合わせる必要があります。以下の例では、HA ペア（アクティブ ピアは Primary_A、パッシブ ピアは Secondary_B）のアップグレード方法を示します。

Panorama を更新する前に、リリース ノートで PAN-OS 10.0 に必要な最低コンテンツ リリース バージョンを確認してください。

STEP 1 | Secondary_B（パッシブ）ピアで、Panorama ソフトウェアをアップグレードします。

次のいずれかのタスクを Secondary_B ピアで実行します。

- Panorama からインターネットに接続できる場合の更新のインストール
- Panorama からインターネットに接続できない場合の更新のインストール

アップグレード後、ピアが同じソフトウェア リリースを実行しなくなるため、この Panorama は非稼働状態に変わります。

STEP 2 | Primary_A ピアをサスペンドして、強制的にフェイルオーバーします。

Primary_A ピアで次のように操作します。

1. **Operational Commands**（操作コマンド）セクション（**Panorama** > **High Availability**（高可用性））で、**Suspend local Panorama**（ローカル **Panorama** をサスペンド）します。
2. 状態が `suspended` であることを確認します（Web インターフェイスの右下に表示）。

   発生するフェイルオーバーにより、Secondary_B ピアは `active` 状態に変わります。

STEP 3 | Primary_A（現在パッシブ）ピアで、Panorama ソフトウェアをアップグレードします。

次のいずれかのタスクを Primary_A ピアで実行します。

- Panorama からインターネットに接続できる場合の更新のインストール
- Panorama からインターネットに接続できない場合の更新のインストール

再起動後、Primary_A ピアは最初はパッシブ状態になります。プリエンプションが有効である場合（デフォルト）、Primary_A ピアは自動的にアクティブ状態に変わり、Secondary_B ピアはパッシブ状態に戻ります。

プリエンプションを無効にしている場合、手動でプライマリ Panorama のアクティブ状態への復元を行います。

STEP 4 | 両方のピアが、新しくインストールしたコンテンツ リリース バージョンおよび新しくインストールした Panorama リリースを実行していることを確認します。

各 Panorama ピアの **Dashboard**（ダッシュボード）で、Panorama ソフトウェア バージョンとアプリケーション バージョンをチェックし、両方のピアで同じであること、および動作している構成が同期されていることを確認します。

STEP 5 | (コレクタグループ内のローカル ログコレクタのみ) コレクタグループ内の残りのログ コレクタをアップグレードします。

- Panorama がインターネットに接続されている状態でログ コレクタをアップグレード
- Panorama がインターネットに接続されていない状態でログ コレクタをアップグレード

© 2019 Palo Alto Networks, Inc.

Panorama からインターネットに接続できる場合の更新のインストール

Panorama™ からインターネットに直接接続できる場合は、必要に応じて次の作業を行って Panorama のソフトウェアとコンテンツの更新をインストールします。Panorama が高可用性（HA）構成で動作している場合は、各ピアで Panorama ソフトウェアをアップグレードしてください（「HA 構成の Panorama に更新をインストール」を参照）。

Panorama バーチャル アプライアンスでソフトウェアをアップグレードしても、システム モードは変更されません。Panorama モードまたは管理専用モードへの切り替えは手動タスクであり、ローカル ログ コレクタで Panorama バーチャル アプライアンスをセットアップするとき、説明に従ってさらに設定する必要があります。

PAN-OS® 9.0 では、ローカルおよび専用ログ コレクタに新しいログデータ形式が導入されています。PAN-OS 10.0 へのアップグレードパスでは、PAN-OS 10.0 にアップグレードする際に、既存のログデータが新しい形式に自動的に移行されます。再フォーマット中、ログデータは **ACC** または **Monitor (監視)** タブには表示されません。さらに、再フォーマットが完了するまで、新しいログデータがログ コレクタに転送されることはありません。再フォーマット中、新しいログはファイアウォールシステムディスクに書き込まれ、処理が正常に完了すると新しいログが適切なログ コレクタに転送されます。

ログデータの損失を防ぐため、コレクタグループ内のすべてのログ コレクタを同時にアップグレードする必要があります。コレクタ グループ内のログ コレクタがすべて同じ PAN-OS バージョンを実行していない場合、ログ転送またはログ収集が発生することはありません。また、コレクタ グループのログ コレクタのログデータは、すべてのログ コレクタが同じ PAN-OS バージョンを実行するまで **ACC** または **Monitor (監視)**タブには表示されません。たとえば、コレクタグループ内にある 3 つのログ コレクタの内 2 つをアップグレードすると、コレクタグループのログ コレクタにログは転送されません。

Panorama を更新する前に、リリース ノートで PAN-OS 10.0 に必要な最低コンテンツ リリース バージョンを確認してください。

Azure 上の Panorama の場合、ソフトウェアバージョンを正常にアップグレードする前に追加の手順を実行する必要があります。アップグレード作業では、Panorama 設定をエクスポートし、コンテンツおよびソフトウェアバージョンをアップグレードし、アップグレードが正常に完了したら設定を Panorama 管理サーバーにインポートする必要があります。

STEP 1 | ご自身の Panorama デプロイ環境に適切な更新をインストールしようとしているかどうか確認します。

- Panorama のソフトウェア リリースに必要な最低コンテンツ リリース バージョンについては、リリース ノートをご覧ください。一部のバージョンにログ コレクタおよびファイアウォールをアップグレードする場合、まずは Panorama をそのバージョンにアップグレードする必要があります。
- ハイパーバイザ上で実行される Panorama バーチャル アプライアンスの場合、必ずインスタンスが Panorama バーチャル アプライアンスのセットアップ前提条件を満たすようにしてください。

STEP 2 | 現在の Panorama 設定ファイルのバックアップを保存します。アップグレードで問題が発生した場合は、これを使用して設定を復元できます。

Panorama は自動的に設定のバックアップを作成しますが、アップグレード前にバックアップを作成して外部に保存しておくことが推奨されます。

1. **Save named Panorama configuration snapshot**（名前を付けて **Panorama** 設定スナップショットを保存）（**Panorama** > **Setup**（セットアップ）> **Operations**（操作））で、設定の **Name**（名前）を入力して **OK** をクリックします。
2. **Export named Panorama configuration snapshot**（名前を付けて保存した **Panorama** 候補設定のスナップショットをエクスポート）をクリックし、先ほど保存した設定の **Name**（名前）を選択して **OK** をクリックし、エクスポートされたファイルを Panorama の外部に保存します。

© 2019 Palo Alto Networks, Inc.

STEP 3 | （必要に応じて）コンテンツ更新をインストールします。

アップグレード後の *Panorama* リリースに必要となる最低コンテンツ バージョンを *Panorama* が実行していない場合は、コンテンツ バージョンを最低（またはそれ以上の）バージョンに更新してから、ソフトウェア更新をインストールする必要があります。*Panorama* のリリースの最低コンテンツ リリース バージョンについては、リリース ノートをご覧ください。

Palo Alto Networks® では、*Panorama*、ログ コレクタ、すべての管理対象ファイア ウォールで同じコンテンツ リリース バージョンを実行することを強くお勧めしています。さらに、自動で行われる定期更新をスケジュールして、常に最新のコンテンツ バージョンを実行することをお勧めします *(9*を参照してください*)*。

1. **Check Now**（今すぐチェック）（**Panorama** > **Dynamic Updates**（ダイナミック更新））により、最新の更新を確認します。Action（アクション）列の値が **Download**（ダウンロード）の場合は、入手可能な更新があります。

   Panorama で実行しているコンテンツ リリースのバージョンが、管理対象ファイア ウォールとログ コレクタで実行しているバージョンと同じか、それ以前であることを確認します。
2. （必要に応じて）コンテンツ リリース バージョンを Panorama で更新する前に、管理対象ファイア ウォールをアップグレードしてからログ コレクタを同じ（またはそれ以上の）コンテンツ リリース バージョンにアップグレードします（「Panorama がインターネットに接続しているときのログ コレクタのアップグレード」を参照）。

   今回はコンテンツ更新をインストールする必要がない場合は、次のステップに進みます。
3. 必要に応じて残りのコンテンツ更新をインストールします。インストールすると、Currently Installed（現在インストール済み）列にチェック マークが表示されます。
   1. アプリケーション更新あるいはアプリケーションおよび脅威更新を**Download**（ダウンロード）、**Install**（インストール）します。どのようなサブスクリプションでも、Panorama には脅威コンテンツではなくアプリケーション コンテンツ更新のみが必要であり、それだけをインストールします。詳細は、「Panorama、ログ コレクタ、ファイアウォール、および WildFire のバージョン互換性」を参照してください。
   2. 必要に応じて任意の順序で一度に一つずつ、他の更新（アンチウイルス、WildFire®、あるいは URL フィルタリング）を **Download**（ダウンロード）、**Install**（インストール）します。

STEP 4 | アップグレード パスを PAN-OS 10.0 に決定します。

現在実行されている PAN-OS バージョンから PAN-OS 10.0 へのパスでは、任意の機能リリース バージョンのインストールをスキップすることはできません。アップグレード パスの一部として通過する各リリースについて、『Release Notes（リリース ノート）』で既知の問題とデフォルト動作の変更を確認し、『New Features Guide（新機能ガイド）』でアップグレード/ダウングレードに関する考慮事項を確認してください。

(7.1 以前のリリースからアップグレードした場合は必須) PAN-OS 8.0 では新しいログ保存形式が導入されました。PAN-OS 8.0 にアップグレードした後、アップグレードパスを続行する前に、Panorama ログを新しいログ形式に移行する必要があります。ログの移行は 1 回限りのタスクです。すでにログ コレクタのログをアップグレードして PAN-OS 8.0 にアップグレードした場合は、再度それらを移行する必要はありません。

複数のログ コレクタをアップグレードする場合は、アップグレードするすべてのログ コレクタのアップグレード パスを確認し、プロセスを合理化してから、イメージのダウンロードを開始してください。

STEP 5 | Panorama 10.0 をインストールします。

© 2019 Palo Alto Networks, Inc.

1. 最新のリリースを **Check Now** (今すぐチェック) (**Panorama** > **Software** (ソフトウェア)) します。ソフトウェアリリースが入手可能な場合は、Action (アクション) 列に **Download** (ダウンロード) が表示されます。
2. アップグレード後のリリース バージョンのモデル固有ファイルを特定して **Download** (ダウンロード) します。例えば、M-Series アプライアンスを Panorama 10.0.0 にアップグレードするには `Panorama_m-10.0.0` イメージをダウンロードし、Panorama バーチャル アプライアンスを Panorama 10.0.0 にアップグレードするには `Panorama_pc-10.0.0` イメージをダウンロードします。正常にダウンロードが完了すると、ダウンロードしたイメージの Action (アクション) 列が **Download** (ダウンロード) から **Install** (インストール) に変わります。
3. (現在実行されている PAN-OS バージョンから PAN-OS 10.0.0 へのパスに機能リリース バージョンのインストールをスキップすることはできません。)ダウンロードしたイメージをインストールしてから再起動します。
   1. イメージをインストールします。
   2. インストールが正常に完了したら、次のいずれかの方法によって再起動します。
      - 再起動を促されたら、**Yes** (はい) をクリックします。CMS Login 画面が表示された場合は、ユーザー名やパスワードを入力せずに Enter を押します。Panorama のログイン画面が表示されたら、初期設定時に指定したユーザー名およびパスワードを入力します。
      - 再起動を要求されない場合は、Device Operations (デバイスの操作) セクションから **Reboot Panorama** (**Panorama** の再起動) によって再起動します (**Panorama** > **Setup** (セットアップ) > **Operations** (操作))。
4. (PAN-OS 9.1.1 以降のリリースにアップグレードする場合に限り必須) PAN-OS 10.0 ベース イメージで上記の手順を完了した後で、手順 1 から 3 を繰り返し、対象のメンテナンス リリースにアップグレードします。

STEP 6 | PAN-OS 10.0 に正常にアップグレードした後、ログ形式の移行ステータスを確認します。

1. Panorama CLI へのログインログ コレクタの Panorama CLI にログインします。
2. 次のコマンドを実行して、ログ形式の移行ステータスを確認します。

```
admin> debug logdb show-es-upgrade-time
```

ログ形式の移行が進行中の場合の応答例：

```
Response
from logger 23456212: 50.98% of indices upgraded complete. Approximately
less than a minute remaining until migration is complete. Once the
log migration is complete, please run the 'show log-collector-es-cluster
health' command to check the ElasticSearch cluster status to verify
logging and reporting functionality is restored.
```

ログ形式の移行が完了したときの応答：

```
Response
from logger 23456212: 100% of indices complete. Please run the 'show
log-collector-es-cluster health' command to check the ElasticSearch
cluster status to verify logging and reporting functionality is
restored.
```

3. ログ形式の移行が完了したら、次のコマンドを実行して ElasticSearch クラスタのステータスを確認し、次の手順に進みます。

```
admin> show log-collector-es-cluster health
```


© 2019 Palo Alto Networks, Inc.

ElasticSearch クラスタの「status」が「green」に表示されたら、次の手順に進みます。

```
admin@Panorama(primary-active)> show log-collector-es-cluster health

{
  "cluster_name" : "__pan_cluster__",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 2,
  "number_of_data_nodes" : 2,
  "active_primary_shards" : 21,
  "active_shards" : 26,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0,
  "task_max_waiting_in_queue_millis" : 0,
  "active_shards_percent_as_number" : 100.0
}
```

STEP 7 | (Azure 上の Panorama のみ) ステップ 2 からエクスポートした Panorama 設定を読み込みます。

1. **Import named Panorama configuration snapshot**（名前を付けて保存した **Panorama** 設定スナップショットをインポート）（**Panorama** > **Setup** (セットアップ) > **Operations** (操作)）し、Panorama 設定ファイルを**Browse** (参照)して選択し、**OK**をクリックします。
2. **Load named Panorama configuration snapshot**（名前を付けて保存した **Panorama** 設定スナップショットを読み込み）、先ほどインポートした設定の**Name**（名前）を選択し、必要な場合は **Decryption Key**（復号化キー）を入力して**OK**をクリックします。
3. Panorama CLI へのログイン.
4. 次のコマンドを入力して Panorama 設定をコミットします：

```
admin> configure
```

```
admin> commit force
```

STEP 8 | (ローカル ログ コレクタがコレクタ グループ内にある場合のみ) コレクタ グループ内の残りのログ コレクタをアップグレードします。

- Panorama がインターネットに接続されている状態でログ コレクタをアップグレード
- Panorama がインターネットに接続されていない状態でログ コレクタをアップグレード

STEP 9 | （推奨設定）定期的に自動で行われるコンテンツ更新のスケジュールを設定します。

Panorama は、コンテンツ更新のスケジュールを *HA* ピア間で同期しません。この作業は、アクティブおよびパッシブ *Panorama* の両方で行う必要があります。

各更新タイプの見出し行（**Panorama** > **Dynamic Updates**（ダイナミック更新））では、**Schedule**（スケジュール）は、最初は **None**（なし）に設定されています。更新タイプごとに次の手順を実行します。

1. **None**（なし）をクリックして更新の頻度を選択します（**Recurrence**（繰り返し））。頻度のオプションは、更新の種類によって異なります。
2. スケジュール アクションを選択します。
   - **Download And Install**（ダウンロードおよびインストール）（推奨設定）— Panorama は更新ファイルをダウンロードした後、自動でインストールを行います。
   - **Download Only**（ダウンロードのみ）—Panoramaが更新ファイルをダウンロードしたら、それを手動でインストールする必要があります。

© 2019 Palo Alto Networks, Inc.

3. 組織のセキュリティに対する姿勢の推奨事項に従って、更新が利用可能になってから Panorama がその更新をダウンロードするまでの遅延（**Threshold**（しきい値））を設定します。
4. **OK** をクリックして変更内容を保存します。
5. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

Panorama からインターネットに接続できない場合の更新のインストール

Panorama™ からインターネットに直接接続できない場合は、必要に応じて次の作業を行って Panorama のソフトウェアとコンテンツの更新をインストールします。Panorama が高可用性（HA）構成でデプロイされている場合は、各ピアをアップグレードする必要があります（「HA 構成の Panorama に更新をインストール」を参照）。

Panorama バーチャル アプライアンスでソフトウェアをアップグレードしても、システム モードは変更されません。Panorama モードまたは管理専用モードへの切り替えは手動タスクであり、ローカル ログ コレクタで Panorama バーチャル アプライアンスをセットアップするとき、説明に従ってさらに設定する必要があります。

PAN-OS® 9.0 では、ローカルおよび専用ログ コレクタ用の新しいログデータ形式が導入されています。PAN-OS 10.0 へのアップグレードパスでは、PAN-OS 10.0 にアップグレードする際に、既存のログデータが新しい形式に自動的に移行されます。再フォーマット中、ログデータは **ACC** または **Monitor (監視)** タブには表示されません。さらに、再フォーマットが完了するまで、新しいログデータがログ コレクタに転送されることはありません。再フォーマット中、新しいログはファイアウォールシステムディスクに書き込まれ、処理が正常に完了すると新しいログが適切なログ コレクタに転送されます。

ログデータの損失を防ぐため、コレクタグループ内のすべてのログ コレクタを同時にアップグレードする必要があります。コレクタ グループ内のログ コレクタがすべて同じ PAN-OS バージョンを実行していない場合、ログ転送またはログ収集が発生することはありません。また、コレクタ グループのログ コレクタのログデータは、すべてのログ コレクタが同じ PAN-OS バージョンを実行するまで **ACC** または **Monitor (監視)**タブには表示されません。たとえば、コレクタグループ内にある 3 つのログ コレクタの内 2 つをアップグレードすると、コレクタグループのログ コレクタにログは転送されません。

Panorama をアップグレードする前に、リリース ノートで PAN-OS® 10.0 に必要な最低コンテンツ リリース バージョンを確認してください。

Azure 上の Panorama の場合、ソフトウェアバージョンを正常にアップグレードする前に追加の手順を実行する必要があります。アップグレード作業では、Panorama 設定をエクスポートし、コンテンツおよびソフトウェアバージョンをアップグレードし、アップグレードが正常に完了したら設定を Panorama 管理サーバーにインポートする必要があります。

STEP 1 | ご自身の Panorama デプロイ環境に適切な更新をインストールしようとしているかどうか確認します。

- Panorama にインストールしている必要がある最低ソフトウェア バージョンについてはリリース ノートをご覧ください。一部のバージョンにログ コレクタおよびファイアウォールをアップグレードする場合、まずは Panorama をそのバージョンにアップグレードする必要があります。
- Panorama バーチャル アプライアンスの場合、必ずインスタンスが Panorama バーチャル アプライアンスのセットアップ前提条件を満たすようにしてください。

STEP 2 | 現在の Panorama 設定ファイルのバックアップを保存します。アップグレードで問題が発生した場合は、これを使用して設定を復元できます。

Panorama は自動的に設定のバックアップを作成しますが、アップグレード前にバックアップを作成して外部に保存しておくことが推奨されます。

© 2019 Palo Alto Networks, Inc.

1. **Save named Panorama configuration snapshot**（名前を付けて **Panorama** 設定スナップショットを保存）（**Panorama** > **Setup**（セットアップ）> **Operations**（操作））で、設定の **Name**（名前）を入力して **OK** をクリックします。
2. **Export named Panorama configuration snapshot**（名前を付けて保存した **Panorama** 候補設定のスナップショットをエクスポート）をクリックし、先ほど保存した設定の **Name**（名前）を選択して **OK** をクリックし、エクスポートされたファイルを Panorama の外部に保存します。

STEP 3 | インストールする必要のあるコンテンツ更新を確認します。

Palo Alto Networks では、*Panorama*、ログ コレクタ、およびすべての管理対象ファイアウォールで実行するコンテンツ リリースのバージョンを同じにすることを強くお勧めしています。

1. コンテンツ更新ごとに、更新が必要かどうか、および次のステップでどのコンテンツ更新をダウンロードする必要があるかを判断します。

   Panorama で実行しているコンテンツ リリースのバージョンが、管理対象ファイアウォールとログ コレクタで実行しているバージョンと同じか、それ以前であることを確認します。
2. （必要に応じて）コンテンツ リリース バージョンを Panorama で更新する前に、管理対象ファイアウォールをアップグレードしてからログ コレクタを同じ（またはそれ以上の）コンテンツ リリース バージョンにアップグレードします（「Panorama がインターネットに接続しているときのログ コレクタのアップグレード」を参照）。

STEP 4 | PAN-OS10.0へのアップグレードパスを決定します。

現在実行中のPAN-OSバージョンからPAN-OS10.0へのパスでは、任意の機能リリース バージョンのインストールをスキップすることはできません。アップグレード パスの一部として通過する各リリースについて、『Release Notes（リリース ノート）』で既知の問題とデフォルト動作の変更を確認し、『New Features Guide（新機能ガイド）』でアップグレード/ダウングレードに関する考慮事項を確認してください。

(7.1 以前のリリースからアップグレードした場合は必須) PAN-OS 8.0 では新しいログ保存形式が導入されました。PAN-OS 8.0 にアップグレードした後、アップグレードパスを続行する前に、Panorama ログを新しいログ形式に移行する必要があります。ログの移行は 1 回限りのタスクです。すでにログ コレクタのログをアップグレードして PAN-OS 8.0 にアップグレードした場合は、再度それらを移行する必要はありません。

複数のログ コレクタをアップグレードする場合は、アップグレードするすべてのログ コレクタのアップグレード パスを確認し、プロセスを合理化してから、イメージのダウンロードを開始してください。

STEP 5 | （必要に応じて）接続できるホストにコンテンツ更新をダウンロードし、SCP または HTTPS で Panorama にコンテンツをアップロードします。

今回はコンテンツ更新をインストールする必要がない場合は、6 に進みます。

1. インターネットにアクセスできるホストを使用して Palo Alto Networks カスタマー サポート ウェブサイトにログインします。
2. 必要に応じてコンテンツ更新をダウンロードします。
   1. Resources (リソース) セクションで**Updates (アップデート)** > **Dynamic Updates (動的アップデート)**をクリックします。
   2. 適切なコンテンツ更新を **Download**（ダウンロード）し、ファイルをホストに保存します。アップデートする必要があるコンテンツ タイプごとにこのステップを繰り返します。

© 2019 Palo Alto Networks, Inc.

STEP 6 | 必要に応じてコンテンツ更新をインストールします。

ソフトウェア更新の前にコンテンツのアップデートをインストールし、最初にファイアウォールのアップグレードを行い、そして *Panorama* 管理サーバーにアップグレードをインストールする前に ログ コレクタをアップグレードしなければなりません。

アプリケーションあるいはアプリケーションおよび脅威更新をまずインストールした後、任意の順序で一度に一つずつ、他の更新 (アンチウイルス、WildFire®、URL フィルタリング) をすべてインストールします。

アプリケーションおよび脅威コンテンツの両方がサブスクリプションに含まれているかどうかに関わらず、*Panorama* にはアプリケーション コンテンツのみが必要であり、それだけをインストールします。詳細は、「Panorama、ログ コレクタ、ファイアウォール、および WildFire のバージョン互換性」を参照してください。

Panorama (**Panorama** > **Dynamic Updates** (ダイナミック更新)) で、コンテンツ タイプごとに次の手順を実行します。

1. **Upload** (アップロード) をクリックし、コンテンツの **Type** (タイプ) を選択し、更新のダウンロード先のホストの場所を **Browse** (参照) によって指定して、更新を選択して **OK** をクリックします。
2. **Install From File** (ファイルからインストール) をクリックし、**Package Type** (パッケージ タイプ) を選択して **OK** をクリックします。

STEP 7 | 接続できるホストにソフトウェア更新をダウンロードし、SCP または HTTPS で Panorama にコンテンツをアップロードします。

1. インターネットにアクセスできるホストを使用して、Palo Alto Networks のカスタマー サポート Web サイトにログインします。
2. ソフトウェア更新のダウンロード :
   1. Palo Alto Networks カスタマー サポート ウェブサイトのメイン ページで、Resources (リソース) セクションの**Updates (アップデート)** > **Software Updates (ソフトウェア アップデート)**をクリックします。
   2. アップグレード パスの最初の (または次の) Panorama リリースで、モデル固有のファイルを特定します。例えば、M-Series アプライアンスを Panorama 10.0.0 にアップグレードするには `Panorama_m-10.0.0` イメージをダウンロードし、Panorama バーチャル アプライアンスを Panorama 10.0.0 にアップグレードするには `Panorama_pc-10.0.0` イメージをダウンロードします。

      Filter By (絞り込み) ドロップダウンから *Panorama M Images* (*Panorama M* イメージ) (*M-Series* アプライアンス) または *Panorama Updates* (*Panorama* 更新) (バーチャル アプライアンス) を選択し、*Panorama* イメージをすぐに特定できます。
   3. ファイル名をクリックして、そのファイルをホストに保存します。
   4. ステップ 4 で判断したアップグレード パスの任意の追加リリース バージョンで、上記のサブステップ 2 を繰り返します。

STEP 8 | Panorama 10.0 をインストールします。

アップグレード パスのリリースごとに (最も古いものから)、次の手順を実行します。

1. Upload (アップロード) をクリックします (**Panorama** > **Software** (ソフトウェア))。
2. 更新のダウンロード先ホストの場所を **Browse** (参照) によって特定し、更新を選択して、Panorama が HA 構成である場合は **Sync To Peer** (ピアと同期) をクリックして (セカンダリ ピアにソフトウェア イメージをプッシュするため)、**OK** をクリックします。

© 2019 Palo Alto Networks, Inc.

3. ソフトウェア イメージをインストールして再起動します。

   HA 構成の場合は、「HA 構成の Panorama に更新をインストール」を参照してください。HA 構成でない場合は、次のように操作します。

   1. ダウンロードしたイメージをインストールします。
   2. インストールが正常に完了したら、次のいずれかの方法によって再起動します。
      - 再起動を促されたら、**Yes**（はい）をクリックします。CMS Login 画面が表示された場合は、ユーザー名やパスワードを入力せずに Enter を押します。Panorama のログイン画面が表示されたら、初期設定時に指定したユーザー名およびパスワードを入力します。
      - 再起動を要求されない場合は、Device Operations（デバイスの操作）セクションから **Reboot Panorama**（**Panorama** の再起動）によって再起動します（**Panorama** > **Setup**（セットアップ）> **Operations**（操作））。
4. 必要に応じて、パスのリリースごとに上記のサブステップ 1 から 3 を繰り返します。

STEP 9 | PAN-OS 10.0 に正常にアップグレードした後、ログ形式の移行ステータスを確認します。

1. Panorama CLI へのログインログ コレクタの Panorama CLI にログインします。
2. 次のコマンドを実行して、ログ形式の移行ステータスを確認します。

```
admin> debug logdb show-es-upgrade-time
```

ログ形式の移行が進行中の場合の応答例：

```
Response from logger 23456212: 50.98% of indices upgraded complete.
 Approximately less than a minute remaining until migration is complete.
 Once the log migration is complete, please run the 'show log-collector-
es-cluster health' command to check the ElasticSearch cluster status to
 verify logging and reporting functionality is restored.
```

ログ形式の移行が完了したときの応答：

```
Response from logger 23456212: 100% of indices complete. Please run the
 'show log-collector-es-cluster health' command to check the ElasticSearch
 cluster status to verify logging and reporting functionality is restored.
```

3. ログ形式の移行が完了したら、次のコマンドを実行して ElasticSearch クラスタのステータスを確認し、次の手順に進みます。

```
admin> show log-collector-es-cluster health
```

ElasticSearch クラスタの「status」が「green」に表示されたら、次の手順に進みます。

```
admin@Panorama(primary-active)> show log-collector-es-cluster health

{
  "cluster_name" : "__pan_cluster__",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 2,
  "number_of_data_nodes" : 2,
  "active_primary_shards" : 21,
  "active_shards" : 26,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0,
  "task_max_waiting_in_queue_millis" : 0,
  "active_shards_percent_as_number" : 100.0
}
```


© 2019 Palo Alto Networks, Inc.

STEP 10 | (Azure 上の Panorama のみ) ステップ 2 からエクスポートした Panorama 設定を読み込みます。

1. **Import named Panorama configuration snapshot**（名前を付けて保存した **Panorama** 設定スナップショットをインポート）（**Panorama** > **Setup** (セットアップ) > **Operations** (操作)）し、Panorama 設定ファイルを**Browse** (参照)して選択し、**OK**をクリックします。
2. **Load named Panorama configuration snapshot**（名前を付けて保存した **Panorama** 設定スナップショットを読み込み）、先ほどインポートした設定の**Name**（名前）を選択し、必要な場合は **Decryption Key**（復号化キー）を入力して**OK**をクリックします。
3. Panorama CLI へのログイン.
4. 次のコマンドを入力して Panorama 設定をコミットします：

```
admin> configure
```

```
admin> commit force
```

STEP 11 | (ローカル ログ コレクタがコレクタ グループ内にある場合のみ) コレクタ グループ内の残りのログ コレクタをアップグレードします。

- Panorama がインターネットに接続されている状態でログ コレクタをアップグレード
- Panorama がインターネットに接続されていない状態でログ コレクタをアップグレード

インターネットに接続せずにPanoramaのアップデートを自動的にインストールする

動的更新を、Panorama™管理サーバー、管理対象ファイアウォール、ログコレクター、およびWildFireアプライアンスがインターネットに接続されていないエアギャップネットワーク内のファイアウォール、ログコレクター、およびWildFire®アプライアンスに自動的にダウンロードします。これを実現するには、インターネット アクセスと SCP サーバーを備えた追加の Panorama をデプロイする必要があります。インターネットにアクセスできる Panorama をデプロイした後、インターネットに接続された Panorama を設定して、ダイナミック更新を SCP サーバーに自動的にダウンロードします。SCP サーバーから、エアギャップの Panorama は、ダイナミック更新スケジュールに従ってダイナミック更新を自動的にダウンロードしてインストールするように設定されています。インターネットにアクセスできる Panorama が SCP サーバーにダイナミック更新をダウンロードするとき、またはエアギャップの Panorama が SCP サーバーからダイナミック更新をダウンロードしてインストールするとき、Panorama はシステム ログを生成します。

インターネットに接続された Panorama から、インターネットに接続されていない Panorama への次のダイナミック更新スケジュールのみがサポートされています。

SCP サーバーに正常にダウンロードした後は、ダイナミック更新ファイル名を操作または変更しないでください。*Panorama* は、ファイル名が変更されたダイナミック更新をダウンロードしてインストールすることはできません。また、自動ダイナミック更新を成功させるためには、*SCP* サーバーに十分なディスク容量があること、ダウンロード開始時に *SCP* サーバーが実行されていること、そして両 *Panorama* の電源がオンになっており再起動中ではないことを確認する必要があります。

この例では、アプリケーションと脅威のダイナミック更新の自動コンテンツ更新を設定する方法を示しています。

STEP 1 | SCP サーバーをデプロイします。

© 2019 Palo Alto Networks, Inc.

マネージドファイアウォール、ログ コレクタ、および WildFire アプライアンスのダイナミック更新は、インターネットに接続された Panorama からダウンロードされます。エアギャップの Panorama は、SCP サーバーからダイナミック更新をダウンロードし、次にマネージド ファイアウォール、WildFire アプライアンス、ログ コレクタで更新をインストールします。



ダイナミック更新用のフォルダのディレクトリを作成するときは、ダイナミック更新の種類ごとにフォルダを作成することをお勧めします。これは、大量のダイナミック更新を管理する負担であり、*SCP* サーバーから削除してはならないダイナミック更新を削除する可能性を減らします。

STEP 2 | インターネットに接続する Panorama をデプロイします。

この Panorama は Palo Alto Networks 更新サーバーと通信し、ダイナミック更新を SCP サーバーにダウンロードします。

1. Panorama 管理サーバーをセットアップします。
   - M-Series アプライアンスのセットアップ
   - Panorama バーチャル アプライアンスのセットアップ
2. Panorama 初期設定を実行します。
   - M-Series アプライアンスの初期設定
   - Panorama バーチャル アプライアンスの初期設定の実行

STEP 3 | インターネット接続せずに Panorama をデプロイします。

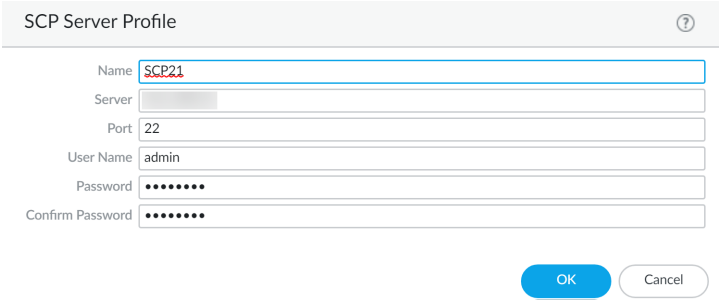
この Panorama は SCP サーバーと通信して、マネージドファイアウォール、ログ コレクタ、WildFire アプライアンスでのダイナミック更新のダウンロードとインストールを行います。

1. Panorama 管理サーバーをセットアップします。
   - M-Series アプライアンスのセットアップ
   - Panorama バーチャル アプライアンスのセットアップ
2. Panorama 初期設定を実行します。
   - M-Series アプライアンスの初期設定
   - Panorama バーチャル アプライアンスの初期設定の実行
3. マネージドファイアウォール、ログ コレクタ、WildFire アプライアンスを追加します。
   - 管理対象デバイスとしてのファイアウォールの追加
   - 管理対象コレクタの設定
   - Panorama で管理するスタンドアロン WildFire アプライアンスの追加

STEP 4 | インターネットに接続された Panorama を設定して、ダイナミック更新を SCP サーバーにダウンロードします。

1. Panorama Web インターフェイスへのログイン.
2. SCP サーバー プロファイルを作成します。
   1. **Panorama** > **Server Profiles**（サーバー プロファイル）> **SCP** を選択し、新しい SCP サーバー プロファイルを **Add**（追加）します。
   2. SCP サーバー プロファイルの説明 **Name**（名前）を入力します。
   3. SCP **Server** (サーバー) のIP アドレスを入力します。
   4. **Port** (ポート) を入力します。
   5. SCP サーバーの **User Name** (ユーザー名) を入力します。
   6. SCP サーバーの **Password** (パスワード) と **Confirm Password** (パスワードの確認)を入力します。
   7. **OK** をクリックして変更内容を保存します。

© 2019 Palo Alto Networks, Inc.



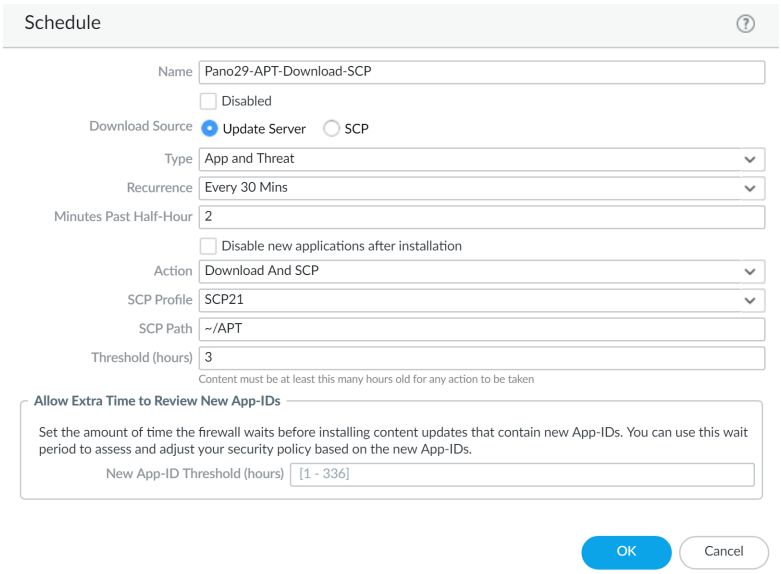
3. ダイナミック更新スケジュールを作成して、ダイナミック更新を SCP サーバーに定期的にダウンロードします。

   マネージドファイアウォール、ログ コレクタ、WildFire アプライアンスに自動的にダウンロードしてインストールする予定のダイナミック更新の種類ごとにスケジュールを作成する必要があります。

   1. **Panorama** > **Device Deployment**（デバイスのデプロイメント）> **Dynamic Updates**（ダイナミック更新）の順に選択し、**Schedules**（スケジュール）を選択し、ダイナミック更新スケジュールを **Add**（追加）します。
   2. ダイナミック更新スケジュールに説明 **Name** (名前) を入力します。
   3. **Download Source** (ソースをダウンロード) のために、**Update Server** (サーバーの更新) を選択します。
   4. ダイナミック更新の **Type** (タイプ) を選択します。
   5. **Recurrence** (繰り返し) を選択して、Panorama が Palo Alto Networks 更新サーバーで新しいダイナミック更新をチェックする間隔を設定します。

      より正確な繰り返しスケジュールを設定するには、選択した繰り返し間隔を過ぎた分数を入力します。同じ繰り返し間隔を使用してダウンロードするようにスケジュールされた複数のダイナミック更新がある場合、*Panorama* サーバーと *SCP* サーバーが過負荷にならないように、それらを重ならないように配置します。
   6. **Action** (アクション) に対して、**Download And SCP** (ダウンロードと **SCP**) を選択します。
   7. 前のステップで設定した **SCP Profile** (**SCP** プロファイル) を選択します。
   8. ダイナミック更新タイプの **SCP Path** (**SCP** パス) を入力します。
   9. (任意) ダイナミック更新の **Threshold** (しきい値)を 1 時間単位で入力します。Panorama は、この数時間 (またはそれ以前) のダイナミック更新のみをダウンロードします
   10. **OK** をクリックして変更内容を保存します。

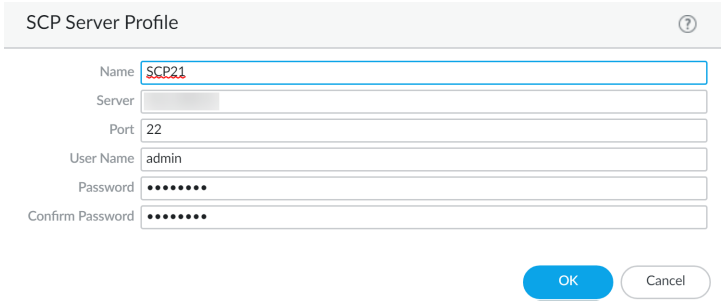
© 2019 Palo Alto Networks, Inc.



4. 変更を**Commit (コミット)** します。

STEP 5 | エアギャップの Panorama を設定して、SCP サーバーからダイナミック更新をダウンロードし、次にマネージド ファイアウォール、ログ コレクタ、WildFire アプライアンスで更新をインストールします。

1. Panorama Web インターフェイスへのログイン.
2. SCP サーバー プロファイルを作成します。
   1. **Panorama** > **Server Profiles** (サーバー プロファイル) > **SCP** を選択し、新しい SCP サーバー プロファイルを **Add** (追加) します。
   2. SCP サーバー プロファイルの説明 **Name** (名前) を入力します。
   3. SCP **Server (サーバー)** のIP アドレスを入力します。
   4. **Port (ポート)** を入力します。
   5. SCP サーバーの **User Name (ユーザー名)** を入力します。
   6. SCP サーバーの **Password (パスワード)** と **Confirm Password (パスワードの確認)**を入力します。
   7. **OK** をクリックして変更内容を保存します。



3. ダイナミック更新スケジュールを作成して、ダイナミック更新を SCP サーバーから定期的にダウンロードしてインストールを実行します。

   マネージドファイアウォール、ログ コレクタ、WildFire アプライアンスに自動的にダウンロードしてインストールする予定のダイナミック更新の種類ごとにスケジュールを作成する必要があります。

© 2019 Palo Alto Networks, Inc.

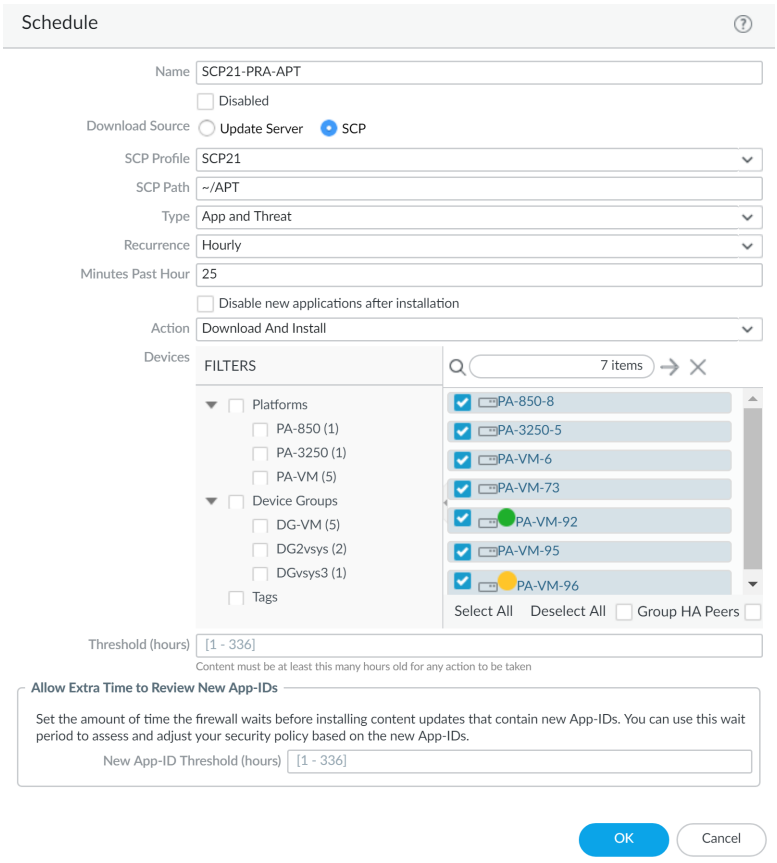
1. **Panorama** > **Device Deployment**（デバイスのデプロイメント）> **Dynamic Updates**（ダイナミック更新）の順に選択し、**Schedules**（スケジュール）を選択し、ダイナミック更新スケジュールを **Add**（追加）します。
2. ダイナミック更新スケジュールに説明 **Name** (名前) を入力します。
3. **Download Source** (ソースをダウンロード) に、**SCP** を選択します。
4. 前のステップで設定した **SCP Profile** (SCP プロファイル) を選択します。
5. ダイナミック更新タイプの **SCP Path** (SCP パス) を入力します。
6. ダイナミック更新の **Type** (タイプ) を選択します。
7. **Recurrence** (繰り返し) を選択して、Panorama が Palo Alto Networks 更新サーバーで新しいダイナミック更新をチェックする間隔を設定します。

   より正確な繰り返しスケジュールを設定するには、選択した繰り返し間隔を過ぎた分数を入力します。同じ繰り返し間隔を使用してダウンロードするようにスケジュールされた複数のダイナミック更新がある場合、*Panorama* サーバーと *SCP* サーバーが過負荷にならないように、それらを重ならないように配置します。
8. **Action** (アクション) に対して、**Download** (ダウンロード) または **Download And Install** (ダウンロードとインストール) を選択し実行します。

   Download Source (ソースのダウンロード) が *SCP* である場合は、*Download* (ダウンロード) と *Download and Install* (ダウンロードとインストール) のみがサポートされます。

   Download (ダウンロード) を選択する場合は、マネージドファイアウォール上でダイナミック更新のインストールを手動で開始する必要があります。
9. ダイナミック更新をインストールする **Devices** (デバイス) を選択します。
10. (任意) ダイナミック更新の **Threshold** (しきい値)を 1 時間単位で入力します。Panorama は、この数時間 (またはそれ以前) のダイナミック更新のみをダウンロードします
11. **OK** をクリックして変更内容を保存します。

© 2019 Palo Alto Networks, Inc.



4. 変更を**Commit (コミット)** します。

Panorama ログの新しいログ形式への移行

Panorama 8.0 以降のリリースにアップグレードした後では、Panorama のログ コレクタで新しいログ ストレージ形式が使用されます。アップグレード後は、8.0 より前のリリースのログ形式になっているログからレポートまたは ACC データを Panorama で生成できないため、Panorama とログ コレクタを PAN-OS® 7.1 以前のリリースから PAN-OS 8.0 以降のリリースにアップグレードした直後、管理対象ファイアウォールをアップグレードする前に、既存のログを移行する必要があります。PAN-OS 8.0 以降のリリースへのアップグレード後、Panorama はログ移行中にも管理対象デバイスからログを継続して収集しますが、着信ログを新しいログ形式で保存します。このため、Panorama がログ移行プロセスを完了するまで、ACC と レポートには一部のデータしか表示されません。

新しい形式へのログの移行は、*PAN-OS 8.0* 以降のリリースにアップグレードする際 (またはアップグレード パスの一部として *PAN-OS 8.0* にアップグレードする際に) に実行する必要がある *1* 回のみのタスクです。後に *PAN-OS* リリースにアップグレードする際にこの移行を再度実行する必要はありません。

Panorama でのログ移行プロセスにかかる時間は、Panorama に書き込まれる新しいログの量、および移行しているログ データベースのサイズによって決まります。ログ移行は CPU に大きな負荷がかかるプロセスであるため、ロギング レートが低い時間帯に移行を開始してください。ピーク時に CPU 利用率が高いことに気付いた場合は、いつでも移行を停止して、着信ログ率が低いときに移行を再開できます。

Panorama 用コンテンツとソフトウェア アップグレードのインストール後に、ログ コレクタをアップグレードしてから次のようにログを移行してください。

- 着信ロギング レートを確認します。

© 2019 Palo Alto Networks, Inc.

着信ログ率が低いときに、ログの移行を開始することをお薦めします。率を確認するには、ログ コレクタの CLI から次のコマンドを実行します。

```
admin@FC-M500-1> debug log-collector log-collection-stats show incoming-logs
```

ログの移行中は *CPU* 利用率が高くなる（*100%* に迫る）ことが予想されますが、操作は通常どおりに機能し続けます。リソースが競合する場合は、着信ログとその他のプロセスが優先されて、ログ移行は抑制されます。

- 各ログ コレクタで、新しい形式へのログ移行を開始します。

  移行を開始するには、各ログ コレクタの CLI から次のコマンドを入力します。

```
admin@FC-M500-1> request logdb migrate lc serial-number <ser_num> 開始日:
```

- ログ移行の状態を確認し、新しい形式への既存のすべてのログの移行にかかる時間を見積もります。

```
admin@FC-M500-1> request logdb migrate lc serial-number <ser_num> Status（状態） Slot: all
Migration State: In Progress
Percent Complete: 0.04
Estimated Time Remaining: 451 hour(s) 47 min(s)
```

- ログ移行プロセスを停止します。

  ログ移行プロセスを一時的に停止するには、ログ コレクタの CLI から次のコマンドを入力します。

```
admin@FC-M500-1 request logdb migrate lc serial-number <ser_num> 脅威の
```


© 2019 Palo Alto Networks, Inc.

別の Panorama モデルへの移行

ネットワークの要件が変わった (例えばロギング率が増加) 際は、この要件に対応できるように Panorama 管理サーバーおよび専用ログ コレクタをPanorama モデルへ移行することができます。

- Panorama バーチャル アプライアンスから M-Series アプライアンスへの移行
- Panorama バーチャル アプライアンスから異なるハイパーバイザへの移行
- M-Series アプライアンスから Panorama バーチャル アプライアンスへの移行
- M-100 アプライアンスから M-500 アプライアンスへの移行

Panorama バーチャル アプライアンスから M-Series アプライアンスへの移行

Panorama 設定は Panorama バーチャル アプライアンスから、Panorama モードの M-Series アプライアンスに移行できます。ただし、Panorama バーチャル アプライアンスと M-Series アプライアンスではログ形式に互換性がないため、ログを移行することはできません。そのため、Panorama バーチャル アプライアンスに保存されている以前のログを使用し続けたい場合は、移行後も Panorama バーチャル アプライアンスを実行しておく必要があります。移行後、M-Series アプライアンスはファイアウォールが転送した新しいログを収集します。移行前のログの有効期限が切れた、あるいは時間が経ったために使い道がなくなれば、Panorama バーチャル アプライアンスをシャットダウンすることができます。

レガシーモードは、PAN-OS 8.1 以降のリリースではサポートされなくなりました。古い Panorama バーチャル アプライアンスがレガシーモードである場合、ログ設定とログ コレクタの転送構成を保持するには、新しいハイパーバイザに移行する前に Panorama を Panorama モードに変更する必要があります。レガシーモードの古い Panorama 設定を Panorama モードの新しい Panorama にインポートすると、すべてのログおよびログ転送設定が削除されます。

ハイパーバイザ間でログを移行することはできません。そのため、古い Panorama バーチャル アプライアンスに保存されているログを使用し続けたい場合は、移行後も古い Panorama バーチャル アプライアンスを実行を継続し、新しい Panorama バーチャル アプライアンスの管理ログ コレクタとして追加する必要があります。これにより、新しい Panorama バーチャル アプライアンスは、古いログデータへのアクセスを維持しながら、ファイアウォールが移行後に転送した新しいログを収集することができます。移行前のログの有効期限が切れた、あるいは時間が経ったために使い道がなくなれば、Panorama バーチャル アプライアンスをシャットダウンすることができます。

ファイアウォール ログを *Panorama* バーチャル アプライアンスではなく専用ログ コレクタ (ログ コレクタ モードの *M-Series* アプライアンス) 上に保存する場合は、*Panorama* モードの *M-Series* アプライアンスに「専用ログ コレクタを移行」することでログへのアクセスを維持できます。

STEP 1 | 移行計画を立てます。

- M-Series アプライアンスで現在のソフトウェアの新しいバージョンが必要な場合 (M-500 アプライアンスには Panorama 7.0 以降のバージョンが必要) は、移行前に Panorama バーチャル アプライアンスのソフトウェアをアップグレードします。M-600 および M-200 アプライアンスの場合、Panorama 8.1 以降のバージョンでなければなりません。ソフトウェア バージョンに関する重要な詳細情報は、「Panorama、ログ コレクタ、ファイアウォール、および WildFire のバージョン互換性」を参照してください。
- 移行用に保守期間をスケジュール設定します。Panorama バーチャル アプライアンスがオフラインになっても、M-Series アプライアンスがオンラインになった後でファイアウォールはログをバッファリングして転送することができますが、移行を保守期間中に完了させることで、Panorama モデルを切り替える際にログがバッファ容量を超過して失われるリスクを最低限に抑えられます。

© 2019 Palo Alto Networks, Inc.

- 移行後も既存のログを利用するために Panorama バーチャル アプライアンスへのアクセスを保持するかどうかを検討します。最も効率の良いアプローチは、新しい IP アドレスを Panorama バーチャル アプライアンスに割り当て、以前の IP アドレスは M-Series アプライアンス用に再利用することです。これにより、ファイアウォールごとに Panorama の IP アドレスを再設定することなく、Panorama バーチャル アプライアンスへのアクセスを維持し、ファイアウォールが M-Series アプライアンスに向かうことができます。

STEP 2 | 新しい M-Series 仮想アプライアンスライセンスを購入し、サブスクリプションを仮想アプライアンスに移行します。

1. 新しい M-Series アプライアンスを購入します。
2. 新しいサポート ライセンスおよび移行ライセンスを購入します。
3. 新しい M-Series アプライアンスのライセンスを購入する際には、販売代理店に、廃止する Panorama バーチャル アプライアンスのシリアル番号とデバイス管理認証コード、および選択したライセンス移行日を伝えます。M-Series アプライアンスを受け取ったら、Palo Alto Networks が提供する移行およびサポート認証コードを使用して、アプライアンスを登録し、デバイス管理とサポートライセンスをアクティブ化します。移行日に、Panorama バーチャル アプライアンスのデバイス管理ライセンスは廃止され、古い Panorama バーチャル アプライアンスを使用してデバイスを管理したり、ログを収集したりすることはできなくなります。ただし、サポートライセンスは保持され、Panorama アプライアンスは引き続きサポートされます。発効日後に移行を完了することは可能ですが、すでに廃止された Panorama バーチャル アプライアンスで構成の変更をコミットすることはできません。

STEP 3 | (レガシーモードのみ) 古い Panorama バーチャル アプライアンスで、Panorama モードに変更します。

この手順は、*Panorama* バーチャル アプライアンスのログデータ、設定、およびログ転送構成を保持するために必要です。レガシーモードで *Panorama* 設定をエクスポートすると、これらの設定は失われます。続行する前に *Panorama* を *Panorama* モードに変更しない場合は、手順 9を完了しなければなりません。

Panorama バーチャル アプライアンスがすでに *Panorama* モードまたは管理専用モードになっている場合は、次の手順に進みます。

1. Panorama モードの Panorama バーチャル アプライアンスのセットアップ.
2. Panorama ログの新しいログ形式への移行古い Panorama バーチャル アプライアンスの既存のログデータを保持するには、Panorama ログを新しいログ形式に移行します。

STEP 4 | Panorama バーチャル アプライアンスから Panorama 設定をエクスポートします。

1. Panorama バーチャル アプライアンスにログインし、**Panorama** > **Setup** > **Operations** (Panorama > セットアップ > 操作) の順に選択します。
2. **Save named Panorama configuration snapshot** (名前を付けて **Panorama** 設定スナップショットを保存) をクリックし、設定を識別できる **Name** (名前) を入力して **OK** をクリックします。
3. **Export named Panorama configuration snapshot** (名前を付けて **Panorama** 設定スナップショットを保存) をクリックし、先ほど保存した設定の **Name** (名前) を選択して **OK** をクリックします。Panorama が XML ファイルの形式で設定をクライアント システムにエクスポートします。

STEP 5 | 移行後に Panorama バーチャル アプライアンスにアクセスする必要が無い場合はパワーオフします。あるいは移行後もアクセスする必要がある場合は新しい IP アドレスをその管理 (MGT) インターフェイスに割り当てます。

Panorama バーチャル アプライアンスの電源を切るには、VMware 製品のドキュメントを参照してください。

Panorama バーチャル アプライアンスの IP アドレスを変更するには :

© 2019 Palo Alto Networks, Inc.

1. **[Panorama]** > [セットアップ] > [管理] の順に選択し、[管理インターフェイス設定] を編集します。
2. 新しい**IP Address**（**IP** アドレス）を入力して **OK** をクリックします。
3. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

STEP 6 | M-Series アプライアンスの初期セットアップを実行します。

1. M-Series アプライアンスをラック マウントします。方法については、M-Series アプライアンスのハードウェア リファレンス ガイドを参照してください。
2. M-Series アプライアンスの初期設定を行い、アクティブなライセンスおよび更新のインストールに必要なネットワーク接続を定義します。
3. Panorama を登録します。
4. Panorama サポート ライセンスのアクティベーションを行います。
5. M-Series アプライアンスにおけるファイアウォール管理ライセンスのアクティベーション/取得を行います。移行ライセンスの認証コードを使用します。
6. Panorama のコンテンツ更新とソフトウェア更新のインストールを行います。Panorama バーチャル アプライアンスのものと同じバージョンをインストールします。

STEP 7 | Panorama バーチャル アプライアンスからエクスポートした Panorama 設定スナップショットを M-Series アプライアンスに読み込みます。

1. M-Series アプライアンスで、**Panorama** > **Setup**（セットアップ）> **Operations**（操作）の順に選択します。
2. **Import named Panorama configuration snapshot**（名前を付けて保存した **Panorama** 設定スナップショットをインポート）をクリックし、Panorama バーチャル アプライアンスからエクスポートした Panorama の設定ファイルを**Browse**（参照）し、**OK** をクリックします。
3. **Load named Panorama configuration snapshot**（名前を付けて保存した **Panorama** 設定スナップショットを読み込み）をクリックし、先ほどインポートした設定の**Name**（名前）を選択し、さらに **Decryption Key**（復号化鍵）（Panorama のマスター鍵）を選択して **OK** をクリックします。読み込んだ設定で Panorama が現在の候補設定を上書きします。設定ファイルのロード時にエラーが発生すると Panorama が表示を行います。
4. エラーが発生した場合は、それらのエラーをローカル ファイルに保存します。必ず各エラーを解決し、正常に設定が移行されるようにします。

STEP 8 | M-Series アプライアンスで設定を変更します。

M-Series アプライアンスが Panorama バーチャル アプライアンスと異なる値を使用する場合は必須です。ログを利用するために Panorama バーチャル アプライアンスへのアクセスを維持する場合は、M-Series アプライアンスに対して別のホスト名および IP アドレスを使用します。

1. **[Panorama]** > [セットアップ] > [管理] の順に選択します。
2. General Settings（一般設定）を編集し、**Hostname**（ホスト名）を変更して **OK** をクリックします。
3. Management Interface Settings（管理インターフェイス設定）を編集し、必要に応じて値を変更して **OK** をクリックします。

STEP 9 | M-Series アプライアンスにデフォルトの管理対象コレクタおよびコレクタ グループを追加し直します。

Panorama バーチャル アプライアンスから構成をロード (ステップ 7) すると、各 M-Series アプライアンスで事前定義されたデフォルトの管理対象コレクタおよびコレクタ グループが削除されます。

1. M-Series アプライアンスのローカルの管理対象コレクタの設定を行います。
2. デフォルトの管理対象コレクタに対してコレクタ グループの設定を行います。

© 2019 Palo Alto Networks, Inc.

3. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、Panorama 設定に対して、変更内容を **Commit**（コミット）します。

STEP 10 | M-Series アプライアンスをファイアウォールと同期してファイアウォールの管理を再開します。

このステップは保守期間中に完了させ、ネットワークの中断を最小限に抑えます。

1. M-Series アプライアンス上で **Panorama** > **Managed Devices**（管理対象のデバイス）の順に選択し、Device State（デバイス状態）列にファイアウォールが **Connected**（接続済み）と表示されることを確認します。

   この段階では、Shared Policy（共有ポリシー）（デバイス グループ）および Template（テンプレート）列にファイアウォールが **Out of sync**（非同期）であると表示されます。
2. 変更をデバイス グループとテンプレートにプッシュします。
   1. **Commit**（コミット）> **Push to Devices**（デバイスへのプッシュ）の順に選択し、**Edit Selections**（選択内容の編集）を行います。
   2. **Device Groups**（デバイス グループ）を選択し、すべてのデバイス グループを選択して、**Include Device and Network Templates**（デバイスおよびネットワーク テンプレートを含める）操作を実行し、**OK** をクリックします。
   3. 変更を **Push**（プッシュ）します。
3. **Panorama** > **Managed Devices**（管理対象デバイス）ページで、Shared Policy（共有ポリシー）および Template（テンプレート）列にファイアウォールが **In sync**（同期中）と表示されることを確認します。

Panorama バーチャル アプライアンスから異なるハイパーバイザへの移行

サポートされているハイパーバイザから、管理専用モードまたは Panorama モードでサポートされている別のハイパーバイザに、Panorama バーチャル アプライアンスの Panorama 構成を移行します。Panorama バーチャル アプライアンスを新しいハイパーバイザに移行する前に、Panorama モデルを確認して、移行先の新しいハイパーバイザがサポートされていることを確認してください。さらに、Panorama 構成にデバイス管理用のインターフェイス構成が複数あり、デバイス管理、ログ収集、コレクタ グループ通信、ライセンスおよびソフトウェア更新用のインターフェイスが複数含まれる場合、Panorama バーチャル アプライアンスのセットアップ前提条件を確認して、移行するハイパーバイザが複数のインターフェイスをサポートしていることを確認してください。

レガシーモードは、PAN-OS 8.1 以降のリリースではサポートされなくなりました。古い Panorama バーチャル アプライアンスがレガシーモードである場合、ログ設定とログ コレクタの転送構成を保持するには、新しいハイパーバイザに移行する前に Panorama を Panorama モードに変更する必要があります。レガシーモードの古い Panorama 設定を Panorama モードの新しい Panorama にインポートすると、すべてのログおよびログ転送設定が削除されます。

Panorama バーチャル アプライアンスからログを移行することはできません。そのため、古い Panorama バーチャル アプライアンスに保存されているログを使用し続けたい場合は、移行後も古い Panorama バーチャル アプライアンスを Log Collector mode (ログ コレクタ モード) で実行を継続し、新しい Panorama バーチャル アプライアンスで管理ログ コレクタとして追加する必要があります。これにより、新しい Panorama バーチャル アプライアンスは、古いログデータへのアクセスを維持しながら、ファイアウォールが移行後に転送した新しいログを収集することができます。移行前のログの有効期限が切れた、あるいは時間が経ったために使い道がなくなれば、Panorama バーチャル アプライアンスをシャットダウンすることができます。

© 2019 Palo Alto Networks, Inc.

ファイアウォール ログを *Panorama* バーチャル アプライアンスではなく専用ログ コレクタ (ログ コレクタ モードの *Panorama* バーチャル アプライアンス) 上に保存する場合は、*Panorama* モードの新しい *Panorama* バーチャル アプライアンスに専用ログ コレクタを移行することでログへのアクセスを維持することができます。

STEP 1 | 移行計画を立てます。

- 新しい Panoprama バーチャル アプライアンスに現在のソフトウェアの新しいリリースが必要な場合は、移行前に Panorama バーチャル アプライアンスのソフトウェアをアップグレードします。AWS および Microsoft Azure の Panorama には 8.1 以降のリリース、Google Cloud Platform (GCP) には 8.1.1 以降のリリース、KVM および AWS GovCloud には 8.1.2 以降のリリース、Hyper-V には 8.1.3 以降のリリースが必要です。ソフトウェアバージョンの重要な詳細については、Panorama、ログ コレクタ、ファイアウォール、および WildFire のバージョン互換性を参照してください。
- 移行用に保守期間をスケジュール設定します。新しい Panorama バーチャル アプライアンスがオフラインになった後でも、ファイアウォールはログをバッファリングすることができますが、移行をメンテナンスウィンドウが表示されている間に完了させることで、バッファ容量を超過してハイパーバイザ間での移行中にログが失われるリスクを最低限に抑えることができます。
- 移行後も既存のログを利用するために古い Panorama バーチャル アプライアンスへのアクセスを保持するかどうかを検討します。最も効率の良いアプローチは、新しい IP アドレスを古い Panorama バーチャル アプライアンスに割り当て、古い IP アドレスを Panorama バーチャル アプライアンス用に再利用することです。これにより、ファイアウォールごとに Panorama の IP アドレスを再設定することなく、古い Panorama バーチャル アプライアンスへのアクセスを維持し、ファイアウォールが新しい Panorama バーチャル アプライアンスに向かうことができます。

STEP 2 | 新しい Panorama バーチャル アプライアンスのライセンスを購入し、サブスクリプションをバーチャル アプライアンスに移行します。

1. 新しい Panorama バーチャル アプライアンスのライセンスを購入します。
2. 新しいサポート ライセンスおよび移行ライセンスを購入します。
3. 新しい Panorama バーチャル アプライアンスのライセンスを購入する際には、販売代理店に、廃止する Panorama バーチャル アプライアンスのシリアル番号とデバイス管理認証コード、および選択したライセンス移行日を伝えます。新しい Panorama バーチャル アプライアンスをデプロイした後、アプライアンスを登録し、Palo Alto Networks が提供する移行およびサポート認証コードを使用してデバイス管理とサポートライセンスをアクティブ化します。古い Panorama バーチャル アプライアンスのデバイス管理ライセンスは移行日に廃止され、古い Panorama バーチャル アプライアンスを使用してデバイスを管理したり、ログを収集したりすることはできなくなります。ただし、サポートライセンスは保持され、Panorama アプライアンスは引き続きサポートされます。発効日後に移行を完了することは可能ですが、すでに廃止された Panorama バーチャル アプライアンスで構成の変更をコミットすることはできません。

STEP 3 | (レガシーモードのみ) 古い Panorama バーチャル アプライアンスで、Panorama モードに変更します。

この手順は、*Panorama* バーチャル アプライアンスのログデータ、設定、およびログ転送構成を保持するために必要です。レガシーモードで *Panorama* 設定をエクスポートすると、これらの設定は失われます。*Panorama* を *Panorama* モードに変更しない場合は、続行する前にステップ 10 を完了する必要があります。

Panorama バーチャル アプライアンスがすでに *Panorama* モードまたは管理専用モードになっている場合は、次の手順に進みます。

1. Panorama モードの Panorama バーチャル アプライアンスのセットアップ.
2. Panorama ログの新しいログ形式への移行古い Panorama バーチャル アプライアンスの既存のログデータを保持するには、Panorama ログを新しいログ形式に移行します。

© 2019 Palo Alto Networks, Inc.

STEP 4 | 古い Panorama バーチャル アプライアンスから Panorama 設定をエクスポートします。

1. Panorama Web インターフェイスへのログイン.
2. **[Panorama]** > [セットアップ] > [操作] の順に選択します。
3. **Save named Panorama configuration snapshot**（名前を付けて **Panorama** 設定スナップショットを保存）をクリックし、設定を識別できる **Name**（名前）を入力して **OK** をクリックします。
4. **Export named Panorama configuration snapshot**（名前を付けて **Panorama** 設定スナップショットを保存）をクリックし、先ほど保存した設定の **Name**（名前）を選択して **OK** をクリックします。Panorama が XML ファイルの形式で設定をクライアント システムにエクスポートします。

STEP 5 | 移行後に古い Panorama バーチャル アプライアンスにアクセスする必要が無い場合は電源を落とします。あるいは移行後もアクセスする必要がある場合は新しい IP アドレスをその管理 (MGT) インターフェイスに割り当てます。

Panorama バーチャル アプライアンスの電源を切るするには、古い Panorama バーチャル アプライアンスがデプロイされているハイパーバイザがサポートされているドキュメントを参照してください。

Panorama バーチャル アプライアンスの IP アドレスを変更するには：

1. 古い Panorama バーチャル アプライアンスの Web インターフェースで、**Panorama** > **Setup (セットアップ)** > **Management (管理)** を選択し、管理インターフェイス設定を編集します。
2. 新しい**IP Address**（**IP** アドレス）を入力して **OK** をクリックします。
3. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

STEP 6 | 新しい Panorama バーチャル アプライアンスの初期セットアップを実行します。

1. Panorama バーチャル アプライアンスのセットアップ.
2. Panorama バーチャル アプライアンスの初期設定の実行ライセンスのアクティブ化と更新のインストールに必要なネットワーク接続を定義するには、Panorama バーチャル アプライアンスの初期設定を実行します。
3. Panorama を登録します。
4. Panorama サポート ライセンスのアクティベーションを行います。
5. Panorama バーチャル アプライアンスがインターネットに接続している時のファイアウォール管理ライセンスのアクティベーション/取得.移行ライセンスの認証コードを使用します。
6. Panorama のコンテンツ更新とソフトウェア更新のインストールを行います。古い Panorama バーチャル アプライアンスのものと同じバージョンをインストールします。

STEP 7 | 古い Panorama バーチャル アプライアンスからエクスポートした Panorama 設定スナップショットを新しい Panoramas バーチャル アプライアンスに読み込みます。

1. Panorama Web インターフェイスへのログイン 新しい Panorama バーチャル アプライアンスの Panorama Web インターフェイスにログインします。
2. **[Panorama]** > [セットアップ] > [操作] の順に選択します。
3. **Import named Panorama configuration snapshot**（名前を付けて保存した **Panorama** 設定スナップショットをインポート）をクリックし、Panorama バーチャル アプライアンスからエクスポートした Panorama の設定ファイルを**Browse**（参照）し、**OK** をクリックします。
4. **Load named Panorama configuration snapshot (名前を付けて保存した Panorama 設定スナップショットを読み込み)** をクリックして、先ほどインポートした設定の **Name (名前)** を選択し、**Decryption Key (復号化キー)** をブランク (空白) のままにして **OK** をクリックします。読み込んだ設定で Panorama が現在の候補設定を上書きします。設定ファイルのロード時にエラーが発生すると Panorama が表示を行います。
5. エラーが発生した場合は、それらのエラーをローカル ファイルに保存します。必ず各エラーを解決し、正常に設定が移行されるようにします。

STEP 8 | 新しい Panorama バーチャル アプライアンスの設定を変更します。

© 2019 Palo Alto Networks, Inc.

新規の Panorama バーチャル アプライアンスが古い Panorama バーチャル アプライアンスと異なる値を使用する場合は必須です。ログにアクセスするために古い Panorama バーチャル アプライアンスへのアクセスを維持する場合は、新しい Panorama バーチャル アプライアンスに対して別のホスト名および IP アドレスを使用します。

AWS、*AWS GovCloud*、*Microsoft Azure*、および *GCP* にデプロイされた *Panorama* では複数のインターフェース設定はサポートされていません。これらのハイパーバイザのいずれかに移行する場合、*MGT* インターフェイスを介して動作するには、デバイス管理、ログ収集、コレクタ グループの通信、ライセンス、およびソフトウェアの更新を再構成する必要があります。

1. **[Panorama]** > [セットアップ] > [管理] の順に選択します。
2. General Settings（一般設定）を編集し、**Hostname**（ホスト名）を変更して **OK** をクリックします。
3. Management Interface Settings（管理インターフェイス設定）を編集し、必要に応じて値を変更して **OK** をクリックします。

STEP 9 | 新しい Panorama バーチャル アプライアンスにデフォルトの管理対象コレクタおよびコレクタ グループを追加します。

古い Panorama バーチャル アプライアンスから構成をロード (ステップ 7) すると、Panorama モードの各 Panorama バーチャル アプライアンスで事前定義されているデフォルトの管理対象コレクタとコレクタ グループが削除されます。

1. Panorama バーチャル アプライアンスのローカルの 管理対象コレクタの設定を行います。
2. デフォルトの管理対象コレクタに対してコレクタ グループの設定を行います。
3. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、Panorama 設定に対して、変更内容を **Commit**（コミット）します。

STEP 10 | (レガシーモードのみ) レガシーモードで Panorama バーチャル アプライアンスから Panorama 構成を エクスポートした場合、Panorama への ログ転送の設定します。

STEP 11 | 新しい Panorama バーチャル アプライアンスをファイアウォールと同期して、ファイアウォールの管理を再開します。

このステップは保守期間中に完了させ、ネットワークの中断を最小限に抑えます。

1. 新しい Panorama バーチャル アプライアンス上で、**Panorama** > **Managed Devices** (管理対象デバイス) の順に選択し、Device State (デバイス状態) 列にファイアウォールが **Connected** (接続済み) と表示されていることを確認します。

   この段階では、Shared Policy（共有ポリシー）（デバイス グループ）および Template（テンプレート）列にファイアウォールが **Out of sync**（非同期）であると表示されます。
2. 変更をデバイス グループとテンプレートにプッシュします。
   1. **Commit**（コミット）> **Push to Devices**（デバイスへのプッシュ）の順に選択し、**Edit Selections**（選択内容の編集）を行います。
   2. **Device Groups**（デバイス グループ）を選択し、すべてのデバイス グループを選択して、**Include Device and Network Templates**（デバイスおよびネットワーク テンプレートを含める）操作を実行し、**OK** をクリックします。
   3. 変更を **Push**（プッシュ）します。
3. **Panorama** > **Managed Devices**（管理対象デバイス）ページで、Shared Policy（共有ポリシー）および Template（テンプレート）列にファイアウォールが **In sync**（同期中）と表示されることを確認します。

© 2019 Palo Alto Networks, Inc.

M-Series アプライアンスから Panorama バーチャル アプライアンスへの移行

Panorama 設定を M-100、M-200、M-500、M-600 アプライアンスから Panorama モードの Panorama バーチャル アプライアンスに移行できます。ただし、M-Series アプライアンスと Panorama バーチャル アプライアンスでは、ログ形式に互換性がないため、ログを移行することはできません。そのため、M-Series アプライアンスに保存されている以前のログを使用し続けるには、移行後も M-Series アプライアンスを専用ログ コレクタとして実行し続け、管理対象コレクタとして Panorama バーチャル アプライアンスに追加する必要があります。

Panorama 管理サーバーが高可用性設定の一部である場合、同じハイパーバイザまたはクラウド環境の 2 番目の Panorama バーチャル アプライアンスをデプロイし、必要なデバイス管理ライセンスおよびサポート ライセンスを購入する必要があります。HA要件の完全なリストについては、Panorama HA の前提条件を参照してください。

STEP 1 | 移行計画を立てます。

- Panorama バーチャル アプライアンスに移行する前に、M-Series アプライアンスを PAN-OS 10.0 以降にアップグレードしてください。Panorama のアップグレード方法については、Panorama のコンテンツ更新とソフトウェア更新のインストールを参照してください。ソフトウェア バージョンに関する重要な詳細情報は、「Panorama、ログ コレクタ、ファイアウォール、および WildFire のバージョン互換性」を参照してください。
- 移行用に保守期間をスケジュール設定します。M-Series アプライアンスがオフラインになっても、Panorama バーチャル アプライアンスがオンラインになった後でファイアウォールはログをバッファリングして転送することができますが、移行を保守期間中に完了させることで、異なる Panorama への移行中にログがバッファ容量を超過して失われるリスクを最低限に抑えられます。

STEP 2 | 新しい Panorama バーチャル アプライアンスの管理およびサポート ライセンスを購入します。

1. 販売代理店に連絡して、新しいデバイス管理ライセンスおよびサポート ライセンスを購入してください。
2. 段階的に廃止する予定の M-Series アプライアンスのシリアル番号、新規に Panorama バーチャル アプライアンスを購入した際に受け取ったシリアル番号およびサポート認証コード、さらに古いデバイスから新しいバーチャル アプライアンスへの移行完了予定日を販売担当者に伝えます。移行日以前に、移行の開始に向けて、新規バーチャル アプライアンスでシリアル番号を登録し、サポート認証コードをアクティブ化します。古い M-Series アプライアンスの容量認証コードは、指定された移行完了予定日に自動的に削除されます。

STEP 3 | Panorama バーチャル アプライアンスの初期セットアップを実行します。

1. Panorama バーチャル アプライアンスのセットアップを行います。
2. Panorama バーチャル アプライアンスの初期設定の実行により、ライセンスをアクティベートして更新をインストールするために必要なネットワーク接続を定義します。
3. Panorama を登録します。
4. Panorama サポート ライセンスのアクティベーションを行います。
5. Panorama バーチャル アプライアンスがインターネットに接続している時のファイアウォール管理ライセンスのアクティベーション/取得
6. Panorama のコンテンツ更新とソフトウェア更新のインストールを行います。M-Series アプライアンスと同じバージョンをインストールします。

STEP 4 | M-Series アプライアンスの Panorama インターフェイス設定を編集して、管理インターフェイスのみを使用します。

Panorama バーチャル アプライアンスは、デバイス管理および ログ収集のための管理インターフェイスのみをサポートしています。

© 2019 Palo Alto Networks, Inc.

1. M-Series アプライアンスの Panorama Web インターフェイスにログインします。
2. **[Panorama]** > [セットアップ] > [管理] の順に選択します。
3. General Settings（一般設定）を編集し、**Hostname**（ホスト名）を変更して **OK** をクリックします。
4. **Interfaces**（インターフェイス）を選択し、**Management**（管理）インターフェイスを編集することで必須のサービスを有効にします。
5. 残りのインターフェイスのサービスを無効にします。
6. **Commit**（コミット）> **Commit to Panorama**（**Panorama** にコミット）を選択します。

STEP 5 | 新しい Panorama バーチャル アプライアンスの IP アドレスを追加します。

M-Series アプライアンスで、Panorama バーチャル アプライアンスのパブリック IP アドレスを 2 番目の Panorama サーバーとして追加し、新しいPanorama 管理サーバーからデバイスを管理します。Panorama バーチャル アプライアンスが AWS、Azure または Google™Cloud Platform にデプロイされている場合は、パブリック IP アドレスを使用します。

1. **[Device]** > [セットアップ] の順に選択します。
2. テンプレート コンテキスト ドロップダウン リスト内で、Panorama サーバー設定を含むテンプレートまたはテンプレート スタックを選択します。
3. Panorama 設定を Edit (編集) します。
4. Panorama バーチャル アプライアンスのパブリック IP アドレスを入力して、**OK** をクリックします。
5. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）を選択します。

STEP 6 | M-Series アプライアンスから設定をエクスポートします。

1. **[Panorama]** > [セットアップ] > [操作] の順に選択します。
2. **Save named Panorama configuration snapshot**（名前を付けて **Panorama** 設定スナップショットを保存）をクリックし、設定を識別できる **Name**（名前）を入力して **OK** をクリックします。
3. **Export named Panorama configuration snapshot**（名前を付けて **Panorama** 設定スナップショットを保存）をクリックし、先ほど保存した設定の **Name**（名前）を選択して **OK** をクリックします。Panorama が XML ファイルの形式で設定をクライアント システムにエクスポートします。設定を Panorama アプライアンスの外側の場所に保存します。

STEP 7 | M-Series アプライアンスの電源を切るか、管理（MGT）インターフェイスに新しい IP アドレスを割り当てます。

M-Series アプライアンスが *Panorama* モードにあり、新しい *Panorama* バーチャル アプライアンスにアクセスする必要があるローカル ログ コレクタにログが保存されている場合は、*Panorama* バーチャル アプライアンスを管理対象のログ コレクタとして追加するために、*M-Series* アプライアンスの *IP* アドレスを変更します。

- **M-Series** アプライアンスをパワーオフするには：

1. Panorama Web インターフェイスにログインします。
2. **Panorama** > **Setup**（セットアップ）> **Operations**（操作）の順に選択し、Device Operations（デバイスの操作）で **Shutdown Panorama**（**Panorama** のシャットダウン）を行います。**Yes**（はい）をクリックしてシャットダウンを確定します。

- **M-Series** アプライアンスで **IP** アドレスを変更するには：

1. Panorama Web インターフェイスにログインします。
2. **[Panorama]** > [セットアップ] > [管理] の順に選択し、[管理インターフェイス設定] を編集します。
3. 新しい**IP Address**（**IP** アドレス）を入力して **OK** をクリックします。

© 2019 Palo Alto Networks, Inc.

4. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

STEP 8 | M-Series アプライアンスからエクスポートした Panorama 設定スナップショットを Panorama バーチャル アプライアンスに読み込みます。

1. Panorama バーチャル アプライアンスの Panorama Web インターフェイスにログインし、**Panorama** > **Setup**（セットアップ）> **Operations**（操作）の順に選択します。
2. **Import named Panorama configuration snapshot**（名前を付けて保存した **Panorama** 設定スナップショットをインポート）をクリックし、M-Series アプライアンスからエクスポートした Panorama 設定ファイルを **Browse**（参照）し、**OK** をクリックします。
3. **Load named Panorama configuration snapshot**（名前を付けて保存した **Panorama** 設定スナップショットを読み込み）をクリックし、先ほどインポートした設定の**Name**（名前）を選択し、さらに **Decryption Key**（復号化鍵）（Panorama のマスター鍵）を選択して **OK** をクリックします。読み込んだ設定で Panorama が現在の候補設定を上書きします。設定ファイルのロード時にエラーが発生すると Panorama が表示を行います。

エラーが発生した場合は、それらのエラーをローカル ファイルに保存します。必ず各エラーを解決し、正常に設定が移行されるようにします。コミットに成功していると、設定が読み込まれています。

STEP 9 | 既存のログ データを保持するには、M-Series アプライアンスを ログ コレクタ モードに変更します。

ロギング ディスクがまだ *M-Series* アプライアンスに挿入されている間にログ コレクタ モードに変更すると、ロギング データは消去されます。ログ データの損失を避けるために、モードを変更する前にログ ディスクを削除する必要があります。

各ディスク ペアのメタデータを生成すると、インデックスが再構築されます。そのため、データ サイズによっては、プロセスの完了に長時間を要する場合があります。複数の *CLI* セッションを立ち上げ、各セッションでメタデータを再生成するコマンドを実行して各ペアのプロセスを同時に完了させれば、プロセスが迅速に進みます。詳細については、「M-Series アプライアンスの RAID ペアのメタデータを再生成」を参照してください。

1. 以前の M-Series アプライアンスから RAID ディスクを取り外します。
   1. システムがシャットダウンするまで Power（電源）ボタンを押し続け、M-Series アプライアンスの電源を切ります。
   2. ディスク ペアを取り除きます。詳細については M-Series アプライアンスのハードウェア リファレンス ガイドに記載されたディスクの交換方法を参照してください。
2. 電源ボタンを押して、M-Series アプライアンスの電源を入れます。
3. `admin`（管理者）superuser administrator account（スーパーユーザー管理者アカウント）を設定します。

   `admin`（管理者）administrator account（管理者アカウント）がすでに作成されている場合は、次の手順に進みます。

   ログ コレクタ モードに切り替える前に、スーパーユーザー権限を持つ `admin`（管理者）アカウントを作成します。でなければ、モードの切り替え後に *M-Series* アプライアンスにアクセスできなくなります。
4. 以前の M-Series アプライアンスの Panorama CLI にログインします。
5. Panorama モードからログ コレクタ モードに切り替えます。
   - 次のコマンドを入力して、ログ コレクタ モードに切り替えます。

© 2019 Palo Alto Networks, Inc.

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

- **y**を入力して、モード変更を確定します。M-Series アプライアンスが再起動します。再起動処理によってターミナル エミュレーション ソフトウェアのセッションが終了した場合は、M-Series アプライアンスに再接続し、Panorama のログイン画面を表示します。

  CMS Login *(CMS*ログイン*)*画面が表示された場合は、ログコレクタが再起動をまだ完了させていないということです。入力を指示されたら、ユーザー名やパスワードは入力せずに *Enter* キーを押します。
- CLI に再度ログインします。
- ログ コレクタ モードへの切り替えが正しく完了したことを、次のコマンドで確認します。

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

モード変更が正しく完了した場合、出力は次のようになります。

```
> system-mode: logger
```

6. 以前の M-Series アプライアンスにディスクを挿入し直します。詳細についてはM-Series アプライアンスのハードウェア リファレンス ガイドに記載されたディスクの交換方法を参照してください。

   ディスクのペアの関係を崩さないようにしてください。スロット A1/A2 からスロット B1/B2 にディスク ペアを移動させることはできますが、ディスクのペアを一緒にして同じスロットに入れるようにしてください。そうしなければ Panorama が正常にデータを復元できなくなるおそれがあります。
7. 各ペアに対して次の CLI コマンドを実行し、ディスク ペアを有効にします。

```
> request system raid add <slot> force no-format
```

以下に例を示します。

```
> request system raid add A1 force no-format
> request system raid add A2 force no-format
```

引数 **force** および **no-format** は必須です。引数 **force** は、ディスク ペアを新しいアプライアンスに関連付けます。引数 **no-format** はドライブが再フォーマットされるのを回避し、ディスクに保存されたログを維持させます。
8. 各ディスク ペアのメタデータを生成します。

```
> request metadata-regenerate slot <slot_number>
```

以下に例を示します。

```
> request metadata-regenerate slot 1
```

9. ログ コレクタおよび Panorama 管理サーバー間の接続を有効にします。

   ログコレクタのCLIで次のコマンド（適宜、*<IPaddress1>*は単独（非HA）あるいはアクティブ（HA）PanoramaのMGTインターフェイスのもの、*<IPaddress2>*はパッシブ（HA）PanoramaのMGTインターフェイスのもの）を入力します。

© 2019 Palo Alto Networks, Inc.

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

STEP 10 | Panorama バーチャル アプライアンスをファイアウォールと同期してファイアウォールの管理を再開します。

このステップは保守期間中に完了させ、ネットワークの中断を最小限に抑えます。

1. Panorama バーチャル アプライアンス上で **Panorama** > **Managed Devices**（管理対象デバイス）の順に選択し、Device State（デバイス状態）列にファイアウォールが **Connected**（接続済み）と表示されることを確認します。

   この段階では、Shared Policy（共有ポリシー）（デバイス グループ）および Template（テンプレート）列にファイアウォールが **Out of sync**（非同期）であると表示されます。
2. 変更をデバイス グループとテンプレートにプッシュします。
   1. **Commit**（コミット）> **Push to Devices**（デバイスへのプッシュ）の順に選択し、**Edit Selections**（選択内容の編集）を行います。
   2. **Device Groups**（デバイス グループ）を選択し、すべてのデバイス グループを選択して、**Include Device and Network Templates**（デバイスおよびネットワーク テンプレートを含める）操作を実行します。
   3. **Collector Groups**（コレクタ グループ）を選択し、すべてのコレクタ グループを選択して、**OK** をクリックします。
   4. 変更を **Push**（プッシュ）します。
3. **Panorama** > **Managed Devices**（管理対象デバイス）ページで、Shared Policy（共有ポリシー）および Template（テンプレート）列にファイアウォールが **In sync**（同期中）と表示されることを確認します。

STEP 11 | （HA のみ）Panorama HA ピアをセットアップします。

Panorama 管理サーバーが高可用性設定にある場合は、HA ピアで以下の ステップ を実行します。

1. Panorama バーチャル アプライアンスの初期セットアップを実行します。
2. M-Series アプライアンスの Panorama インターフェイス設定を編集して、管理インターフェイスのみを使用します。
3. 新しい Panorama バーチャル アプライアンスの IP アドレスを追加します。
4. M-Series アプライアンスの電源を切るか、管理（MGT）インターフェイスに新しい IP アドレスを割り当てます。
5. 既存のログ データを保持するには、M-Series アプライアンスを ログ コレクタ モードに変更します。

STEP 12 | （HA のみ）Panorama バーチャル アプライアンスの HA ピア設定を変更します。

1. HA ピアで、Panorama Web インターフェイスにログインして、, select **Panorama** > **High Availability**（高可用性）を選択して、**Setup**（セットアップ）を編集します。
2. **Peer HA IP Address**（ピア **HA IP** アドレス）フィールドに、HA ピアの新しい IP アドレスを入力して **OK** をクリックします。
3. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。
4. HA ピアの他のピアでこれらの ステップ を繰り返します。

© 2019 Palo Alto Networks, Inc.

STEP 13 | （HA のみ）Panorama ピアを同期します。

1. HA ピアのいずれかの **Dashboard**（ダッシュボード）にアクセスし、**Widgets**（ウィジット）> **System**（システム）> **High Availability**（高可用性）の順に選択して HA ウィジットを表示します。
2. **Sync to peer**（ピアと同期）を行い、**Yes**（はい）をクリックして、**Running Config**（実行中の設定）で **Synchronized**（同期済み）が表示されるまで待ちます。
3. HA ピアの残った **Dashboard**（ダッシュボード）にアクセスし、**Widgets**（ウィジット）> **System**（システム）> **High Availability**（高可用性）の順に選択して HA ウィジットを表示します。
4. **Running Config**（実行中の設定）で **Synchronized**（同期済み）が表示されることを確認します。

M-100 アプライアンスから M-500 アプライアンスへの移行

Panorama 設定およびファイアウォール ログは M-100 アプライアンスから Panorama モードの M-500 アプライアンスに移行することができます（Panorama 管理サーバー）。また、ファイアウォール ログを M-100 アプライアンスからログ コレクタ モードの M-500 アプライアンスに移行することもできます（専用ログ コレクタ）。コレクタ グループのログ コレクタはすべて同じ Panorama モデルでなければならないため、コレクタ グループ内の M-100 アプライアンスを移行する場合はすべて移行する必要があります。

Panorama 管理サーバーをアクティブ/パッシブ高可用性（HA）設定でデプロイし、構成ファイルおよびログをどちらも移行し、M-100 アプライアンスから得た IP アドレスを M-500 アプライアンスで再利用する流れは次のようになります。

この手順では、ユーザーがデバイス管理またはログ収集において *M-100* を使用していないことを前提としています。廃止された *M-100* アプライアンスを専用ログ コレクタとして使用する場合、*M-100* ではデバイス管理ライセンスが必要です。デバイス管理ライセンスがないと、*M-100* を専用ログ コレクタとして使用できません。

M-100 アプライアンスを専用ログ コレクタとして使用する予定はないが、*M-100* アプライアンスに今後アクセスする必要があるログデータが含まれている場合も、既存のログデータを使用してレポートを照会および生成することができます。*Palo Alto Networks* は、*M-100* アプライアンスを廃止する前にログ保存ポリシーを確認することをお勧めしています。

Panorama 設定は移行せず、ログのみを移行する場合は、ログ コレクタ モードでログを新しい M-Series アプライアンスに移行あるいは Panorama モードでログを新しい M-Series アプライアンスに移行する作業を行います。

HA 設定でデプロイされていない新しい *Panorama* 管理サーバーに移行する場合で、かつ新しい *Panorama* が既存の専用ログ コレクタのログにアクセスしなければならない場合は、非 HA の Panorama で障害/RMA が発生した後のログ コレクタの移行の作業を行います。

STEP 1 | 移行計画を立てます。

- M-100　アプライアンスの現在のソフトウェアが 7.0 より前のバージョンである場合はソフトウェアをアップグレードします。M-500 アプライアンスでは Panorama 7.0 以降のバージョンが必要です。ソフトウェア バージョンに関する重要な詳細情報は、「Panorama、ログ コレクタ、ファイアウォール、および WildFire のバージョン互換性」を参照してください。
- システムおよび設定ログを保持したい場合は、移行前に Panorama およびログ コレクタが生成するシステムおよび設定ログを外部の宛先に転送します。Panorama モードの M-Series アプライアンスがこれらのログ タイプを保存する SSD は、モデル間で移動することができません。移動できるのはファイアウォール ログを保存する RAID ドライブのみです。
- 移行用に保守期間をスケジュール設定します。M-100 アプライアンスがオフラインになっても、M-500 アプライアンスがオンラインになった後でファイアウォールはログをバッファリングし

© 2019 Palo Alto Networks, Inc.

て転送することができますが、移行を保守期間中に完了させることで、Panorama モデルを切り替える際にログがバッファ容量を超過して失われるリスクを最低限に抑えられます。

STEP 2 | 新しい M-500 アプライアンスを購入し、サブスクリプションを新しいアプライアンスに移行します。

1. 新しい M-500 アプライアンスを購入します。
2. 新しいサポート ライセンスおよび移行ライセンスを購入します。
3. 新しい M-500 アプライアンスのライセンスを購入する際は、廃止する M-100 アプライアンスのシリアル番号とデバイス管理認証コード、および選択したライセンス移行日を販売代理店に伝えます。M-500 アプライアンスを受け取ったら、Palo Alto Networks が提供する移行およびサポート認証コードを使用してアプライアンスを登録し、デバイス管理とサポートライセンスをアクティブ化します。M-100 のデバイス管理ライセンスは移行日に廃止され、M-100 アプライアンスを使用してデバイスを管理したり、ログを収集したりすることはできなくなります。ただし、サポートライセンスは保持され、Panorama アプライアンスは引き続きサポートされます。発効日後に移行を完了することはできますが、すでに廃止された M-100 アプライアンスで構成の変更をコミットすることはできません。

STEP 3 | Panorama モードの各 M-100 アプライアンスから Panorama 設定をエクスポートします。

M-100 アプライアンス HA ピアに対してこの作業を実行します。

1. M-100 アプライアンスにログインし、**Panorama** > **Setup**（セットアップ）> **Operations**（操作）の順に選択します。
2. **Save named Panorama configuration snapshot**（名前を付けて **Panorama** 設定スナップショットを保存）をクリックし、設定を識別できる **Name**（名前）を入力して **OK** をクリックします。
3. **Export named Panorama configuration snapshot**（名前を付けて **Panorama** 設定スナップショットを保存）をクリックし、先ほど保存した設定の **Name**（名前）を選択して **OK** をクリックします。Panorama が XML ファイルの形式で設定をクライアント システムにエクスポートします。

STEP 4 | Panorama モードの M-100 アプライアンスの電源をオフにします。

1. 電源を切る M-100 アプライアンス HA ピアにログインします。
2. **Panorama** > **Setup** > **Operations** (デバイス > 設定 > 操作) を開き、**Shutdown Panorama** (Panoramaのシャットダウン) をクリックします。

STEP 5 | 各 M-500 アプライアンスの初期セットアップを実行します。

1. M-500 アプライアンスをラックマウントします。方法については、『M-500 アプライアンスのハードウェア リファレンス ガイド』を参照してください。
2. M-Series アプライアンスの初期設定を行い、アクティブなライセンスおよび更新のインストールに必要なネットワーク接続を定義します。
3. Panorama を登録します。
4. Panorama サポート ライセンスのアクティベーションを行います。
5. ファイアウォール管理ライセンスのアクティベーションを行います。移行ライセンスの認証コードを使用します。
6. Panorama のコンテンツ更新とソフトウェア更新のインストールを行います。M-100 アプライアンスのものと同じバージョンをインストールします。
7. （専用ログ コレクタのみ）M-Series アプライアンスをログ コレクタとしてセットアップします。

STEP 6 | 各 M-100 アプライアンスからエクスポートした Panorama 設定スナップショットを Panorama モードの各 M-500 アプライアンス（両方の HA ピア）に読み込みます。

M-500 アプライアンス HA ピアに対してこの作業を実行します。

1. M-500 アプライアンスにログインし、**Panorama** > **Setup**（セットアップ）> **Operations**（操作）の順に選択します。

© 2019 Palo Alto Networks, Inc.

2. **Import named Panorama configuration snapshot**（名前を付けて保存した **Panorama** 設定スナップショットをインポート）をクリックし、M-500 アプライアンスに付与するのと同じ HA 優先度（プライマリあるいはセカンダリ）を持つ M-100 アプライアンスからエクスポートした設定ファイルを **Browse**（参照）し、**OK** をクリックします。
3. **Load named Panorama configuration snapshot**（名前を付けて保存した **Panorama** 設定スナップショットを読み込み）をクリックし、先ほどインポートした設定の**Name**（名前）を選択し、さらに **Decryption Key**（復号化鍵）（Panorama のマスター鍵）を選択して **OK** をクリックします。読み込んだ設定で Panorama が現在の候補設定を上書きします。設定ファイルのロード時にエラーが発生すると Panorama が表示を行います。エラーが発生した場合は、それらのエラーをローカルファイルに保存します。必ず各エラーを解決し、正常に設定が移行されるようにします。
4. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、**Validate Commit**（コミットの検証）を行います。次に進む前にすべてのエラーを解決します。
5. Panorama 設定に対する変更を **Commit**（コミット）します。

STEP 7 | Panorama モードの M-500 アプライアンス HA ピア間で設定を同期します。

1. アクティブ M-500 アプライアンス上で **Dashboard**（ダッシュボード）タブを選択し、High Availability（高可用性）ウィジットで **Sync to peer**（ピアと同期）をクリックします。
2. High Availability（高可用性）ウィジットで、**Local**（ローカル）（プライマリ M-500 アプライアンス）が **active**（アクティブ）であり、**Peer**（ピア）がパッシブであり、**Running Config**（実行中の設定）が **synchronized**（同期済み）であることを確認します。

STEP 8 | RAID ドライブを各 M-100 アプライアンスから交換先の M-500 アプライアンスに移動させ、ファイアウォールから収集したログを移行します。

次の作業では、M-500 アプライアンスに対してすでに行ったステップはすべて飛ばしてください。

- Panorama モードでログを新しい M-Series アプライアンスに移行します。M-100 アプライアンスがデフォルトの管理対象コレクタを使用してログ収集を行う場合のみ、M-100 アプライアンスからログを移行してください。
- ログ コレクタ モードでログを新しい M-Series アプライアンスに移行します。

STEP 9 | Panorama モードのアクティブ M-500 アプライアンスをファイアウォールと同期してファイアウォールの管理を再開します。

このステップは保守期間中に完了させ、ネットワークの中断を最小限に抑えます。

1. アクティブ M-500 アプライアンスで **Panorama** > **Managed Devices**（管理対象のデバイス）の順に選択し、Device State（デバイス状態）列にファイアウォールが **Connected**（接続済み）と表示されることを確認します。

   この段階では、Shared Policy（共有ポリシー）（デバイス グループ）および Template（テンプレート）列にファイアウォールが **Out of sync**（非同期）であると表示されます。
2. 変更をデバイス グループとテンプレートにプッシュします。
   1. **Commit**（コミット）> **Push to Devices**（デバイスへのプッシュ）の順に選択し、**Edit Selections**（選択内容の編集）を行います。
   2. **Device Groups**（デバイス グループ）を選択し、すべてのデバイス グループを選択して、**Include Device and Network Templates**（デバイスおよびネットワーク テンプレートを含める）操作を実行し、**OK** をクリックします。
   3. 変更を **Push**（プッシュ）します。
3. **Panorama** > **Managed Devices**（管理対象デバイス）ページで、Shared Policy（共有ポリシー）および Template（テンプレート）列にファイアウォールが **In sync**（同期中）と表示されることを確認します。

© 2019 Palo Alto Networks, Inc.

Panorama 管理インターフェイスへのアクセスおよびナビゲート

Panorama には以下の 3 つの管理インターフェイスがあります。

- **Web** インターフェイス – Panorama Web インターフェイスの外観と操作感は、ファイアウォールの Web インターフェイスのものに似ています。ファイアウォールを使い慣れていれば、Panorama Web インターフェイスでのナビゲートや管理タスクの実行、レポートの生成を簡単に行うことができます。このグラフィカル インターフェイスでは、HTTPS を使用して Panorama にアクセスできます。これは、管理タスクを実行するための最適な方法です。Panorama Web インターフェイスへのログインおよびPanorama Web インターフェイスへのナビゲートを参照してください。Panorama への HTTP アクセスを有効にする必要がある場合は、**[Panorama]** > [セットアップ] > [管理] タブで [管理インターフェイス設定] を編集します。
- コマンド ライン インターフェイス (**CLI**) – CLI は、コマンドを入力して一連のタスクを完了できる実質的なインターフェイスです。CLI では、2 つのコマンド モード (操作および設定) がサポートされており、それぞれにコマンドとステートメントの独自の階層があります。コマンドのネスト構造と構文に慣れると、CLI の応答時間を短縮し、効率的な管理が可能になります。「Panorama CLI へのログイン」を参照してください。
- **XML API** – XML ベースの API は、HTTP/HTTPS の要求と応答を使用して実装される Web サービスとして提供されます。内部的に開発された既存のアプリケーションやリポジトリの操作および統合を合理化できます。Panorama API の詳細な使用方法は、『PAN-OS および Panorama XML API 利用ガイド』を参照してください。

Panorama Web インターフェイスへのログイン

STEP 1 | インターネット ブラウザを起動させ、安全な接続 (https://<IP address>) を使ってPanoramaのIPアドレスを指定します。

STEP 2 | アカウントに対して使用される認証のタイプに従って Panorama にログインします。Panorama にログインするのが初めての場合は、ユーザー名とパスワードにデフォルト値の `admin` を使用します。

- **SAML** – **Use Single Sign-On** (シングル サインオンの使用) をクリックします (シングル サインオン: SSO)。Panorama が管理者に対して認証 (ロール割り当て) を実行する場合は、**Username** (ユーザー名) を入力して、**Continue** (続行) します。SAML アイデンティティ プロバイダ (IdP) が認証を実行する場合は、**Username** (ユーザー名) を入力せずに **Continue** (続行) します。いずれの場合も、ユーザーは、IdP にリダイレクトされ、ユーザー名とパスワードを入力するように求められます。IdP に対する認証が完了すると、Panorama Web インターフェイスが表示されます。
- 他のタイプの認証 – ユーザーの **Name** (名前) と **Password** (パスワード) を入力します。ログイン ページにバナーとチェック ボックスがある場合は、ログイン バナーを読み、**I Accept and Acknowledge the Statement Below** (次の内容に同意・承認します) を選択します。次に、**Login** (ログイン) をクリックします。

STEP 3 | 本日のメッセージがあれば確認し、**Close** (閉じる) をクリックします。

Panorama Web インターフェイスへのナビゲート

Panorama の設定、ファイアウォール、ログ コレクタ、WildFire アプライアンス、アプライアンス クラスタの管理とモニター、および **Context** (コンテクスト) ドロップダウン メニューを使用した各ファイア

© 2019 Palo Alto Networks, Inc.

ウォールの Web インターフェイスへのアクセスを行うには、Panorama Web インターフェイスを使用します。Web インターフェイスの各タブのオプションおよびフィールドの詳細については、Panorama のオンライン ヘルプを参照してください。各タブの概要を以下の表に示します。

タブ	説明
Dashboard（ダッシュボード）	Panorama モデルとネットワーク アクセスの設定に関する一般情報を表示します。このタブには、アプリケーション、ログ、システム リソース、およびシステム設定に関する情報を表示するウィジットが含まれています。
ACC	Panorama が管理対象ファイアウォールから収集した情報に基づいて、ネットワークの全体的なリスクと脅威レベルを表示します。
監視する	ログおよびレポートを表示および管理します。
[デバイス グループ] > [ポリシー]	ポリシールールを一元的に作成し、複数のファイアウォール/デバイス グループに設定を適用します。 このタブを表示するには、「デバイス グループの追加」を行う必要があります。
[デバイス グループ] > [オブジェクト]	ポリシールールが参照できるポリシーオブジェクト、および管理対象のファイアウォール/デバイスグループが共有できるポリシーオブジェクトを定義します。 このタブを表示するには、「デバイス グループの追加」を行う必要があります。
[テンプレート] > [ネットワーク]	ネットワーク プロファイルなどのネットワーク設定を行い、複数のファイアウォールに適用します。 このタブを表示するには、「 テンプレートの追加」を行う必要があります。
[テンプレート] > [デバイス]	サーバー プロファイルや管理者ロールなどのデバイス設定を行い、複数のファイアウォールに適用します。 このタブを表示するには、「 テンプレートの追加」を行う必要があります。
Panorama	Panorama の設定、ライセンス管理、高可用性のセットアップ、ソフトウェア更新およびセキュリティ アラートへのアクセス、管理アクセスの管理、導入済みファイアウォール、ログ コレクタ、WildFire アプライアンス、アプライアンス クラスタの管理を行います。

Panorama CLI へのログイン

Panorama CLI にログインするには、シリアル ポート接続を使用するか、リモートからSSH（Secure Shell）クライアントを使用します。

- SSH を使用して、Panorama CLI にログインします。

  ログコレクタ モードのM-Seriesアプライアンスでも、同じ手順を使用します。

© 2019 Palo Alto Networks, Inc.

必要に応じて、 SSH 鍵ベースで CLI への認証を行う管理者を設定ができます。

1. 以下の前提条件が満たされることを確認します。
   - Panorama にネットワーク アクセスできるコンピュータがあること。
   - PanoramaのIPアドレスが分かること。
   - 管理インターフェイスが、デフォルト設定であるSSHをサポートしていること。管理者が SSH を無効にしたが、再び有効にしたい場合は、**Panorama** > **Setup**（セットアップ）> **Interfaces**（インターフェイス）の順に選択します。次に、**Management**（管理）をクリックし、**SSH** を選択して **OK** をクリックします。続いて、**Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、Panorama 設定に対して、変更内容を **Commit**（コミット）します。
2. SSH を使用して CLI にアクセスするには、以下の手順を実行します。
   1. SSH クライアントで Panorama IP アドレスを入力し、ポート 22 を使用します。
   2. 管理アクセス認証情報を指示に従って入力します。ログイン後は message of the day（本日のメッセージ）が表示され、次にCLIのプロンプトが操作モードで表示されます。以下に例を示します。

      ```
      admin@ABC_Sydney>
      ```

- シリアル ポート接続を使用して、Panorama CLI にログインします。
  1. 以下のものがあることを確認します。
     - DB-9 シリアル ポートを使用して Panorama をコンピュータに接続するヌル モデム シリアル ケーブル
     - コンピュータで実行中の端末エミュレーション プログラム
  2. ターミナル エミュレーション ソフトウェアで次の設定を使用して接続を行います。9600 ボー、8 データ ビット、1 ストップ ビット、パリティなし、ハードウェア フロー制御なし。
  3. 管理アクセス認証情報を指示に従って入力します。ログイン後は本日のメッセージが表示され、次にCLIのプロンプトが操作モードで表示されます。

- 設定モードに変更します。

  設定モードに切り替えるには、プロンプトで以下のコマンドを入力します。

  ```
  admin@ABC_Sydney> configure
  ```

  プロンプトが `admin@ABC_Sydney#` に変わります。

© 2019 Palo Alto Networks, Inc.

Panorama への管理アクセスのセットアップ

Panoramaはロールベースのアクセス制御（RBAC）を実装しているため、管理者の権限および役割を指定することができます。以下のトピックでは、Panorama Webインターフェイスおよびコマンドラインインターフェイス（CLI）にアクセスするための管理者ロール、アクセスドメイン、アカウントを作成する方法を示します。

- 管理者ロール プロファイルの設定
- アクセス ドメインの設定
- 管理者アカウントおよび認証の設定

管理者ロール プロファイルの設定

管理者ロール プロファイルとは、管理アクセス権限を詳細に定義し、会社の機密情報とエンド ユーザーのプライバシーを保護できるカスタム「管理ロール」です。作業を行う必要がある管理インターフェイスの領域のみへのアクセスを管理者に許可する管理者ロール プロファイルを作成することが推奨されます。

STEP 1 | ファイアウォールの 管理者ロール プロファイルを設定します。

管理者による Panorama と管理対象ファイアウォール Web インターフェース間のコンテキスト切り替えを許可するために、ファイアウォール上で管理者ロール プロファイルを作成し、そのプロファイルを Panorama 管理サーバーの管理者ロール プロファイルに割り当てる必要があります。

STEP 2 | **Panorama** > **Admin Roles** (Panorama > 管理者ロール)の順に選択して **Add** (追加)をクリックします。

STEP 3 | プロファイルの **Name** (名前)を入力し、認証の **Role** (ロール)タイプを選択します。**Panorama**または**Device Group and Template**(デバイス グループとテンプレート)。

STEP 4 | 目的の設定のアイコンを次の中から切り替えることで、Panorama（**Web UI**）およびファイアウォール（**Context Switch UI** (コンテキスト切り替えUI)）の機能領域ごとにアクセス レベルを設定します。Enable（読込・書込）、Read Only (読込のみ)、Disable (無効)。



カスタムロールを持つ管理者がデバイスグループあるいはテンプレートの変更を管理対象のファイアウォールにコミットする場合、そのロールに*Panorama* > *Device Groups* *(Panorama* > デバイスグループ*)*および*Panorama* > *Templates (Panorama* > テンプレート*)*への読込・書込権限を与える必要があります。以前のバージョンの *Panorama* からアップグレードする場合、アップグレード プロセスでそれらのノードへの読み取り専用アクセス権が提供されます。

Panorama ロールのコンテキスト切り替え権限によってファイアウォールの CLI あるいは XML API へのアクセスを管理することはできません。

STEP 5 | **Role**（ロール）タイプが **Panorama** の場合、各機能領域の Enabled/Disabled（有効/無効）のアイコンを切り替えて **XML API** へのアクセスを設定します。

STEP 6 | **Role** (ロール)タイプが**Panorama**の場合、**Command Line** (コマンドライン)インターフェイスへのアクセス レベルを次の中から選択します。**None** (なし)（デフォルト）、**superuser** (スーパーユーザー)、**superreader** (スーパーリーダー)、あるいは**panorama-admin**。

STEP 7 | コンテキスト切り替えを有効にするには、ステップ 1 で作成した **Device Admin Role** (デバイス管理者ロール) を選択します。

© 2019 Palo Alto Networks, Inc.

STEP 8 | **OK** をクリックしてプロファイルを保存します。

アクセス ドメインの設定

「アクセス ドメイン」を使用すれば、特定のデバイス グループおよびテンプレートに対する「デバイス グループおよびテンプレート管理者」を定義したり、その管理者がコンテキストを管理対象ファイアウォールの Web インターフェイスに切り替える権限を制御したりすることができます。Panorama では、最大 4,000 件のアクセス ドメインがサポートされます。

STEP 1 | **[Panorama]** > [アクセス ドメイン] の順に選択し、[追加] をクリックします。

STEP 2 | アクセス ドメインの識別に使用する **Name**（名前）を入力します。

STEP 3 | **Shared Objects**（共有オブジェクト）に対するアクセス権限を選択します。

- **write**（書き込み）— 管理者は共有オブジェクトに対してすべての操作を実行できます。これがデフォルトの値です。
- **read**（読み取り）— 管理者は共有オブジェクトの表示とコピーができますが、その他の操作を実行することはできません。非共有オブジェクトの追加または共有オブジェクトのコピーを行う場合、宛先を、共有領域ではなく、アクセス ドメイン内のデバイス グループにする必要があります。
- **shared-only**（共有のみ）— 管理者はオブジェクトを共有領域にのみ追加できます。管理者は、共有オブジェクトの表示、編集、および削除ができますが、共有オブジェクトの移動とコピーはできません。

このオプションを選択すると、管理者は、非共有オブジェクトに対して表示以外のどの操作も実行できなくなります。たとえば、すべてのオブジェクトをグローバルな単一のレポジトリに入れる必要がある組織などでこのオプションを選択します。

STEP 4 | **Device Groups**（デバイス グループ）タブのアイコンを切り替えて、アクセス ドメイン内のデバイス グループの読み取り/書き込み,あるいは読み取り専用の権限を有効にします。

Shared Objects（共有オブジェクト）に対するアクセス権限を *shared-only*（共有のみ）に設定した場合、読み取り/書き込みアクセス権を指定したすべてのデバイス グループのオブジェクトに読み取り専用アクセス権が割り当てられます。

STEP 5 | **Templates**（テンプレート）タブを選択し、アクセス ドメインに割り当てる各テンプレートを **Add**（追加）します。

STEP 6 | **Device Context**（デバイス コンテキスト）タブを選択し、アクセス ドメインに割り当てるファイアウォールを選択して **OK** をクリックします。管理者は、Panorama の **Context**（コンテキスト）ドロップダウンを使用してこれらのファイアウォールの Web インターフェイスにアクセスできます。

管理者アカウントおよび認証の設定

すでに認証プロファイルを設定しているか、管理者の認証に認証プロファイルが不要な場合は、「Panorama 管理者アカウントの設定」ができます。そうでない場合、次にリストアップされている他のいずれかの作業を行い、特定の種類の認証のために管理者アカウントを設定します。

- Panorama 管理者アカウントの設定
- Panorama 管理者用にローカルあるいは外部認証を設定
- 証明書ベースで Web インターフェイスへの認証を行う Panorama 管理者を設定
- SSH 鍵ベースで CLI への認証を行う管理者を設定
- Panorama 管理者用に RADIUS 認証を設定

© 2019 Palo Alto Networks, Inc.

- Panorama 管理者用に TACACS+ 認証を設定
- Panorama 管理者用に SAML 認証を設定

Panorama 管理者アカウントの設定

管理者アカウントにより、Panorama 管理者の管理ロールおよび認証が指定されます。ロールを割り当てて認証を実行するために使用するサービスにより、アカウントを Panorama、外部サーバー、その両方（「管理認証」を参照）のいずれかで追加するかが決まります。外部認証サービスの場合、管理者アカウントを追加する前に認証プロファイルを設定する必要があります（「管理者アカウントおよび認証の設定」を参照）。すでに認証プロファイルを設定しているか、Panorama に対してローカルな認証メカニズムを使用する場合は、次の手順を実行して Panorama で管理者アカウントを追加します。

管理者アカウントを専用ログ コレクタ（ログ コレクタ モードの *M-Series* アプライアンス）に追加することはできません。専用ログ コレクタでは、デフォルトのユーザー名（*admin*）を持つ事前定義済みの管理者アカウントのみを利用できます。

STEP 1 | **Panorama** > **Administrators**（管理者）の順に選択し、アカウントを **Add**（追加）します。

STEP 2 | **Name**（名前）に管理者のユーザー名を入力します。

STEP 3 | **Authentication Profile**（認証プロファイル）を選択するか、管理者の認証を複数設定している場合はシーケンスを選択します。

これは、Panorama が認証に Kerberos SSO または外部サービスを使用する場合に必要です。

Panorama がローカル認証を使用する場合は、**Authentication Profile**（認証プロファイル）を **None**（なし）に設定し、**Password**（パスワード）および **Confirm Password**（確認用パスワード）を入力します。

STEP 4 | **Administrator Type**（管理者タイプ）を選択します。

- **Dynamic**（動的）– 事前定義済みの管理者ロールを選択します。
- **Custom Panorama Admin**（カスタム **Panorama** 管理者）– この管理者のために作成した管理者ロールの **Profile**（プロファイル）を選択します（「管理者ロール プロファイルの設定」を参照）。
- **Device Group and Template Admin**（デバイス グループおよびテンプレート管理者）– 次のステップで説明しているように、アクセス ドメインを管理ロールにマッピングします。

STEP 5 | （デバイス グループおよびテンプレート管理者のみ）Access Domain to Administrator Role（管理者ロールに対するアクセス ドメイン）セクションで、**Add**（追加）をクリックし、ドロップダウンから Access Domain（アクセス ドメイン）を選択して（「アクセスドメインの設定」を参照）、隣接する Admin Role（管理者ロール）セルをクリックして Admin Role（管理者ロール）プロファイルを選択します。

STEP 6 | **OK** をクリックして変更内容を保存します。

STEP 7 | **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

Panorama 管理者用にローカルあるいは外部認証を設定

外部認証サービスまたは Panorama に対してローカルなサービスを使用して、Panorama にアクセスする管理者を認証できます。これらの認証方式では、ユーザー名とパスワードを入力するためのログイン ページなど、1 つ以上の認証チャレンジに応答することを管理者に要求します。

© 2019 Palo Alto Networks, Inc.

外部サービスを使用して認証と承認（ロールおよびアクセス ドメインの割り当て）の両方を管理する場合は、以下を参照してください。

- Panorama 管理者用に RADIUS 認証を設定
- Panorama 管理者用に TACACS+ 認証を設定
- Panorama 管理者用に SAML 認証を設定

チャレンジ応答メカニズムを使用せずに管理者を認証するには、証明書ベースで Web インターフェイスへの認証を行う Panorama 管理者を設定する方法と SSH 鍵ベースで CLI への認証を行う管理者を設定する方法があります。

STEP 1 | （外部認証のみ）管理者を認証するために Panorama が外部サーバーに接続できるようにします。

1. **Panorama** > **Server Profiles**（サーバー プロファイル）の順に選択し、サービス タイプ（**RADIUS**、**TACACS+**、**SAML**、**LDAP**、または **Kerberos**）を選択して、サーバー プロファイルを設定します。

   - Panorama 管理者用に RADIUS 認証を設定。

     RADIUS サーバーを使用して、*RADIUS* 認証サービスまたはマルチファクタ認証（MFA）サービスをサポートできます。

   - Panorama 管理者用に TACACS+ 認証を設定。
   - SAML IdP サーバー プロファイルを追加します。Kerberos シングル サインオン（SSO）を SAML SSO と統合することはできません。1 つのタイプの SSO サービスのみを使用できます。
   - Kerberos サーバー プロファイルを追加。
   - LDAP サーバー プロファイルを追加。

STEP 2 | （任意）Panorama がローカル認証を使用する場合、パスワードの複雑性と有効期限設定を定義します。

この設定によって攻撃者がパスワードを推定することが難しくなるため、Panorama への不正なアクセスを防止するのに役立ちます。

1. パスワードの複雑性をグローバルに定義し、すべてのローカル管理者の有効期限を設定します。
   1. **Panorama** > **Setup**（セットアップ）> **Management**（管理）の順に選択し、Minimum Password Complexity（パスワード複雑性）設定を編集します。
   2. **Enabled**（有効）を選択します。
   3. パスワード設定を定義し、**OK** をクリックします。
2. パスワード プロファイルを定義します。

   グローバルなパスワード有効期限設定をオーバーライドする管理者アカウントにプロファイルを割り当てます。

   1. **Panorama** > **Password Profiles**（パスワード プロファイル）の順に選択し、プロファイルを **Add**（追加）します。
   2. プロファイルを識別する **Name**（名前）を入力します。
   3. パスワードの有効期限設定を行い、**OK** をクリックします。

STEP 3 | （Kerberos SSO のみ）Kerberos キータブを作成します。

キータブとは、Panorama の Kerberos アカウント情報が含まれるファイルです。Kerberos SSO をサポートするには、ネットワークに Kerberos インフラストラクチャが必要です。

STEP 4 | 認証プロファイルを設定します。

© 2019 Palo Alto Networks, Inc.

管理者アカウントが複数のタイプのサーバーに分かれて保存されている場合、各タイプの認証プロファイルを作成し、すべてのプロファイルを認証シーケンスに追加できます。

認証プロファイルで、認証サービスの **Type**（タイプ）および関連する設定を指定します。

- 外部サービス – 外部サービスの **Type**（タイプ）を選択し、その外部サービス用に作成した **Server Profile**（サーバー プロファイル）を選択します。
- ローカル認証 – **Type**（タイプ）を **None**（なし）に設定します。
- **Kerberos SSO** – **Kerberos Realm**（**Kerberos** レルム）を指定し、作成した **Kerberos Keytab**（**Kerberos** キータブ）を **Import**（インポート）します。

STEP 5 | （デバイス グループおよびテンプレート管理者のみ）アクセス ドメインの設定を行います。

1 つ以上のアクセス ドメインを設定します。

STEP 6 | （カスタム ロールのみ）管理者ロール プロファイルの設定を行います。

1 つ以上の管理者ロール プロファイルを設定します。

カスタム Panorama 管理者の場合、プロファイルによってアカウントのアクセス権限が定義されます。デバイス グループおよびテンプレート管理者の場合、プロファイルによってアカウントに関連する 1 つ以上のアクセス ドメインのアクセス権限が定義されます。

STEP 7 | 管理者を設定します。

1. Panorama 管理者アカウントの設定を行います。
   - **Authentication Profile**（認証プロファイル）または設定したシーケンスを割り当てます。
   - （デバイス グループおよびテンプレート管理者のみ）アクセス ドメインを管理者ロール プロファイルにマッピングします。
   - （ローカル認証のみ）設定している場合、**Password Profile**（パスワード プロファイル）を選択します。
2. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。
3. （任意）認証サーバーの接続をテストし、Panorama が認証プロファイルを使用して管理者を認証できることを確認します。

証明書ベースで *Web* インターフェイスへの認証を行う *Panorama* 管理者を設定

Panorama Web インターフェイスに対するパスワード ベース認証のより安全な方法として、Panorama に対してローカルな管理者アカウントの証明書ベースの認証を設定できます。証明書ベースの認証では、パスワードの代わりにデジタル署名の交換と検証が行われます。

いずれかの管理者の証明書ベースの認証を設定すると、*Panorama* およびすべての管理者のユーザー名/パスワード ログインが無効になり、その後管理者がログインするには証明書が必要になります。

STEP 1 | Panorama の認証局（CA）証明書を生成します。

この CA 証明書を使用して、各管理者のクライアント証明書に署名します。

自己署名ルート CA 証明書を作成します。

© 2019 Palo Alto Networks, Inc.

または、エンタープライズ *CA* から証明書をインポートすることもできます。

STEP 2 | Web インターフェイスへのアクセスをセキュリティ保護するための証明書プロファイルを設定します。

1. **[Panorama]** > **[証明書の管理]** > **[証明書プロファイル]** の順に選択し、**[追加]** をクリックします。
2. 認証プロファイルの **Name**（名前）を入力し、（ユーザー名フィールド）を **Subject**（サブジェクト）に設定します。
3. CA Certificates（CA 証明書）セクションで **Add**（追加）を選択し、作成した **CA Certificate**（**CA** 証明書）を選択します。
4. **OK** をクリックしてプロファイルを保存します。

STEP 3 | 管理者の認証に証明書プロファイルを使用するように Panorama を設定します。

1. **Panorama** > **Setup** > **Management** (Panorama > セットアップ > 管理) の順に選択し、Authentication Settings (認証設定)を編集します。
2. 先ほど作成した **Certificate Profile**（証明書プロファイル）を選択し、**OK** をクリックします。

STEP 4 | クライアント証明書の認証を使用するように管理者アカウントを設定します。

Panorama 管理者アカウントの設定Panorama Web インターフェイスにアクセスする各管理者が対象です。**Use only client certificate authentication (Web)**（クライアント証明書認証のみを使用（**Web**））チェック ボックスをオンにします。

エンタープライズ CA が生成したクライアント証明書をすでにデプロイしている場合は、ステップ「8」に進みます。そうでない場合はステップ「5」に進みます。

STEP 5 | 各管理者のクライアント証明書を生成します。

Panorama で証明書を生成します。**Signed By**（署名者）ドロップダウンで、作成した CA 証明書を選択します。

STEP 6 | クライアント証明書をエクスポートします。

1. 証明書をエクスポートします。
2. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

   Panorama が再起動し、ログイン セッションが終了します。その後、管理者は生成されたクライアント証明書のあるクライアント システムからのみ Web インターフェイスにアクセスできます。

STEP 7 | Web インターフェイスにアクセスする各管理者のクライアント システムにクライアント証明書をインポートします。

このステップを完了させる際、必要に応じて Web ブラウザのドキュメントを参照してください。

STEP 8 | 管理者が Web インターフェイスにアクセスできることを確認します。

1. クライアント証明書があるコンピュータのブラウザで Panorama の IP アドレスを開きます。
2. 入力画面が表示されたら、インポートした証明書を選択して **OK** をクリックします。ブラウザに証明書警告が表示されます。
3. ブラウザの例外リストに証明書を追加します。
4. **Login**（ログイン）をクリックします。ユーザー名やパスワードのプロンプトは表示されずに Web インターフェイスが表示されます。

© 2019 Palo Alto Networks, Inc.

SSH 鍵ベースで CLI への認証を行う管理者を設定

Panorama CLI へのアクセスにセキュア シェル（SSH）を使用する管理者の場合、SSH 鍵によってパスワードよりも安全な認証方式が提供されます。SSH キーでは、ブルート フォース攻撃のリスクがほぼなくなり、2 要素認証（秘密鍵とパスフレーズ）のオプションが提供され、ネットワーク上でパスワードが送信されることはありません。さらに、CLI にアクセスするための自動スクリプトも有効になります。

STEP 1 | SSH キー生成ツールを使用して、管理者のクライアント システムで非対称のキー ペアを作成します。

サポートされているキー フォーマットは、IETF SECSH と Open SSH です。サポートされているアルゴリズムは、DSA（1,024 ビット）と RSA（768 ~ 4096 ビット）です。

キー ペアを生成するコマンドは、SSH クライアントのドキュメントを参照してください。

公開鍵と秘密鍵は個別のファイルです。Panorama がアクセスできる場所に両方のファイルを保存します。セキュリティ強化のため、パスフレーズを入力して、秘密鍵を暗号化します。ログイン中に、Panorama によってこのパスフレーズの入力が管理者に促されます。

STEP 2 | 公開鍵の認証を使用するように管理者アカウントを設定します。

1. Panorama 管理者アカウントの設定.
   - SSH 鍵認証が失敗した場合にフォールバックとして使用する認証方式の 2 つのうち、いずれかを設定します。

     外部認証サービス – **Authentication Profile**（認証プロファイル）を選択します。

     ローカル認証 – **Authentication Profile**（認証プロファイル）を **None**（なし）に設定し、**Password**（パスワード）および **Confirm Password**（確認用パスワード）を入力します。
   - **Use Public Key Authentication**（**SSH**）（公開鍵認証（**SSH**）の使用）チェック ボックスをオンにし、**Import Key**（鍵のインポート）をクリックし、生成した公開鍵を **Browse**（参照）して **OK** をクリックします。
2. **OK** をクリックして管理者アカウントを保存します。
3. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

STEP 3 | Panorama に対する認証に秘密鍵を使用するよう SSH クライアントを設定します。

管理者のクライアント システムでこのタスクを実行します。このステップを完了させる際、必要に応じて SSH クライアントのドキュメントを参照してください。

STEP 4 | 管理者が SSH 鍵認証を使用して Panorama CLI にアクセスできることを確認します。

1. 管理者のクライアント システムのブラウザを使用して、Panorama の IP アドレスに移動します。
2. 管理者として Panorama CLI にログインします。ユーザー名を入力すると、以下の出力が表示されます（キー値は例です）。

   ```
   Authenticating with public key “dsa-key-20130415”
   ```
3. プロンプトが表示されたら、キーの作成時に定義したパスフレーズを入力します。

Panorama 管理者用に RADIUS 認証を設定

RADIUS サーバーを使用して、Panorama Web インターフェイスへの管理アクセスを認証できます。RADIUS サーバーでベンダー固有属性（VSA）を定義し、管理者認証を管理することもできます。VSA を使用すれば、ディレクトリ サービスを介してロール、アクセス ドメイン、管理者のユーザー グループをすばやく変更できます。この方法は多くの場合、Panorama で設定し直すよりも簡単です。

© 2019 Palo Alto Networks, Inc.

RADIUS サーバーを使用して、*Panorama Web* インターフェイスへの管理アクセスを認証できます。*RADIUS* サーバーでベンダー固有属性（VSA）を定義し、管理者認証を管理することもできます。*VSA* を使用すれば、ディレクトリ サービスを介してロール、アクセス ドメイン、管理者のユーザー グループをすばやく変更できます。この方法は多くの場合、*Panorama* で設定し直すよりも簡単です。

Palo Alto Networks RADIUS ディクショナリーを *RADIUS* サーバーにインポートして、*Panorama* と *RADIUS* サーバー間の通信に必要な認証属性を定義することができます。

RADIUS サーバーを使用して、管理者用に多要素認証（MFA）を実装することもできます。

STEP 1 | RADIUS サーバー プロファイルを追加します。

プロファイルにより、Panorama が RADIUS サーバーに接続する方法が定義されます。

1. **Panorama** > **Server Profiles**（サーバー プロファイル）> **RADIUS** の順に追加し、プロファイルを **Add**（追加）します。
2. サーバー プロファイルを識別する **Profile Name**（プロファイル名）を入力します。
3. 認証要求がタイムアウトするまでの**Timeout (**タイムアウト**)** 時間を秒単位で入力します（デフォルトは 3、範囲は1 ~ 20）。

   サーバー プロファイルを使用して *Panorama* を *MFA* サービスと統合する場合、管理者が認証チャレンジに応答する時間が十分に確保されるよう考慮して時間を入力します。たとえば、*MFA* サービスがワンタイム パスワード（*OTP*）を要求する場合、管理者には自分のエンドポイント デバイスで *OTP* を確認し、*MFA* ログイン ページに *OTP* を入力するまでの時間が必要です。
4. Panorama が RADIUS サーバーに認証するために使用する **Authentication Protocol**（認証プロトコル）（デフォルトは **CHAP**）を選択します。

   RADIUS サーバーがサポートする場合は *CHAP* を選択します。このプロトコルは *PAP* よりも安全です。
5. 各 RADIUS サーバーを **Add**（追加）して、以下を入力します。
   - サーバーの識別に使用する **Name**（名前）
   - **RADIUS Server**（**RADIUS** サーバー）の IP アドレスまたは FQDN
   - **Secret**（シークレット）/**Confirm Secret**（再入力 シークレット）（ユーザー名とパスワードを暗号化するための鍵）
   - 認証要求用のサーバー **Port**（ポート）（デフォルトは 1812）
6. **OK** をクリックしてサーバー プロファイルを保存します。

STEP 2 | RADIUS サーバー プロファイルを認証プロファイルに割り当てます。

認証プロファイルにより、一連の管理者に共通の認証設定が定義されます。

1. **Panorama** > **Authentication Profile**（認証プロファイル）の順に選択し、プロファイルを **Add**（追加）します。
2. 認証プロファイルを識別する **Name**（名前）を入力します。
3. **Type**（タイプ）を **RADIUS** に設定します。
4. 設定した **Server Profile**（サーバー プロファイル）を選択します。
5. **Retrieve user group from RADIUS**（**RADIUS** からユーザー グループを取得）を選択して、RADIUS サーバーで定義された VSA からユーザー グループ情報を収集します。

   Panorama は、グループ情報を認証プロファイルの Allow List（許可リスト）で指定したグループと照合します。

© 2019 Palo Alto Networks, Inc.

6. **Advanced**（詳細）を選択し、Allow List（許可リスト）で、この認証プロファイルで認証することが許可された管理者を **Add**（追加）します。
7. **OK** をクリックして認証プロファイルを保存します。

STEP 3 | すべての管理者に認証プロファイルを使用するように Panorama を設定します。

1. **Panorama** > **Setup**（セットアップ）> **Management**（管理）の順に選択し、Authentication Settings（認証設定）を編集します。
2. 設定した **Authentication Profile**（認証プロファイル）を選択し、**OK** をクリックします。

STEP 4 | 管理者用に、認証設定を定義するアクセスドメインおよびロールを設定します。

1. 管理者が事前定義済みの（動的）ロールの代わりにカスタム ロールを使用する場合、管理者ロール プロファイルの設定を行います。
2. 管理者がデバイス グループとテンプレート ロールを使用する場合は、アクセス ドメインの設定を行います。

STEP 5 | 変更をコミットします。

Commit（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

STEP 6 | RADIUS サーバーを設定します。

これらの手順を実行するには、RADIUS サーバーのドキュメントで各手順を参照してください。

1. Panorama の IP アドレスまたはホスト名を RADIUS クライアントとして追加します。
2. 管理者アカウントを追加します。

   RADIUS サーバー プロファイルで *Authentication Protocol*（認証プロトコル）として *CHAP* を指定している場合、逆暗号化されたパスワードを使用してアカウントを定義する必要があります。定義していないと *CHAP* 認証に失敗します。
3. Panorama のベンダー コード（25461）を定義し、各管理者のロール、アクセス ドメイン、ユーザー グループ用に RADIUS VSA を定義します。

   ユーザーの動的管理者ロールを事前定義する場合、小文字を使用してロールを指定します (例えば、`SuperUser` ではなく、`superuser` と入力します。)

STEP 7 | RADIUS サーバーが管理者の認証および承認を実行することを確認します。

1. RADIUS サーバーに追加した管理者アカウントを使用して Panorama Web インターフェイスにログインします。
2. 管理者に関連付けたロールに許可された Web インターフェイス ページにしかアクセスできないことを確認します。
3. **Monitor**（監視）タブ、**Policies**（ポリシー）タブ、**Objects**（オブジェクト）タブで、管理者に関連付けたアクセス ドメインに許可されたデバイス グループにしかアクセスできないことを確認します。

Panorama 管理者用に *TACACS+* 認証を設定

TACACS+ サーバーを使用して、Panorama Web インターフェイスへの管理アクセスを認証できます。TACACS+ サーバーでベンダー固有属性（VSA）を定義し、管理者認証を管理することもできます。VSA を使用すれば、ディレクトリ サービスを介してロール、アクセス ドメイン、管理者のユーザー グループをすばやく変更できます。この方法は多くの場合、Panorama で設定し直すよりも簡単です。

STEP 1 | TACACS+サーバー プロファイルを追加します。

プロファイルにより、Panorama が TACACS+ サーバーに接続する方法が定義されます。

© 2019 Palo Alto Networks, Inc.

1. **Panorama** > **Server Profiles**（サーバー プロファイル）> **TACACS+** の順に選択し、プロファイルを **Add**（追加）します。
2. サーバー プロファイルを識別する **Profile Name**（プロファイル名）を入力します。
3. 認証要求がタイムアウトするまでの**Timeout (**タイムアウト**)** 時間を秒単位で入力します（デフォルトは 3、範囲は1 ~ 20）。
4. Panorama が TACACS+ サーバーに認証するために使用する **Authentication Protocol**（認証プロトコル）（デフォルトは **CHAP**）を選択します。

   TACACS+ サーバーがサポートする場合は *CHAP* を選択します。このプロトコルは *PAP* よりも安全です。
5. 各 TACACS+ サーバーを **Add**（追加）して、以下を入力します。
   - サーバーの識別に使用する **Name**（名前）
   - **TACACS+ Server**（**TACACS+** サーバー）の IP アドレスまたは FQDN
   - **Secret**（シークレット）/**Confirm Secret**（再入力 シークレット）（ユーザー名とパスワードを暗号化するための鍵）
   - 認証要求用のサーバー **Port**（ポート）（デフォルトは49）
6. **OK** をクリックしてサーバー プロファイルを保存します。

STEP 2 | TACACS+ サーバー プロファイルを認証プロファイルに割り当てます。

認証プロファイルにより、一連の管理者に共通の認証設定が定義されます。

1. **Panorama** > **Authentication Profile**（認証プロファイル）の順に選択し、プロファイルを **Add**（追加）します。
2. プロファイルを識別する **Name**（名前）を入力します。
3. **Type**（タイプ）を **TACACS+** に設定します。
4. 設定した **Server Profile**（サーバー プロファイル）を選択します。
5. **Retrieve user group from TACACS+**（**TACACS+** からユーザー グループを取得）を選択して、TACACS+ サーバーで定義された VSA からユーザー グループ情報を収集します。

   Panorama は、グループ情報を認証プロファイルの Allow List（許可リスト）で指定したグループと照合します。
6. **Advanced**（詳細）を選択し、Allow List（許可リスト）で、この認証プロファイルで認証することが許可された管理者を **Add**（追加）します。
7. **OK** をクリックして認証プロファイルを保存します。

STEP 3 | すべての管理者に認証プロファイルを使用するように Panorama を設定します。

1. **Panorama** > **Setup**（セットアップ）> **Management**（管理）の順に選択し、Authentication Settings（認証設定）を編集します。
2. 設定した **Authentication Profile**（認証プロファイル）を選択し、**OK** をクリックします。

STEP 4 | 管理者用に、認証設定を定義するアクセスドメインおよびロールを設定します。

1. 管理ユーザーが定義済みの（動的）ロールではなくカスタムロールを使用する場合は、管理者ロール プロファイルの設定を行います。
2. 管理者がデバイス グループとテンプレート ロールを使用する場合は、アクセス ドメインの設定を行います。

STEP 5 | 変更をコミットします。

Commit（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

© 2019 Palo Alto Networks, Inc.

STEP 6 | 管理者を認証して承認するように TACACS+ サーバーを設定します。

これらの手順を実行するには、TACACS+ サーバーのドキュメントで各手順を参照してください。

1. Panorama の IP アドレスまたはホスト名を TACACS+ クライアントとして追加します。
2. 管理者アカウントを追加します。

   Authentication Protocol（認証プロトコル）として *CHAP* を選択した場合、逆暗号化されたパスワードを使用してアカウントを定義する必要があります。定義していないと *CHAP* 認証に失敗します。
3. 各管理者のロール、アクセス ドメイン、ユーザー グループ用に TACACS+ VSA を定義します。

   ユーザーの動的管理者ロールを事前定義する場合、小文字を使用してロールを指定します *(*例えば、***`SuperUser`*** ではなく、***`superuser`*** と入力します。*)*

STEP 7 | TACACS+ サーバーが管理者の認証および承認を実行することを確認します。

1. TACACS+ サーバーに追加した管理者アカウントを使用して Panorama Web インターフェイスにログインします。
2. 管理者に関連付けたロールに許可された Web インターフェイス ページにしかアクセスできないことを確認します。
3. **Monitor**（監視）タブ、**Policies**（ポリシー）タブ、**Objects**（オブジェクト）タブで、管理者に関連付けたアクセス ドメインに許可された仮想システムにしかアクセスできないことを確認します。

Panorama 管理者用に *SAML* 認証を設定

Panorama Web インターフェイス（CLI を除く）への管理アクセスに Security Assertion Markup Language（SAML）2.0 を使用できます。SAML 属性を使用して管理者の認証を管理することもできます。SAML 属性を使用すれば、Panorama で設定し直す代わりに、ディレクトリ サービスを介してロール、アクセス ドメイン、管理者のユーザー グループをすばやく変更できます。

SAML シングル サインオン (SSO)およびシングル ログアウト (SLO)を設定するには、Panorama と ID プロバイダ (IdP)を互いに登録して、両者間の通信を有効にする必要があります。IdP によって登録情報が含まれるメタデータ ファイルが提供される場合、Panorama にインポートして IdP を登録し、IdP サーバー プロファイルを作成できます。サーバー プロファイルにより、IdP に接続する方法が定義され、IdP が SAML メッセージに署名するために使用する証明書が指定されます。Panorama 用の証明書を使用して SAML メッセージに署名することもできます。証明書の使用は任意ですが、Panorama と IdP 間の通信を保護するために使用することをお勧めします。

STEP 1 | （推奨）IdP と Panorama が SAML メッセージに署名するために使用する証明書を取得します。

証明書で鍵の用途の属性が指定されない場合、デフォルトではメッセージへの署名を含めてすべての用途が許可されます。この場合、どのような方法で証明書を取得しても構いません。

証明書で鍵の用途の属性が指定されている場合、属性の 1 つはデジタル署名である必要があります。デジタル署名は Panorama で生成する証明書では使用できません。この場合、証明書をインポートする必要があります。

- **Panorama** が **SAML** メッセージに署名するために使用する証明書 – エンタープライズ認証局（CA）またはサードパーティの CA から証明書をインポートします。
- **IdP** が **SAML** メッセージに署名するために使用する証明書 – IdP から証明書が含まれるメタデータ ファイルをインポートします（次のステップを参照）。IdP 証明書は以下のアルゴリズムに制限されています。
  - 公開鍵アルゴリズム – RSA（1,024 ビット以上）および ECDSA（すべてのサイズ）。
  - シグネチャ アルゴリズム – SHA1、SHA256、SHA384、SHA512。

© 2019 Palo Alto Networks, Inc.

STEP 2 | SAML IdP サーバー プロファイルを追加します。

サーバー プロファイルは IdP を Panorama に登録し、接続方法を定義します。

この例では、SAML メタデータ ファイルを IdP からインポートするため、Panorama は自動的にサーバー プロファイルを作成し、接続、登録、IdP 証明書に関する情報を入力できます。



IdP によってメタデータ ファイルが提供されない場合、*Panorama* > *Server Profiles*（サーバー プロファイル）> *SAML Identity Provider*（*SAML* アイデンティティ プロバイダ）の順に選択し、サーバー プロファイルを *Add*（追加）して、情報を手動で入力します（値については *IdP* 管理者にお尋ねください）。

1. SAML メタデータ ファイルを IdP から Panorama がアクセスできるクライアント システムにエクスポートします。

   ファイルで指定された証明書は、前のステップで示した要件を満たす必要があります。ファイルのエクスポート手順については、IdP のドキュメントを参照してください。
2. **Panorama** > **Server Profiles**（サーバー プロファイル）> **SAML Identity Provider**（**SAML** アイデンティティ プロバイダ）の順に選択し、メタデータ ファイルを Panorama に **Import**（インポート）します。
3. サーバー プロファイルを識別する **Profile Name**（プロファイル名）を入力します。
4. **Identity Provider Metadata**（アイデンティティ プロバイダ メタデータ）ファイルを **Browse**（参照）します。
5. （推奨）**Validate Identity Provider Certificate**（アイデンティティ プロバイダ証明書の検証）を選択（デフォルト）して、Panorama が **Identity Provider Certificate**（アイデンティティ プロバイダ証明書）を検証するようにします。

   検証は、サーバー プロファイルを認証プロファイルに割り当てて **Commit**（コミット）した後にのみ行われます。Panorama は認証プロファイルの **Certificate Profile**（証明書プロファイル）を使用して証明書を検証します。

   セキュリティを高めるために証明書を検証することをお勧めします。
6. **Maximum Clock Skew**（最大クロック スキュー）を入力します。これは、Panorama が IdP メッセージを検証するときに IdP と Panorama で許可されるシステム時間の誤差（秒単位）です（デフォルトは 60、範囲は 1 ~ 900）。誤差がこの値を超えると、認証が失敗します。
7. **OK** をクリックしてサーバー プロファイルを保存します。
8. サーバー プロファイルの Name（名前）をクリックしてプロファイル設定を表示します。インポートした情報が正しいことを確認し、必要に応じて編集します。

STEP 3 | 認証プロファイルを設定します。

認証プロファイルにより、SAML IdP サーバー プロファイルが指定され、SLO などの認証プロセスのオプションが定義されます。

1. **Panorama** > **Authentication Profile**（認証プロファイル）の順に選択し、プロファイルを **Add**（追加）します。
2. プロファイルを識別する **Name**（名前）を入力します。
3. **Type**（タイプ）を **SAML** に設定します。
4. 設定した **IdP Server Profile**（**IdP** サーバー プロファイル）を選択します。
5. **Certificate for Signing Requests**（署名要求の証明書）を選択します。

   Panorama はこの証明書を使用して、IdP に送信するメッセージに署名します。
6. （任意）**Enable Single Logout**（シングル ログアウトの有効化）を行います（デフォルトでは無効）。

© 2019 Palo Alto Networks, Inc.

7. Panorama が **Identity Provider Certificate**（アイデンティティ プロバイダ証明書）を検証するために使用する **Certificate Profile**（証明書プロファイル）を選択します。
8. IdP メッセージがユーザーを識別するために使用する **Username Attribute (ユーザー名属性)** を入力します（デフォルトは **`username`**）。

   ユーザーの動的管理者ロールを事前定義する場合、小文字を使用してロールを指定します (例えば、***`SuperUser`*** ではなく、***`superuser`*** と入力します。)*IdP* アイデンティティ ストアを介して管理者の認証を管理する場合、*Admin Role Attribute*（管理者ロール属性）および *Access Domain Attribute*（アクセス ドメイン属性）も指定します。
9. **Advanced**（詳細）を選択し、この認証プロファイルで認証できる管理者を **Add**（追加）します。
10. **OK** をクリックして認証プロファイルを保存します。

STEP 4 | すべての管理者に認証プロファイルを使用するように Panorama を設定します。

1. **Panorama** > **Setup**（セットアップ）> **Management**（管理）の順に選択し、Authentication Settings（認証設定）を編集し、設定した **Authentication Profile**（認証プロファイル）を選択します。
2. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、Panorama で変更をアクティベートし、SAML IdP サーバー プロファイルに割り当てた **Identity Provider Certificate**（アイデンティティ プロバイダ証明書）を検証します。

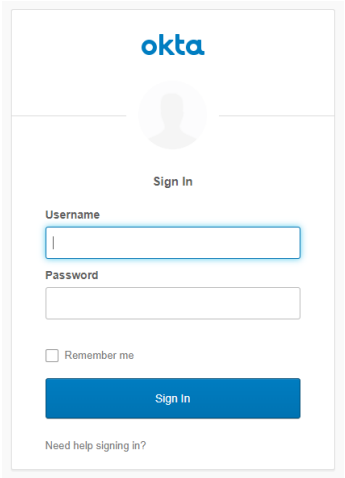
STEP 5 | SAML メタデータ ファイルを作成して IdP で Panorama を登録します。

1. **Panorama** > **Authentication Profile**（認証プロファイル）の順に選択し、設定した認証プロファイルの Authentication（認証）列で **Metadata**（メタデータ）をクリックします。
2. **Management Choice**（管理方法の選択）を **Interface**（インターフェイス）（デフォルトで選択済み）に設定し、管理（MGT）インターフェイスを選択します。
3. **OK** をクリックして、メタデータ ファイルをクライアント システムに保存します。
4. メタデータ ファイルを IdP サーバーにインポートして Panorama を登録します。手順は、IdP のドキュメントを参照してください。

STEP 6 | 管理者が SAML SSO を使用して認証できることを確認します。

1. Panorama Web インターフェイスの URL に移動します。
2. **Use Single Sign-On**（シングル サインオンの使用）をクリックします。
3. **Continue**（続行）をクリックします。

   Panorama によって IdP に対して認証するようにリダイレクトされ、ログイン ページが表示されます。以下に例を示します。



© 2019 Palo Alto Networks, Inc.

4. SSO ユーザー名とパスワードを使用してログインします。

   IdP で認証に成功したら、再び Panorama にリダイレクトされ、Web インターフェイスが表示されます。
5. Panorama 管理者アカウントを使用して別の SSO アプリケーションへのアクセスを要求します。

   正常にアクセスできれば、SAML SSO の認証に成功したことになります。

© 2019 Palo Alto Networks, Inc.

カスタム証明書を使用する認証のセットアップ

デフォルトでは、Palo Alto Networks デバイスは、管理アクセスおよびデバイス間通信に使用される SSL 接続を確立するための相互認証に事前定義済みの証明書を使用します。ただし、代わりにカスタム証明書を使用して認証を設定することもできます。さらに、カスタム証明書を使用して Panorama HA ピア間の高可用性（HA）接続を保護することもできます。カスタム証明書を使用すれば、Panorama、管理対象ファイアウォール、ログ コレクタ間の相互認証を確認する固有のトラストのチェーンを確立できます。証明書の詳細と、Panorama、ログ コレクタ、ファイアウォールでの証明書のデプロイ方法は、「Certificate Management（証明書の管理）」を参照してください。

次のトピックでは、Panorama を使用してカスタム証明書を設定および管理する方法について説明します。

- SSL/TLS 接続を相互に認証する方法
- Panorama でのカスタム証明書を使用する認証の設定
- 管理対象デバイスでのカスタム証明書を使用する認証の設定
- 新しいクライアント デバイスの追加
- 証明書の変更

SSL/TLS 接続を相互に認証する方法

通常の SSL 接続では、サーバーのみが証明書を提示してクライアントに対して自分自身を証明する必要があります。相互 SSL 認証では、クライアントもサーバーに対して証明書を提示します。プライマリ Panorama HAピア、ログ コレクタ、WildFire アプライアンス、および PAN-DB アプライアンスは、サーバーとして機能します。ファイアウォール、ログ コレクタ、WildFire アプライアンス、セカンダリ Panorama HA ピアは、クライアントとして動作できます。デバイスが取るロールはデプロイ環境によって決まります。たとえば次の図では、Panorama は多くのファイアウォールとコレクタ グループを管理し、ファイアウォールとログ コレクタのサーバーとして動作します。ログ コレクタは、ログを送信するファイアウォールのサーバーとして動作します。

デプロイ環境で相互認証のカスタム証明書をデプロイするには、次のものが必要となります。

- **SSL/TLS** サービス プロファイル — SSL/TLS サービス プロファイルでは、カスタム証明書を参照して、サーバー デバイスがクライアント デバイスとの通信に使用する SSL/TLS プロトコル バージョンを確立し、接続のセキュリティを定義します。
- サーバーの証明書とプロファイル — サーバー ロールのデバイスには、クライアント デバイスに対して自分自身を証明するため、証明書と証明書プロファイルが必要です。この証明書は、会社の公開鍵基盤（PKI）からデプロイするか、信頼できるサードパーティ CA から購入するか、自己署名証明書をローカルで生成することができます。サーバー証明書の証明書共通名（CN）またはサブジェクト代替名には、デバイスの管理インターフェイスの IP アドレスか FQDN を含める必要があります。クライアント ファイアウォールまたはログ コレクタは、サーバーが提示する証明書の CN またはサブジェクト代替名をサーバーの IP アドレスまたは FQDN と照合し、サーバーのアイデンティティを確認します。

  証明書の失効状態（OCSP/CRL）および失効状態に基づいて取るアクションを定義するには、証明書プロファイルを使用します。
- クライアントの証明書とプロファイル — 各管理対象デバイスには、クライアント証明書と証明書プロファイルが必要です。クライアント デバイスは、その証明書を使用して、サーバー デバイスに対して自身を識別します。証明書は、SCEP（Simple Certificate Enrollment Protocol）を使用して会社の PKI からデプロイするか、信頼できるサードパーティ CA から購入するか、自己署名証明書をローカルで生成することができます。

© 2019 Palo Alto Networks, Inc.

カスタム証明書は、各クライアント デバイスで固有にするか、すべてのデバイスで共通にすることができます。固有のデバイス証明書では、管理対象デバイスのシリアル番号と CN のハッシュが使用されます。サーバーは、CN またはサブジェクト代替名を管理対象デバイスで設定されているシリアル番号と照合します。クライアント証明書を CN に基づいて検証するには、ユーザー名をサブジェクト共通名に設定する必要があります。クライアント証明書の動作は、Panorama HA ピア接続にも適用されます。

クライアント証明書と証明書プロファイルは、各クライアント デバイスで設定するか、Panorama から各デバイスに設定をテンプレートの一部としてプッシュできます。

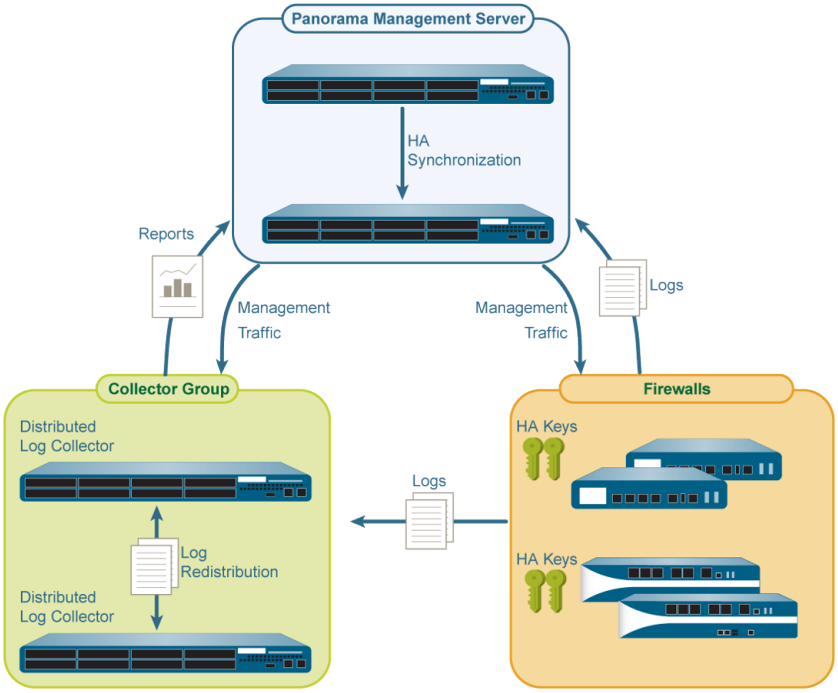


図 **11 : SSL/TLS** 認証

Panorama でのカスタム証明書を使用する認証の設定

サーバー側（Panorama）がデプロイメントに含まれる管理対象デバイスとの相互認証に事前定義済みの証明書ではなくカスタム証明書を使用するように設定するには、以下の手順を実行します。HA ピア間のカスタム証明書を使用する認証のセットアップを参照して、Panorama HA ペアでカスタム証明書を設定します。

STEP 1 | サーバー証明書をデプロイします。

自己署名証明書を Panorama で生成するか、エンタープライズ認証局 (CA) または信頼できるサードパーティ CA から証明書を取得し、Panorama かサーバー ログ コレクタで証明書をデプロイできます。

STEP 2 | Panorama で証明書プロファイルを設定します。この証明書プロファイルにより、使用する証明書と、IP アドレスまたは FQDN を検索する証明書フィールドが定義されます。

1. **Panorama** > **Certificate Management**（証明書の管理）> **Certificate Profile**（証明書プロファイル）の順に選択します。
2. 証明書プロファイルの設定を行います。

証明書プロファイルの一部として中間 *CA* を設定する場合、ルート *CA* も含める必要があります。

© 2019 Palo Alto Networks, Inc.

STEP 3 | SSL/TLS サービス プロファイルの設定を行います。

1. **Panorama** > **Certificate Management**（証明書の管理） > **SSL/TLS Service Profile**（**SSL/TLS** サービス プロファイル）の順に選択します。
2. SSL/TLS プロファイルを設定し、Panorama およびその管理対象デバイスを SSL/TLS サービス用に使用する証明書とプロトコルを定義します。

STEP 4 | サーバー ロールの Panorama またはログ コレクタで Secure Server Communication（保護されたサーバー通信）を設定します。

1. 以下のいずれかのナビゲーション パスを選択します。
   - Panorama の場合：**Panorama** > **Setup**（セットアップ） > **Management**（管理）を行い、セキュア通信設定を **Edit**（編集）します。
   - ログ コレクタの場合：**[Panorama]** > [管理対象コレクタ] > [追加] > の順に選択します。**Communication**.
2. **Customize Secure Server Communication**（セキュリティで保護されたサーバー通信のカスタマイズ）オプションを選択します。
3. **Allow Custom Certificate Only**（カスタム証明書のみを許可）チェック ボックスがオフになっていることを確認します。これにより、カスタム証明書への移行中もすべてのデバイスの管理を続行できます。

   Custom Certificate Only（カスタム証明書のみ）チェック ボックスをオンにしていると、*Panorama* は事前定義済みの証明書を使用したデバイスを認証せず、管理することができません。
4. **SSL/TLS Service Profile**（**SSL/TLS** サービスプロファイル）を選択します。この SSL/TLS サービス プロファイルは、Panorama、ファイアウォール、ログ コレクタ、Panorama HA ピア間のすべての SSL 接続に適用されます。
5. ファイアウォールなどのクライアントとの保護された通信を確立するために使用する証明書を識別する **Certificate Profile**（証明書プロファイル）を選択します。
6. （任意）認証リストを設定します。承認リストにより、証明書認証に新たなセキュリティの層が追加されます。承認リストは、クライアント証明書の Subject（サブジェクト）または Subject Alt Name（サブジェクト代替名）をチェックします。クライアント証明書で示された Subject（サブジェクト）または Subject Alt Name（サブジェクト代替名）が承認リストの識別子と一致しない場合、認証は拒否されます。

   シリアル番号に基づいてクライアント デバイスを承認することもできます。

   1. Authorization List（承認リスト）を **Add**（追加）します。
   2. 識別子タイプとして証明書プロファイルで設定した **Subject**（サブジェクト）または **Subject Alt Name**（サブジェクト代替名）を選択します。
   3. 識別子が Subject（サブジェクト）の場合は Common Name（共通名（CN））を入力し、識別子が Subject Alt Name（サブジェクト代替名）の場合は IP アドレス、ホスト名、または電子メール アドレスを入力します。
   4. **OK** をクリックします。
   5. **Check Authorization List**（承認リストのチェック）を選択して認証リストを適用します。
7. **Authorize Client Based on Serial Number**（シリアル番号に基づいてクライアントを承認）を選択し、サーバーが管理対象デバイスのシリアル番号に基づいてクライアントを認証するようにします。クライアント証明書の CN またはサブジェクトには、このタイプの認証を有効するために特殊キーワード $UDID が必要です。
8. **Customize Communication (**コミュニケーションのカスタマイズ**)** セクションの **Data Redistribution (**データの再配信**)** オプションを選択し、カスタム証明書を使用して、データ再配信クライアントとの発信通信を保護します。
9. **Disconnect Wait Time (min)**（切断待機時間（分））で、現在のセッションを終了して管理対象デバイスとの接続を再開するまで Panorama が待機する時間を指定します。このフィールドはデフォル

© 2019 Palo Alto Networks, Inc.

トで空白であり、範囲は 0 ~ 44,640 分です。このフィールドを空白のままにすると、0 に設定したのと同じことになります。



切断待機時間は、新しい設定をコミットするまでカウント ダウンを開始しません。

10.**OK** をクリックします。
11.変更を **Commit** (コミット)します。

管理対象デバイスでのカスタム証明書を使用する認証の設定

クライアント側 (ファイアウォールまたはログ コレクタ) がデプロイメントに含まれる管理対象デバイスとの相互認証に事前定義済みの証明書ではなくカスタム証明書を使用するように設定するには、以下の手順を実行します。

STEP 1 | 各管理対象ファイアウォールまたはログ コレクタをアップグレードします。すべての管理対象デバイスは、カスタム証明書認証を適用するために PAN-OS 8.0 以降を実行している必要があります。

ファイアウォールをアップグレードします。アップグレード後、各ファイアウォールはデフォルトの事前定義済みの証明書を使用して Panorama に接続します。

STEP 2 | デバイス証明書を取得するか生成します。

自己署名証明書を Panorama で生成するか、エンタープライズ認証局 (CA) または信頼できるサードパーティ CA から証明書を取得し、Panorama かサーバー ログ コレクタで証明書をデプロイできます。

シリアル番号に基づいてクライアント デバイスを承認する場合は、共通名を $UDID に設定するかサブジェクトを CN=$UDID に設定します (SCEP プロファイル) 。

- 自己署名証明書を Panorama で生成するか、エンタープライズ CA または信頼できるサードパーティ CA から証明書を取得できます。
- デバイス証明書に SCEP を使用している場合は、SCEP プロファイルを設定します。SCEP では、管理対象デバイスに証明書を自動的にデプロイできます。SCEP プロファイルを含む新しいクライアント デバイスが Panorama で認証しようとすると、証明書は SCEP サーバーによってデバイスに送信されます。

STEP 3 | クライアント デバイスの証明書プロファイルを設定します。

これは各クライアント デバイスで個々に設定することも、テンプレートの一部として管理対象デバイスにこの設定をプッシュすることもできます。

1. 以下のいずれかのナビゲーション パスを選択します。
   - ファイアウォールの場合 – **Device** (デバイス) > **Certificate Management** (証明書の管理) > **Certificate Profile** (証明書プロファイル) の順に選択します。
   - ログ コレクタの場合 – **Panorama** > **Certificate Management** (証明書の管理) > **Certificate Profile** (証明書プロファイル) の順に選択します。
2. 証明書プロファイルを設定します。

STEP 4 | 各ファイアウォールまたはログ コレクタにカスタム証明書をデプロイします。

1. 以下のいずれかのナビゲーション パスを選択します。
   - ファイアウォールの場合 : **[Device]** > [セットアップ] > [管理] の順に選択し、[Panorama 設定] を編集します。

© 2019 Palo Alto Networks, Inc.

- ログ コレクタの場合：**Panorama** > **Managed Collectors**（管理対象コレクタ）の順に選択し、新しいログ コレクタを **Add**（追加）するか、既存のログ コレクタを選択します。**Communication**（通信）を選択します。

2. **Secure Client Communication**（保護されたクライアント通信）チェック ボックスをオンにします（ファイアウォールのみ）。
3. **Certificate Type**（証明書タイプ）を選択します。
   - ローカル デバイス証明書を使用している場合、**Certificate**（証明書）および **Certificate Profile**（証明書プロファイル）を選択します。
   - デバイス証明書のデプロイに SCEP を使用している場合、**SCEP Profile**（**SCEP** プロファイル）および **Certificate Profile**（証明書プロファイル）を選択します。
   - デフォルトの Panorama 証明書を使用している場合は、**Predefined (事前定義済み)** を選択します。
4. （任意）**Check Server Identity**（サーバー アイデンティティのチェック）を有効にします。ファイアウォールまたはログ コレクタは、Panorama の IP アドレスまたは FQDN と照合してサーバー証明書内の CN をチェックし、そのアイデンティティを確認します。
5. **OK** をクリックします。
6. 変更を **Commit (コミット)**します。

   変更をコミットしても、管理対象デバイスは Disconnect Wait Time（切断待機時間）が経過するまで Panorama との現在のセッションを終了しません。

STEP 5 | カスタム証明書を使用する通信タイプを選択します。

- **HA Communication (高可用性通信)**
- **WildFire Communication (WildFire 通信)**
- **Data Redistribution (データの再配信)**

STEP 6 | すべての管理対象デバイスにカスタム証明書をデプロイした後で、カスタム証明書を使用した認証を適用します。

WildFire アプライアンスは、現在のところカスタム証明書をサポートしていません。*Panorama* で *WildFire* アプライアンスを管理している場合、*Allow Custom Certificates Only*（カスタム証明書のみを許可）を選択しないでください。

1. **[Panorama]** > **[セットアップ]** > **[管理]** の順に選択し、**[Panorama 設定]** を編集します。
2. **Allow Custom Certificate Only**（カスタム証明書のみを許可）を選択します。
3. **OK** をクリックします。
4. 変更を **Commit (コミット)**します。

   この変更をコミットした後では、Panorama で管理するすべてのデバイスでカスタム証明書を使用する必要があります。カスタム証明書を使用しないと、Panorama とデバイスとの間の認証で障害が発生します。

新しいクライアント デバイスの追加

Panorama に新しいファイアウォールまたはログ コレクタを追加する場合は、これらのデバイスが相互認証のためだけにカスタム証明書を使用するように設定されているかどうかによって、ワークフローが変わります。

- Panorama で Custom Certificates Only（カスタム証明書のみ）が選択されていない場合は、Panorama にデバイスを追加してから、「管理対象デバイスでのカスタム証明書を使用する認証の設定」のステップで始まるプロセスに従って、カスタム証明書をデプロイします。
- Panorama で Custom Certificates Only（カスタム証明書のみ）が選択されている場合は、カスタム証明書をファイアウォールにデプロイしてから、Panorama に追加する必要があります。そうしないと、

© 2019 Palo Alto Networks, Inc.

管理対象デバイスは、Panorama に対して認証を行うことができません。これは、ファイアウォール Web インターフェイスを介して手動で行うことも、bootstrap.xml ファイルの一部としてブートストラッピングを通じて行うこともできます。

証明書の変更

デプロイ環境でカスタム証明書の期限が切れるか、カスタム証明書が無効になって置き換える必要がある場合は、以下のいずれかのタスクを実行します。

- サーバー証明書の変更
- クライアント証明書の変更
- ルートまたは中間 CA 証明書の変更

サーバー証明書の変更

サーバー証明書を置き換えるには、以下のタスクを実行します。

STEP 1 | 新しいサーバー証明書をデプロイします。

自己署名証明書を Panorama で生成するか、エンタープライズ CA または信頼できるサードパーティ CA から証明書を取得し、Panorama かサーバー ログ コレクタで証明書をデプロイできます。

STEP 2 | SSL/TLS サービス プロファイルで証明書を変更します。

1. **Panorama** > **Certificate Management**（証明書の管理）> **SSL/TLS Service Profile**（**SSL/TLS** サービス プロファイル）の順に選択し、SSL/TLS サービス プロファイルを選択します。
2. **Certificate**（証明書）を選択します。
3. **OK** をクリックします。

STEP 3 | サーバー（Panorama またはログ コレクタ）とクライアント デバイスとの間で接続を再確立します。

1. **Panorama** > **Setup**（セットアップ）> **Management**（管理）の順に選択し、Panorama の Panorama 設定を **Edit**（編集）するか、ログ コレクタで **Panorama** > **Managed Collectors**（管理対象コレクタ）> **Add**（追加）> **Communication**（通信）の順に選択します。
2. **Disconnect Wait Time**（切断待機時間）を設定します。
3. **OK** をクリックします。
4. 変更を **Commit** (コミット)します。

クライアント証明書の変更

クライアント証明書を置き換えるには、以下のタスクを実行します。

STEP 1 | デバイス証明書を取得するか生成します。

自己署名証明書を Panorama で生成するか、エンタープライズ CA または信頼できるサードパーティ CA から証明書を取得し、Panorama かサーバー ログ コレクタで証明書をデプロイできます。

シリアル番号に基づいてクライアント デバイスを承認する場合は、共通名を $UDID に設定するかサブジェクトを CN=$UDID に設定します（SCEP プロファイル）。

- 自己署名証明書を Panorama で生成するか、エンタープライズ CA または信頼できるサードパーティ CA から証明書を取得できます。
- デバイス証明書に SCEP を使用している場合は、SCEP プロファイルを設定します。SCEP では、管理対象デバイスに証明書を自動的にデプロイできます。SCEP プロファイルを含む新しいクライアント デバイスが Panorama で認証しようとすると、証明書は SCEP サーバーによってデバイスに送信されます。

© 2019 Palo Alto Networks, Inc.

STEP 2 | 証明書プロファイルで証明書を変更します。

1. **Device**（デバイス）> **Certificate Management**（証明書の管理）> **Certificate Profile**（証明書プロファイル）の順に選択し、証明書プロファイルを選択します。
2. CA 証明書の下で新しい証明書を **Add**（追加）し、証明書プロファイルに割り当てます。
3. **OK** をクリックします。
4. 変更を **Commit** (コミット)します。

ルートまたは中間 *CA* 証明書の変更

ルートまたは中間 CA 証明書を置き換えるには、以下のタスクを実行します。

STEP 1 | 事前定義済み証明書をクライアントから受け入れるようにサーバーを設定します。

1. **[Panorama]** > [セットアップ] > [管理] の順に選択し、[Panorama 設定] を 編集します。
2. **Custom Certificate Only**（カスタム証明書のみ）をオフにします。
3. Certificate Profile（証明書プロファイル）ドロップダウンから **None**（なし）を選択します。
4. **OK** をクリックします。
5. 変更を **Commit** (コミット)します。

STEP 2 | 新しいルートまたは中間 CA 証明書をデプロイします。

自己署名証明書を Panorama で生成するか、エンタープライズ CA または信頼できるサードパーティ CA から証明書を取得し、Panorama かサーバー ログ コレクタで証明書をデプロイできます。

STEP 3 | サーバー証明書プロファイルで CA 証明書を更新します。

1. **Panorama** > **Certificate Management**（証明書の管理）> **Certificate Profile**（証明書プロファイル）の順に選択し、更新する証明書プロファイルを選択します。
2. 古い CA 証明書を **Delete**（削除）します。
3. 新しい CA 証明書を **Add**（追加）します。
4. **OK** をクリックします。

STEP 4 | 新しいクライアント証明書を生成するかインポートします。

1. **Device**（デバイス）> **Certificate Management**（証明書の管理）> **Certificates**（証明書）
2. 自己署名ルート CA 証明書を作成するかエンタープライズ CA から証明書をインポートします。

STEP 5 | クライアント証明書プロファイルで CA 証明書を更新します。

1. **Device**（デバイス）> **Setup**（セットアップ）> **Management**（管理）の順に選択し、ファイアウォールの Panorama 設定で **Edit**（編集）アイコンをクリックするか、ログ コレクタで **Panorama** > **Managed Collectors**（管理対象コレクタ）> **Add**（追加）> **Communication**（通信）の順に選択し、更新する証明書プロファイルを選択します。
2. 古い CA 証明書を **Delete**（削除）します。
3. 新しい CA 証明書を **Add**（追加）します。
4. **OK** をクリックします。

STEP 6 | すべての管理対象デバイスで CA 証明書を更新した後で、カスタム証明書認証を適用します。

1. **[Panorama]** > [セットアップ] > [管理] の順に選択し、[Panorama 設定] を 編集します。
2. **Custom Certificate Only**（カスタム証明書のみ）を選択します。
3. **OK** をクリックします。
4. 変更を **Commit** (コミット)します。

© 2019 Palo Alto Networks, Inc.

この変更をコミットした後では、Panorama で管理するすべてのデバイスでカスタム証明書を使用する必要があります。カスタム証明書を使用しないと、Panorama とデバイスとの間の認証で障害が発生します。

© 2019 Palo Alto Networks, Inc.

ファイアウォールの管理

Palo Alto Networks のファイアウォールの管理に Panorama™ 管理サーバーを使用するには、ファイアウォールを管理対象デバイスとして追加し、それらをデバイス グループとテンプレートあるいはテンプレート スタックに割り当てる必要があります。以下のタスクは、ファイアウォールを初めてデプロイする場合に最適です。作業に入る前に、Panorama のデプロイメント計画の内容を確認してデプロイのオプションについて理解してください。

- 管理対象デバイスとしてのファイアウォールの追加
- 管理対象ファイアウォールのデバイス証明書のインストール
- ゼロタッチプロビジョニングのセットアップ
- デバイス グループの管理
- テンプレートおよびテンプレート スタックの管理
- Panorama からマスターキーを管理
- データをマネージドファイアウォールに再配信する
- エンタープライズ データ消失防止 (DLP) のセットアップ
- ファイアウォールを Panorama 管理に移行
- Panoramaでのデバイスモニタリング
- ユース ケース:Panorama を使用してファイアウォールを構成

Panorama Web インターフェイスに **Objects**（オブジェクト）および**Policies**（ポリシー）タブを表示するには、まず少なくとも 1 つのデバイス グループを作成する必要があります。**Network**（ネットワーク）および**Device**（デバイス）タブを表示するには、少なくともテンプレートを1つ作成する必要があります。これらのタブには、ネットワーク上のファイアウォールを設定して管理する際に使用するオプションが含まれています。

管理対象デバイスとしてのファイアウォールの追加

Panorama を使用してファイアウォールを管理するには、ファイアウォールと Panorama 間の接続を有効にする必要があります。接続に成功するには、Panorama が管理する各ファイアウォールに Panorama IP アドレスを入力し、Panorama の各ファイアウォールのシリアル番号を入力する必要があります。ファイアウォールを管理対象デバイスとして追加する場合、初回デプロイ時に新しいファイアウォールをデバイス グループ、テンプレート スタック、コレクタグループ、およびログ コレクタに関連付けることができます。さらに、ファイアウォールが初めて Panorama に接続するときに新しく追加されたファイアウォールに構成を自動的にプッシュすることが可能です。これにより、ファイアウォールがすぐに構成され、ネットワークを保護する準備が整います。

Panorama で管理するファイアウォールに一括インポートできるのは、*1* つの *vsys* ファイアウォールのみです。

ファイアウォールは、Panorama 管理サーバーの IP アドレスを使用して SSL 接続をセットアップし、Panorama への登録を行います。Panorama とファイアウォールは、2,048 ビットの証明書と、AES-256 で暗号化される SSL 接続を使用して互いに認証を行い、設定の管理とログの収集を行います。Panorama と各ファイアウォールを以下の手順で準備します。

STEP 1 | Panorama と通信するようにファイアウォールを設定します。

Panorama で管理されるファイアウォールごとに、この手順を繰り返します。

1. ファイアウォールで初期設定を行い、ネットワーク経由でアクセスし、Panorama と通信できるようにします。
2. ファイアウォールで使用する予定の各データ インターフェイスを設定した後、それらのインターフェイスをセキュリティ ゾーンに接続し、Panorama から設定とポリシーをプッシュできるようにします。
3. Panorama の IP アドレスをファイアウォールに追加します。
   1. **[Device]** > [セットアップ] > [管理] の順に選択し、[Panorama 設定] を編集します。
   2. 先頭のフィールドに Panorama の IP アドレスを入力します。

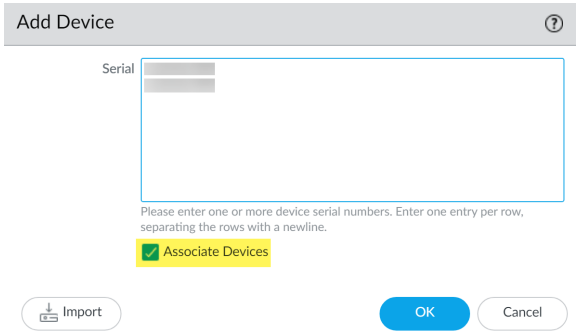
      Panorama は、デバイス管理、ログ収集、レポート、および動的更新を行うために *IP* アドレスを発行します。外部のインターネット方向の *IP* アドレスを入力して、*Panorama* が既存および新しい管理対象デバイスとログ コレクタに正常にアクセスできるようにします。内部 *Panorama IP* アドレスが設定されている場合、一部のデバイスを管理できない場合があります。例えば、ユーザーが*AWS* で Panorama をインストールして内部 *IP* アドレスを入力すると、*Panorama* は *AWS* セキュリティグループ外のデバイスまたはログ コレクタを管理することはできません。
   3. (任意) Panorama で高可用性 (HA) ペアをセットアップした場合は、2 番目のフィールドにセカンダリ Panorama の IP アドレスを入力します。
   4. **OK** をクリックします。
   5. **Commit** (コミット) を選択し、変更内容を **Commit** (コミット) します。

STEP 2 | Panorama に 1 つ以上のインターフェイスを追加します。

- 1 つ以上のファイアウォールを追加します。
  1. 新しい管理対象デバイスを追加します (**Panorama** > **Managed Devices** (管理対象デバイス) > **Summary** (サマリー))。

© 2019 Palo Alto Networks, Inc.

2. ファイアウォールの **Serial** (シリアル) 番号を入力します。複数のファイアウォールを追加する場合、各シリアル番号を行を分けて入力します。新しいファイアウォールを初期デプロイのデバイス グループ、テンプレート スタック、コレクタ グループ、またはログ コレクタに関連付ける場合は、次の手順に進みます。各ファイアウォールを手動で割り当てるには、**OK** をクリックしてステップ 3 に進みます。
3. **Associate Devices** (デバイスの関連付け) チェックボックスを選択して、**OK** をクリックします。

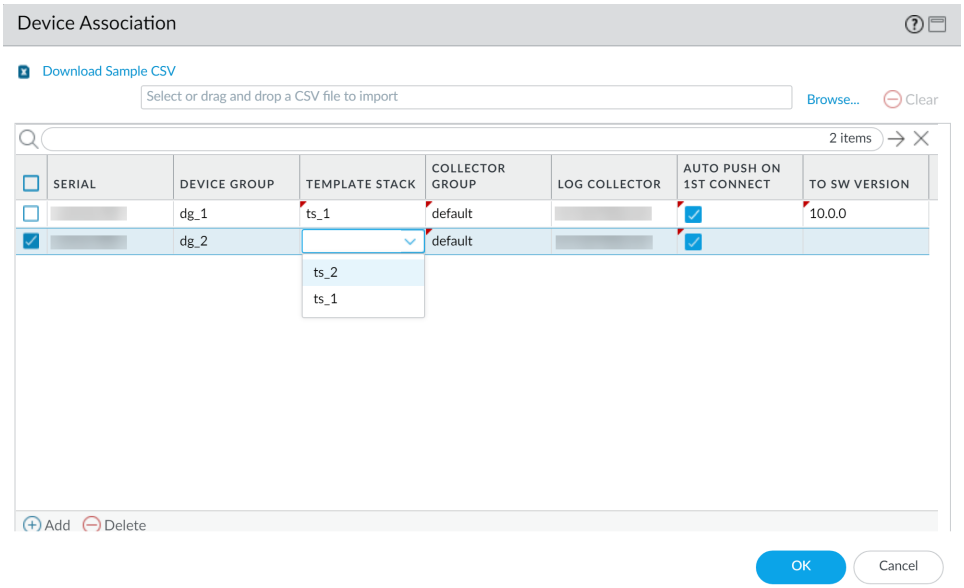


4. 必要に応じて、各列のドロップダウンから **Device Group** (デバイス グループ)、**Template Stack** (テンプレート スタック)、**Collector Group** (コレクタ グループ)、および **Log Collector** (ログ コレクタ) を割り当てます。
5. Panorama に正常に接続したときに、デバイス グループとテンプレート スタック構成を新しいデバイスに自動的にプッシュするには、**Auto Push on 1st connect** (最初の接続時に自動プッシュ) チェックボックスをオンにします。

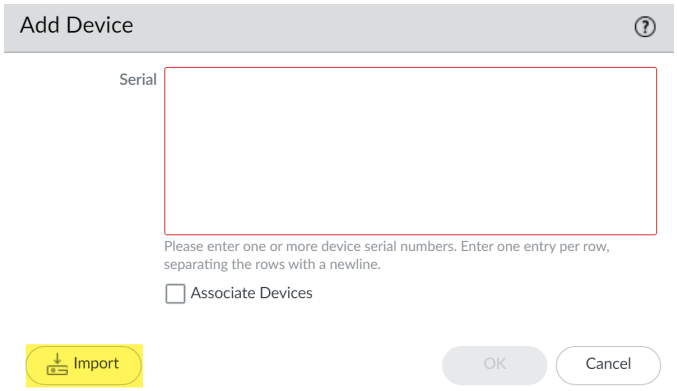
   Auto Push on 1st connect (最初の接続時に自動プッシュ) オプションは、*PAN-OS 8.1* 以降のリリースを実行しているファイアウォールでのみサポートされています。*Panorama* から *PAN-OS 8.1* 以降のリリースを実行している管理対象デバイスに `commit all` ジョブを実行します。
6. (任意) Panorama への接続の成功と同時にマネージド ファイアウォールを指定された PAN-OS リリースバージョンへ自動的にアップグレードを開始するように設定するには、**To SW Version** 列で PAN-OS のリリース バージョンを選択します。

   マネージド ファイアウォールを自動的にアップグレードしない場合は、この列を空のままにします。
7. **OK** をクリックしてデバイスを追加します。

© 2019 Palo Alto Networks, Inc.



- コンマ区切り値 (CSV) ファイルを使用して、複数のファイアウォールを一括インポートします。
  1. 新しい管理対象デバイスを追加します (**Panorama** > **Managed Devices** (管理対象デバイス) > **Summary** (サマリー))。
  2. [インポート] をクリックします。

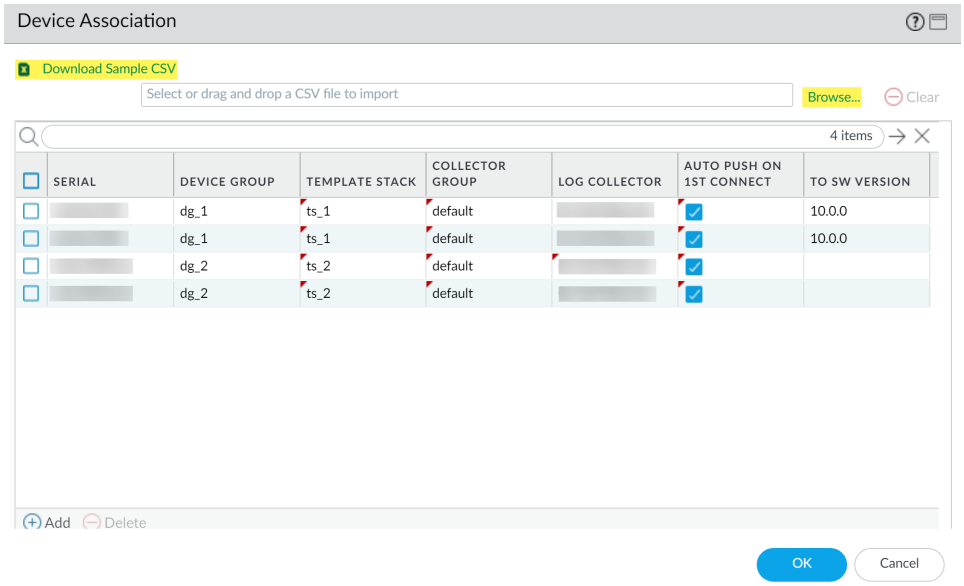


  3. **Download Sample CSV** (サンプル **CSV** のダウンロード) を行い、ダウンロードした CSV ファイルを編集してファイアウォールを加えます。CSV からファイアウォールをデバイス グループ、テンプレート スタック、コレクタ グループ、ログ コレクタに割り当てるか、ファイアウォールのシリアル番号のみを入力して Web インターフェイスから割り当てることができます。編集が完了したら、CSV を保存します。
  4. 前の手順で編集した CSV ファイルを **Browse** (参照) して選択します。
  5. CSV でまだ割り当てられていない場合は必要に応じて、各列のドロップダウンからファイアウォールに **Device Group** (デバイス グループ)、**Template Stack** (テンプレート スタック)、**Collector Group** (コレクタ グループ)、および **Log Collector** (ログ コレクタ) を割り当てます。
  6. Panorama に正常に接続したときに、デバイス グループとテンプレート スタック構成を新しいデバイスに自動的にプッシュするには、**Auto Push on 1st connect** (最初の接続時に自動プッシュ) するチェックボックスをオンにします (CSV で有効になっていない場合)。
  7. (任意) Panorama への接続の成功と同時にマネージド ファイアウォールを指定された PAN-OS リリースバージョンへ自動的にアップグレードを開始するように設定するには、**To SW Version** 列で PAN-OS のリリース バージョンを選択します。

© 2019 Palo Alto Networks, Inc.

マネージド ファイアウォールを自動的にアップグレードしない場合は、この列を空のままにします。

8. **OK** をクリックしてデバイスを追加します。



STEP 3 | （任意）**Tag**（タグ）を追加します。タグを付けると、長いリストからファイアウォールを見つけやすくなり、ファイアウォールのリストをダイナミックにフィルタリングして表示を絞り込みやすくなります。たとえば、「branch office」というタグを追加すると、ネットワーク全体から支店のファイアウォールすべてを検索できます。

1. 各ファイアウォールを選択して、**Tag (タグ)** をクリックします。
2. **Add**（追加）をクリックし、最大 31 文字の文字列（空白なし）を入力し、**OK** をクリックします。

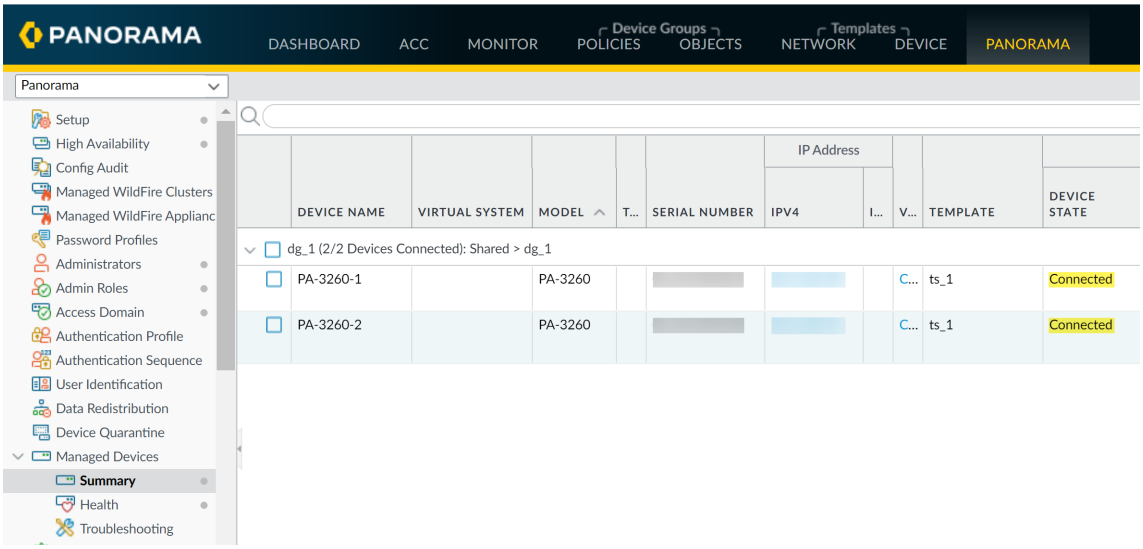
STEP 4 | 導入環境で Panorama と管理対象デバイス間の認証にカスタム証明書を使用している場合は、カスタム クライアント デバイス証明書をデプロイします。詳細は、「カスタム証明書を使用する認証のセットアップ」と「新しいクライアント デバイスの追加」を参照してください。

STEP 5 | **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

STEP 6 | ファイアウォールが Panorama に接続されていることを確認します。

1. **Panorama** > **Managed Devices (管理対象デバイス)** > **Summary (サマリー)** をクリックします。
2. 新規デバイスの **Device State (デバイス状態)** に `Connected` と表示されていることを確認します。

© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

管理対象ファイアウォールのデバイス証明書のインストール

PAN-OS 10.0 以降のリリースでは、デバイス テレメトリ IoT、エンタープライズ データ漏洩防止 (DLP) などの Palo Alto Networks クラウド サービスを活用するためにマネージド ファイアウォールを正常に認証するには、管理対象ファイアウォールにデバイス証明書をインストールする必要があります。1 つの管理対象ファイアウォール、または複数の管理対象ファイアウォールのデバイス証明書を同時にインストールできます。



ファイアウォール デバイス証明書をローカルにインストールするには、Device Certificates（デバイス証明書）を参照してください。

- 管理対象ファイアウォールのデバイス証明書のインストール
- 複数の管理対象ファイアウォールのデバイス証明書のインストール

管理対象ファイアウォールのデバイス証明書のインストール

PAN-OS 10.0 以降のリリースでは、Panorama 管理サーバから管理対象ファイアウォール用のデバイス証明書をインストールする必要があります。デバイス証明書を正常にインストールするには、マネージド ファイアウォールからインターネットにアクセス可能であることが必要です。

STEP 1 | Palo Alto Networks の Customer Support Portal（カスタマーサポートポータル）（CSP）Panorama の登録でファイアウォールを管理する。

STEP 2 | 管理ユーザーとしてPanorama Web インターフェイスへのログイン。

STEP 3 | Network Time Protocol（NTP）サーバーを設定します。

NTP サーバは、デバイス証明書の有効期限を検証し、デバイス証明書が早期に期限切れになったり、無効になっていないことを確認します。

1. **Device**（デバイス）> **Setup**（セットアップ）> **Services**（サービス）を選択して、**Template** (テンプレート) を選択します。
2. ご利用のプラットフォームに応じて、以下のいずれかを選択します。
   - マルチ仮想システム プラットフォームの場合は、**Global** [グローバル]を選択して Services [サービス]セクションを編集します。
   - 1 つの仮想システム プラットフォームの場合は、Services [サービス]セクションを編集します。
3. **NTP** を選択し、ホスト名 `pool.ntp.org` を **Primary NTP Server**（プライマリ **NTP** サーバー）として入力するか、プライマリ NTP サーバーの IP アドレスを入力します。
4. （任意）**Secondary NTP Server** [セカンダリ NTP サーバー]のアドレスを入力します。
5. （任意）NTP サーバーからの時間の更新を認証するには、各サーバーの **Authentication Type**（認証タイプ）で以下のいずれかを選択します。
   - **None**（なし）（デフォルト）– NTP 認証を無効にします。
   - **Symmetric Key** [対称キー] – ファイアウォールで対象キー交換（共有のシークレット）を使用して時間の更新を認証します。
     - **Key ID** – Key ID（1 ~ 65534）を入力します。
     - **Algorithm**（アルゴリズム）– NTP 認証に使用するアルゴリズムを選択します（**MD5** または **SHA1**）。
6. **OK** をクリックして、設定の変更を保存します。

© 2019 Palo Alto Networks, Inc.

7. **Commit (コミット)** を選択し、マネージド ファイアウォールへの設定の変更を **Commit and Push (コミットしてプッシュ)** します。

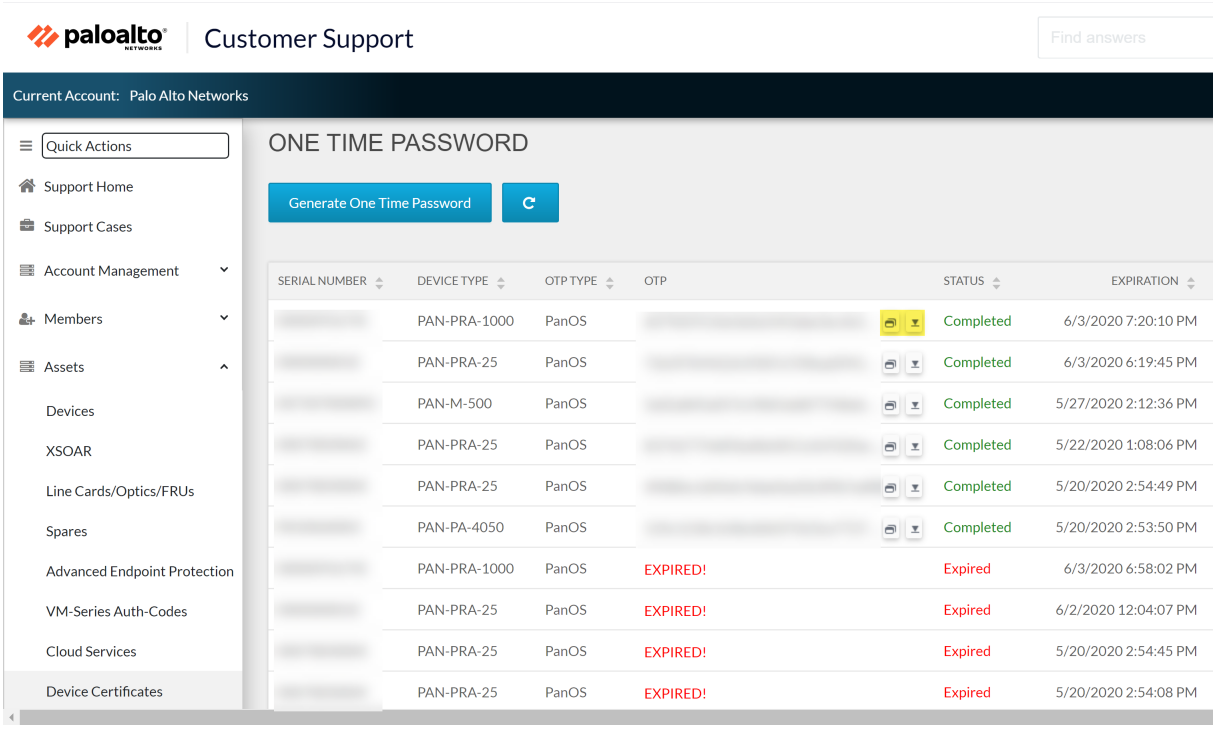
STEP 4 | **Panorama** > **Managed Devices** > **Summary**を選択して、管理対象ファイアウォールを選択します。

STEP 5 | **Request OTP From CSP（CSP から OTP を要求）** > **Custom selected devices（カスタム選択デバイス）**を選択します。

STEP 6 | OTP 要求トークン全体をコピーします。

STEP 7 | 管理対象ファイアウォールのワンタイムパスワード（OTP）を生成します。

1. カスタマーサポート ポータルにログインします。
2. **Assets** > **Device Certificates（デバイス証明書）**および **Generate OTP（OTPの生成）**を選択します。
3. **Device Type（デバイス タイプ）**で、**Panorama** で管理されているファイアウォールの **OTP** を生成を選択します。
4. 前のステップでコピーした OTP 要求をペーストし、**Generate OTP (OTP を生成)** します。
5. **Done (完了)** をクリックし、OTP が正常に生成されるまで数分間待ちます。新しい OTP が表示されない場合は、ページを更新することができます。
6. **Copy to Clipboard (クリップボードにコピー)** または OTP を **Download (ダウンロード)** します。



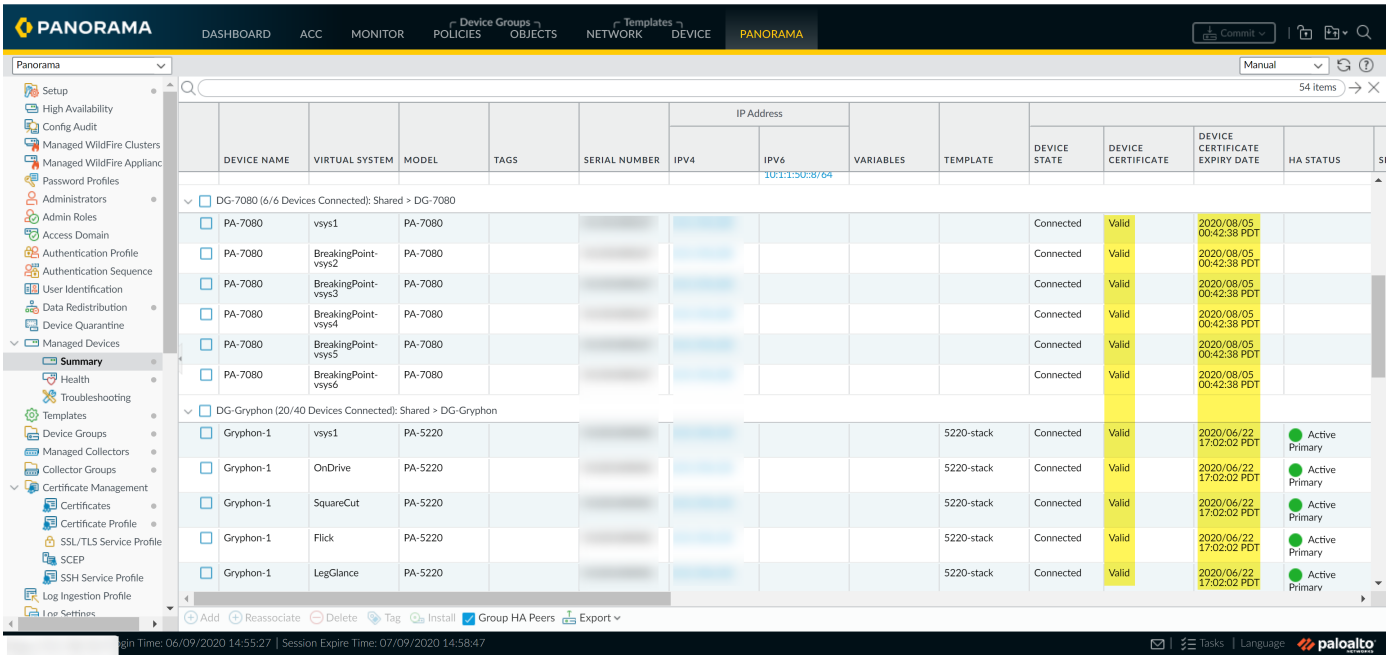
STEP 8 | 管理ユーザーとしてPanorama Web インターフェイスへのログイン。

STEP 9 | **Panorama** > **Managed Devices** > **Summary**および**Upload OTP（OTPをアップロード）**を選択します。

STEP 10 | 生成した OTP を貼り付けて、**Upload (アップロード)** をクリックします。

© 2019 Palo Alto Networks, Inc.

STEP 11 | **Device Certificate (デバイス証明書) 列に `Valid` (有効) と表示されており、Device Certificate Expiry Date (デバイス証明書有効期限) に有効期限が表示されることを確認します。**



複数の管理対象ファイアウォールのデバイス証明書のインストール

PAN-OS 10.0 以降のリリースでは、Panorama 管理サーバーから、マネージド ファイアウォール用のデバイス証明書をインストールする必要があります。デバイス証明書を正常にインストールするには、マネージドファイアフォールがインターネットにアクセス可能であることが必要です。

STEP 1 | Palo Alto Networks の Customer Support Portal（カスタマーサポートポータル）（CSP）Panorama の登録でファイアウォールを管理する。

STEP 2 | 管理ユーザーとしてPanorama Web インターフェイスへのログイン。

STEP 3 | Network Time Protocol（NTP）サーバーを設定します。

NTP サーバは、デバイス証明書の有効期限を検証し、デバイス証明書が早期に期限切れになったり、無効になっていないことを確認します。

1. **Device**（デバイス）> **Setup**（セットアップ）> **Services**（サービス）を選択して、**Template (テンプレート)** を選択します。
2. ご利用のプラットフォームに応じて、以下のいずれかを選択します。
   - マルチ仮想システム プラットフォームの場合は、**Global** [グローバル]を選択して Services [サービス]セクションを編集します。
   - 1 つの仮想システム プラットフォームの場合は、Services [サービス]セクションを編集します。
3. **NTP** を選択し、ホスト名 `pool.ntp.org` を **Primary NTP Server**（プライマリ **NTP** サーバー）として入力するか、プライマリ NTP サーバーの IP アドレスを入力します。
4. （任意）**Secondary NTP Server** [セカンダリ NTP サーバー]のアドレスを入力します。
5. （任意）NTP サーバーからの時間の更新を認証するには、各サーバーの **Authentication Type**（認証タイプ）で以下のいずれかを選択します。

© 2019 Palo Alto Networks, Inc.

- **None**（なし）（デフォルト）– NTP 認証を無効にします。
- **Symmetric Key** [対称キー] – ファイアウォールで対象キー交換（共有のシークレット）を使用して時間の更新を認証します。
  - **Key ID** – Key ID（1 ~ 65534）を入力します。
  - **Algorithm**（アルゴリズム）– NTP 認証に使用するアルゴリズムを選択します（**MD5** または **SHA1**）。

6. **OK** をクリックして、設定の変更を保存します。
7. **Commit** (コミット) を選択し、マネージド ファイアウォールへの設定の変更を **Commit and Push** (コミットしてプッシュ) します。

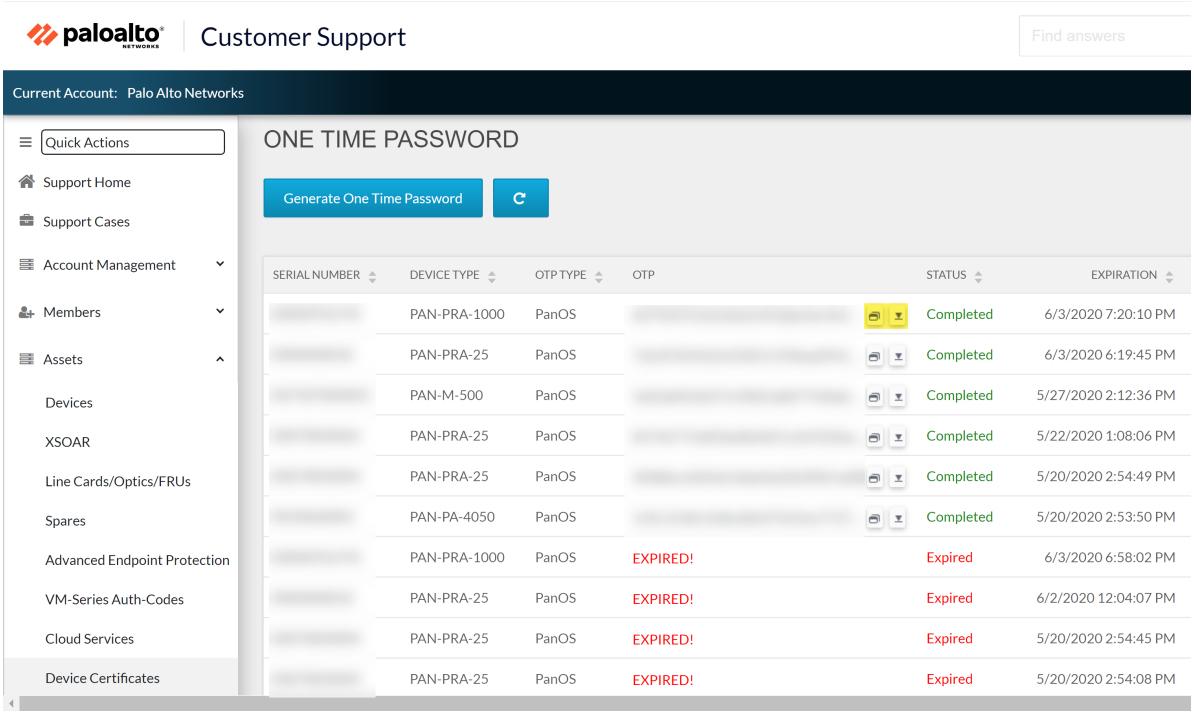
STEP 4 | **Panorama** > **Managed Devices**（管理対象デバイス）> **Summary**を選択します。

STEP 5 | **Request OTP From CSP**（**CSP** から **OTP** を要求）を選択し、 > 証明書のないすべてのデバイスを選択します。

STEP 6 | OTP 要求トークン全体をコピーします。

STEP 7 | 管理対象ファイアウォールのワンタイムパスワード（OTP）を生成します。

1. カスタマーサポート ポータルにログインします。
2. **Assets** > **Device Certificates**（デバイス証明書）および**Generate OTP**（**OTP**の生成）を選択します。
3. **Device Type**（デバイス タイプ）で、**Panorama** で管理されているファイアウォールの **OTP** を生成を選択します。
4. 前のステップでコピーした OTP 要求をペーストし、**Generate OTP** (**OTP** を生成) します。
5. **Done** (完了) をクリックし、OTP が正常に生成されるまで数分間待ちます。新しい OTP が表示されない場合は、ページを更新することができます。
6. **Copy to Clipboard** (クリップボードにコピー) または OTP を **Download** (ダウンロード) します。



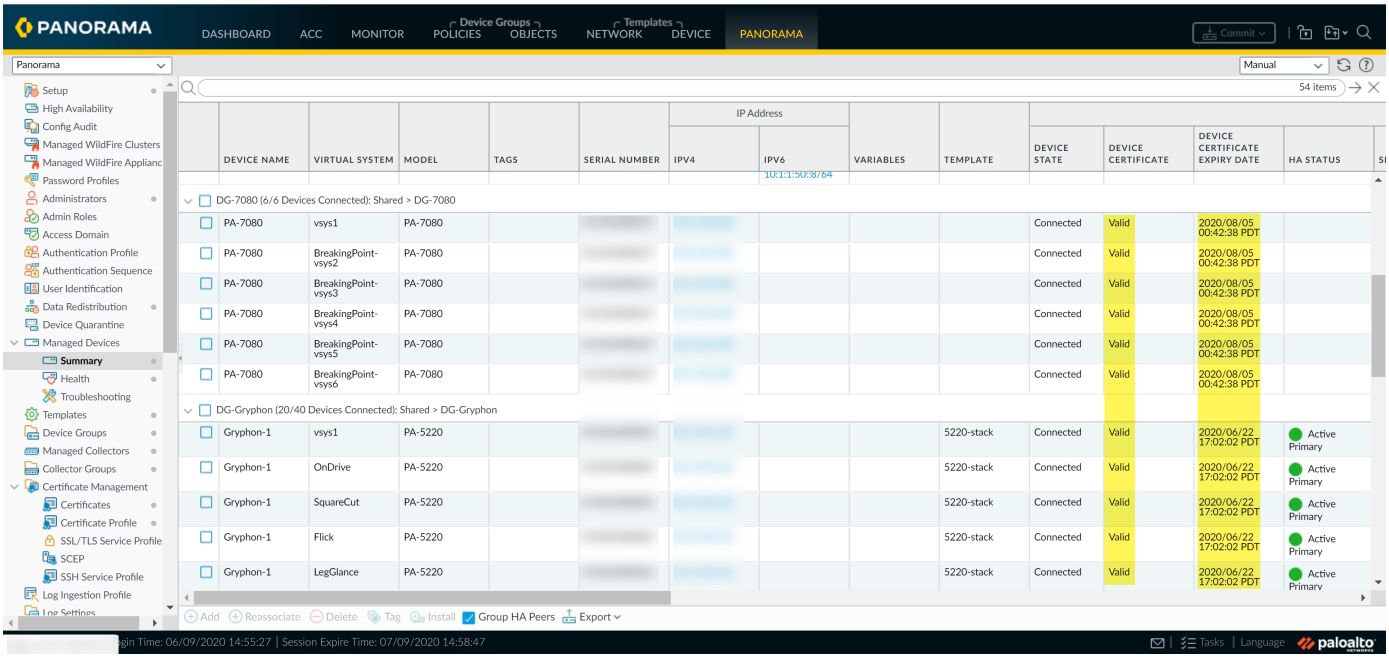
STEP 8 | 管理ユーザーとしてPanorama Web インターフェイスへのログイン。

© 2019 Palo Alto Networks, Inc.

STEP 9 | **Panorama** > **Managed Devices** > **Summary**および**Upload OTP**（**OTP**をアップロード）を選択します。

STEP 10 | 生成した OTP を貼り付けて、**Upload** (アップロード) をクリックします。

STEP 11 | **Device Certificate** (デバイス証明書) 列に **`Valid`** （有効）と表示されており、**Device Certificate Expiry Date** (デバイス証明書有効期限) に有効期限が表示されることを確認します。



© 2019 Palo Alto Networks, Inc.

ゼロタッチプロビジョニングのセットアップ

ゼロタッチプロビジョニング（ZTP）を設定して、ネットワーク管理者が手動でファイアウォールをプロビジョニングする必要がなく、新しい管理対象ファイアウォールのオンボーディングを自動化することにより、初期ファイアウォールのデプロイメントを簡素化および合理化します。

ZTP サービスを正常に利用するには、*PAN-OS 10.0.0* 以降のリリースにアップグレードする前に、工場出荷のデフォルトの *PAN-OS* バージョンの *ZTP* ファイアウォールをオンボードします。

ZTP は、*PAN-OS 10.0.1* 以降のリリースでサポートされています。

- ZTP の概要
- ZTP プラグインのインストール
- ZTP インストーラ管理者アカウントの設定
- Panorama への ZTP ファイアウォールの追加
- ZTP タスクでの CLI の使用
- ZTP プラグインのアンインストール

ZTP の概要

ゼロタッチプロビジョニング（ZTP）とその設定要素の詳細をご覧ください。

- ZTP について
- ZTP の設定要素

ZTP について

ゼロタッチプロビジョニング（ZTP）は、Panorama™ 管理サーバへの新規ファイアウォールのオンボーディングを簡素化および自動化するように設計されています。ZTP は、ネットワーク管理者が管理対象ファイアウォールをブランチに直接出荷し、ZTP ファイアウォールが Palo Alto Networks ZTPサービスに正常に接続した後、ファイアウォールを Panorama™ 管理サーバに自動的に追加できるようにすることで、初期ファイアウォール導入プロセスを合理化します。これにより、IT 管理者が新規管理対象ファイアウォールを手動でプロビジョニングする必要がなくなるため、ブランチロケーションに新規ファイアウォールを導入する際、時間とリソースの節約が可能になります。オンボーディングが正常に完了した後、Panorama は ZTP の設定とファイアウォール設定を管理する手段を提供します。

ZTP Service Status (ZTP サービスのステータス) イベントを確認して登録し、スケジュールされたメンテナンス ウィンドウ、停止、および回避策について通知します。

ZTP は、PAN-OS 9.1.3 以降のリリースを実行している、以下の ZTP ファイアウォールでサポートされています。

- PA-220-ZTP および PA-220R-ZTP
- PA-820-ZTP および PA-850-ZTP
- PA-3220-ZTP、PA-3250-ZTP、および PA-3260-ZTP

ZTP の設定要素

次の要素は連携して動作し、ZTP サービスを使用して Panorama 管理サーバにファイアウォールを自動で追加することにより、新規に導入された ZTP ファイアウォールを迅速にオンボードできます。

© 2019 Palo Alto Networks, Inc.

- **ZTP** プラグイン – ZTP プラグインを使用すると、Panorama は ZTP サービスに接続し、オンボーディングを簡素化するために ZTP ファイアウォールを要求できます。
- カスタマー サポート ポータル（**CSP**） – Palo Alto Networks カスタマー サポート ポータルは、Panorama を登録して CSP に接続し、新規に追加された ZTP ファイアウォールを自動で登録するために使用されます。
- ワンタイム パスワード（**OTP**） – CSP と ZTP サービスと通信するために、Panorama で証明書を取得してインストールするために使用される、Palo Alto Networks によって提供されるワンタイム パスワード。
- インストーラ – ZTP ファイアウォールのオンボーディング用に `installeradmin` 管理者ロールを使用して作成された管理者ユーザー。この管理者ユーザーは、Panorama Web インターフェイスへのアクセスが制限されており、ZTP ファイアウォールのシリアル番号とクレームキーを入力して、CSP と Panorama にファイアウォールを登録するアクセスのみを許可しています。インストーラー管理者は、Panorama で作成するか、RADIUS、SAML、または TACACS + などのリモート認証を使用して作成できます。
- クレームキー – ZTP ファイアウォールを CSP に登録するために使用される ZTP ファイアウォールに物理的に付与された 8 桁の数字キー。
- **To-SW-Version**（**SW** バージョン指定） – ZTP ファイアウォールの PAN-OS ソフトウェアバージョンを指定します（**Panorama**（**Panorama**） > **Managed Devices**（管理対象デバイス） > **Summary**（概要） の順で移行）。ターゲットの PAN-OS リリースを選択して、ファイアウォールが指定されたバージョンよりも古いリリースを実行している場合、ファイアウォールはターゲットのリリースが正常にインストールされるまでアップグレードループを開始します。



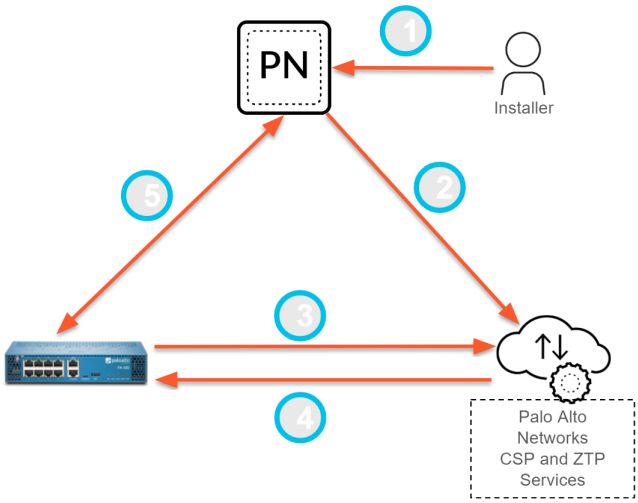
Panorama は、*Panorama* にインストールされているものと同じか、それより古い *PAN-OS* リリースを実行しているファイアウォールのみを管理できます。

Panorama で ZTP プラグインをインストールし、ZTP サービスで Panorama を登録した後、ZTP オンボーディング プロセスは以下のように続行します。

1. Installer (インスーラ) または IT 管理者は、ファイアウォール シリアル番号を使用して Panorama に追加し、鍵を取得することで、ZTP ファイアウォールを登録します。
2. Panorama は CSP でファイアウォールを登録します。ファイアウォールが正常に登録されると、ファイアウォールは ZTP サービスの Panorama と同じ ZTP テナントに関連付けられます。

   ZTP サービスで正常に登録された ZTP ファイアウォールは、Panorama 上で管理対象ファイアウォールとして自動的に追加されます (**Panorama** > **Managed Devices** (管理対象デバイス))。
3. ファイアウォールがインターネットに接続すると、ZTP ファイアウォールは、ZTP サービスに接続するために、CSP にデバイス証明書を要求します。
4. ZTP サービスは、Panorama IP または FQDN に ZTP ファイアウォールにプッシュします。
5. ZTP ファイアウォールは Panorama に接続し、デバイス グループとテンプレートの設定は Panorama から ZTP ファイアウォールにプッシュされます。

© 2019 Palo Alto Networks, Inc.



ZTP プラグインのインストール

Panorama™ 管理サーバに ZTP プラグインをインストールして、オンボーディングを簡略化するために、ZTP ファイアウォールを要求して、Panorama を ZTP サービスに登録します。

Panorama が高可用性 (HA) 設定にある場合は、ZTP プラグインをインストールして両方のPanorama HA ピアを ZTP サービスに登録します。

- Panorama に ZTP プラグインをインストールする
- Panorama の ZTP サービスへの登録

Panorama に ZTP プラグインをインストールする

Panorama 管理サーバに ZTP プラグインをインストールして、ZTP ファイアウォールのオンボーディングと管理を簡素化します。

STEP 1 | Panorama デバイス証明書のインストール.

STEP 2 | Panorama Web インターフェース、または Panorama プラグイン（**Panorama** > **Plugins** ）へのアクセス権を持つ スーパーユーザーもしくは Panorama 管理者として ログインします。

STEP 3 | **Panorama** > プラグインの順に選択して、`ztp`プラグインを検索します。

STEP 4 | ZTP プラグインの最新バージョンをダウンロードおよびインストールします。

Panorama の ZTP サービスへの登録

新規および既存のデプロイメント用に、Panorama™ 管理サーバを ZTP サービスに登録します。

- 新規導入の場合の Paranoma の ZTP サービスへの登録
- 導入済みの場合の Paranoma の ZTP サービスへの登録

新規導入の場合の **Paranoma** の **ZTP** サービスへの登録

Panorama™ 管理サーバに ZTP プラグインをインストールした後、ZTP サービスがファイアウォールを Panorama に関連付けることができるように、Panorama を ZTP サービスに登録しなければなりません。新規の ZTP デプロイメントの登録手順の一環として、ZTP ファイアウォールを ZTP サービスに接続するために必要なデバイス グループとテンプレート 設定を自動で生成します。デバイス グループとテンプレートが自動で生成されたら、ZTP ファイアウォールをデバイス グループとテンプレートに追加して、最初に Panorama に接続した後に ZTP サービスに接続できるようにしなければなりません。

© 2019 Palo Alto Networks, Inc.

STEP 1 | Panorama デバイス証明書のインストール.

STEP 2 | Palo Alto Networks カスタマー サポート ポータル（CSP）にログインします。

STEP 3 | Panorama を Palo Alto Networks CSP の ZTP サービスに関連付けます。

ZTP サービスは、高可用性（HA）設定の場合に限り、最大 2 つの Panoramas の関連付けをサポートします。Panorama が HA 設定でない場合は、単一の Panorama のみが関連付け可能です。

1. **Assets**（アセット）> **ZTP Service**（**ZTP** サービス）、そして **Associate Panorama(s)**（**Panorama** を関連付ける）を選択します。
2. ZTP ファイアウォールを管理する Panorama のシリアル番号を選択します。
3. （HA のみ）Panorama HA ピアのシリアル番号を選択します。
4. **OK** をクリックします。

STEP 4 | Panorama Web インターフェイスへのログイン.

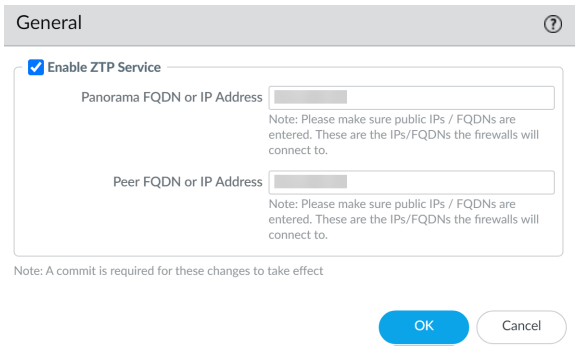
STEP 5 | **Panorama** > **Zero Touch Provisioning**（ゼロタッチプロビジョニング）> **Setup**（設定）の順に選択し、**General**（一般）ZTP 設定を編集します。

STEP 6 | ZTP サービスに Panorama を登録します。

1. **ZTP** サービスの有効化.
2. **Panorama FQDN** または **IP** アドレスを入力します。

   これは、ZTPプラグインがインストールされているPanoramaのFQDNまたはパブリックIPアドレスであり、CSPがZTPファイアウォールにプッシュします。
3. （HA のみ）ピアの **FQDN** または **IP** アドレスを入力します。

   これは、ZTP プラグインがインストールされている Panorama ピアの FQDN またはパブリック IP アドレスであり、フェイルオーバーが発生した場合に CSP がZTP にプッシュします。
4. **OK** をクリックして、設定の変更を保存します。

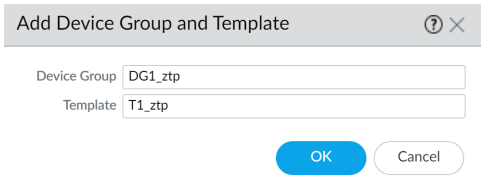


STEP 7 | デフォルトのデバイス グループとテンプレートを作成して、ZTP ファイアウォールを Panorama に接続するために必要な設定を自動で生成します。

デバイス グループとテンプレートを追加すると、Panorama と ZTP ファイアウォールを接続するためのデフォルト設定を含む、新規のデバイス グループとテンプレートが自動で生成されます。

1. デバイス グループとテンプレートを追加します。
2. デバイス グループ名を入力します。
3. テンプレート名を入力します。
4. **OK** をクリックして、設定の変更を保存します。

© 2019 Palo Alto Networks, Inc.



STEP 8 | 前の手順で指定したデバイス グループとテンプレートに ZTP ファイアウォールを追加します。

1. **Panorama**（**Panorama**）> **Device Groups**（デバイス グループ）の順に選択して、次に自動で作成されたデバイス グループを選択します。
2. ZTP の **Devices**（デバイス）を選択します。
3. **OK** をクリックして、設定の変更を保存します。
4. **Panorama** > **Templates**（テンプレート）の順に選択し、**Add Stack**（スタックを追加）します。
5. **Templates**（テンプレート）セクションで、自動で生成されたテンプレートを **Add**（追加）します。
6. ZTP の **Devices**（デバイス）を選択します。
7. **OK** をクリックして、設定の変更を保存します。

STEP 9 | 必要なデバイス グループとテンプレート設定が正常に生成されたことを確認します。

1. **Network**（ネットワーク）> **Interfaces**（インターフェイス）> **Ethernet**（イーサネット）の順に選択して、次に前のステップで作成した**Template**（テンプレート）を選択します。
2. `ethernet1/1`に IP アドレス、仮想ルーターおよびセキュリティ ゾーンが設定されていることを確認します。
3. **Network**（ネットワーク）> **Interfaces**（インターフェイス）> **Loopback**（ループバック）の順に選択して、次に前のステップで作成した**Template**（テンプレート）を選択します。
4. `loopback.900` インターフェースが正常に作成されていることを確認します。
5. **Policies**（ポリシー）> **Security**（セキュリティ）> **Pre Rules**（プレ ルール）の順に選択して、次に前の手順で作成した **Device Group**（デバイス グループ）を選択します。
6. `rule 1` が正常に作成されたことを確認します。
7. **Policies**（ポリシー）> **NAT**（NAT）> **Pre Rules**（プレ ルール）の順に選択して、次に前の手順で作成した **Device Group**（デバイス グループ）を選択します。
8. `ztp-nat` が正常に作成されたことを確認します。

STEP 10 | 必要に応じて、デバイス グループとテンプレートを変更します。

新規または既存のデバイス グループとテンプレートを作成して設定し、デプロイメントを完了します。

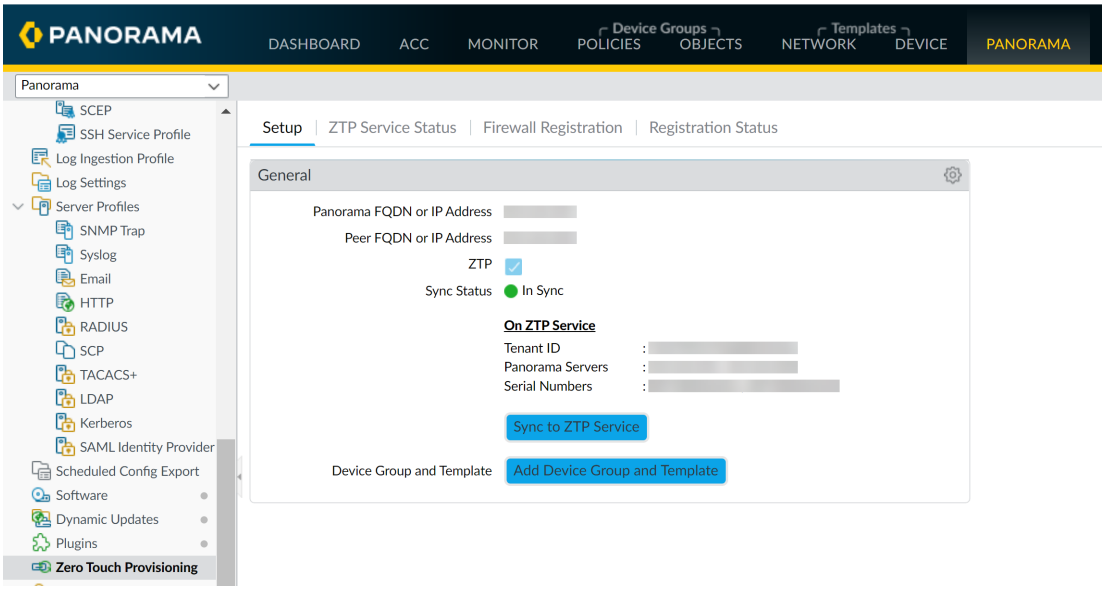
テンプレート スタックのデバイス グループの階層とテンプレートの優先度を検討するときは、ZTP ファイアウォールと Panorama が、通信ができるために必要な ZTP 設定を含む、デバイス グループとテンプレートは、設定が競合しても上書きされない優先度があることを確認します。

`ethernet1/1` インターフェース、`loopback.900` ループバック インターフェース、`rule 1` セキュリティ ポリシー ルールまたは `ztp-nat` NAT ポリシー ルールの IP アドレス、仮想ルーターおよびセキュリティゾーンは変更しないでください 。これらの設定は、ZTP ファイアウォールを Panorama に接続するために必要です。

STEP 11 | **Commit**（コミット）**Commit to Panorama**（**Panorama** へのコミット）の順に選択します。

STEP 12 | **ZTP** サービスに同期して、Panorama 同期状態が同期中と表示されることを確認します。

© 2019 Palo Alto Networks, Inc.



導入済みの場合の **Paranoma** の **ZTP** サービスへの登録

Panorama™ 管理サーバに ZTP プラグインをインストールした後、ZTP サービスがファイアウォールを Panorama に関連付けることができるように、Panorama を ZTP サービスに登録しなければなりません。登録手順の一環として、ZTP ファイアウォールが、初めて Panorama に接続した後で、ZTP ファイアウォールを ZTP サービスに接続するために必要な ZTP 設定を含んでいる、デバイス グループとテンプレートに ZTP ファイアウォールを追加します。

STEP 1 | Panorama デバイス証明書のインストール.

STEP 2 | Palo Alto Networks カスタマー サポート ポータル（CSP）にログインします。

STEP 3 | Panorama を Palo Alto Networks CSP の ZTP サービスに関連付けます。

ZTP サービスは、高可用性（HA）設定の場合に限り、最大 2 つの Panoramas の関連付けをサポートします。Panorama が HA 設定でない場合は、単一の Panorama のみが関連付け可能です。

1. **Assets**（アセット）> **ZTP Service**（**ZTP** サービス）そして **Modify Association**（関連の変更）の順に選択します。
2. ZTP ファイアウォールを管理する Panorama のシリアル番号を選択します。
3. （HA のみ）Panorama HA ピアのシリアル番号を選択します。
4. **OK** をクリックします。

STEP 4 | Panorama Web インターフェイスへのログイン.

STEP 5 | **Panorama** > **Zero Touch Provisioning**（ゼロタッチプロビジョニング）> **Setup**（設定）の順に選択し、**General**（一般）ZTP 設定を編集します。

STEP 6 | ZTP サービスに Panorama を登録します。

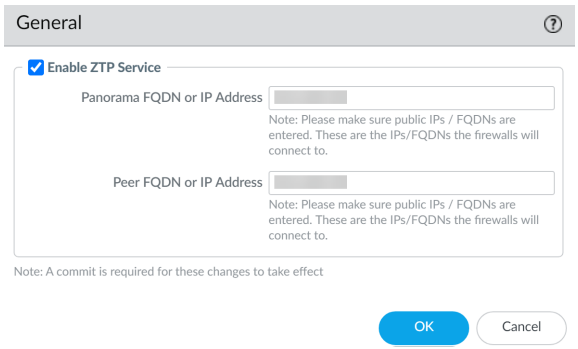
1. **ZTP** サービスの有効化.
2. **Panorama FQDN** または **IP** アドレスを入力します。

   これは、ZTP プラグインがインストールされ、CSP が ZTP ファイアウォールにプッシュする Panorama の FQDN またはパブリック IP アドレスです。
3. （HA のみ）ピアの **FQDN** または **IP** アドレスを入力します。

© 2019 Palo Alto Networks, Inc.

これは、ZTP プラグインがインストールされている Panorama ピアの FQDN またはパブリック IP アドレスであり、フェイルオーバーが発生した場合に CSP がZTP にプッシュします。

4. **OK** をクリックして、設定の変更を保存します。



STEP 7 | 必要な ZTP 設定を含むデバイス グループとテンプレートに、ZTP ファイアウォールを追加します。

1. **Panorama**（**Panorama**）> **Device Groups**（デバイス グループ）の順に選択して、必要な ZTP 設定を含むデバイス グループを選択します。
2. ZTP の **Devices**（デバイス）を選択します。
3. **OK** をクリックして、設定の変更を保存します。
4. **Panorama**（**Panorama**）> **Templates**（テンプレート）の順に選択して、必要な ZTP 設定があるテンプレートを含むテンプレート スタックを選択します。
5. ZTP の **Devices**（デバイス）を選択します。
6. **OK** をクリックして、設定の変更を保存します。

STEP 8 | 必要に応じて、デバイス グループとテンプレートを変更します。

テンプレート スタックのデバイス グループの階層とテンプレートの優先度を検討するときは、ZTP ファイアウォールと Panorama が、通信ができるために必要な ZTP 設定を含む、デバイス グループとテンプレートは、設定が競合しても上書きされない優先度があることを確認します。

1. Ethernet 1/1 インターフェイスを設定します。
   1. **Network**（ネットワーク）> **Interfaces**（インターフェイス）> **Ethernet**（イーサネット）の順に選択して、次に ZTP 設定を含む **Template**（テンプレート）を選択し、そして **ethernet1/1**を選択します 。
   2. **Interface Type (**インターフェイス タイプ**)** については、**Layer3** を選択します。
   3. **Config**（設定）を選択し、**Virtual Router**（バーチャル ルータ）を設定して、**Security Zone**（セキュリティ ゾーン）を**Untrust**（信用しない）に設定します。
   4. **IPv4** を選択し、**Type**（タイプ）には **DHCP Client**（**DHCP**クライアント）を選択します。

      ZTP ファイアウォールが *ZTP* サービスと通信するには、*DHCP* クライアントが必要です。

   5. **OK** を押下して、設定の変更を保存します。
2. ループバック インターフェイスの作成
   1. **Network**（ネットワーク）> **Interfaces**（インターフェイス）> **Loopback**（ループバック）の順に選択して、次に ZTP 設定を含む **Template**（テンプレート）を選択し、そしてループバック インターフェイスを追加します。
   2. **Interface Name**（インターフェイス名）には、`loopback`（ループ バック）と入力し、サフィックスの `900` を入力します。

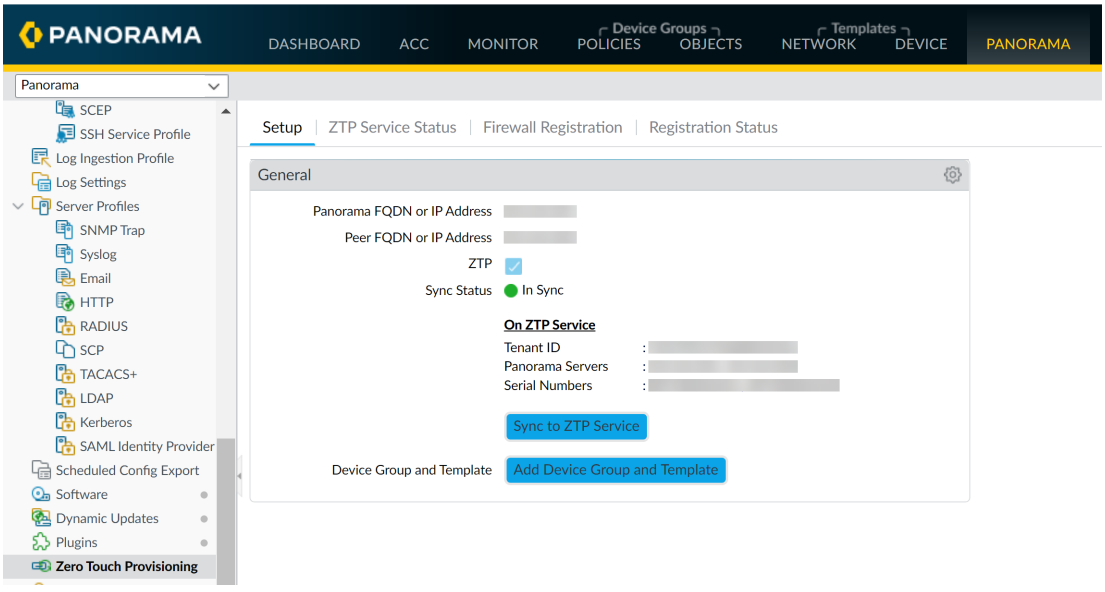
© 2019 Palo Alto Networks, Inc.

3. **Config**（設定）**Virtual Router**（バーチャル ルータ）の順に選択し、**Security Zone**（セキュリティ ゾーン）を **Trust**（信用する）に設定します。
4. **OK** を押下して、設定の変更を保存します。

3. ZTP ファイアウォールと Panorama の通信を許可するセキュリティ ポリシー ルールを作成します。
   1. **Policies**（ポリシー）> **Security**（セキュリティ）> **Pre Rules**（プレ ルール）の順に選択して、次に ZTP ポリシー ルールを含む **Device Group**（デバイス グループ）を選択し、新規のルールを **Add**（追加）します。
   2. ポリシー ルールに分かりやすい **Name**（名前）を入力します。
   3. **Source**（発信元）> **Source Zone**（発信元 ゾーン）の順に選択して、 **Trust**（信用する）ゾーンを **Add**（追加）します。
   4. **Destination**（宛先）> **Destination Zone**（宛先ゾーン）を選択して、**Untrust**（信用しない）ゾーンを **Add**（追加）します。
   5. **Action**（アクション）> **Action Settings**（アクション設定）> **Action**（アクション）の順に選択して、次に **Allow**（許可）を選択します。
4. ZTP ファイアウォールと Panorama の通信を許可する NAT ポリシー ルールを作成します。
   1. **Policies**（ポリシー）> **NAT**（**NAT**）> **Pre Rules**（プレ ルール）の順に選択して、次に ZTP ポリシー ルールを含む **Device Group**（デバイス グループ）を選択し、新規のルールを **Add**（追加）します。
   2. ポリシー ルールに分かりやすい **Name**（名前）を入力します。
   3. **Original Packet**（オリジナル パケット）を選択して、以下を設定します：
      1. **Source Zone**（発信元 ゾーン）に、**Trust**（信頼する）ゾーンを **Add**（追加）します。
      2. **Destination Zone**（宛先ゾーン）に、**Untrust**（信用しない）ゾーンを選択します。
      3. **Destination Interface**（宛先 インターフェイス）に、**ethernet1/1** インターフェイスを選択します。
   4. **OK** をクリックして、設定の変更を保存します。

STEP 9 | **Commit**（コミット）**Commit to Panorama**（**Panorama** へのコミット）の順に選択します。

STEP 10 | **ZTP** サービスに同期して、Panorama 同期状態が同期中と表示されることを確認します。



© 2019 Palo Alto Networks, Inc.

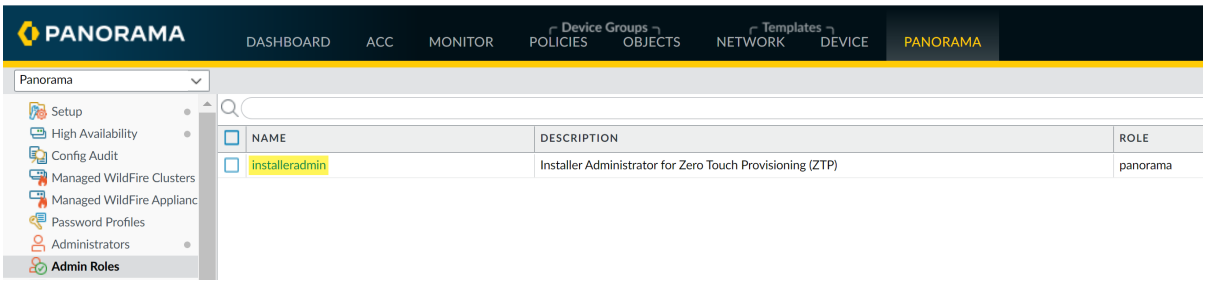
ZTP インストーラ管理者アカウントの設定

ZTP インストーラーの管理者ユーザーは、非 IT スタッフまたはインストール請負業者が新規 ZTP ファイアウォールをオンボードするために作成された管理者アカウントです。インストーラー管理者は、自動的に作成された `installeradmin` 管理者ロールを使用して、Panorama Web インターフェースの表示を制限し、Panorama で ZTP ファイアウォールのクレームキーとシリアル番号を入力することのみを許可します。

STEP 1 | Panorama Web インターフェイスへのログイン.

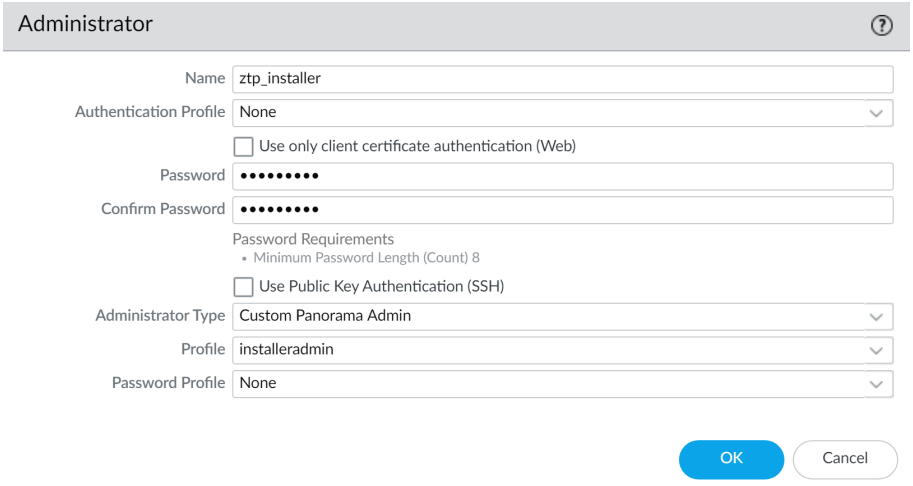
STEP 2 | **Panorama**（**Panorama**）> **Admin Roles**（管理者ロール）の順に選択し、**`installeradmin`** 管理者ロールが作成されていることを確認します。

Panorama に ZTP プラグインを正常にインストールした後、 `installeradmin` が自動的に作成されます。



STEP 3 | ZTP インストーラーの管理者ユーザーを構成します。

1. **Panorama**（**Panorama**）> **Administrators**（管理者）の順に選択し、新規管理者ユーザーを **Add**（追加）します。
2. ZTP インストーラーの管理ユーザーに記述する**Name**（名前）を入力します。
3. セキュアな**Password**（パスワード）を入力し、**Confirm Password**（パスワードを確認）します。
4. 管理者タイプには、**Custom Panorama Admin**（カスタム Panorama 管理）を選択します。
5. **Profile**（プロファイル）には、 **installeradmin** を選択します。
6. **OK** をクリックして、設定の変更を保存します。



STEP 4 | **Commit (コミット) および Commit to Panorama (Panorama へのコミット)** をクリックします。

© 2019 Palo Alto Networks, Inc.

Panorama への ZTP ファイアウォールの追加

1 つの ZTP ファイアウォールを追加するか、複数の ZTP ファイアウォールを Panorama™ 管理サーバにインポートできます。

- Panorama への ZTP ファイアウォールの追加
- Panorama への 複数の ZTP ファイアウォールの インポート

Panorama への ZTP ファイアウォールの追加

Panorama™ 管理サーバの Webインターフェースに、スーパーユーザー、Panorama 管理者、または ZTP installer admin（ZTP インストーラー管理者）としてログインし、ZTP ファイアウォールを Panorama に追加します。ZTP ファイアウォールを追加するには、Palo Alto Networks から提供されたファイアウォールのシリアル番号およびクレームキーを入力し、ファイアウォールを ZTP サービスに登録する必要があります。ファイアウォールを登録すると、カスタマサポートポータル（CSP）のアカウントのアセットとしてファイアウォールが要求され、ZTP サービスがファイアウォールを Panorama に関連付けることができます。

ZTP ファイアウォールを *Panorama* に追加中は、ファイアウォールがステップ 4 で*Panorama* に正常に追加したことを確認する前に、*ZTP* ファイアウォールで一切コミットを実行することはできません。*ZTP* ファイアウォールでローカル コミットを実行すると、*ZTP* 機能が無効になり、ファイアウォールを *Panorama* に正常に追加できなくなります。

STEP 1 | Panorama Web インターフェイスへのログイン.

STEP 2 | ZTP ファイアウォールを Panorama に追加します。

ZTP ファイアウォールを *CSP* に正常に登録し、ポリシーとネットワーク設定をプッシュするには、*ZTP* ファイアウォールの *Eth1/1* インターフェースを接続する必要があります。

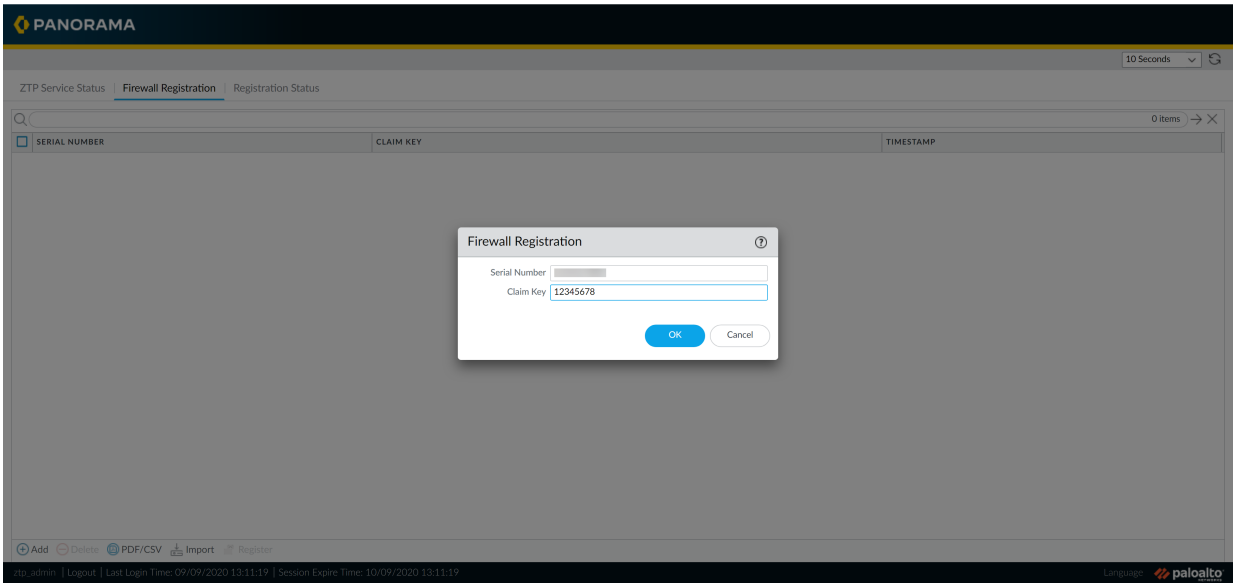
1. **Firewall Registration**（ファイアウォール登録）を選択し、新規 ZTP ファイアウォールを **Add**（追加）します。
2. ZTP ファイアウォールの **Serial Number**（シリアル番号）を入力します。
3. Palo Alto Networks が提供する ZTP ファイアウォールの **Claim Key**（クレームキー）を入力します。

   8桁の数字のクレームキーは、Palo Alto Networks から受け取った ZTP ファイアウォールの背面に貼付された物理ラベルに印刷されています。



4. **OK** をクリックして、設定の変更を保存します。

© 2019 Palo Alto Networks, Inc.



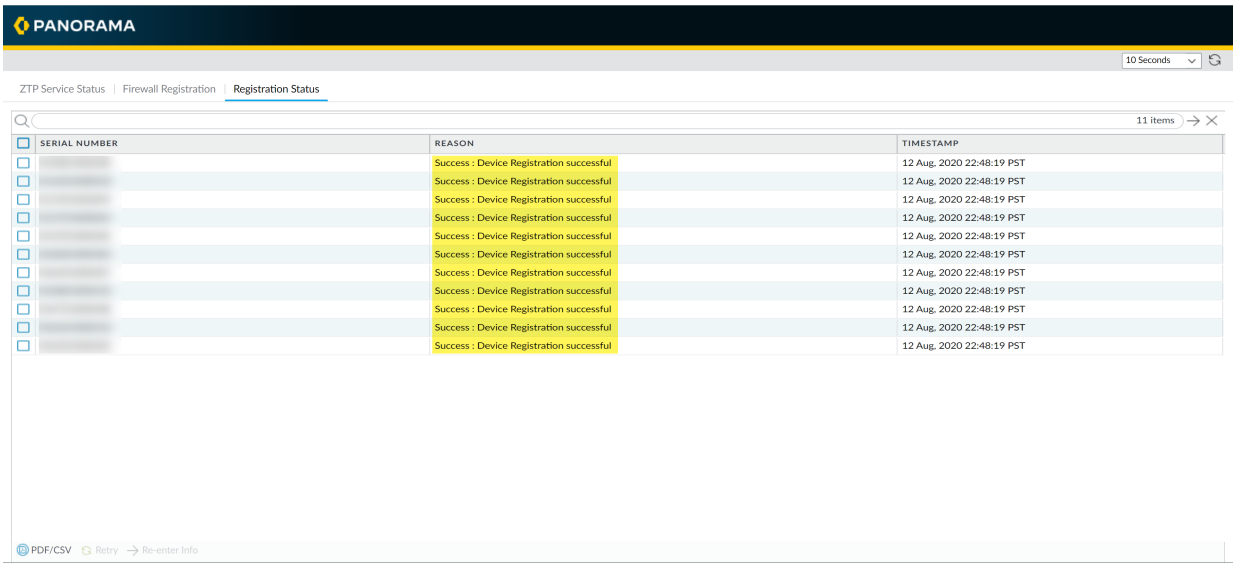
STEP 3 | ZTP ファイアウォールを登録します。

1. 新たに追加した ZTP ファイアウォールを選択し、ファイアウォールを **Register**（登録）します。
2. プロンプトが表示されたら、**Yes**（はい）をクリックして、ZTP ファイアウォールの登録を確定します。

STEP 4 | ファイアウォールが、CSP に正常に登録されていることを確認します。

デバイス証明書を正常に取得するには、ファイアウォールが *CSP* に正常に登録されている必要があります。

1. **Registration Status**（登録ステータス）を選択し、CSP が ZTP サービスに正常に登録されたことを確認します。



2. 管理者認証情報を使用するPanorama Web インターフェイスへのログイン。
3. **Panorama**（**Panorama**）> **Managed Devices**（管理対象デバイス）> **Summary**（概要）の順に選択し、ZTP ファイアウォールが管理対象ファイアウォールとして正常に追加されていることを確認します。

© 2019 Palo Alto Networks, Inc.

ファイアウォールが意図せずにアップグレードまたはダウングレードしないように、*To SW Version*（*SW* バージョンに）列が正しい *PAN-OS* バージョンに設定されていることを確認してください。*ZTP* 機能は、*PAN-OS 10.0.1* 以降のリリースでサポートされます。さらに、*PAN-OS* のバージョンは、*Panorama* で実行されている *PAN-OS* のバージョンと同じか、それ以前のバージョンでなければなりません。

詳細は、「ZTP ファイアウォールのアップグレード」を参照してください。

STEP 5 | ZTP ファイアウォールをデバイスグループとテンプレートスタックに追加します。

ファイアウォールで `Connected`（接続済み）と表示させて、ポリシーとネットワーク設定をプッシュするには、ZTP ファイアウォールをデバイスグループとテンプレートスタックに追加する必要があります。

1. 管理者認証情報を使用するPanorama Web インターフェイスへのログイン。
2. **Panorama** > **Device Groups**、を選択し、デバイス グループを追加し、ZTP ファイアウォールをデバイス グループに追加します。

   デバイス グループを追加して、ZTP ファイアウォールのポリシーオブジェクトとルールを含む新規デバイスグループを作成および設定します。
3. **Panorama** > **Templates** (テンプレート) を選択し、テンプレート スタックを設定し、ZTP ファイアウォールをテンプレート スタックに設定します。

   テンプレートスタックを設定して、ZTP ファイアウォールのネットワーク設定を含む新規テンプレートスタックを作成および設定します。

Panorama への 複数の *ZTP* ファイアウォールの インポート

Panorama™ 管理サーバの Web インターフェースに、スーパーユーザー、Panorama 管理者、またはZTP installer admin（ZTP インストーラー管理者）としてログインし、複数の ZTP ファイアウォールを Panorama にインポートします。複数の ZTP ファイアウォールをインポートするには、Palo Alto Networks から提供された ZTP ファイアウォールのシリアル番号と対応するクレームキーの CSV ファイルをインポートしてから、ファイアウォールを ZTP サービスに登録します。ファイアウォールを登録すると、カスタマーサポートポータルのアカウントの資産としてファイアウォールが要求され、ZTP サービスがファイアウォールを Panorama に関連付けることができます。

ZTP ファイアウォールを *Panorama* に追加中は、ステップ 5 でファイアーウォールが *Panorama* に正常に追加されたことを確認する前に *ZTP* ファイアウォールで一切コミットを実行してはいけません。*ZTP* ファイアウォールでローカル コミットを実行すると、*ZTP* 機能が無効になり、ファイアウォールを *Panorama* に正常に追加できなくなります。

STEP 1 | ZTP ファイアウォールのシリアル番号とクレームキーを収集します。

8桁の数字のクレームキーは、Palo Alto Networks から受け取った ZTP ファイアウォールの背面に貼付された物理ラベルに印刷されています。



© 2019 Palo Alto Networks, Inc.

STEP 2 | ZTP ファイアウォールのシリアル番号とクレームキーを含む CSV ファイルを作成します。最初の列にはシリアル番号が含まれ、2番目の列にはそのファイアウォールに対応するクレームキーが含まれている必要があります。以下の例を参照してください。

	A	B
1	Serial Number	Claim Key
2	abcd1234	123456789
3	xyz7890	987654321

STEP 3 | ZTP ファイアウォールを Panorama にインポートします。

ZTP ファイアウォールを *CSP* に正常に登録し、ポリシーとネットワーク設定をプッシュするには、*ZTP* ファイアウォールの *Eth1/1* インターフェースを接続する必要があります。

1. ZTP インストーラーの管理者認証情報を使用して、Panorama Web インターフェイスへのログイン。
2. **Panorama**（**Panorama**）> **Zero Touch Provisioning**（ゼロタッチプロビジョニング）> **Firewall Registration**（ファイアウォールの登録）の順に選択して、ZTP ファイアウォールを **Import**（インポート）します。
3. **Browse**（参照）して、ZTP ファイアウォール情報を含む CSV ファイルを選択し、**OK** をクリックします。

STEP 4 | ZTP ファイアウォールを登録します。

1. 新規に追加した ZTP ファイアウォールを選択し、ファイアウォールを **Register**（登録）します。
2. プロンプトが表示されたら、**Yes**（はい）をクリックして、ZTP ファイアウォールの登録を確認します。

STEP 5 | ファイアウォールが、ZTP サービスに正常に登録されていることを確認します。

1. **Registration Status**（登録状態）を選択し、ZTP ファイアウォールが ZTP サービスに正常に登録されたことを確認します。
2. 管理者認証情報を使用するPanorama Web インターフェイスへのログイン。
3. **Panorama**（**Panorama**）> **Managed Devices**（管理対象デバイス）> **Summary**（概要）の順に選択して、ZTP ファイアウォールが管理対象ファイアウォールとして正常に追加されていることを確認します。

ファイアウォールが意図せずにアップグレードまたはダウングレードしないように、*To SW Version*（*SW* バージョンに）列が正しい *PAN-OS* バージョンに設定されていることを確認してください。*ZTP* 機能は、*PAN-OS 10.0.1* 以降のリリースでのみサポートされます。さらに、*PAN-OS* のバージョンは、*Panorama* で実行されている *PAN-OS* のバージョンと同じか、それ以前のバージョンでなければなりません。

詳細は、「ZTP ファイアウォールのアップグレード」を参照してください。

STEP 6 | ZTP ファイアウォールをデバイス グループとテンプレート スタックに追加します。

ファイアウォールで `Connected`（接続済み）と表示させて、ポリシーとネットワーク設定をプッシュするには、ZTP ファイアウォールをデバイスグループとテンプレートスタックに追加しなければなりません。

1. 管理者認証情報を使用するPanorama Web インターフェイスへのログイン。
2. **Panorama**（**Panorama**）> **Device Groups**（デバイス グループ）の順に選択し、適切なデバイス グループにファイアウォールを割り当てます。

© 2019 Palo Alto Networks, Inc.

デバイス グループを追加して、ZTP ファイアウォールのポリシーオブジェクトとルールを含む新規デバイスグループを作成および設定します。

3. **Panorama**（**Panorama**）> **Templates**（テンプレート）の順に選択して、適切なテンプレート スタックにファイアウォールを割り当てます。

   テンプレートスタックを設定して、ZTP ファイアウォールのネットワーク設定を含む新規テンプレートスタックを作成および設定します。

ZTP タスクでの CLI の使用

次の CL Iコマンドを使用して、ゼロタッチプロビジョニング（ZTP）タスクを実行し、ZTP サービスのステータスを表示します。

実行したい内容	以下を使用
ファイアウォール **CLI** からファイアウォールを管理する	
ZTP サービスへの接続ステータスを表示します。	`> show system ZTP status`
Panorama 管理サーバーへの接続ステータスを表示します。	`> show panorama status`
ZTP モデル番号とファイアウォールのシステム情報を表示します。	`> show system info`
ファイアウォールの ZTP ステータス マシンを無効にします。 このコマンドを実行しても、既存の ZTP 設定は一切削除されません。 *CLI* から無効化した後は、ファイアウォールの *ZTP* ステータス マシンを再有効化することはできません。 再有効化するには、ファイアウォールを工場出荷時設定にリセットする必要があります。	`> request disable ztp`
Panorama からの **ZTP** ファイアウォールの登録、設定、管理	
Eth1/1 インターフェースで ZTP サービスを使用して、管理対象ファイアウォールを Panorama に接続するために必要な設定を含むデバイス グループまたはテンプレートを作成します。	`> request plugins ztp create dgroup-template device-group <device group name>` `> request plugins ztp create dgroup-template template <template name>`

© 2019 Palo Alto Networks, Inc.

実行したい内容	以下を使用
ファイアウォールのリストに ZTP ファイアウォールを追加して、ZTP サービスに今後登録できるようにします。	`> request plugins ztp firewall-add <serial number> claim-key <claim key>`
ファイアウォールのリストにすでに追加されている ZTP ファイアウォールのシリアル番号を、今後の ZTP サービスへの登録のために変更します。	`> request plugins ztp firewall-add-modify firewall <old serial number> claim-key <claim key> new-serial <new serial number>`
ファイアウォールのリストから ZTP ファイアウォールを削除して、ZTP サービスに今後登録できるようにします。	`> request plugins ztp firewall-delete firewall <serial number>`
ファイアウォールのリストに ZTP ファイアウォールを追加して、ZTP サービスに今後、再登録できるようにします。 このコマンドは、ZTP ファイアウォールが最初に ZTP サービスへの登録に失敗し、必要になったときに使用します。	`> request plugins ztp firewall-re-enter-info firewall <serial number> claim-key <claim key>`
Panorama™ 管理サーバを ZTP サービスに登録します。	`> request plugins ztp panorama-registration`
ZTP サービスに ZTP ファイアウォールを登録します。	`> request plugins ztp firewall-registration firewall <serial number> claim-key <claim key>`
ZTP サービスに ZTP ファイアウォールを再登録します。 このコマンドを使用して、ZTP サービスへの初期登録に失敗した ZTP ファイアウォールの再登録プロセスを開始します。	`> request plugins ztp firewall-register-retry firewall <serial number> claim-key <claim key>`
ZTP ファイアウォールのシリアル番号をインポートし、主要な情報を要求します。 指定するファイルは CSV 形式でなければなりません。	`> request plugins ztp ztp-add-import import-path <file path>`
Panorama からの ZTP ファイアウォール情報と ZTP サービスステータスの表示	
Panorama に登録されている ZTP ファイアウォールのリストを ZTP サービスから取得します。	`> request plugins ztp ztp-service-info` 以下の詳細が表示されます。

© 2019 Palo Alto Networks, Inc.

実行したい内容	以下を使用
	• first-firewall-connect-time — ZTP ファイアウォールが ZTP サービスに最初に接続したときのタイムスタンプ。 • last-firewall-connect-time — ZTP ファイアウォールが ZTP サービスに最後に接続したときのタイムスタンプ。 • registration-time — ZTP ファイアウォールが ZTP サービスに登録されたときのタイムスタンプ。 • isZTPFirewall — ファイアウォールが ZTP ファイアウォールかどうかの確認。 • created_by — ZTP ファイアウォールを追加した管理ユーザー。 • IP address — ZTP ファイアウォールの IP アドレス。
ZTP サービスに登録するファイアウォールのリストで、ZTP ファイアウォールのリストを表示します。	> **show plugins ztp device-add-list**
ZTP ファイアウォールの登録ステータスを表示します。	> **show plugins ztp device-reg-status**
ZTP ファイアウォールの ZTP サービス同期ステータスを表示します。	> **request plugins ztp ztp-sync-status**
管理プレーン ZTP 接続全履歴を表示します。 これは、ZTP サービスへの接続のトラブルシューティングに役立ちます。	> **tail follow yes mp-log ms.log**

ZTP プラグインのアンインストール

手順に従って ZTP 設定を Panorama™ 管理サーバーから ZTP 設定を削除して、ZTP プラグインをアンインストールします。Panorama が高可用性 (HA) 設定の場合、両方の Panorama HA ピアでこれらのステップを繰り返します。

STEP 1 | Panorama Web インターフェイスへのログイン.

STEP 2 | ZTP インストーラ管理者アカウントを削除します。

1. **Panorama** > **Administrators** (管理者) を選択し、以前に設定した ZTP installer administrator account (ZTP インストーラ管理者アカウント) を選択します。
2. ZTP インストーラ管理者アカウントを **Delete** (削除) します。
3. **Panorama** > **Administrators** (管理者) を選択し、installeradmin 管理者ロールを選択します。
4. installeradmin 管理者ロールを **Delete** (削除) します。
5. **Commit** (コミット) および **Commit to Panorama** (Panorama へのコミット) をクリックします。

STEP 3 | ZTP プラグインのアンインストール

1. **Panorama** > **Plugins** (プラグイン) を選択して、Panorama にインストールした ZTP プラグインに移動します。

© 2019 Palo Alto Networks, Inc.

2. Panorama から ZTP 関連の設定を削除するには、Actions (アクション) 列で **Remove Config (設定の削除)** を実行します。
3. Panorama からの ZTP 設定の削除を確認するプロンプトが表示されたら、**OK** をクリックします。
4. **Commit (コミット)** および **Commit to Panorama (Panorama へのコミット)** をクリックします。
5. ZTP プラグインを **Uninstall (アンインストール)** します。
6. Panorama からの ZTP プラグインのアンインストールを確認するプロンプトが表示されたら、**OK** をクリックします。

© 2019 Palo Alto Networks, Inc.

デバイス グループの管理

- デバイス グループの追加
- デバイス グループの階層を作成
- 共有またはデバイス グループ ポリシーで使用するオブジェクトの作成
- 継承したオブジェクトの値を復元
- 未使用の共有オブジェクトの管理
- 継承したオブジェクトの優先度を管理
- ポリシー ルールあるいはオブジェクトを別のデバイス グループに移動/コピー
- Panorama で URL フィルタリング ベンダーを選択
- ファイアウォールのサブセットにポリシー ルールをプッシュ
- ルール階層の管理

デバイス グループの追加

追加したファイアーウォール (管理対象デバイスとしてのファイアウォールの追加を参照) は、次のようにしてDevice Groups（デバイス グループ）(1,024 件まで) にグループ化することができます。必ずアクティブ-パッシブの高可用性（HA）設定のファイアウォールを両方とも同じデバイス グループに割り当て、Panorama が同じポリシー ルールおよびオブジェクトをそのファイアウォールにプッシュするようにしてください。PAN-OS はプッシュされたルールを HA ピア間で同期することはありません。組織内の別の管理レベルでルールやオブジェクトを管理する方法については デバイス グループの階層を作成をご覧ください。

STEP 1 | **Panorama** > **Device Groups**（デバイス グループ）を選択し、**Add**（追加）をクリックします。

STEP 2 | デバイス グループを識別するために、一意の **Name**（名前）と **Description**（内容）を入力します。

STEP 3 | Devices（デバイス）セクションでチェック ボックスを選択し、ファイアウォールをグループに割り当てます。ファイアウォールのリストが大きい場合は、検索時にフィルタを使用します。



ファイアウォールは *1* つのデバイス グループにのみ割り当てることができます。ファイアウォール上の各仮想システムは異なるデバイス グループに割り当てられます。

STEP 4 | 参照テンプレートセクションで、デバイス グループ構成によって参照されるオブジェクトを含む、テンプレートまたはテンプレート スタックを **Add** (追加) します。

テンプレートまたはテンプレート スタックをデバイス グループに関連付けるには、デバイス グループに適切なテンプレートまたはテンプレート スタック参照を割り当てる必要があります。これにより、テンプレートスタックに無関係なデバイスを追加することなく、テンプレートまたはテンプレートスタックで設定されたオブジェクトを参照できます。

デバイス グループ設定がテンプレートまたはテンプレート スタックで設定されたオブジェクトを参照しない場合は、この手順をスキップします。

STEP 5 | （任意）HA ピアであるファイアウォールの **Group HA Peers**（HA ピアのグループ化）を選択します。

管理対象ファイアウォールの HA ピアは、同じデバイスグループ内にある場合にのみグループ化できます。

© 2019 Palo Alto Networks, Inc.



パッシブあるいはアクティブのセカンダリ ピアのファイアウォール名は括弧付きで表示されます。*HA* ピアのグループ化は視覚的な変更であり、設定の変更は発生しません。

STEP 6 | デバイス グループの階層構造で現在作成しようとしているデバイス グループの直接の親にあたる **Parent Device Group**（親デバイス グループ）（デフォルトは **Shared**（共有））を選択します。

STEP 7 | ポリシー ルールがユーザーおよびグループを参照する場合は **Master**（マスター）ファイアウォールを割り当てます。

これはそのデバイス グループのうち、Panorama がユーザー名やユーザー グループの情報を取得する唯一のファイアウォールになります。

STEP 8 | **OK** をクリックして変更内容を保存します。

STEP 9 | **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択してから、Panorama 設定の変更内容と追加したデバイス グループの変更内容を **Commit and Push**（コミットしてプッシュ）します。

デバイス グループの階層を作成

STEP 1 | デバイス グループの階層構造を計画します。

1. デバイス グループのレベル、さらに各デバイス グループおよび共有領域に割り当てるファイアウォールや仮想システムを決定します。単体のファイアウォールあるいは仮想システム（vsys）は一つのデバイス グループにのみ割り当てることができます。デバイス グループが低い階層のデバイス グループを含有するためのコンテナに過ぎない場合、ファイアウォールを割り当てる必要はありません。
2. 計画中の階層構造で不要になる場合は、既存のデバイス グループに対するファイアウォールあるいは vsys の割り当てを解除します。
    1. **Panorama** > **Device Groups**(Panorama > デバイスグループ) の順に選択し、デバイスグループを選択します。
    2. 削除したいファイアウォールや仮想システムのチェックを Devices（デバイス）セクションで解除し、**OK** をクリックします。
3. 必要に応じて、デバイス グループに割り当てるファイアウォールを追加します（「管理対象デバイスとしてのファイアウォールの追加」を参照）。
4. エンドポイント モニタリングを実行するために複数の Panorama プラグインを使用している場合、特定のハイパーバイザにデプロイされたファイアウォールを含むデバイス グループを、別のハイパーバイザにデプロイされたファイアウォールを含むデバイス グループの子または親にすることはできません。詳細は、「デバイス グループ階層」を参照してください。

STEP 2 | トップレベルにある各デバイス グループに対してデバイス グループの追加を行います。

1. **Panorama** > **Device Groups** (Panorama > デバイスグループ)ページで**Add** (追加)をクリックし、**Name** (名前)にデバイスグループを識別するための名前を入力します。
2. Devices（デバイス）セクションでチェック ボックスを選択し、ファイアウォールおよび仮想システムをデバイス グループに割り当てます。
3. **Parent Device Group**（親デバイス グループ）オプションは**Shared**（共有）（デフォルト）のままにして **OK** をクリックします。

STEP 3 | 下層にある各デバイス グループに対してデバイス グループの追加を行います。

© 2019 Palo Alto Networks, Inc.

- 下層にある新しいデバイスグループに対して前の ステップ を繰り返しますが、**Parent Device Group (親デバイスグループ)**は一層上のデバイスグループに設定します。
- 既存の各デバイス グループについて、**Device Groups**（デバイス グループ）ページでデバイス グループを選択して編集し、**Parent Device Group**（親デバイス グループ）を選択して **OK** をクリックします。



デバイス グループを別の親の下に移動させると、そのデバイス グループあるいは子孫デバイス グループに関連するすべてのファイアウォール、ポリシー ルール、オブジェクトとともにその子孫デバイス グループも移動します。新しい親が別のアクセス ドメインにある場合、移動したデバイス グループは元のアクセス ドメインのメンバーではなくなります。新しいアクセス ドメインに親デバイス グループの読み取り/書き込みアクセス権がある場合、移動したデバイス グループの読み取り/書き込みアクセス権も付与されます。新しいアクセスドメインに親デバイス グループの読み取り専用アクセス権がある場合、移動したデバイス グループに対するアクセス権は一切付与されません。デバイス グループのアクセス権を再設定する方法については、「アクセス ドメインの設定」を参照してください。

STEP 4 | 必要に応じてオブジェクトおよびポリシー ルールを設定、移動、コピーし、デバイス グループの階層構造における継承関係を構成します。

- 共有またはデバイス グループ ポリシーで使用するオブジェクトの作成を行うか、既存のオブジェクトを編集します。

オブジェクトはオブジェクトの口ケーション（オブジェクトが割り当てられているデバイス グループ）でのみ編集できます。子孫デバイス グループはその口ケーションからオブジェクトの読み取り専用のインスタンスを継承します。ただし、必要な場合は、「継承したオブジェクトの値をオーバーライドします。」のステップを参照してください。

- ポリシーを作成あるいは編集します。
- ポリシー ルールあるいはオブジェクトを別のデバイス グループに移動/コピーします。

STEP 5 | 継承したオブジェクトの値をオーバーライドします。

特定のデバイス グループのオブジェクトの値を、先祖デバイス グループから継承した値以外に設定する場合のみ。

オブジェクトをオーバーライドした後、子孫デバイス グループでさらにオーバーライドすることができます。ただし、共有または事前設定の（デフォルト）オブジェクトをオーバーライドすることはできません。

Objects（オブジェクト）タブの Name（名前）列では継承したオブジェクトに緑色のアイコンが付き、Location（口ケーション）列に先祖デバイス グループが表示されます。

1. **Objects (オブジェクト)**タブでオブジェクト タイプを選択します（例：**Objects** > **Addresses (オブジェクト > アドレス)**）。
2. オーバーライド インスタンスを持たせる **Device Group**（デバイス グループ）を選択します。
3. オブジェクトを選択して **Override**（オーバーライド）をクリックします。
4. 値を変更します。**Name**（名前）や **Shared**（共有）設定は変更できません。
5. **OK** をクリックします。Name（名前）列では、オーバーライドされたオブジェクトに黄色い線のある緑色のアイコンが表示されます。



必要に応じて、後で継承したオブジェクトの値を復元します。

STEP 6 | 変更を保存してコミットします。

© 2019 Palo Alto Networks, Inc.

階層を変更したら、*Panorama* にコミットし、デバイス グループにプッシュします。

テンプレートがデバイス グループ内のオブジェクトを参照しており（アドレスを参照するインターフェイスなど）、階層が変更されたためにそのテンプレートに割り当てられているファイアウォールがそのデバイス グループに割り当てられなくなった場合は、テンプレートにも変更内容をプッシュする必要があります。

Commit（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択してから、Panorama 設定および追加または変更したデバイス グループに対して、変更内容を **Commit and Push**（コミットしてプッシュ）します。

共有またはデバイス グループ ポリシーで使用するオブジェクトの作成

共有領域、そのオブジェクトと同じデバイス グループ、あるいはそのデバイス グループの子孫に含まれるあらゆるポリシー ルールでそのオブジェクトを使用できます (詳細はデバイス グループ オブジェクトを参照してください)。

動的アドレスグループを使用してネットワーク内の変更に自動的に適応するポリシーを作成する場合は、ポリシー内でのダイナミック アドレス グループの使用を参照して、*Panorama* でサポートされる登録された *IP* アドレスの数を確認してください。

- 共有オブジェクトを作成します。

  この例では、アラートを発生させたい URL フィルタリング カテゴリの共有オブジェクトを追加します。

  1. **[Objects]** > **[セキュリティ プロファイル]** > **[URL フィルタリング]** タブの順に移動し、**[追加]** をクリックします。

     Objects (オブジェクト) タブは デバイス グループの追加(少なくとも 1 回) を行った後でしか表示されません。
  2. **Name**（名前）と **Description**（内容）を入力します。
  3. **Shared**（共有）を選択します。
  4. **Disable Override**（オーバーライドを無効化）オプションはデフォルトでオフになっているため、すべてのデバイス グループで継承されたオブジェクトのインスタンスをオーバーライドすることができます。オブジェクトのオーバーライドを無効にするには、チェック ボックスをオンにします。
  5. **Categories**（カテゴリ）タブで、通知を受けたいすべてのカテゴリを選択します。
  6. **Action**（アクション）列で **Alert**（アラート）を選択します。
  7. **OK** をクリックして、オブジェクトに対する変更を保存します。
  8. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

- デバイス グループ オブジェクトを作成します。

  この例では、ネットワーク上の特定の Web サーバーについてアドレス オブジェクトを追加します。

  1. **Objects** > **Addresses** (オブジェクト > アドレス)を選択し、オブジェクトを使用する**Device Group** (デバイスグループ)を選択します。
  2. **Add**（追加）をクリックして、オブジェクトを識別する **Name**（名前）を入力します。
  3. **Shared**（共有）オプションがオフになっていることを確認してください。
  4. **Disable Override**（オーバーライドを無効化）オプションはデフォルトでオフになっているため、選択した **Device Group**（デバイス グループ）の子孫であるデバイス グループで継承されたオブジェ

© 2019 Palo Alto Networks, Inc.

クトのインスタンスをオーバーライドすることができます。オブジェクトのオーバーライドを無効にするには、**Disable Override**（オーバーライドを無効化）オプションを選択します。

5. アドレス オブジェクトの **Type**（タイプ）および関連する値を選択します。たとえば、**IP Range**（**IP** 範囲）を選択し、その Web サーバーの IP アドレスの範囲を入力します。
6. **OK** をクリックして、オブジェクトに対する変更を保存します。
7. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択してから、Panorama 設定、およびオブジェクトを追加したデバイス グループに対して、変更内容を **Commit and Push**（コミットしてプッシュ）します。

- Panorama 内の共有オブジェクトとデバイス グループ オブジェクトを表示します。

  Objects（オブジェクト）タブの Location（ロケーション）列に、オブジェクトが共有されているか、デバイス グループに固有かが表示されます。

  1. **Objects** (オブジェクト)タブでオブジェクト タイプを選択します（この例では**Objects** > **Addresses** (オブジェクト > アドレス)）。
  2. オブジェクトを追加した **Device Group**（デバイス グループ）を選択します。

     選択した *Device Group*（デバイス グループ）にあるオブジェクト、あるいは先祖デバイス グループあるいは共有領域から継承したオブジェクトのみが *Objects*（オブジェクト）タブに表示されます。
  3. デバイス グループのオブジェクトが表示されていることを確認します。Location（ロケーション）列にあるデバイス グループ名が、**Device Group**（デバイス グループ）のドロップダウンの選択項目と一致していることに注意してください。

継承したオブジェクトの値を復元

親デバイスグループから継承したデバイスグループオブジェクトの値を上書きした後、いつでも、その子オブジェクトの値を親オブジェクトの値に戻すことができます。**Objects**（オブジェクト）タブの Name（名前）列では、オーバーライドされたオブジェクトに黄色い線のある緑色のアイコン（）が付きます。

特定のオブジェクトをもとに戻すのではなく、オーバーライドされたすべてのオブジェクトに先祖の値をプッシュする場合は継承したオブジェクトの優先度を管理をご覧ください。

値をオーバーライドする手順については、次のステップを参照してください： 5

オブジェクトの継承およびオーバーライドの詳細については デバイス グループ オブジェクトをご覧ください。

STEP 1 | **Objects** (オブジェクト)タブでオブジェクト タイプ（この例では**Objects** > **Addresses** (オブジェクト > アドレス)）を選択し、オーバーライドされたオブジェクトのインスタンスを持つ**Device Group** (デバイスグループ)を選択します。

STEP 2 | オブジェクトを選択して**Revert**（元に戻す）をクリックし、さらに**Yes**（はい）をクリックします。Name（名前）列にあるオブジェクトに緑色のアイコンが付き、現在このオブジェクトが先祖デバイスグループのすべての値を継承していることが分かります。

STEP 3 | **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択してから、Panorama 設定、およびオブジェクトを復元したデバイス グループに対して、変更内容を **Commit and Push**（コミットしてプッシュ）します。

© 2019 Palo Alto Networks, Inc.

未使用の共有オブジェクトの管理

Device Groups（デバイス グループ）の設定変更をプッシュする際、共有あるいはデバイス グループのポリシー ルールがそのオブジェクトを参照しているかどうかに関わらず、Panorama はデフォルトですべての共有オブジェクトをファイアウォールにプッシュします。ただし、デバイス グループを参照するルールを持つ共有オブジェクトのみを Panorama にプッシュさせるように設定することもできます。**Share Unused Address and Service Objects with Devices**（未使用のアドレスとサービス オブジェクトをデバイスと共有）オプションにより、Panorama が管理対象のファイアウォールにプッシュするオブジェクトを制限することができます。



*Share Unused Address and Service Objects with Devices (*未使用のアドレスとサービス オブジェクトをデバイスと共有*)* が無効になっている場合、ファイアウォールのサブセットにポリシー ルールをプッシュの際に、*Panorama* は *Target (*ターゲット*)* ファイアウォールを無視します。つまり、ルールによって参照されるすべてのオブジェクトは、デバイス グループ内のすべてのファイアウォールにプッシュされます。

一連の管理対象のファイアウォールにプッシュされるオブジェクト数を制限するには、ポリシー ルールを子デバイス グループに追加し、必要に応じて共有オブジェクトを参照します。子デバイス グループの作成の詳細については、デバイス グループの階層を作成を参照してください。

PA-220 などのローエンドのモデルでは、関連する共有オブジェクトのみを管理対象のファイアウォールにプッシュすることを検討してください。これは、ローエンドのモデルに保存できるオブジェクトの数が、ミドルレンジからハイエンドのモデルに比べ、大幅に少ないためです。また、未使用のアドレスおよびサービス オブジェクトの数が多い場合、**Share Unused Address and Service Objects with Devices**（未使用のアドレスとサービス オブジェクトをデバイスと共有）をオフにすると、各ファイアウォールにプッシュされる設定が小さくなるため、ファイアウォールでのコミット時間が大幅に削減されます。ただし、このオプションを無効にすると、Panorama は、ポリシー ルールが特定のオブジェクトを参照するかどうかを動的に確認する必要があるため、コミット時間が増加する場合があります。

STEP 1 | **[Panorama]** > [セットアップ] > [管理] の順に選択し、[Panorama 設定] を編集します。

STEP 2 | **Share Unused Address and Service Objects with Devices**（未使用のアドレスとサービス オブジェクトをデバイスと共有）オプションをオフにして、そのルールが参照している共有オブジェクトのみをプッシュするか、このオプションをオンにして、すべての共有オブジェクトのプッシュを再び有効にします。

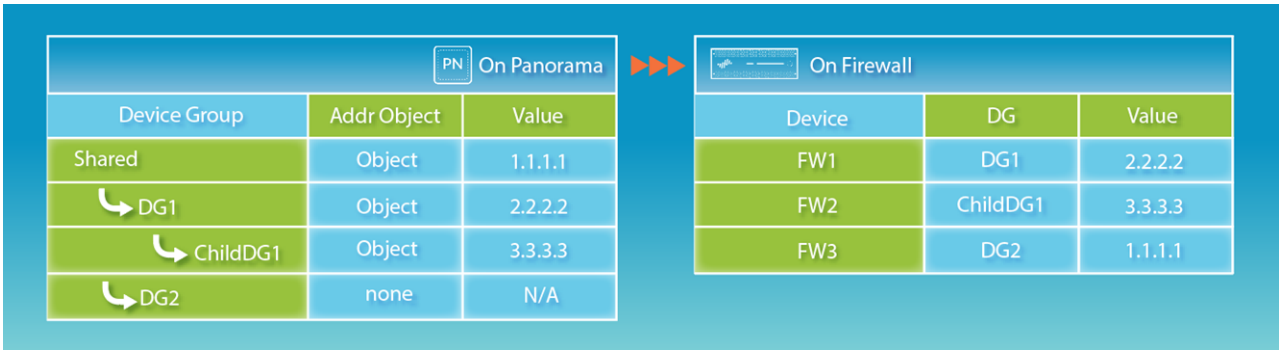
STEP 3 | **OK** をクリックして変更内容を保存します。

STEP 4 | **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

継承したオブジェクトの優先度を管理

デフォルト設定では、デバイス グループ階層内の異なる階層にあるデバイス グループが同じ名前のオブジェクトを持っていながら値が異なっている (例えばオーバーライドにより)場合、子孫デバイス グループのポリシー ルールは先祖デバイス グループから継承したオブジェクトの値ではなく、その子孫オブジェクトの値を使用します。また、任意でこの優先度を逆にして、オブジェクトを含有するトップレベルの先祖の値をすべての子孫デバイスグループにプッシュすることもできます。このオプションを有効にすると、次回設定変更をデバイス グループにプッシュしたときに、子孫デバイス グループのオーバーライドされるオブジェクトの値が、継承したオブジェクトの値によって置き換えられます。下の図は、デバイス グループ内の継承したオブジェクトの優先順位を示しています。

© 2019 Palo Alto Networks, Inc.



*Panorama*がプッシュする共有オブジェクトまたはデバイス グループ オブジェクトと同じ名前のオブジェクトがデバイスのローカルにあると、コミットは失敗します。

先祖の値をすべてのオーバーライドされたオブジェクトにプッシュするのではなく、オーバーライドされた特定のオブジェクトを元に戻す場合は継承したオブジェクトの値を復元をご覧ください。

STEP 1 | **[Panorama]** > [セットアップ] > [管理] の順に選択し、[Panorama 設定] を編集します。

STEP 2 | デフォルトの優先度を逆順にしたい場合は、**Objects defined in ancestors will take higher precedence**（上位で定義されたオブジェクトを優先）をオンにします。そうするとダイアログに**Find Overridden Objects**（オーバーライドされたオブジェクトを探す）リンクが表示され、この変更をコミットした後で先祖の値を持つオーバーライドされた（シャドーイング）オブジェクトの数を確認することもできます。数値のテキストにカーソルを合わせるとオブジェクト名が表示されます。

デフォルトの優先度に戻したい場合は、**Objects defined in ancestors will take higher precedence**（上位で定義されたオブジェクトを優先）をオフにします。

*Find Overridden Objects (*オーバーライドされたオブジェクトを探す*)* は、デバイス グループ内の別のオブジェクトと名前を共有する共有デバイス グループオブジェクトのみを検出します。

STEP 3 | **OK** をクリックして変更内容を保存します。

STEP 4 | **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

STEP 5 | （任意）**Objects defined in ancestors will take higher precedence**（上位で定義されたオブジェクトを優先）を選択した場合、Panorama は、設定変更がデバイス グループにプッシュされるまで、上位オブジェクトをプッシュしません。**Commit**（コミット）> **Push to Devices**（デバイスへのプッシュ）を選択して、変更内容を **Push**（プッシュ）してください。

ポリシー ルールあるいはオブジェクトを別のデバイス グループに移動/コピー

Panoramaでは、デバイスグループから移動あるいはコピーするポリシールールやオブジェクトが、変更先のデバイスグループ（**Destination**（宛先））では利用できないオブジェクトを参照している場合、参照されているオブジェクトおよび参照ルールあるいは同様の働きを持つオブジェクトを移動またはコピーする必要があります。デバイス グループ階層では、参照されているオブジェクトが継承関係を通して利用

© 2019 Palo Alto Networks, Inc.

できる場合があることに注意してください。例えば、共有オブジェクトはすべてのデバイスグループで利用できます。グローバル検索を実行して参照を確認できます。オーバーライドされたオブジェクトを移動あるいはコピーする場合、**Destination**（宛先）の親デバイスグループでそのオブジェクトに対するオーバーライドを必ず有効にするようにしてください（共有またはデバイス グループ ポリシーで使用するオブジェクトの作成を参照）。

複数のポリシー ルールをコピーするとき、ルールを選択する順序により、ルールがデバイス グループにコピーされる順序が決まります。たとえば、ルール *1* ～ *4* があり、選択順序が、*2*、*1*、*4*、*3* である場合、このルールがコピーされるデバイス グループでは、この選択順序でルールが表示されます。ただし、正常にコピーされた後で、ルールの順序を適切に変更できます。

STEP 1 | Panoramaにログインし、ルールベース（例：**Policy** > **Security** > **Pre Rules** (ポリシー > セキュリティ > プレルール)）あるいはオブジェクト タイプ（例：**Objects** > **Addresses** (オブジェクト > アドレス)）を選択します。

STEP 2 | **Device Group**（デバイスグループ）を選択し、1 つ以上のルールまたはオブジェクトを選択します。

STEP 3 | 以下のいずれかの手順を実行します。

- （ルールのみ）**Move**（移動）> **Move to other device group**（他のデバイス グループに移動）
- （オブジェクトのみ）**Move**（移動）
- （ルールまたはオブジェクト）**Clone**（コピー）

STEP 4 | **Destination**（宛先）ドロップダウン リストで、新しいデバイスグループまたは **Shared**（共有）を選択します。デフォルトは以前に選択された **Device Group**（デバイス グループ）です。

STEP 5 | （ルールのみ）**Rule order**（ルール順序）を選択します。

- **Move top**（最上部へ）— （デフォルト）他のすべてのルールの前の位置を選択します。
- **Move bottom**（最下部へ）— 他のすべてのルールの後の位置を選択します。
- **Before rule**（事前ルール）— 隣接するドロップダウン リストで、選択されたルールの直後のルールを選択します。
- **After rule**（事後ルール）— 隣接するドロップダウン リストで、選択されたルールの直前のルールを選択します。

STEP 6 | **Error out on first detected error in validation**（検証で最初に検出されたエラーを報告）のチェックボックスはデフォルトでオンになっているため、Panoramaは最初に発見したエラーを表示し、他のエラーのチェックを停止します。たとえば、移動するルールで参照されているオブジェクトが **Destination**（宛先）デバイスグループに存在しないと、エラーが発生します。同時に大量の項目を移動またはコピーするときにこのチェック ボックスをオンにしていると、単純にトラブルシューティングを行えます。このチェックボックスをオフにすると、Panoramaはすべてのエラーを検出してから表示します。この設定に関わらず、選択されたすべての項目についてエラーが解決されるまでの間、Panoramaは移動あるいはコピーを行いません。

STEP 7 | **OK** をクリックしてエラーの検証を開始します。Panoramaがエラーを発見した場合は、エラーを修正してから移動またはコピー操作を再試行します。Panoramaがエラーを発見しなかった場合、操作を実行します。

© 2019 Palo Alto Networks, Inc.

STEP 8 | **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択し、プッシュ スコープで **Edit Selections**（選択内容の編集）を行い、**Device Groups**（デバイス グループ）を選択し、プッシュ元のデバイス グループとプッシュ先のデバイス グループを選択し、**OK** をクリックしてから、Panorama 設定とデバイス グループに変更を **Commit and Push**（コミットしてプッシュ）します。

Panorama で URL フィルタリング ベンダーを選択

URL フィルタリングにより、ファイアウォールがユーザーの Web アクセスを監視・制御できるようになります。Web アクセスを制御するために設定したポリシールール（セキュリティ、QoS、キャプティブ ポータル、復号化ルール）は、URLカテゴリを参照します。Panorama で選択するURL フィルタリング ベンダーにより、デバイス グループに追加してファイアウォールにプッシュするルール内での参照に使用できる URL カテゴリが決まります。

デフォルト設定では、PanoramaはPAN-OS および Palo Alto Networks 脅威インテリジェンス クラウドと緊密に統合されているURL フィルタリング データベースである、PAN-DBを使用します。PAN-DBにより高パフォーマンスのローカル キャッシュが可能になるため、URLルックアップを行う際にインラインのパフォーマンスを最大限に引き出すことができます。もう一つのベンダーオプションは、サードパーティ製のデータベースである、BrightCloudです。

ファイアウォールと異なり、*Panorama*は*URL*データベースをダウンロードせず、*URL* フィルタリング ライセンスを必要としません。

以下のトピックでは、Panorama、あるいはPanoramaと管理対象ファイアウォールの両方でURLフィルタリング ベンダーを変更する方法を説明します。また、ファイアウォール上だけでURLフィルタリング ベンダーを変更することもできます。

- Panorama およびファイアウォールの URL フィルタリング ベンダーはマッチする必要があるかどうか
- HA Panorama で URL フィルタリング ベンダーを変更
- 非 HA Panorama で URL フィルタリング ベンダーを変更
- Panorama および HA ファイアウォールを BrightCloud から PAN-DB に移行
- Panorama および非 HA ファイアウォールを BrightCloud から PAN-DB に移行

Panorama およびファイアウォールの *URL* フィルタリング ベンダーはマッチする必要があるかどうか

1 つのPanorama管理サーバーあるいはファイアウォールでアクティブにできる URL フィルタリング ベンダーは 1 つのみです。PAN-DBあるいはBrightCloud。Panorama 用のベンダーを選択する場合は、管理対象ファイアウォールのベンダーと PAN-OS バージョンを考慮する必要があります。

- PAN-OS 5.0.x 以前のバージョン — Panorama およびファイアウォールで、URL フィルタリング ベンダーが一致している必要があります。
- PAN-OS 6.0 以降のバージョン — Panorama およびファイアウォールで、URL フィルタリング ベンダーが一致している必要はありません。ベンダーの不一致が検出されるとファイアウォールは、ファイアウォールで有効にされているベンダーのカテゴリと一致するURLカテゴリに、Panorama から受信した URL フィルタリングのプロファイルおよびルールに含まれる URL カテゴリをマッピングします。

したがって、一部のファイアウォールで PAN-OS 6.0以降が実行され、別の一部のファイアウォールで以前のバージョンの PAN-OS が実行されているデプロイ環境の場合、Panorama では、以前のバージョンの PAN-OS が実行されているファイアウォールと同じ URL フィルタリング ベンダーを使用する必要があります。たとえば、PAN-OS 5.0 が実行されているファイアウォールでPAN-DBを使用し、PAN-OS 7.0 が実行されているファイアウォールでBrightCloudを使用する場合、Panorama では、PAN-DB を使用する必要があります。

© 2019 Palo Alto Networks, Inc.

HA Panorama で URL フィルタリング ベンダーを変更

URL フィルタリング ベンダーを変更する際、高可用性 (HA) デプロイメント環境の場合は各 Panorama ピアが機能していない状態でなければなりません。そのため、Panorama 操作が中断されることがないよう、パッシブ Panorama (この例では Panorama2) 上で URL フィルタリング ベンダーを変更し、次にフェイルオーバーをトリガーしてから、アクティブ Panorama (この例では Panorama1) 上でベンダーを変更します。

STEP 1 | 各 Panorama HA ピアで URL フィルタリング ベンダーを変更します。

Panorama1 (アクティブ ピア) の前に *Panorama2* (パッシブ ピア) 上でこのタスクを実行します。

1. Panorama Web インターフェイスにログインします。
2. **Panorama** > **High Availability** (Panorama > 高可用性) の順に選択し、**Suspend local Panorama**(ローカルPanoramaをサスペンド)します。

   Panorama1 に対してこのステップを実行すると、フェイルオーバーが発生して Panorama2 がアクティブになります。
3. **[Panorama]** > **[セットアップ]** > **[管理]** の順に選択し、[一般設定] を編集します。
4. **[URL フィルタリング データベース]** ドロップダウンでベンダー (**[brightcloud]** または **[paloaltonetworks]** (PAN-DB)) を選択します。
5. **Panorama** > **High Availability** (Panorama > 高可用性) の順に選択し、**Make local Panorama functional**(ローカル Panorama を稼働状態に切り替え)ます。

   両方の HA ピアでプリエンプションが有効になっている状態で Panorama1 に対してこのステップを実行すると、自動的に Panorama1 がアクティブ状態に、Panorama2 がパッシブ状態に戻ります。

STEP 2 | URL カテゴリがポリシーで参照できることを確認します。

1. **Objects (オブジェクト)** > **Security Profiles (セキュリティ プロファイル)** > **URL Filtering (URL フィルタリング)** の順に選択します。
2. **Add** (追加) をクリックし、選択したベンダーに関連する URL カテゴリが URL Filtering (URL フィルタリング) プロファイル ダイアログの **Categories** (カテゴリ) タブに表示されることを確認します。

非 HA Panorama で URL フィルタリング ベンダーを変更

高可用性 (HA) 設定でデプロイされていない Panorama 管理サーバー上でこの作業を行い、URL フィルタリング ベンダーを変更します。

STEP 1 | URL フィルタリング ベンダーを変更します。

1. **[Panorama]** > **[セットアップ]** > **[管理]** の順に選択し、[一般設定] を編集します。
2. **[URL フィルタリング データベース]** ドロップダウンでベンダー (**[brightcloud]** または **[paloaltonetworks]** (PAN-DB)) を選択します。

STEP 2 | URL カテゴリがポリシーで参照できることを確認します。

1. **Objects (オブジェクト)** > **Security Profiles (セキュリティ プロファイル)** > **URL Filtering (URL フィルタリング)** の順に選択します。
2. **Add** (追加) をクリックし、選択したベンダーに関連する URL カテゴリが URL Filtering (URL フィルタリング) プロファイル ダイアログの **Categories** (カテゴリ) タブに表示されることを確認します。

© 2019 Palo Alto Networks, Inc.

Panorama および *HA* ファイアウォールを *BrightCloud* から *PAN-DB* に移行

ファイアウォールが高可用性（HA）設定でデプロイされている場合に、Panorama およびファイアウォール上で URL フィルタリング ベンダーを BrightCloud から PAN-DB に移行する際は、この作業を行います。この例では、アクティブ（あるいはアクティブ-プライマリ）ファイアウォールの名前は fw1、パッシブ（あるいはアクティブ-セカンダリ）ファイアウォールの名前は fw2 です。この移行により、自動的に BrightCloud URL カテゴリが PAN-DB URL カテゴリにマッピングされます。

STEP 1 | どのファイアウォールに新しい PAN-DB URL フィルタリング ライセンスが必要か判断します。

1. Panoramaにログインして、**Panorama** > **Device Deployment** > **Licenses** (Panorama > デバイスのデプロイ > ライセンス) を選択します。
2. URL 列を確認し、どのファイアウォールが PAN-DB ライセンスを持っており、有効/期限切れになっているライセンスを確認します。

   ファイアウォールには、BrightCloud と PAN-DB 両方の有効なライセンスを取り込むことができますが、アクティブにすることができるライセンスは 1 つのみです。

   PAN-DB URL フィルタリング ライセンスがアクティブかどうか定かでない場合は、*Device* > *Licenses* (デバイス > ライセンス)を選択し、*PAN-DB URL Filtering* (*PAN-DB URL*フィルタリング)セクションの*Active* (アクティブ)フィールドに*Yes* (はい)と表示されているかどうかを確認します。
3. 有効な PAN-DB ライセンスを持っていない各ファイアウォールについて、新しいライセンスを購入してください。

   HA デプロイメントでは、各ファイアウォール ピアに個別の PAN-DB ライセンスおよび認証コードが必要になります。ライセンスを購入すると、アクティベーションコードが記載されたメールが Palo Alto Networks から送られてきます。このメールが届かない場合は、作業を進める前にお手数ですがカスタマー サポートにお問い合わせください。

STEP 2 | Panorama で URL フィルタリング ベンダーを PAN-DB に変更します。

Panorama Web インターフェイスにアクセスして、以下のいずれかの作業を行います。

- HA Panorama で URL フィルタリング ベンダーを変更
- 非 HA Panorama で URL フィルタリング ベンダーを変更

STEP 3 | 両方のファイアウォール HA ピア上で TCP セッション設定を行い、ピアを保留する際にまだ同期されていないセッションに対して必ずフェイルオーバーが行われるようにします。

各ファイアウォールの CLIにログインし、次のコマンドを実行します。

```
> set session tcp-reject-non-syn no
```

STEP 4 | 各ファイアウォール HA ピアで URL フィルタリング ベンダーを PAN-DB に移行します。

Fw1（アクティブあるいはアクティブ-プライマリ ピア）の前に *Fw2*（パッシブあるいはアクティブ-セカンダリ ピア）上でこの作業を行います。

1. ファイアウォールのWebインターフェイスにアクセスし、**Device** > **High Availability** > **Operational Commands** (デバイス > 高可用性 > 操作コマンド)を選択し、**Suspend local device** (ローカルデバイスをサスペンド)します。

   fw1 上でこのステップを行うと、fw2 のフェイルオーバーが実行されます。

© 2019 Palo Alto Networks, Inc.

2. **Device** > **Licenses** (デバイス > ライセンス)を選択します。
3. License Management（ライセンス管理）セクションで **Activate feature using authorization code**（認証コードを使用して機能をアクティベート）を選択し、**Authorization Code**（認証コード）を入力して **OK** をクリックします。

   PAN-DB ライセンスを有効にすると、自動的に BrightCloud ライセンスが無効になります。
4. PAN-DB URL Filtering（PAN-DB URLフィルタリング）セクションでシード ファイルを **Download**（ダウンロード）し、リージョンを選択して **OK** をクリックします。
5. 設定変更をコミットしてプッシュします。
   1. Panorama Web インターフェイスにアクセスします。
   2. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択し、Push Scope（プッシュ スコープ）で **Edit Selections**（選択内容の編集）を行います。
   3. **Device Groups**（デバイス グループ）を選択し、ファイアウォールを選択して **OK** をクリックします。
   4. Panorama 設定とデバイス グループに対して、変更内容を **Commit and Push**（コミットしてプッシュ）します。
6. ファイアウォールのWebインターフェイスにアクセスし、**Device** > **High Availability** > **Operational Commands** (デバイス > 高可用性 > 操作コマンド)を選択し、**Make local device functional** (ローカルデバイスの機能を有効化)します。

   両方のファイアウォールでプリエンプションが有効になっている状態で fw1 に対してこのステップを実行すると、fw1 が自動的にアクティブ（あるいはアクティブ-プライマリ）状態に、fw2 がパッシブ（あるいはアクティブ-セカンダリ）状態に戻ります。

STEP 5 | 両方のファイアウォール HA ピアを元の TCP セッション設定に戻します。

各ファイアウォールの CLI で次のコマンドを実行します。

```
> set session tcp-reject-non-syn yes
```

Panorama および非 HA ファイアウォールを BrightCloud から PAN-DB に移行

ファイアウォールが高可用性（HA）構成でデプロイされていない場合に、Panoramaおよびファイアウォール上でURLフィルタリング ベンダーをBrightCloudからPAN-DBに移行する際は、この作業を行います。この移行により、自動的に BrightCloud URL カテゴリが PAN-DB URL カテゴリにマッピングされます。

STEP 1 | どのファイアウォールに新しい PAN-DB URL フィルタリング ライセンスが必要か判断します。

1. Panoramaにログインして、**Panorama** > **Device Deployment** > **Licenses** (Panorama > デバイスのデプロイ > ライセンス) を選択します。
2. URL 列を確認し、どのファイアウォールが PAN-DB ライセンスを持っており、有効/期限切れになっているライセンスを確認します。

   ファイアウォールには、BrightCloud と PAN-DB 両方の有効なライセンスを取り込むことができますが、アクティブにすることができるライセンスは 1 つのみです。

   PAN-DB URL フィルタリング ライセンスがアクティブかどうか定かでない場合は、*Device* > *Licenses* (デバイス > ライセンス)を選択し、*PAN-DB URL Filtering* (*PAN-DB URL*フィルタリング)セクションの*Active* (アクティブ)フィールドに*Yes* (はい)と表示されているかどうかを確認します。

© 2019 Palo Alto Networks, Inc.

3. ファイアウォールが有効なPAN-DBライセンスを持っていない場合は新しいライセンスを購入してください。

   ライセンスを購入すると、アクティベーションコードが記載されたメールが Palo Alto Networks から送られてきます。このメールが届かない場合は、作業を進める前にお手数ですがカスタマー サポートにお問い合わせください。

STEP 2 | Panorama で URL フィルタリング ベンダーを PAN-DB に変更します。

Panorama Web インターフェイスにアクセスして、以下のいずれかの作業を行います。

- HA Panorama で URL フィルタリング ベンダーを変更
- 非 HA Panorama で URL フィルタリング ベンダーを変更

STEP 3 | 各ファイアウォールでURLフィルタリング ベンダーをPAN-DBに移行します。

1. ファイアウォールの Web インターフェイスにアクセスし、**Device**（デバイス）> **Licenses**（ライセンス）の順に選択します。
2. License Management（ライセンス管理）セクションで **Activate feature using authorization code**（認証コードを使用して機能をアクティベート）を選択し、**Authorization Code**（認証コード）を入力して **OK** をクリックします。

   PAN-DB ライセンスを有効にすると、自動的に BrightCloud ライセンスが無効になります。
3. PAN-DB URL Filtering（PAN-DB URLフィルタリング）セクションでシード ファイルを **Download**（ダウンロード）し、リージョンを選択して **OK** をクリックします。
4. 設定変更をコミットしてプッシュします。
   1. Panorama Web インターフェイスにアクセスします。
   2. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択し、Push Scope（プッシュ スコープ）で **Edit Selections**（選択内容の編集）を行います。
   3. **Device Groups**（デバイス グループ）を選択し、ファイアウォールを選択して **OK** をクリックします。
   4. Panorama 設定とデバイス グループに対して、変更内容を **Commit and Push**（コミットしてプッシュ）します。

ファイアウォールのサブセットにポリシー ルールをプッシュ

ポリシー ターゲットを使用すると、ポリシーのプッシュ先になるデバイス グループ内のファイアウォールを指定できます。1 台以上のファイアウォールや仮想システムを除外したり、デバイス グループ内の特定のファイアウォールまたは仮想システムに対してのみルールを適用することができます。

ルールベースが増える中、新しいルールまたは変更されたルールをファイアウォールにプッシュすると、ルールの作成時または変更時にアーカイブしない限り、変更および監査情報は時間の経過とともに失われます。監査コメントアーカイブを使用して、選択したルールの監査コメントと構成ログ履歴を表示し、2 つのポリシー ルールバージョンを比較してルールがどのように変更されたかを確認します。Panorama からプッシュされたルールの監査コメント履歴は、Panorama 管理サーバーからのみ表示することができます。その場合も、監査コメントは管理対象のファイアウォールから Panorama に転送された構成ログで表示することができます。ただし、監査コメントアーカイブは、ファイアウォールでローカルに作成または変更されたルールについては表示することはできません。ルールの作成時または変更時に監査コメントが確実にキャプチャされるようにするには、ポリシー ルール、説明、タグ、および監査コメントを適用します。

ルールをターゲットに設定すると、ポリシーを Panorama で集中管理できます。ターゲット ルールでは、Panorama のルール (共有またはデバイス グループのプレ ルールまたはポスト ルール) を定義することができるため、ルールを管理する際の可視性と効率を向上させることができます (詳細はデバイス グループポリシーを参照)。監査コメントアーカイブを使用するとポリシー ルールがなぜ変更されたのかを

© 2019 Palo Alto Networks, Inc.

時系列で追跡できるため、ルールのライフサイクルを通じてルールの拡張過程を監査することができます。

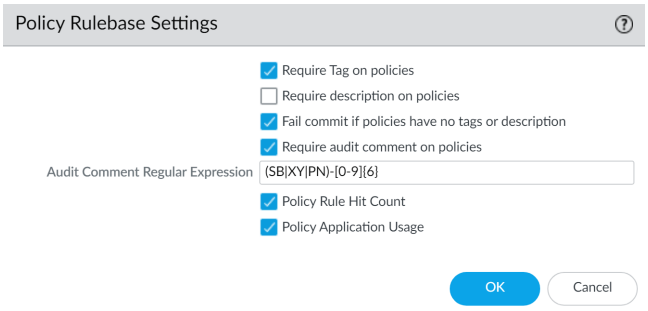
STEP 1 | (ベストプラクティス) ポリシー ルールの監査コメントを適用します。

この手順は任意ですが、ポリシー ルールの監査コメントを適用して、ルールを作成または変更する理由を確実に把握することをお勧めします。これは、監査のために正確なルール履歴を維持するのにも役立ちます。

1. **Panorama** > **Setup** (セットアップ) > **Management** (管理) の順に選択し、ポリシー ルールベース設定を編集します。
2. **Require audit comment on policies** (ポリシーの監査コメントを要求する) オプションを有効にします。
3. 監査コメント正規表現を設定し、監査コメントの書式を指定します。

   ルールを作成または変更する場合、文字と数字の表現を指定して、業務および監査のニーズに基づいて特定の形式に従うように監査コメントを要求します。例えば、この設定を使用して発券番号の形式に一致する正規表現を指定できます。

   - `[0-9] {<桁数>}` —監査コメントに 0 ~ 9 からなる最少桁数を含めるよう指定します。例えば、`[0-9]{6}` の場合、0〜9 の数字からなる最小 6 桁の数式を含める必要があります。必要に応じて、最小桁数を設定します。
   - <文字表現>—文字表現が含まれる監査コメントを求めます。例えば、変更理由と設定すると、管理者は監査コメントを記入する際にこの文字表現を冒頭に記載する必要があります。
   - <文字表現>-`[0-9]{<桁数>}`—規定の文字からなるプレフィックスを 0〜9 からなる最小桁数で監査コメントに含めるよう指定します。例えば、`SB-[0-9]{6}`と設定すると、`SB-`で始まり、`SB-012345` など、最小 6 桁の 0 から 9 からなる数式が続く監査コメント形式が求められます。
   - `(`<文字表現>`)|(`<文字表現>`)|(`<文字表現>`)|-[0-9]{`<桁数>`}`—設定された一連の文字表現のいずれかを使用したプレフィックス、および 0〜9 からなる最小桁数の数字を監査コメントに含めるよう指定します。例えば、`(SB|XY|PN)-[0-9]{6}` と設定すると、`SB-`、`XY-` または `PN-` で始まり、`SB-012345`、`XY-654321` または `PN-012543` などの 0〜9 の数字で構成された最小 6 桁の数式が続く監査コメント形式が求められます。
4. **OK** をクリックして新しいポリシー ルールベースの設定を適用します。



5. **Commit** (コミット) および **Commit to Panorama** (Panorama へのコミット) をクリックします。

STEP 2 | ルールを作成します。

この例では、セキュリティ ルールベースで、内部ネットワークのユーザーに DMZ のサーバーへのアクセスを許可するプレ ルールを定義します。

1. **Policies** (ポリシー) タブで、ルールを定義する **Device Group** (デバイス グループ) を選択します。
2. ルールベースを選択します。この例では、**Policies** (ポリシー) > **Security** (セキュリティ) > **Pre-Rules** (プレ ルール) を選択し、ルールを **Add** (追加) します。
3. **General** (全般) タブで分かりやすいルールの **Name** (名前) と **Audit Comment** (監査コメント) を入力します。
4. **Source** (送信元) タブで**Source Zone** (送信元ゾーン) を **Trust** に設定します。

© 2019 Palo Alto Networks, Inc.

5. **Destination**（宛先）タブで **Destination Zone**（宛先ゾーン）を**DMZ**に設定します。
6. **Service/ URL Category**（サービス/URL カテゴリ）タブで、**Service**（サービス）を **application-default** に設定します。
7. **Actions**（アクション）タブで、**Action**（アクション）を **Allow**（許可）に設定します。
8. それ以外のオプションは、すべてデフォルト値にしておきます。

STEP 3 | ルールのターゲットを指定して、ファイアウォールのサブセットを含めるか、除外します。

選択したファイアウォールのセットにルールを適用するには、以下の手順を実行します。

1. ポリシー ルールダイアログで、**Target (ターゲット)** タブを選択します。
2. ルールを適用するファイアウォールを選択します。

   ターゲットとなるファイアウォールを選択しない場合、ルールはデバイス グループの（オフになっている）すべてのファイアウォールに追加されます。

   デフォルトでは、デバイス グループ内の仮想システムのチェックボックスは無効になっていますが、ルールを適用する *1* つ以上の仮想システムを選択しない限り、すべての仮想システムはコミット時にルールを継承します。
3. (任意) ファイアウォールのサブセットをルールの継承から除外するには、**Install on all but specified devices (指定したデバイスを除くすべてにインストール)** し、除外するファイアウォールを選択します。

   Install on all but specified devices (指定したデバイスを除くすべてにインストール) する場合、ルールはデバイス グループのどのファイアウォールにも追加されません。
4. **OK** をクリックしてルールを追加します。

STEP 4 | 設定変更をコミットしてプッシュします。

1. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択し、Push Scope（プッシュ スコープ）で **Edit Selections**（選択内容の編集）を行います。
2. **Device Groups**（デバイス グループ）を選択し、ルールを追加したデバイス グループを選択して **OK** をクリックします。
3. Panorama 設定とデバイス グループに対して、変更内容を **Commit and Push**（コミットしてプッシュ）します。

STEP 5 | ポリシー ルールのトラフィックマッチのトラブルシューティングポリシー ルールのトラフィックマッチのトラブルシューティングを行い、ルールが意図したとおりにトラフィックを許可および拒否することを確認します。

ルール階層の管理

ネットワークのセキュリティを維持する上で、ポリシールールの順序は極めて重要です。あらゆるポリシー層（共有、デバイスグループ、あるいはローカルで定義されたルール）およびルールベース（例えば共有セキュリティ プレルール）について、ファイアウォールは **Policies**（ポリシー）タブに表示される順序でルールを上から順に評価します。ファイアウォールは、定義済みの基準を満たす最初のルールに対してパケットを照合し、それ以降のルールは無視します。そのため、より具体的なルールを一般的なルールよりも上位に移動させ、最も具体的に一致するルールが適用されるようにします。



デバイスグループの階層全体にかけてファイアウォールがルールをレイヤーごと、タイプごと（プレルール、ポストルール、デフォルトルール）に評価する順序の詳細はデバイスグループ ポリシーをご覧ください。

STEP 1 | 各ルールベースのルール階層を表示します。

1. **Policies**（ポリシー）タブを選択し、**Preview Rules**（ルールのプレビュー）をクリックします。

© 2019 Palo Alto Networks, Inc.

2. プレビューを **Rulebase**（ルールベース）（例：**Security**（セキュリティ）あるいは**QoS**）でフィルタリングします。
3. プレビューをフィルタリングし、特定の **Device Group**（デバイスグループ）のルール、および共有領域や先祖デバイスグループから継承されたルールを表示します。ファイアウォールが割り当てられたデバイスグループを選択する必要があります。
4. プレビューを **Device**（デバイス）でフィルタリングし、ローカルで定義されたルールを表示します。
5. 緑色の矢印アイコンをクリックし、選択したフィルターをプレビューに適用します（デバイス グループ ポリシーを参照）。
6. ルールのプレビューが終わったら Combined Rules Preview（結合ルール プレビュー）のダイアログを閉じます。

STEP 2 | 必要に応じてルールを削除あるいは無効化します。



現在ファイアウォールが使用していないルールを確認するには、*Panorama*の*Context (*コンテキスト*)*ドロップダウンリストでそのファイアウォールを選択し、ルールベース（例えば*Policies* > *Security (*ポリシー > セキュリティ*)*）を選択して*Highlight Unused Rules (*未使用のルールをハイライト表示*)*のチェックボックスをオンにします。背景がオレンジ色で網掛けされている場合、そのルールはファイアウォールで使用されていないことを示します。

1. 削除あるいは無効にするルールを含むルールベース（例えば**Policies** > **Security** > **Pre Rules** (ポリシー > セキュリティ > プレルール)）を選択します。
2. そのルールを含む **Device Group**（デバイスグループ）を選択します。
3. ルールを選択して **Delete**（削除）あるいは **Disable**（無効化）を適宜クリックします。無効にされたルールは斜体文字で表示されます。

STEP 3 | 必要に応じてルールベース内でルールの位置を再度調整します。



ファイアウォールのローカル ルールを再配置するには、このステップを実行する前に *Context*（コンテキスト）ドロップダウンリストでそのファイアウォールを選択し、*Web*インターフェイスにアクセスします。

1. 移動するルールを含むルールベース（例えば**Policies** > **Security** > **Pre Rules** (ポリシー > セキュリティ > プレルール)）を選択します。
2. そのルールを含む **Device Group**（デバイスグループ）を選択します。
3. ルール、次に **Move**（移動）を選択し、さらに次のいずれかを選択します。
   - **Move Top**（最上部に移動）—デバイスグループの他のすべてのルールより上にルールを移動させます（ただし、共有あるいは先祖デバイスグループから継承されたルールよりも下になります）。
   - **Move Top**（上に移動）—先行するルールの上に移動させます（ただし、共有あるいは先祖デバイスグループから継承されたルールよりも下になります）。
   - **Move Down**（下に移動）—後のルールの下に移動させます。
   - **Move Bottom**（最下部に移動）—他のすべてのルールより下にルールを移動させます。
   - **Move to other device group** (他のデバイスグループに移動)—ポリシールールあるいはオブジェクトを別のデバイスグループに移動/コピーを参照してください。

STEP 4 | ルールを変更した場合は、変更内容をコミットしてプッシュします。

1. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択し、Push Scope（プッシュ スコープ）で **Edit Selections**（選択内容の編集）を行います。
2. **Device Groups**（デバイス グループ）を選択し、変更または削除したルールを含むデバイス グループを選択して **OK** をクリックします。

© 2019 Palo Alto Networks, Inc.

3. Panorama 設定とデバイス グループに対して、変更内容を **Commit and Push**（コミットしてプッシュ）します。

© 2019 Palo Alto Networks, Inc.

テンプレートおよびテンプレート スタックの管理

テンプレートおよびテンプレート スタックを使用し、ネットワーク内でファイアウォールが動作できるようにする共通の基本設定を定義します。どのファイアウォールをどのテンプレートに追加するのかを決定する際、スタック内のテンプレートの順序を変えて共通およびファイアウォール グループに固有の設定のレイヤーを管理する際、ファイアウォールに固有の値でテンプレートの設定をオーバーライドする際の問題については、テンプレートおよびテンプレート スタックにまとめられています。

テンプレートを削除するには、まずファイアウォールのローカルでテンプレート設定の無効化/削除を行う必要があります。スーパーユーザーのロールを持った管理者だけがテンプレートを削除できます。

- テンプレートの機能および例外
- テンプレートの追加
- テンプレート スタックの設定
- テンプレートまたはテンプレートスタック変数の設定
- 既存のテンプレートスタック変数のインポートおよび上書き
- テンプレート設定のオーバーライド
- テンプレート設定の無効化/削除

テンプレートの機能および例外

テンプレートおよびテンプレート スタック を使用してさまざまな設定を定義することができますが、以下のタスクは管理対象の各ファイアウォールのローカルでしか実行できません。

- デバイスのブロックリストを設定する。
- ログをクリアする。
- 通常モード、マルチ VSS モード、FIPS-CC モードなどの動作モードを有効にする。
- ファイアウォール HA ペアの IP アドレスを設定する。
- マスター キーおよび診断を設定する。
- 設定ファイルを比較する（設定監査）。

  ファイアウォールのライセンスの管理と更新（ソフトウェアあるいはコンテンツ）を行うには、テンプレートではなく *Panorama* > *Device Management*（デバイス管理）タブのオプションを使用します。
- multi-vsys ファイアウォールの名前を変更します。

テンプレートの追加

ファイアウォールのネットワークのセットアップやデバイス設定要素を定義するために必要な **Device**（デバイス）タブと **Network**（ネットワーク）タブを Panorama™ が表示する前に、1 つ以上のテンプレートを追加しておく必要があります。Panorama では、最大 1,024 個のテンプレートがサポートされます。すべての管理対象ファイアウォールはテンプレート スタックに属している必要があります。テンプレートには管理対象デバイスの設定が含まれていますが、テンプレート スタックを使用すると、テンプレート スタックに割り当てられたすべての管理対象ファイアウォールにテンプレート設定を管理しプッシュすることができます。

© 2019 Palo Alto Networks, Inc.

テンプレートをテンプレートスタックに結合して、テンプレート間で多くの設定が重複しないようにします（テンプレートおよびテンプレート スタックおよび テンプレート スタックの設定を参照してください）。

STEP 1 | テンプレートを追加します。

1. **[Panorama]** > **[テンプレート]** の順に選択します。
2. **Add**（追加）をクリックして、テンプレートを識別する一意の **Name**（名前）を入力します。
3. （任意）テンプレートの**Description**（説明）入力します。
4. **OK** をクリックしてテンプレートを保存します。
5. 仮想システムを持たないファイアウォールに Panorama によってプッシュさせたい設定（たとえばインターフェイス）を伴う仮想システム（vsys）がテンプレートにある場合、作成したテンプレートを選択し、**Default VSYS**（デフォルト **VSYS**）ドロップダウンでその vsys を選択してから、**OK**をクリックします。
6. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択してから、Panorama 設定およびテンプレートに対して変更内容を **Commit and Push**（コミットしてプッシュ）します。

STEP 2 | テンプレートが使用できることを確認します。

最初のテンプレートを追加すると、**Device**（デバイス）タブと **Network**（ネットワーク）タブが Panorama に表示されます。これらのタブに **Template**（テンプレート）ドロップダウンが表示されます。先ほど追加したテンプレートがドロップダウンに表示されていることを確認します。

STEP 3 | テンプレート スタックを設定して、テンプレートをテンプレート スタックに追加します。

STEP 4 | テンプレートを使用し、設定変更をファイアウォールにプッシュします。

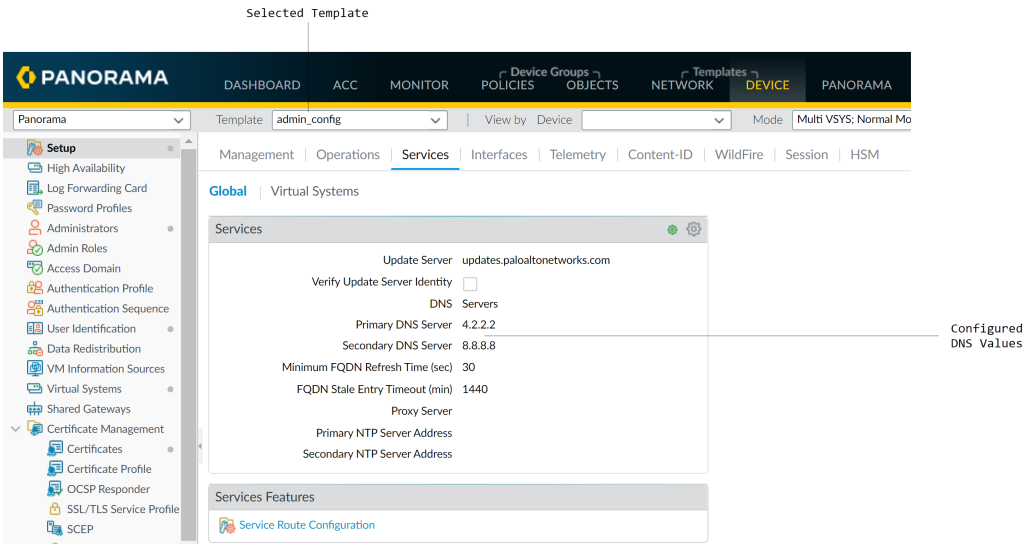
vsys の名前を変更すると、ローカルのファイアウォールでのみ許可され、*Panorama* ではなく、まったく新しい *vsys* になるか、新しい *vsys* 名がファイアウォール上の間違った *vsys* にマップされます。

テンプレートにあるファイアウォールのプライマリ DNS（Domain Name System）サーバーの定義を例に挙げます。

また、テンプレートまたはテンプレートスタック変数の設定を行うことでデバイス固有の値を管理対象のデバイスをプッシュできます。

1. **Device**（デバイス）タブで、ドロップダウンから **Template**（テンプレート）を選択します。
2. **Device** > **Setup** > **Services** > **Global**(デバイス > セットアップ > サービス > グローバル) の順に選択し、Services (サービス)セクションを編集します。
3. **Primary DNS Server**（プライマリ **DNS** サーバー）の IP アドレスを入力します。

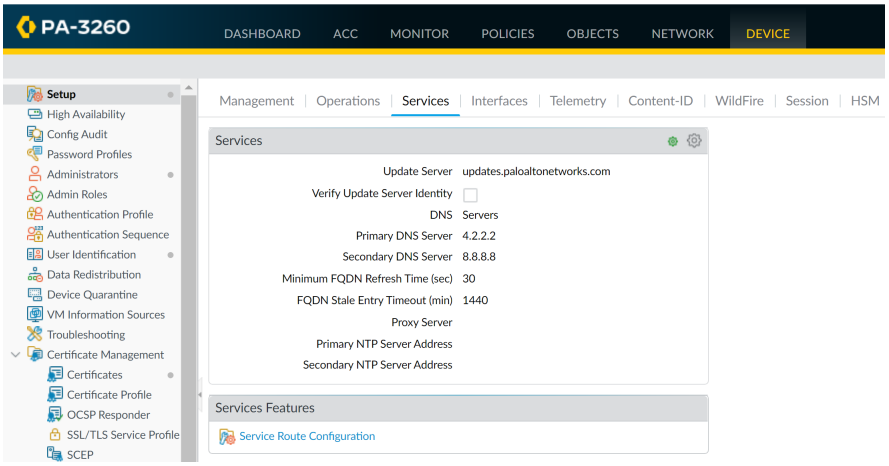
© 2019 Palo Alto Networks, Inc.



4. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択してから、Panorama 設定およびテンプレートに対して変更内容を **Commit and Push**（コミットしてプッシュ）します。

STEP 5 | ファイアウォールが、Panorama からプッシュしたテンプレート設定を使用して設定されていることを確認します。

1. テンプレート設定をプッシュしたファイアウォールのいずれかを **Context**（コンテキスト）ドロップダウンで選択します。
2. **Device**（デバイス）> **Setup**（セットアップ）> **Services**（サービス）> **Global**を選択します。テンプレートからプッシュされた IP アドレスが表示されます。Services（サービス）セクションのヘッダーにテンプレートのアイコン（）が表示され、そのセクションの設定がテンプレートからプッシュされた値になっていることが分かります。



STEP 6 | ネットワーク リソースへの接続のトラブルシューティングして、ファイアウォールがネットワーク リソースにアクセスできることを確認します。

テンプレート スタックの設定

テンプレート スタックは設定可能で、複数のテンプレートを組み合わせて、管理対象のファイアウォールにすべての設定をプッシュできます。テンプレートはファイアウォール設定のモジュール化された部分で、異なるスタック間で再利用できますが、スタックに割り当てられたすべてのファイアウォールに適用

© 2019 Palo Alto Networks, Inc.

する必要がある残りの設定を満たすようにテンプレートスタックを設定することもできます。Panorama では最大 1,024 個のテンプレート スタックがサポートされており、各スタックのテンプレートの割り当て上限数は 8 になっています。テンプレート スタックに設定されているオブジェクトは、テンレート スタックに属するテンプレートから参照できます。テンプレート スタックとスタック内のテンプレートに競合する値がある場合、テンプレート スタックで設定された値がプッシュされます。詳細と計画に関する内容は、「テンプレートおよびテンプレート スタック」を参照してください。

インターフェイス、*VLAN*、仮想ワイヤ、*IPSec* トンネル、*DNS* プロキシ、仮想システムを設定するためのテンプレートを追加します。これらのオブジェクトは、テンプレート スタックではなく、テンプレートから設定およびプッシュする必要があります。テンプレートからプッシュすると、テンプレート スタック内の仮想システムを除いて、これらのオブジェクトをオーバーライドできます。

STEP 1 | テンプレート、およびスタック内の順序を計画します。

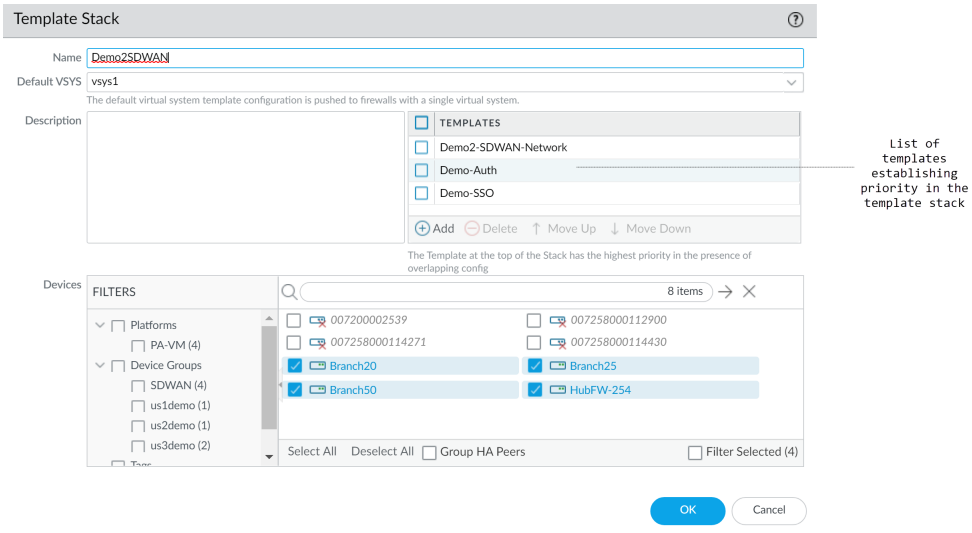
テンプレート スタックに割り当てる予定のテンプレート スタックを追加します。

スタック内のテンプレートの優先順位を計画する際（オーバーラップする設定用）、誤った設定を防ぐために順序を確認する必要があります。例えば、*Template_A* の *Ethernet1/1* インターフェイスの種類がレイヤー *3*、*Template_B* の *VLAN* ではそれがレイヤー *2* であるとします。*Template_A* の優先順位が高い場合、*Panorama* は *Ethernet1/1* を、*VLAN* に割り当てられたレイヤー *3* タイプとしてプッシュします。

また、2 つのテンプレートが同じスタック内にある場合でも、1 つのテンプレートの設定が別のテンプレートの設定を参照することができないということにも注意してください。たとえば、Template_A のゾーン構成は、Template_B のゾーン保護プロファイルを参照できません。

STEP 2 | テンプレート スタックを作成します。

1. **Panorama** > **Templates**（テンプレート）の順に選択し、**Add Stack**（スタックを追加）します。
2. スタックの識別に使用する一意の **Name**（名前）を入力します。
3. スタックに統合するテンプレート（最大 8 個）ごとに、**Add**（追加）し、テンプレートを選択します。追加したテンプレートが重複した設定の優先度順にダイアログにリストアップされます。このリストでは、高位にあるテンプレートの値が下位のものをオーバーライドします。この順番を変更するには、テンプレートを選択して **Move Up**（上へ）または **Move Down**（下へ）移動します。



4. デバイス セクションで、スタックに割り当てるファイアウォールを設定します。複数の仮想システムを持つファイアウォールでは、ファイアウォール全体を割り当てることはできても、個々の仮想

© 2019 Palo Alto Networks, Inc.

システムを割り当てることはできません。ファイアウォールはそれぞれ 1 つのテンプレートまたはテンプレート スタックに割り当てることができます。



新しい管理対象ファイアウォールを *Panorama* に追加するたびに、そのファイアウォールを適切なテンプレート スタックに割り当てる必要があります。*Panorama* によって新しいファイアウォールがテンプレートまたはテンプレート スタックに自動的に割り当てられることはありません。設定変更をテンプレートにプッシュすると、*Panorama* は、テンプレート スタックに割り当てられているすべてのファイアウォールにその設定をプッシュします。

5. （任意）**Group HA Peers**（グループ **HA** ピア）を選択し、高可用性（HA）設定の複数のファイアウォールに対して 1 つのチェック ボックスを表示します。アイコンは HA の状態を表します（緑色はアクティブ、黄色はパッシブ）。セカンダリ ピアのファイアウォール名は括弧付きで表示されます。

   アクティブ/パッシブ HA の場合は、両方のピアを同じテンプレートに追加し、両方が設定を受信するようにします。アクティブ/アクティブ HA の場合、両方のピアを同じテンプレートに追加するかどうかは、各ピアで同じ設定が必要かどうかによります。PAN-OS が HA ピア間で同期する設定の一覧については、「High Availability Synchronization（高可用性の同期）」を参照してください。
6. **OK** をクリックしてテンプレート スタックを保存します。

STEP 3 | （任意）テンプレートまたはテンプレートスタック変数を設定します。

STEP 4 | 必要に応じて **Network**（ネットワーク）および **Device**（デバイス）設定を編集します。



vsys の名前は、ローカル ファイアウォールでのみ変更できます。*Panorama* で *vsys* の名前を変更する場合、完全に新規の *vsys* になるか、新しい *vsys* 名がファイアウォール上の間違った *vsys* にマップされます。

個々のファイアウォールについては、テンプレートからプッシュされた設定をオーバーライドする時と同じ方法で、Panorama がスタックからプッシュした設定をオーバーライドできます（「テンプレートまたはテンプレート スタック値のオーバーライド」を参照）。

1. タブをフィルタリングし、変更したいモード固有の設定のみを表示します。

   Panorama がモード固有の設定をそのモードをサポートしているファイアウォールのみにプッシュする際、この選択的なプッシュによってモード固有の値が調整されることはありません。たとえば、テンプレートに連邦情報処理標準（*FIPS*）モードのファイアウォール、および非 *FIPS* アルゴリズムを使用する *IKE* 暗号化プロファイルがある場合、このテンプレートのプッシュは失敗します。このようなエラーを防ぐため、*Network*（ネットワーク）および *Device*（デバイス）タブの *Mode*（モード）ドロップダウンを使用してモード固有の機能および値のオプションをフィルタリングします。

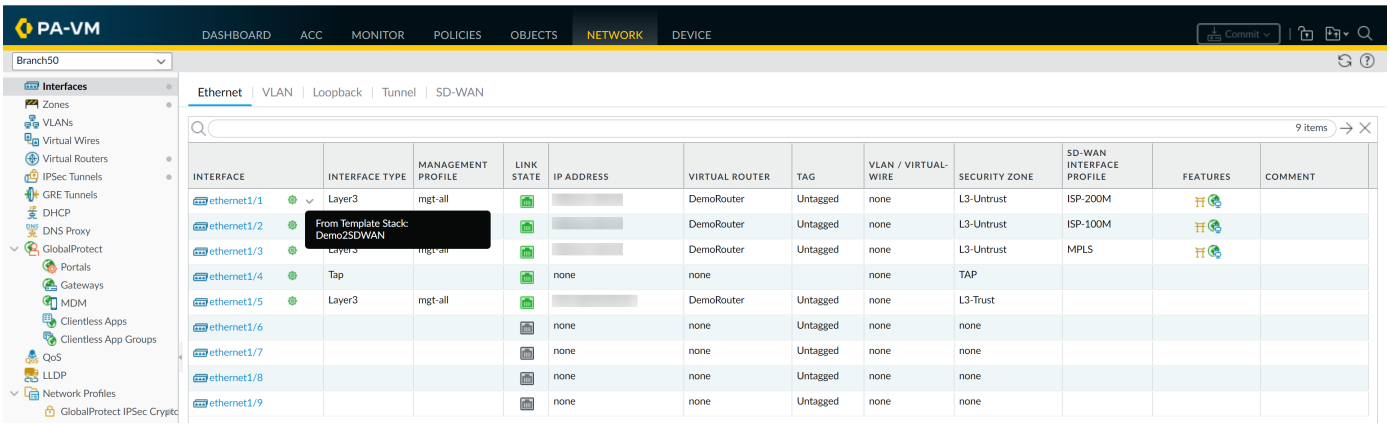
   - **Mode**（モード）ドロップダウンで **Multi VSYS**（マルチ **VSYS**）、**Operational Mode**（操作モード）、および **VPN Mode**（**VPN** モード）のフィルター オプションを選択、あるいは選択解除します。
   - 特定のファイアウォールのモード設定が反映されるように、すべての **Mode**（モード）オプションを **Device**（デバイス）ドロップダウンで選択します。
2. インターフェイスとネットワーク接続をセットアップします。たとえば、ファイアウォールを通過するトラフィックを管理および制御する目的で、ネットワークをセグメント化するようにゾーンとインターフェイスを設定します。
3. 必要に応じて設定を編集します。
4. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択し、Push Scope（プッシュ スコープ）で **Edit Selections**（選択内容の編集）を行い、**Templates**（テンプレー

© 2019 Palo Alto Networks, Inc.

ト）を選択して、テンプレート スタックに割り当てるファイアウォールを選択してから、変更を Panorama 設定とテンプレート スタックに **Commit and Push**（コミットしてプッシュ）します。

STEP 5 | テンプレート スタックが適切に動作することを検証します。

1. **Context**（コンテキスト）ドロップダウン リストから、テンプレート スタックを割り当てるデバイスを選択します。
2. テンプレート スタックを使用して設定の変更をプッシュしたタブを選択します。
3. テンプレート スタックからプッシュされた値にテンプレート アイコン（ ）が表示され、そのセクションの設定がテンプレートからプッシュされた値になっていることが分かります。スタック上にマウスを置くと、値がプッシュされたテンプレート スタックが表示されます。



STEP 6 | ネットワーク リソースへの接続のトラブルシューティングして、ファイアウォールがネットワーク リソースにアクセスできることを確認します。

テンプレートまたはテンプレートスタック変数の設定

テンプレートまたはテンプレート スタックをより簡単に再利用できるようにするには、テンプレートおよびテンプレート スタック変数を使用して、設定内の IP アドレス、グループ ID、およびインターフェイスを置き換えることができます。テンプレート変数はテンプレートまたはテンプレートスタックレベルで定義され、変数を使用して IP アドレス、IP 範囲、FQDN、IKE、VPN および HA 設定のインターフェイス、およびグループ ID を置き換えることができます。テンプレート設定はテンプレート スタック設定よりも高い優先度を持つため、テンプレートに定義されている変数はテンプレート スタックに定義されている変数よりも優先されます。変数を使用すると、管理する必要のあるテンプレートとテンプレート スタックの総数を減らすことができ、ファイアウォールやアプライアンス固有の値は保持できます。たとえば、基本設定のテンプレート スタックがある場合は、変数を使用して、テンプレートまたはテンプレート スタック内のすべてのファイアウォールに適用されない値を作成できます。これにより、新しいテンプレートやテンプレート スタックを作成する前に必要なファイアウォールやアプライアンス固有の値を考慮しながら、より少数のテンプレートやテンプレート スタックから設定を管理およびプッシュすることができます。

テンプレートまたはテンプレート スタック変数の作成方法：

STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | テンプレートとテンプレート スタックを作成します。

1. テンプレートの追加
2. テンプレート スタックの設定。

STEP 3 | **Panorama** > **Templates**（テンプレート）を選択して、変数を作成するテンプレートまたはテンプレート スタックを **Manage**（管理）します（変数列）。

© 2019 Palo Alto Networks, Inc.

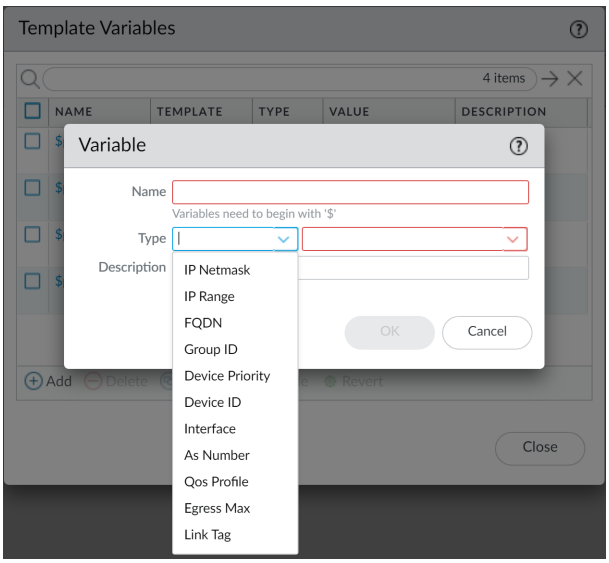
STEP 4 | 新しい変数を **Add**（追加）します。

変数名はドル（$）記号で始まる必要があります。

1. 新しい変数に名前を付けます。例えば、`$DNS-primary` と `$DNS-secondary` という名前の変数があるとします。
2. 変数 **Type (型)** を選択し、選択した変数型に対応する値を入力します。

   この例では、**IP Netmask** を選択します。
3. （任意）変数の説明を入力します。
4. **OK**、**Close**（閉じる）の順にクリックします。

変数がサポートされているインラインで変数を作成することもできます。



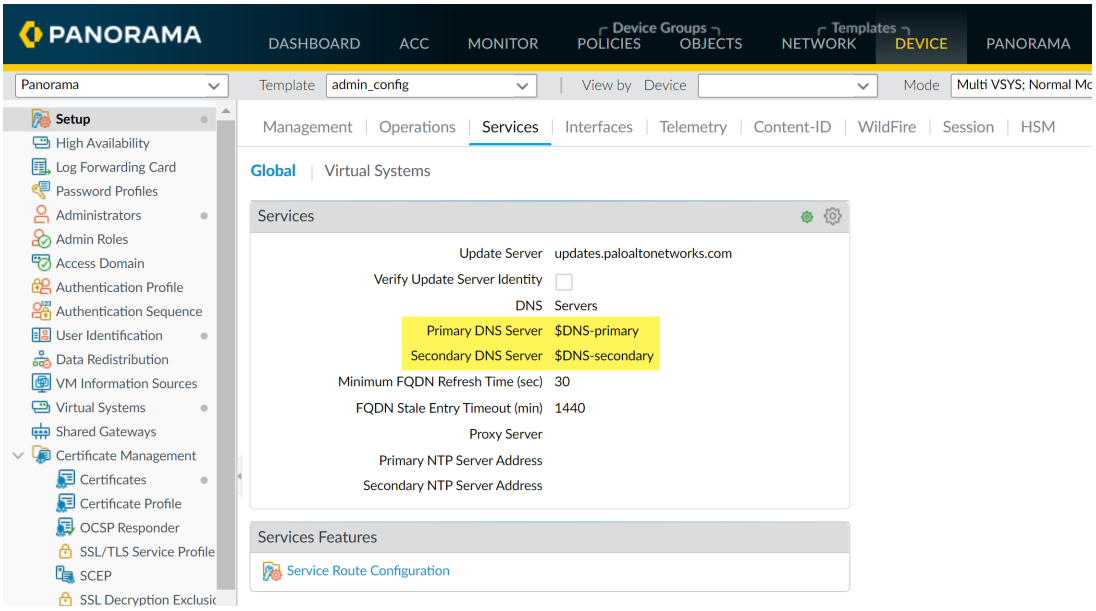
STEP 5 | テンプレート（テンプレート）ドロップダウン リストから、変数が属するテンプレートまたはテンプレート スタックを選択します。

STEP 6 | 適切な場所に変数を入力します。

この例では、前に定義した DNS 値を参照します。

1. （デバイス）> **Setup**（セットアップ）> **Services**（サービス）およびサービスを編集します。
2. **`$DNS-primary`** を入力するか、**Primary DNS**（プライマリ **DNS**）のドロップダウン リストから選択します。
3. **$DNS-secondary** 入力するか、**Secondary DNS Server**（セカンダリ **DNS** サーバー）のドロップダウンリストから選択します。
4. **OK** をクリックします。

© 2019 Palo Alto Networks, Inc.

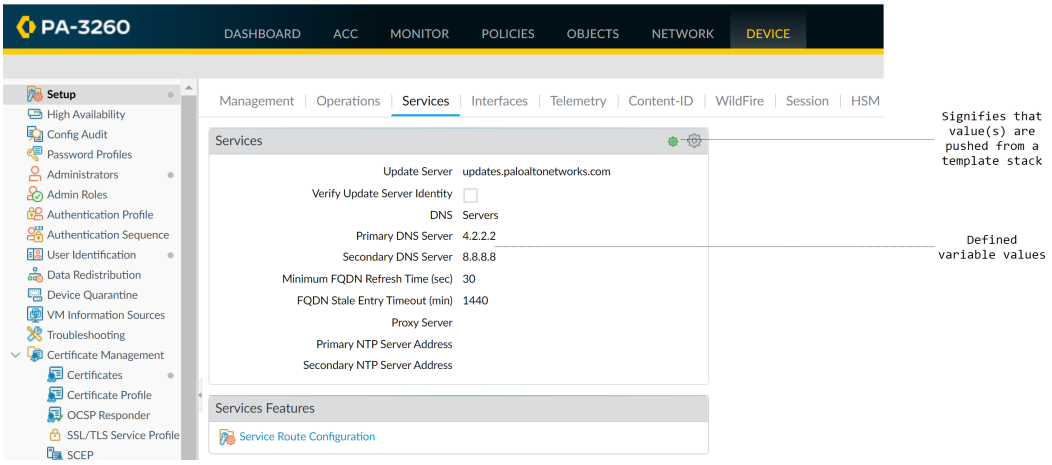


STEP 7 | **Commit**（コミット）をクリックして、管理対象のファイアウォールへの変更を **Commit and Push**（コミットしてプッシュ）。

テンプレートまたはテンプレート スタック変数を参照してデバイス グループ構成をプッシュするには、*Edit Selections* (選択内容の編集) を行い、*Include Device and Network Templates* (デバイスおよびネットワーク テンプレートを含める) 必要があります。

STEP 8 | すべての変数の値が管理対象デバイスにプッシュされていることを確認します。

1. **Context**（コンテキスト）ドロップダウン リストから、変数が作成されたテンプレート スタックに属するファイアウォールを選択します。
2. **Device**（デバイス）> **Setup**（セットアップ）> **Services**（サービス）を選択します。
3. テンプレートまたはテンプレート スタックによって定義された値を持つ設定は、テンプレート シンボル（ . ）で示されます。インジケータの上にカーソルを置くと、変数定義が属するテンプレートまたはテンプレート スタックが表示されます。ファイアウォール コンテキストから表示すると、変数は、変数に設定した IP アドレスとして表示されます。



STEP 9 | ネットワーク リソースへの接続のトラブルシューティングして、ファイアウォールがネットワーク リソースにアクセスできることを確認します。

© 2019 Palo Alto Networks, Inc.

既存のテンプレートスタック変数のインポートおよび上書き

テンプレート スタック変数を使用して、ファイアウォール設定の IP アドレス、IP 範囲、FQDN、インターフェース、またはグループ ID を置き換えます。変数を使用すると、管理する必要のあるテンプレートとテンプレート スタックの総数を減らすことができ、ファイアウォール固有の値は保持できます。

テンプレート スタックの変数をインポートすることで、既存の複数の変数を上書きできます。インポート時に新しいテンプレート スタックの変数を作成することはできません。新規テンプレートまたはテンプレート スタック変数を作成する方法の詳細については、テンプレートまたはテンプレートスタック変数の設定を参照してください。

STEP 1 | Panorama Web インターフェイスへのログイン.

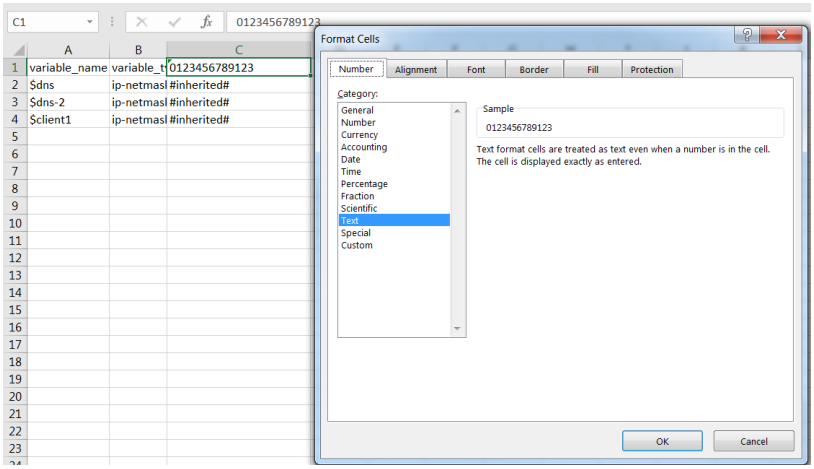
STEP 2 | 既存のテンプレート スタックの変数をエクスポートします。

1. **Panorama**（**Panorama**）> **Templates**（テンプレート）の順に選択し、テンプレートまたはテンプレート スタックを選択します。
2. **Variable CSV** > **Export**（変数 **CSV** のエクスポート）を選択します。設定されたテンプレート スタック変数は、CSV ファイルとしてローカルにダウンロードされます。
3. エクスポートした CSV を開きます。

STEP 3 | Panorama にインポートするテンプレート スタックの変数を含む CSV ファイルを、以下の書式で編集します：

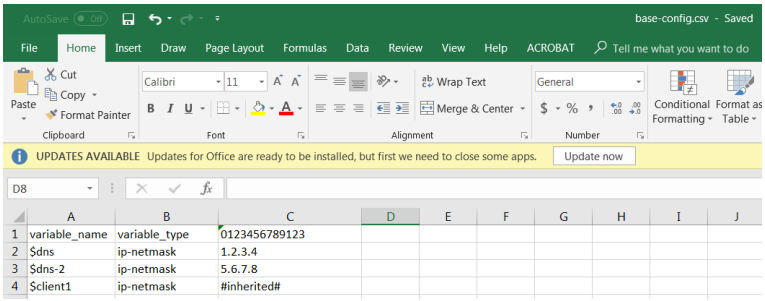
`#inherited#`として表示される値は、テンプレート スタックで定義されている値です。

1. ファイアウォールのシリアル番号を含むセルの番号を修正します。CSV ファイルに含まれるすべてのファイアウォールに対してこのステップを繰り返します。
   1. ファイアウォールのシリアル番号が含まれるセルを右クリックし、**Format Cells** (セルのフォーマット)を選択します。
   2. **Number** (数値) > **Text** (テキスト)を選択して**OK**をクリックします。
   3. シリアル番号の頭に**0**を追加します。



2. 適切なテンプレート変数の値を新たに入力します。
3. **File** (ファイル) > **Save As** (次として保存)を選択して**CSV UTF-8**形式でファイルを保存します。

© 2019 Palo Alto Networks, Inc.



STEP 4 | CSV ファイルをテンプレート スタックにインポートします。

1. Panorama Web インターフェイスへのログイン.
2. **Panorama**（**Panorama**）> **Templates**（テンプレート）の順に選択して、ステップ 2 で変数をエクスポートしたテンプレート スタックを選択します。
3. ステップ 3 で編集した CSV ファイルの**Variable CSV** > **Import**（変数 **CS V** のインスポート）および**Browse**（ブラウズ）を選択します。
4. **OK**をクリックしてテンプレート スタックの変数をインポートします。

STEP 5 | **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

STEP 6 | 適切な場所に変数を入力します。

STEP 7 | **Commit**（コミット）をクリックして、管理対象のファイアウォールへの変更を **Commit and Push**（コミットしてプッシュ）。

テンプレートまたはテンプレート スタック変数を参照してデバイス グループ構成をプッシュするには、*Edit Selections (*選択内容の編集*)* を行い、*Include Device and Network Templates (*デバイスおよびネットワーク テンプレートを含める*)* 必要があります。

テンプレートまたはテンプレートスタック値のオーバーライド

テンプレートおよびテンプレートスタックを使用すると、複数のファイアウォールに基本設定を適用できますが、テンプレートあるいはテンプレート スタック内のすべてのファイアウォールに適用しないファイアウォール固有の設定が必要な場合もあります。逆に、テンプレート設定をオーバーライドして、すべての管理対象ファイアウォールに基本設定として適用できるテンプレート スタック設定を作成することができます。オーバーライドを使用すると、設定ニーズに合わせた例外や変更が可能です。たとえば、テンプレートを使用して基本設定を作成したが、テスト ラボ環境の数台のファイアウォールは、DNS（Domain Name System）サーバーの IP アドレスまたは NTP（Network Time Protocol）サーバーに異なる設定が必要な場合、テンプレートおよびテンプレート スタックの設定をオーバーライドできます。

個々の設定をオーバーライドするのではなく、ファイアウォール上のすべてのテンプレートあるいはスタックの値を無効化/削除したい場合は、テンプレート設定の無効化/削除をご覧ください。

次のいずれかの方法で、テンプレートまたはテンプレート スタック値を上書きできます。

- ファイアウォールのテンプレートをオーバーライドするか、 変数を使用してテンプレートまたはテンプレート スタックをオーバーライドする–テンプレートまたはテンプレート スタックからプッシュされた値をオーバーライドするには、2 つの方法があります。前者の目的は、テンプレートまたはテンプレート スタックからプッシュされた値をオーバーライドするためにファイアウォール上にローカルに値を定義することです。後者の目的は、テンプレートまたはテンプレート スタックからプッシュされた値を上書きするためのファイアウォール固有の変数を定義することです。

© 2019 Palo Alto Networks, Inc.

- テンプレート スタックを使用してテンプレート値をオーバーライドする–テンプレートからプッシュされた値をオーバーライドするために、テンプレート スタック上の値または変数を定義します。

ファイアウォールのテンプレート値のオーバーライド

ファイアウォール固有の設定を作成するために、テンプレートまたはテンプレート スタックからプッシュされたローカル ファイアウォールの設定をオーバーライドします。これにより、他のファイアウォールには適用されない、ファイアウォール固有の設定を維持しながら、Panorama™ の基本テンプレートまたはテンプレート スタック設定を管理できます。

STEP 1 | ファイアウォール Web インターフェイスにアクセスします。

ブラウザの URL フィールドに IP アドレスを入力して直接ファイアウォールにアクセスするか、Panoramaの**Context**（コンテキスト）ドロップダウンリストを使用してファイアウォールの設定に切り替えるます。

STEP 2 | テンプレートまたはテンプレート Stack からプッシュされた値をオーバーライドします。

この例では、テンプレートの追加にてテンプレートを使用して割り当てた DNS サーバーの IP アドレスをオーバーライドします。

1. **Device**（デバイス）> **Setup**（セットアップ）> **Services**（サービス）の順に選択し、[サービス] セクションを編集します。
2. **Primary DNS Server**（プライマリ **DNS** サーバー）のテンプレート アイコン（ ）をクリックし、その項目のオーバーライドを有効にします。
3. **Primary DNS Server**（プライマリ **DNS** サーバー）の新しい IP アドレスを入力します。テンプレートのオーバーライドのシンボル（ ）はテンプレート値がにオーバーライドされたことを示します。
4. **OK** をクリックし、変更を **Commit** (コミット) します。

テンプレート スタックを使用してテンプレート値をオーバーライドする

テンプレート スタック値を使用して、テンプレートから管理対象ファイアウォールにプッシュされた設定をオーバーライドし、Panorama™ から管理対象ファイアウォールの基本設定を管理するために使用できるテンプレート スタック設定を作成できます。これにより、Panorama の管理機能を活用して、設定の変更を 1 つの場所から複数のデバイスにプッシュできます。この例では、テンプレート スタックを使用して、テンプレートからプッシュされた `$DNS` というプライマリ DNS サーバーの IP アドレス変数をオーバーライドします。

Panorama は、テンプレート スタックを使用して、集約インターフェースのレイヤー *2* サブインターフェースを除き、テンプレートで設定されたインターフェースのオーバーライドをサポートします。

STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | **Template**（テンプレート） のドロップダウン リストから、テンプレート設定をオーバーライドするテンプレート スタックを選択します。

STEP 3 | プッシュされたテンプレート設定をオーバーライドします。

1. **Device**（デバイス）> **Setup**（セットアップ）> **Services**（サービス）の順に選択し、[サービス] セクションを編集します。
2. **Primary DNS**（プライマリ **DNS**）を IP アドレスで設定してプッシュされたテンプレート設定をオーバーライドして、**OK** をクリックします。

STEP 4 | 設定変更を **Commit and Push**（コミットしてプッシュ）します。

© 2019 Palo Alto Networks, Inc.

テンプレート スタック変数を使用してテンプレート値をオーバーライドする

テンプレート スタック値と変数を使用して、テンプレートから管理対象ファイアウォールにプッシュされた設定をオーバーライドし、Panorama™ から管理対象ファイアウォールの基本設定を管理するために使用できるテンプレート スタック設定を作成できます。これにより、Panorama の管理機能を活用して、設定の変更を 1 つの場所から複数のファイアウォールにプッシュできます。この例では、テンプレート スタックを使用して、テンプレートからプッシュされた `$DNS` というプライマリ DNS サーバーの IP アドレス変数をオーバーライドすることでテンプレートスタック変数を作成します。

Panorama は、テンプレート スタックを使用して、集約インターフェースのレイヤー *2* サブインターフェースを除き、テンプレートで設定されたインターフェースのオーバーライドをサポートします。

STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | テンプレート変数をオーバーライドします。

1. **[Panorama]** > [テンプレート] の順に選択します。
2. オーバーライドする必要があるテンプレート変数を含むテンプレート スタックを **Manage**（管理）（変数列）します。
3. **$DNS** 変数を検索して選択します。
4. **Override**（オーバーライド）を選択します。
5. 新しい変数値を入力し、**OK** をクリックします。

STEP 3 | 変更を **Commit and Push**（コミットしてプッシュ）します。

変数を使用してテンプレートまたはテンプレートスタック値をオーバーライドする

ファイアウォール固有の変数を使用して、管理対象ファイアウォールにプッシュされた変数をテンプレートまたはテンプレート スタックからオーバーライドし、ファイアウォール固有の設定を作成することができます。これにより、他のファイアウォールには適用されない、ファイアウォール固有の設定を維持しながら、基本テンプレートまたはテンプレート スタック設定を管理できます。これにより、個々のファイアウォールに必要な特定の設定を考慮しながら、Panorama の管理機能を活用できます。この例では、テンプレートからプッシュされた `$ DNS` というプライマリ DNS サーバーの IP アドレス変数は、ファイアウォール固有の変数を作成するためにオーバーライドされます。

オーバーライドされていないテンプレートまたはテンプレート スタック変数をオーバーライドできます。テンプレートまたはテンプレート スタック変数がすでにオーバーライドされている場合は、オーバーライドを*Revert*（元に戻す）ことでファイアウォール固有の変数を作成します。

STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | テンプレートまたはテンプレート スタック変数をオーバーライドします。

1. **Panorama** > **Managed Devices**（管理対象デバイス）> **Summary**を選択します。
2. オーバーライドする必要がある変数を含むファイアウォールを **Edit**（編集）（変数列）します。
3. **$DNS** 変数を検索して選択します。
4. **Override**（オーバーライド）を選択します。
5. 新しいファイアウォール固有の IP アドレスを入力して **OK** をクリックします。

STEP 3 | 変更を **Commit and Push**（コミットしてプッシュ）します。

© 2019 Palo Alto Networks, Inc.

テンプレート設定の無効化/削除

管理対象のファイアウォール上の設定の管理にテンプレートあるいはテンプレート スタックを使用することを停止する場合は、テンプレートあるいはテンプレート スタックを無効にできます。無効化する際、テンプレート/スタックの値をファイアウォールのローカル設定にコピーするか、値を削除することができます。

すべてのテンプレートあるいはスタックの設定を無効化あるいは削除するのではなく、単一の設定をオーバーライドしたい場合はテンプレート設定のオーバーライドをご覧ください。

ファイアウォールを管理する際にこれらを使用することについては、テンプレートおよびテンプレートスタックを参照してください。

STEP 1 | スーパーユーザーのロールを持つ管理者として管理対象のファイアウォールの Web インターフェイスにアクセスします。ブラウザの URL フィールドに IP アドレスを入力して直接にアクセスするか、**Context**（コンテキスト）ドロップダウンリストでファイアウォールを選択することができます。

STEP 2 | **Device**（デバイス）> **Setup**（セットアップ）> **Management**（管理）の順に選択し、Panorama 設定を Edit（編集）します。

STEP 3 | **Disable Device and Network Template**（デバイスとネットワーク テンプレートを無効にする）をクリックします。

STEP 4 | （任意）ファイアウォールに設定をローカルに保存するには、**Import Device and Network Template before disabling**（無効にする前にデバイスとネットワーク テンプレートをインポート）を選択します。このオプションを選択しない場合、PAN-OS は、Panorama がプッシュした設定すべてをファイアウォールから削除します。

STEP 5 | **OK** を 2 回クリックして、変更を **Commit**（コミット）します。

© 2019 Palo Alto Networks, Inc.

Panorama からマスターキーを管理

Panorama、ファイアウォール、ログ コレクタ、および WF-500 アプライアンスは、マスター キーを使用して構成内の機密要素を暗号化し、パスワードと構成要素を暗号化するために使用するデフォルトのマスター キーがあります。

標準のセキュリティ慣行の一環として、デフォルトのマスター キーを交換して、マスター キーの有効期限が切れる前に、個々のファイアウォール、ログ コレクタ、WildFire アプライアンス、および Panorama でキーを更新する必要があります。Panorama から管理対象デバイスにその設定を正常にプッシュするには、すべての管理対象デバイスに同じをデプロイし、Panorama でマスターキーを設定するマスター キー必要があります。キーを同じようにデプロイするには、新しいマスター キーをデプロイするか、期限切れになるマスター キーを Panorama から直接、複数のファイアウォール、ログ コレクタ、WF-500 アプライアンスで更新します。マスター キーの構成に関する詳細については、マスター キーの設定を参照してください。

STEP 1 | Panorama Web インターフェイスへのログイン.

STEP 2 | (ベストプラクティス) **Commit (コミット)** を選択して、保留中の構成変更を **Commit and Putsh (コミットしてプッシュ)** します。

Panorama は、新しいマスター キーを使用してデータを再暗号化する必要があります。すべての構成要素を新しいマスター キーで暗号化するには、新しいマスター キーをデプロイする前に、保留中のすべての変更をコミットする必要があります。

STEP 3 | キーの有効期限が切れた後、同じマスター キーで自動的に更新されるように、ファイアウォール、ログ コレクタ、および WildFire アプライアンスのマスター キーを設定します。

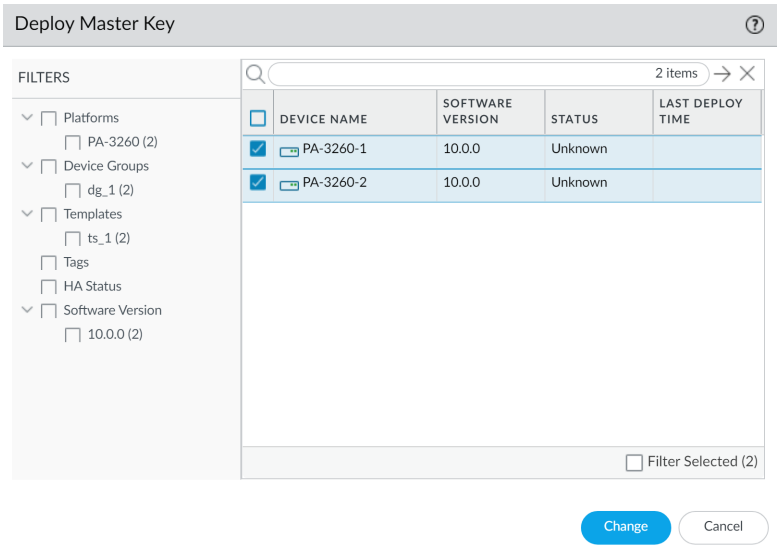
マスター キーを自動的に更新すると、メンテナンス期間前にキーが期限切れになった場合でも設定の暗号化を保持できますが、キーの有効期限が切れた後に新しいマスター キーをデプロイすることの代わりにはなりません。キーの有効期限が切れたときに自動的に更新されるようにマスター キーを構成する場合、次に利用可能なメンテナンス期間までの日数を考慮してください。

1. **Device (デバイス)** > **Master Key and Diagnostics (マスター キーおよび診断)** の順に選択し、マスター キー設定を編集します。
2. 指定した日数および時間数で **Auto Renew with Same Master Key (同じマスター キーを自動更新)** するよう Panorama を設定します。

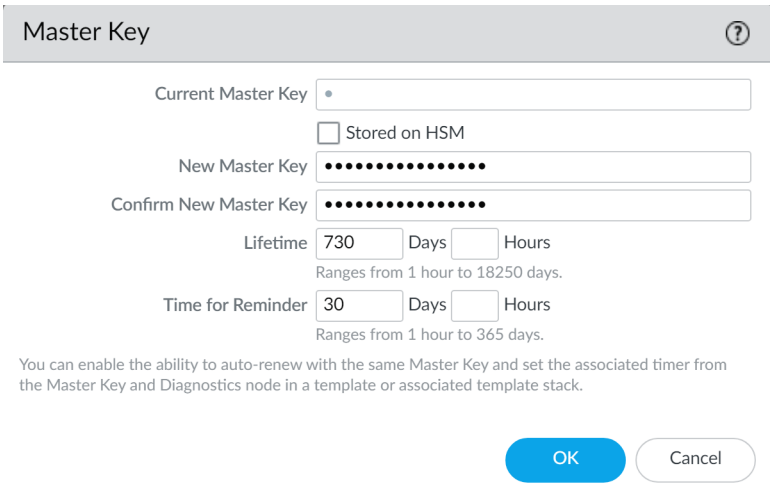
STEP 4 | マスター キーを管理対象のファイアウォールにデプロイします。

1. **Panorama** > **Managed Devices (管理対象デバイス)** > **Summary (サマリー)** を選択し、**Deploy Master Key (マスター キーをデプロイ)** します。
2. すべてのデバイスを選択し、マスター キーを **Change (変更)** します。

© 2019 Palo Alto Networks, Inc.



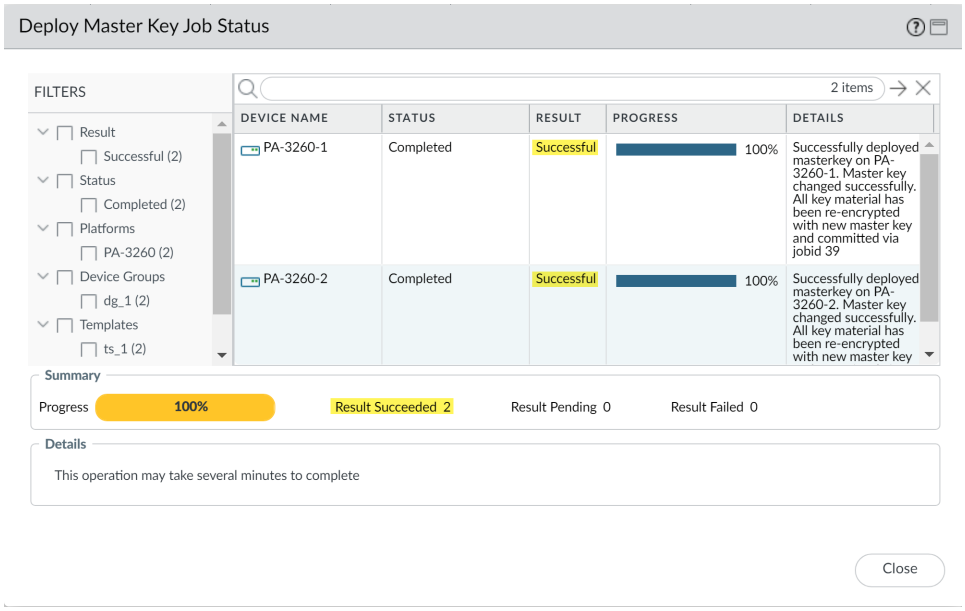
3. マスター キーを次のように構成します。
   1. マスター キーを更新する場合は、**Current Master Key** (現在のマスター キー) を入力します。デフォルトのマスター キーを新しいマスター キーに置き換える場合は、**Current Master Key** (現在のマスター キー) を指定しないでください。
   2. **New Master Key** (新規マスター キー) を指定し、**Confirm New Master** (マスター キーの確認) を行います。
   3. マスター キーの **Lifetime** (有効期間) と **Time for Reminder** (リマインダーの時間) を構成します。
   4. **OK** をクリックします。



4. 選択したすべてのデバイスにマスター キーが正常にデプロイされたことを確認します。

   Panorama から新しいマスター キーをデプロイすると、システムログが生成されます。

© 2019 Palo Alto Networks, Inc.



STEP 5 | マスター キーをログ コレクタにデプロイします。マスターキーは、ステップ 3 でデプロイしたものと同じでなければなりません。

1. **Panorama** > **Managed Collectors** (管理対象コレクタ) を選択し、**Deploy Master Key** (マスター キーをデプロイ)します。
2. すべてのデバイスを選択し、マスター キーを **Change** (変更) します。
3. マスター キーを次のように構成します。
    1. マスター キーを更新する場合は、**Current Master Key** (現在のマスター キー) を入力します。デフォルトのマスター キーを新しいマスター キーに置き換える場合は、**Current Master Key** (現在のマスター キー) を指定しないでください。
    2. **New Master Key** (新規マスター キー) を指定し、**Confirm New Master** (マスター キーの確認) を行います。
    3. マスター キーの **Lifetime** (有効期間) と **Time for Reminder** (リマインダーの時間) を構成します。
    4. **OK** をクリックします。
4. 選択したすべてのデバイスにマスター キーが正常にデプロイされたことを確認します。

    Panorama から新しいマスター キーをデプロイすると、システムログが生成されます。

STEP 6 | マスター キーを管理対象の WildFire アプライアンスにデプロイします。マスターキーは、ステップ 3 でデプロイしたものと同じでなければなりません。

1. **Panorama** > **Managed WildFire Appliances** (管理対象 **WildFire** アプライアンス) を選択し、**Deploy Master Key** (マスター キーをデプロイ)します。
2. すべてのデバイスを選択し、マスター キーを **Change** (変更) します。
3. マスター キーを次のように構成します。
    1. マスター キーを更新する場合は、**Current Master Key** (現在のマスター キー) を入力します。デフォルトのマスター キーを新しいマスター キーに置き換える場合は、**Current Master Key** (現在のマスター キー) を指定しないでください。
    2. **New Master Key** (新規マスター キー) を指定し、**Confirm New Master** (マスター キーの確認) を行います。
    3. マスター キーの **Lifetime** (有効期間) と **Time for Reminder** (リマインダーの時間) を構成します。
    4. **OK** をクリックします。
4. 選択したすべてのデバイスにマスター キーが正常にデプロイされたことを確認します。

© 2019 Palo Alto Networks, Inc.

Panorama から新しいマスター キーをデプロイすると、システムログが生成されます。

STEP 7 | Panorama でマスター キーを設定します。マスターキーは、ステップ 3 から 5 でファイアウォール、ログ コレクタ、および WildFire アプライアンスにデプロイされたキーと同じでなければなりません。

1. **Panorama** > **Master Key and Diagnostics** (マスター キーおよび診断) の順に選択し、マスター キーを構成します。
    1. マスター キーを更新する場合は、**Current Master Key** (現在のマスター キー) を入力します。デフォルトのマスター キーを新しいマスター キーに置き換える場合は、**Current Master Key** (現在のマスター キー) を指定しないでください。
    2. **New Master Key** (新規マスター キー) を設定し、**Confirm New Master** (マスター キーの確認) を行います。
    3. マスター キーの **Lifetime** (有効期間) と **Time for Reminder** (リマインダーの時間) を構成します。
    4. **OK** をクリックします。
2. **Commit** (コミット) > **Commit to Panorama** (**Panorama** へのコミット) の順に選択し、変更を **Commit** (コミット) します。

© 2019 Palo Alto Networks, Inc.

エンタープライズ データ消失防止 (DLP) のセットアップ

組織のデータセキュリティ標準を採用して、エンタープライズ Data Loss Prevention (データ損失防止 - DLP) を使って、偶発的なデータの誤用、損失、または盗難を防止してください。

- エンタープライズ データ漏洩防止 (DLP) の概要
- エンタープライズ データ損失防止 (DLP) のサポート対象。
- 事前定義済みデータ フィルタリングプロファイル
- エンタープライズ データ漏洩防止 (DLP) プラグインのインストール
- データ パターンの作成
- データ フィルタリング プロファイルの作成
- エンタープライズ データ漏洩防止 (DLP) の有効化
- エンタープライズ データ消失防止 (DLP) のログ詳細を見る
- エンタープライズ データ消失防止 (DLP) の設定の編集
- 既存のデータ パターンの有効化とプロファイルのフィルタリングの有効化
- エンタープライズ データ消失防止 (DLP) プラグインのアンインストール

エンタープライズ データ漏洩防止 (DLP) の概要

データ漏洩防止 (DLP) は、機密情報を不正なアクセス、誤用、入手、または共有から保護するための、一連のツールとプロセスです。DLP プラグインは Panorama 管理サーバーにインストールされ、所属組織のデータ セキュリティ標準を適用し、モバイルユーザーとマネージドファイアウォールのリモート ネットワーク全体で機密データの損失を防止するデータ パターンとデータ フィルタリング プロファイルを一元管理できます。データ パターンとデータ フィルタリングプロファイルは、すべての口ケーションで一貫したデータ セキュリティを提供するために、対応するすべての PAN-OS 10.0.2 以降のリリースを実行する Panorama とファイアウォールモデルで機能するように設計されています。エンタープライズ DLP を利用するには、Panorama とマネージドファイアウォールがインターネット接続している必要があります。

エンタープライズ DLP は、データの暴露、損失、および流出を防止するために、機密ドキュメントを金融、法務、医療、およびその他の分野に分類するための、機械学習アルゴリズムを使用するクラウドベースのサービスです。これらのパターンにより、ネットワークを流れるトラフィックの機密情報を識別し、その暴露を防止することができます。

エンタープライズ DLP では、機密データを次の方法で保護できます。

- 許可されていない**Web**アプリケーションへのファイルのアップロードを防止—信頼されていないWebアプリケーションへのデータ漏洩を検出して、条件付きで中止します。
- 許可されている**Web**アプリケーションの監視—機密データが許可されていない企業アプリケーションにアップロードされている場合、それを検出して監視します。

機密データを正確に識別、保護して、インシデントを防止するためにコンテンツを検査して、正しいコンテキスト内のデータを分析します。そのために、Enterprise DLP はクラウドサービスを介して有効になっています。エンタープライズ DLP は 380 以上のデータ パターンと多数の事前定義済みデータ フィルタリング プロファイルをサポートします。Enterprise DLP は、新しいパターンとプロファイルがクラウドサービスに追加されるとすぐに、セキュリティ ポリシー ルール内で自動的に利用可能になるよう設計されています。エンタープライズ DLP を設定するには、次のツールを使用してください。

- データパターン—機密コンテンツ、およびそのコンテンツがネットワークでどのように共有またはアクセスされているかを検出するために役立ちます。

© 2019 Palo Alto Networks, Inc.

事前定義パターンとビルトイン設定により、特定のファイルプロパティ（文書のタイトルや作成者など）、クレジットカード番号、さまざまな国の規制されている情報（運転免許証番号など）、およびサードパーティの DLP ラベルなどを含むファイルを手軽に保護することができます。組織内の機密データの検出率を向上するために、事前定義データパターンを補足する、コンテンツ検査およびデータ保護要件に固有のカスタムデータパターンを作成することができます。カスタムデータパターンでは、ファイルのカスタムプロパティまたは拡張プロパティ内のメタデータや属性を検索する、正規表現やファイルのプロパティを定義して、それをデータフィルタリングプロファイル内で使用することができます。

- データフィルタリングプロファイル—マネージドファイアウォールで利用できるデータ分類およびモニタリング機能を強化して、データロスを防止して、ビジネスリスクを緩和することができます。

  データフィルタリングプロファイルは、特定のオブジェクトやコンテンツタイプをスキャンするための、グループ化されたデータパターンの集合体です。コンテンツ解析を実行するために、事前定義データ フィルタリング プロファイルには法務または金融業界の標準のデータID、キーワード、および内蔵ロジックが、機械学習、正規表現、およびチェックサムの形式で定義されています。セキュリティ ポリシールールでデータフィルタリングプロファイルを使用する場合、ファイアウォールは一致するトラフィックを検査して、アクションを実施することができます。

  データパターン（事前定義またはカスタム）を活用した後は、Panorama からデータフィルタリングプロファイルを管理します。事前定義されているデータフィルタリングプロファイルを使用する、または新しいプロファイルの作成してそれにデータパターンを追加することができます。次にセキュリティポリシーを作成して、作成したポリシーに追加したプロファイルを適用します。ユーザーがファイルをアップロードしており、そのファイル内のデータがポリシー内の条件に一致した場合、マネージドファイアウォールによってアラート通知が作成されるか、またはファイルのアップロードがブロックされます。

データ フィルタリング プロファイルをセキュリティ ポリシー ルールに適用するとき、マネージドファイアウォールは、データ フィルタリング プロファイルの 1 つ以上のデータ パターンに一致するトラフィックに関する詳細情報を含んだ データ フィルタリング ログ を生成します。このログ詳細を利用することで、ファイルのアップロードがアラート通知の生成またはアップロードのブロックにつながった理由を検証して、フォレンジックを行うことができます。

スニペットは、Data Filtering（データフィルタリング）ログから参照できます。デフォルトでは、マネージドファイアウォールでは機密データの暴露を防止するために、スニペットのデータの部分的なマスキングが行われます。機密情報を完全にマスキングする、またはスニペットのマスキングを解除する、またはスニペットの抽出と表示を無効にするようにマネージドファイアウォールを設定することができます。

検出精度を向上して、誤判定を減らすために、次の事項を指定することもできます。

- 近接キーワード—キーワードが式の200文字以内にある場合、アセットはには高い精度の確実性が割り当てられます。ドキュメントに16桁の数字が存在しており、その直後に`Visa`と言う文字がある場合、それがクレジットカード番号である可能性が高くなります。しかし、Visaがタイトルとして登場し、16桁の番号が22ページのドキュメントの最後のページに記載されている場合は、それがクレジットカード番号である可能性は低くなります。

  キーワードグループで複数のキーワードを使って、キーワードを指定したり除外したりすることで、式の200文字以内に特定の単語が登場するまたは登場しないことを検索することも可能です。
- 確実度レベル—近接キーワードとともに、確実度レベルによりパターンマッチ内の近接キーワードの登場の可能性を指定することができます。確実度 **Low**（低） の場合、マネージド ファイアウォールは一致項目の識別に近接キーワードを使用しません。**High**（高）の場合は、マネージドファイアウォールではパターン内の正規表現の200文字以内の近接キーワードが検索されて、その後ファイル内のデータパターンが一致しているとみなされるかどうかが判断されます。
- 基本および重み付き正規表現—正規表現（regex）は、特定のテキストパターンの検索方法を記述しており、パターンの一致が見つかった場合、一致項目を表示します。*basic*（基本）と*weighted*（重み付き）の2種類の正規表現が存在しています。

© 2019 Palo Alto Networks, Inc.

- 基本正規表現は、特定のテキストパターンを検索します。パターンの一致が見つかると、一致項目が表示されます。
- 重み付き正規表現は、テキストエントリにスコアを割り当てます。スコアの閾値を超えた場合、パターンの一致項目が返されます。

  正規表現の誤判定を減らし、検索パフォーマンスを向上するために、データパターンの作成時にスコアを割り当てて、重要な情報を検索し、スコアを算出することができます。スコアリングは一致閾値に適用されます。十分な数のパターンからの表現がアセットと一致した場合など、スコアの閾値を超えた時に、そのアセットはパターンに一致したとみなされます。

  使用事例とベストプラクティスも含めた詳細については、『Prisma Access管理者ガイド』の「正規表現の設定」を参照してください。

エンタープライズ データ損失防止 (DLP) のサポート対象。

エンタープライズ データ損失防止 (DLP) は、Application & Threats 最低コンテンツバージョン 8334-6362 で PAN-OS 10.0.2 以降のリリースを実行するCN-Series ファイアウォールを除くすべてのハードウェアベースのファイアウォールと VM-Series ファイアウォールでサポートされます。

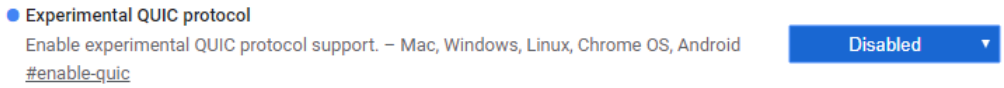
エンタープライズ データ損失防止 (DLP) で使用できる、サポートされているアプリケーションについて説明しています。

Webアプリケーション	PDF	doc/docx	ppt/pptx	xls/xlsx	rtf	CSV	複数ファイルのアップロード	ファイルサイズ
Webブラウジング	あり。	あり。	あり。	あり。	あり。	あり。	あり。	20MB
Onedrive Webアプリケーション	あり。	あり。	あり。	あり。	あり。	あり。	あり。	20MB
Sharepoint Webアプリケーション	あり。	あり。	あり。	あり。	あり。	あり。	あり。	20MB
Gmail Webアプリケーション	あり。	あり。	あり。	あり。	あり。	あり。	あり。	20MB
Box Webアプリケーション	あり。	あり。	あり。	あり。	あり。	あり。	あり。	20MB
Slack Webアプリケーション	あり。	あり。	あり。	あり。	あり。	あり。	あり。	20MB

© 2019 Palo Alto Networks, Inc.

- アプリケーション—次のアプリケーションのWebベース（HTTPまたはHTTPSベース）のアップロードに、DLPを適用できます。
  - Box（App-IDはboxnet-uploading）
  - Gmail（App-IDはgmail-uploading）

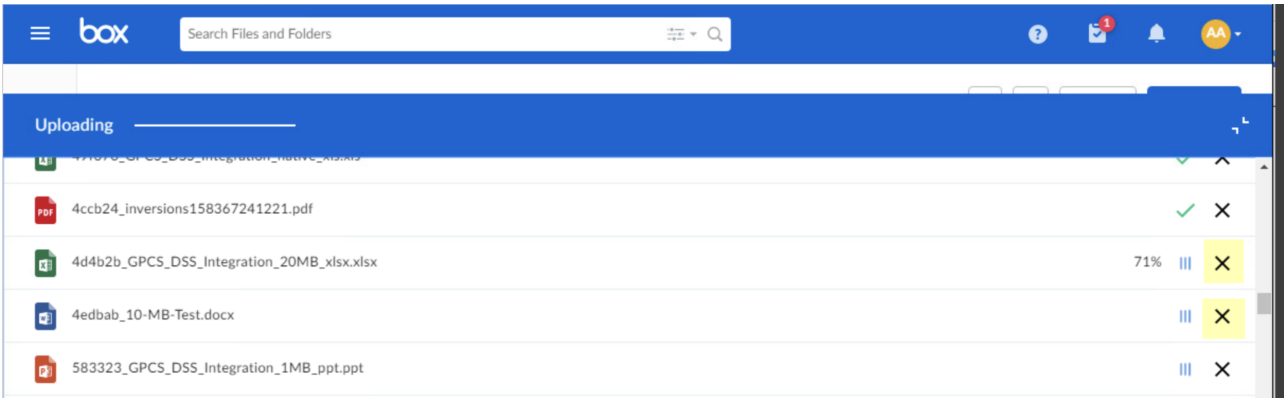
    Gmail を使用するには、*QUIC* プロトコルを無効化する必要があります。*Palo Alto Networks* は、*Chrome* では *QUIC* を無効化することを推奨します。無効化するには、*Chrome* の *URL* バーで `chrome://flags/` と入力し、*Experimental QUIC Protocol* (試験運用 *QUIC* プロトコル) を探し、*Disabled* (無効) を選択します。

  - Microsoft OneDrive（App-IDはsharepoint-online-uploading）
  - Microsoft SharePoint（App-IDはsharepoint-online-uploading）
  - Slack（App-IDはslack-uploading）
  - Webブラウジング（App-IDはweb-browsing）
- ファイル操作—HTTPおよびHTTPS（HTTP/1.1）を使って（FTPまたはSMTPは不可)、ファイルをアップロードできます。

  *SharePoint*や*OneDrive*など、一部のアプリケーションは、デフォルトで*HTTP/2*を使用しています。*HTTP/1.1*で*HTTP/2*ファイルを使用するには、*ALPN*ヘッダーを削除するために、復号化プロファイルとセキュリティポリシーを作成する必要があります。詳細は、「エンタープライズ データ漏洩防止 (DLP) の有効化」を参照してください。
- データフロー—ファイルのあっぷろーどがサポートされています（ファイルのダウンロードはサポートされていません）。
- 同時ファイルアップロード数—25 個のファイルの同時アップロードがサポートされます。
- ファイルサイズ—最高20 MBのファイルをサポートしています。

  Box を使って複数のファイルをアップロードする際に、1つ以上のファイルのサイズが20 MBを超えている場合、すべてのファイルのアップロードは完了しなくなります。続行するには、Box内の 20 MBを超えるファイルを探して、**X**をクリックして、それらのファイルのアップロードを中止してください。



- ファイルタイプ—Microsoft Office（.doc、.docx、.ppt、.pptx、.xls、.xlsx）、.csv、.pdf、および.rtf。
- レスポンス—HTTPおよびHTTPSファイルの、Block（ブロック）およびAlert（アラート）アクションがサポートされています。Block（ブロック）ページには、マネージドファイアウォールがブロックしたファイル名は表示されません。
- データパターンおよびデータフィルタリングプロファイル—事前定義されているデータパターンおよびデータフィルタリングプロファイルを使用するか、または独自のデータパターンおよびデータフィルタリングプロファイルを作成します。データパターンの複製は現在サポートされていません。ただ

© 2019 Palo Alto Networks, Inc.

し、既存のプロファイルにデータIDを追加、削除、または変更したい場合は、事前定義済みデータ フィルタリングプロファイルを複製することができます。

各データフィルタリングプロファイルに対して、エンタープライズ DLP では1つのBlock（ブロック）ルールに対して最大10件のデータパターンが、1つのAlert（アラート）ルールに対して最大50件のデータパターンが許可されています。

事前定義されたデータ パターンは、スキャンされたファイルに対して機械学習または正規表現ベースの検出のいずれかを使用します。エンタープライズ DLP は、最大 1MB のスキャンファイルについて、次の事前定義済みの機械学習ベースのデータ パターンの判定を返します。

- 銀行 – 破産申請
- 銀行 – ステートメント
- 金融 – 財務会計
- 金融 – 一般
- 金融 – 請求書
- 金融 – パーソナル ファイナンス
- 健康 – 一般
- 法務 – 一般
- 法務 – 訴訟
- 法務 – 合併買収
- 法務 – 特許申請
- 法務 – 標準ビジネス合意
- ソースコード- `Cfamily`
- ソースコード- 一般
- ソースコード- `java`
- ソースコード- `javascript`
- ソースコード- `perl`
- ソースコード- `powershell`
- ソースコード- `python`
- ソースコード- `r`
- ソースコード- `ruby`
- ソースコード- `vbs`
- ソースコード- `verilog`
- ソースコード- `vhd1`
- ソースコード- `x86_assembly`

事前定義済みデータ フィルタリングプロファイル

次の表は、エンタープライズ データ損失防止 (DLP) で提供される、事前定義済みのデータ フィルタリング プロファイルを説明するものです。

事前定義済みデータ フィルタリングプロファイル	スキャン対象
Bulk CCN	クレジットカード番号またはVoyagerクレジットカード番号（100以上）。
CCPA	カリフォルニア州プライバシー規制法コンプライアンス。
Corporate financial docs	金融アカウントおよび全般的な金融情報。

© 2019 Palo Alto Networks, Inc.

事前定義済みデータ フィルタリング プロファイル	スキャン対象
Financial Information	銀行取引明細書、銀行ルーティングナンバー、クレジットカード番号（厳密チェック）、破産申請書。
GDPR	運転免許証番号、税ID、国民識別番号、パスポート番号。
Gramm-Leach-Bliley Act（GLBA）	クレジットカード番号、Voyagerクレジットカード番号、磁気ストライプ情報、Tax Id-US（TIN）、National ID-US、社会保障番号（SSN）。
医療業界	臨床検査改善修正法案（CLIA）番号、麻薬取締局（DEA）番号、およびその他の医療文書。
Intellectual Property	ソースコード、AWS秘密鍵、アクセスキー、会社の機密情報。 知的財産には、2種類のタイプが存在しています。**Intellectual Property - Basic**データフィルタリングプロファイルには、**Intellectual Property**データフィルタリングプロファイルに含まれているデータパターンのサブセットが含まれています。
Legal	訴訟、 M&A、標準ビジネス契約、特許、破産申請書類などを含む法的文書。
Malware	すべてのMicrosoft Officeドキュメント、PDF、および, and portable executableファイル、およびWildFireに対する既知の脅威。判定は、ファイルの一意の指紋となるハッシュに基づいて行われます。
Personally-Identifiable Information（PII）	税ID、国民識別番号、パスポート番号、および運転免許証番号。
Profanity	検閲、個人、包含/除外、同性愛嫌悪、セクシュアル。
Self Harm	自殺観念。
Sensitive content	国民識別番号、銀行情報、AWS秘密鍵またはアクセスキー、会社の機密情報、CCN。
U.K.PIOCP	税IDまたは国民識別番号。

エンタープライズ データ漏洩防止 (DLP) プラグインのインストール

Panorama™ 管理サーバーとマネージドファイアウォールでエンタープライズ データ漏洩防止 (DLP) プラグインをインストールするには、Palo Alto Networks カスタマー サポート ポータルからプラグインをダウンロードし、プラグインを Panorama にアップロードし、プラグインをインストールする必要があります。エンタープライズ DLP を利用するには、Panorama とマネージドファイアウォールでプラグインをインストールする必要があります。

既存のデータ パターン *(Objects (オブジェクト) > Custom Objects (カスタム オブジェクト) > Data Patterns (データ パターン))* とデータ フィルタリング プロファイル *(Objects (オブジェクト) > Security Profiles (セキュリティ プロファイル) > Data Filtering (データ フィルタリング))* は、*Panorama* の エンタープライズ *DLP* プラグインのインストール後に自動的に

© 2019 Palo Alto Networks, Inc.

非表示になります。既存のデータ パターンの有効化とプロファイルのフィルタリングを表示するには、既存のデータ パターンの有効化とプロファイルのフィルタリングの有効化を参照します。

STEP 1 | Palo Alto Networks の Customer Support Portal（カスタマーサポートポータル）（CSP）で、Panorama とマネージドファイアウォールを登録します。

STEP 2 | Panorama でデバイス証明書をインストールします。

STEP 3 | マネージドファイアウォールのデバイス証明書をインストールします。

エンタープライズ DLP を利用するすべてのマネージドファイアウォールにデバイス証明書をインストールする必要があります。

STEP 4 | Panorama にプラグインをインストールします。

1. Panorama Web インターフェースにログインします。
2. **Panorama** > **Plugins (プラグイン)**の順に選択して、最新の dlp のバージョンのプラグインを検索します。
3. Panorama でエンタープライズ DLP プラグインの **Download (ダウンロード)** と **Install (インストール)** を実行します。

STEP 5 | マネージド ファイアウォールでプラグインをインストール。

1. **Panorama** > **Device Deployment (デバイスのデプロイメント)** > **Plugins (プラグイン)**を選択して、最新のエンタープライズ DLP のバージョンのプラグインを検索します。
2. マネージドファイアウォールでエンタープライズ DLP プラグインの **Download (ダウンロード)** と **Install (インストール)** を実行します。
3. プラグインをインストールする **Devices (デバイス)** を選択します。
4. **OK** をクリックしてプラグインをインストールします。

STEP 6 | マネージド ファイアウォールにコミットしてプッシュすると、エンタープライズ DLP プラグインのインストールが完了します。

この手順は、エンタープライズ DLP データ フィルタリング プロファイル名をデータ フィルタリング ログに表示するために必要です。

Commit and Push (コミットしてプッシュ) の実行がサポートされていますが、エンタープライズ *DLP* 設定の変更は推奨されません。また、プッシュ スコープの選択で影響を受けるテンプレートとマネージド ファイアウォールを手動で選択する必要があります。

1. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、設定変更を **Commit**（コミット）します。
2. **Commit**（コミット）> **Push to Devices**（デバイスへのプッシュ）の順に選択し、**Edit Selections**（選択内容の編集）を行います。
3. **Device Groups (デバイス グループ)** を選択して、（ **Include Device and Network Templates** ネットワークのテンプレートを含める) を実行します。
4. **OK** をクリックします。
5. 設定の変更をマネージドファイアウォールに **Push (プッシュ)** します。

STEP 7 | Palo Alto Networks Customer Support Portal (CSP) でエンタープライズ DLP ライセンスをアクティベートします。

エンタープライズ DLP を利用するすべてのファイアウォールに対してこのステップを繰り返します。

1. Palo Alto Networksカスタマーサポートポータルにログインします。

© 2019 Palo Alto Networks, Inc.

2. **Assets (アセット)** > **Devices (デバイス)** を選択して、Action (アクション) 列の編集ボタン ( ) をクリックします。
3. Device Licenses (デバイス ライセンス) ウィンドウで、**Activate Auth-Code (承認コードのアクティベート)** を選択し、**Authorization Code (承認コード)** を入力します。

   認証コード (auth code) は、エンタープライズ DLP プラグイン ライセンスの購入時に、Palo Alto Networks から電子メールで自動的に提供されます。
4. **Agree and Submit (同意して送信)** をクリックします。

STEP 8 | Palo Alto Networks Support ticket (Palo Alto Networks サポート チケット) を作成して、ファイアウォール間のエンタープライズ DLP ライセンスの転送を有効化します。

エンタープライズ DLP ライセンスを転送可能にするように要求すると、DLP ライセンスを他のマネージドファイアウォールに転送できます。

サポート チケット内に、次の情報を含ませます:

- エンタープライズ DLP ライセンスのファイアウォール転送をリクエストします。
- ご利用の CSP アカウント ID と、CSP アカウントに紐づけられた電子メール。
- マネージドファイアウォールのシリアル番号。複数のマネージドファイアウォールでエンタープライズ DLP ライセンスをアクティブ化した場合は、すべてのマネージドファイアウォールのシリアル番号を 1 つのサポートチケットに含めます。
- マネージドファイアウォールでエンタープライズ DLP ライセンスをアクティブ化するために使用される認証コード。
- (任意) 別の CSP アカウントに属するマネージドファイアウォールがある場合は、これらの管理対象ファイアウォールが関連付けられている CSP アカウント ID を提供します。

STEP 9 | Panorama とマネージドファイアウォールが同じ CSP アカウントに属していることを確認します。

データ プロファイルを共有して、一貫したセキュリティ ポリシーを適用するには、Panorama とマネージド ファイアウォールを同じ CSP アカウントに所属させる必要があります。

1. Palo Alto Networksカスタマーサポートポータルにログインします。
2. **Assets (アセット)** > **Devices (デバイス)** を選択し、Panorama とマネージド ファイアウォールを探します。

STEP 10 | マネージドファイアウォールでエンタープライズ DLP プラグインをアクティベートします。

1. **Panorama** > **Device Deployment (デバイスのデプロイメント)** > **License (ライセンス)** を選択し、エンタープライズ DLP プラグインを **Activate (アクティベート)** します。
2. ターゲット マネージド ファイアウォールの **Auth Code (認証コード)** を入力します。

   認証コード (auth code) は、エンタープライズ DLP プラグイン ライセンスの購入時に、Palo Alto Networks から電子メールで自動的に提供されます。
3. マネージドファイアウォールのエンタープライズ DLP プラグイン ライセンスを **Activate (アクティベート)** します。

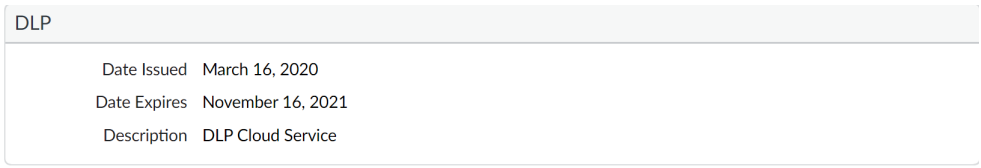
STEP 11 | **Objects (オブジェクト)** > **DLP** > **DLP Data Filtering (DLP データ フィルタリング)** を選択して、事前定義済みのデータ フィルタリング プロファイルが表示されることを確認します。

Panorama が DLP クラウド サービスに正常に接続すると、Panorama には事前定義されたデータ フィルタリング プロファイルが自動的に入力されます。

STEP 12 | マネージドファイアウォールでエンタープライズ DLP ライセンスが正常にアクティブ化されることを確認します。

© 2019 Palo Alto Networks, Inc.

1. ファイアウォール Web インターフェースを起動します。
2. **Device**（デバイス）> **Licenses**（ライセンス）を選択し、ライセンスが正常にアクティベートされていることを確認します。



データ パターンの作成

データパターンを利用することで、一致条件を指定して、ネットワーク上の機密情報を表す正規表現、ファイルのプロパティ、またはキーワードを使って各種パターンを識別することができます。作成されたすべてのデータ パターンは、すべてのデバイス グループ間で共有されます。

STEP 1 | Panorama Web インターフェースにログインします。

STEP 2 | **Objects (オブジェクト)** > **DLP** > **DLP Data Patterns (DLP データ パターン)** を選択して、**Device Group (デバイス グループ)** を指定します。

STEP 3 | 新しいデータ プラットフォームを **Add (追加)** します。

STEP 4 | データパターンの**Type**（タイプ）および条件を指定して、それに**Name**（名前）を指定します。

次のデータパターンタイプを使用します。

- **Regular Expression**（正規表現）– データパターンで使用する正規表現を作成します。

  Basic（基本）または**Advanced**（詳細）データパターンを選択できます。基本または重み付け正規表現を作成する場合は、**Advanced**（詳細）データパターンを使用します。重み付け正規表現では、各テキストエントリにスコアが割り当てられます。十分な数のパターンからの表現がアセットと一致した場合など、スコアの閾値を超えた時に、そのアセットはパターンに一致したとみなされます。

  次に、**Regular Expressions**（正規表現）エリアでクエリビルダーを使用して通常（**Basic**）または重み付け（**Advanced**）正規表現を追加することができます。

  データフィルタリングパターンで使用する**Proximity Keywords**（近接キーワード）を1つまたは複数入力できます。データフィルタリングプロファイル内の、High Confidence（確実度高）で近接キーワードを使用します。ファイルをアップロードする場合、マネージドファイアウォールは指定されたデータパターンによるファイルの照合を検討する前に、正規表現の200文字以内の指定した近接キーワードでを検索します。
- **File Property**（ファイルのプロパティ）–照合するファイルプロパティパターンを追加します。

  データガバナンスと情報の保護のため、MS OfficeおよびPDFドキュメント内で、監査や追跡の目的で分類ラベルまたは埋め込みタグを使用してその他の情報を含めている場合、ファイルプロパティデータパターンを作成して、ファイル内のカスタムまたは拡張プロパティの一部となるメタデータや属性と照合することができます。Titusのような自動分類機構を使用する、またはユーザーにタグの追加を要求するかどうかに関係なく、ファイルに埋め込まれているカスタムまたは拡張プロパティと照合する名前と値のペアを指定することができます。

  エンタープライズ DLPは、MS Office および PDF ドキュメントのファイルプロパティデータパターンをサポートしています。MS OfficeのOLE（.doc/.ppt）またはXML（.docx/.pptx）フォーマットの両方をサポートしています。

  次に**Tag Name**（タグ名）および**Tag Value**（タグ値）を追加します。

© 2019 Palo Alto Networks, Inc.

Tag Name（タグ名）および**Tag Value**（タグ値）は、検索するプロパティを示す関連するペアになります（たとえば、**Tag Name**に**Label**および**Tag Value**に**Confidential**を指定できます。）。必要な数だけファイルのプロパティを追加することができます。データフィルタリングプロファイル内のファイルプロパティデータパターンを参照する場合、一致条件には論理演算子のORが適用されます。

STEP 5 | **OK** をクリックしてデータパターンを保存します。

STEP 6 | コミットを実行し、設定の変更内容をエンタープライズ DLP を活用するマネージド ファイアウォールへの設定の変更にプッシュします。

*Commit and Push (*コミットしてプッシュ*)* の実行がサポートされる間は、エンタープライズ *DLP* 設定の変更は推奨されません。また、プッシュ スコープの選択で影響を受けるテンプレートとマネージド ファイアウォールを手動で選択する必要があります。

1. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、設定変更を **Commit**（コミット）します。
2. **Commit**（コミット）> **Push to Devices**（デバイスへのプッシュ）の順に選択し、**Edit Selections**（選択内容の編集）を行います。
3. **Device Groups (**デバイス グループ**)** を選択して、（ **Include Device and Network Templates** ネットワークのテンプレートを含める**)** を実行します。
4. **OK** をクリックします。
5. 設定の変更をマネージドファイアウォールに **Push (**プッシュ**)** します。

STEP 7 | 1 つ以上の データ パターンを使用する データ フィルタリング プロファイルの作成。

データ フィルタリング プロファイルの作成

複数のデータパターンを追加して、一致条件および確実度レベルを指定するには、データフィルタリングプロファイルを作成します。すべての事前定義およびカスタム データ フィルタリング プロファイルは、すべてのデバイス グループで利用できます。

事前定義済みのデータ パターンを使用してデータ フィルタリング プロファイルを作成する際は、事前定義済みのデータ パターンで使用される検出タイプを検討してください。これにより、エンタープライズ DLP がスキャンされたファイルの判定に到達する方法が決まります。例えば、3 つの機械学習ベースのデータ パターンと 7 つの正規表現ベースのデータ パターンを含むデータ フィルタリング プロファイルを作成する時は、スキャンされたファイルが 1MB を超える場合、エンタープライズ DLP は 7 つの正規表現ベースのパターンに基づいて判定を返します。

STEP 1 | Panorama Web インターフェースにログインします。

STEP 2 | (任意) 1 つ以上の データ パターンを作成します。

STEP 3 | **Objects (**オブジェクト**)** > **DLP** > **DLP Data Filters (DLP** データ フィルタ**)** を選択して、**Device Group (**デバイス グループ**)** を指定します。

STEP 4 | 新しいデータ フィルタリング プロファイルを **Add (**追加**)** します。

STEP 5 | データ フィルタリング プロファイルのプライマリ パターンを設定します。

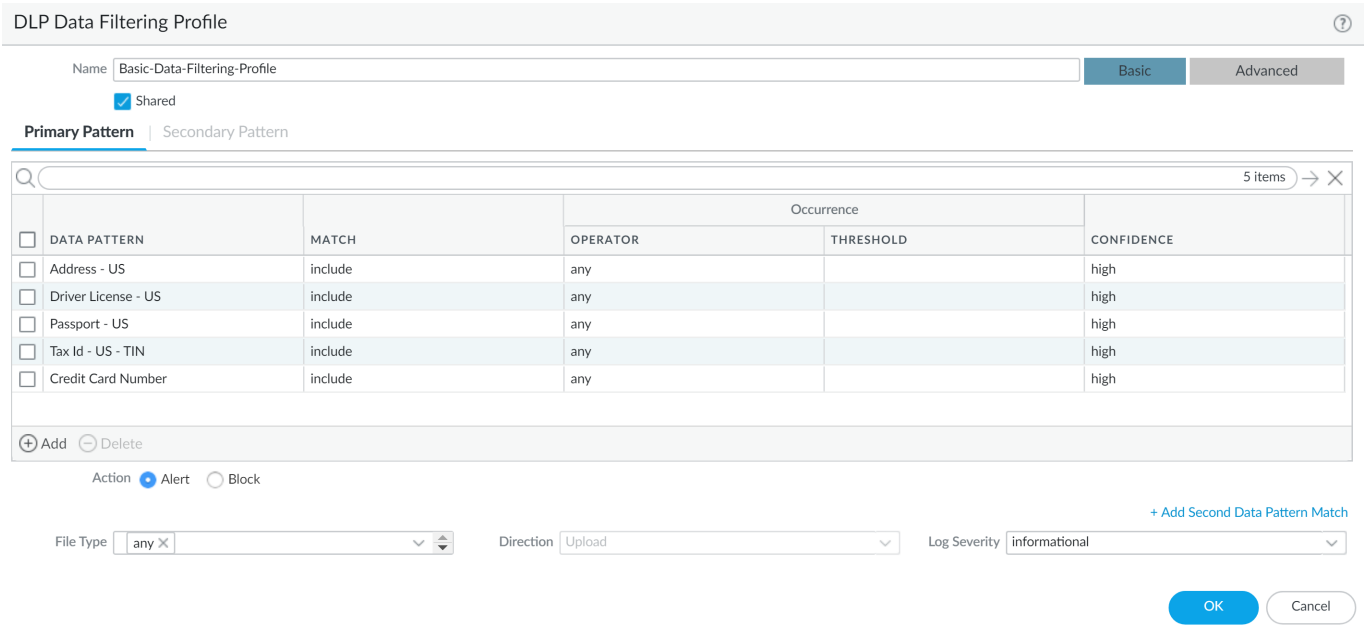
- **Basic (**基本**)** オプションを選択する場合、以下を設定します。
  - **Primary Pattern**（プライマリパターン）—一致条件として1つまたは複数のデータ パターンを**Add**（追加）します。

© 2019 Palo Alto Networks, Inc.

複数のデータパターンを指定した場合、それらの一致条件は論理演算子 OR を使ってマネージドファイアウォールで評価されます。

- **Match**（一致）—指定したパターンが指定条件に一致（**include**）するのか、または一致しない（**exclude**）のかを指定します。
- **Operator**（演算子）—**Threshold**（しきい値）パラメータと一緒に使用する演算子を選択します。しきい値を無視する場合は、**Any**（任意）を指定します。
- **Threshold**（しきい値）—指定した**Operator**（演算子）と一緒に使用する値を指定します。

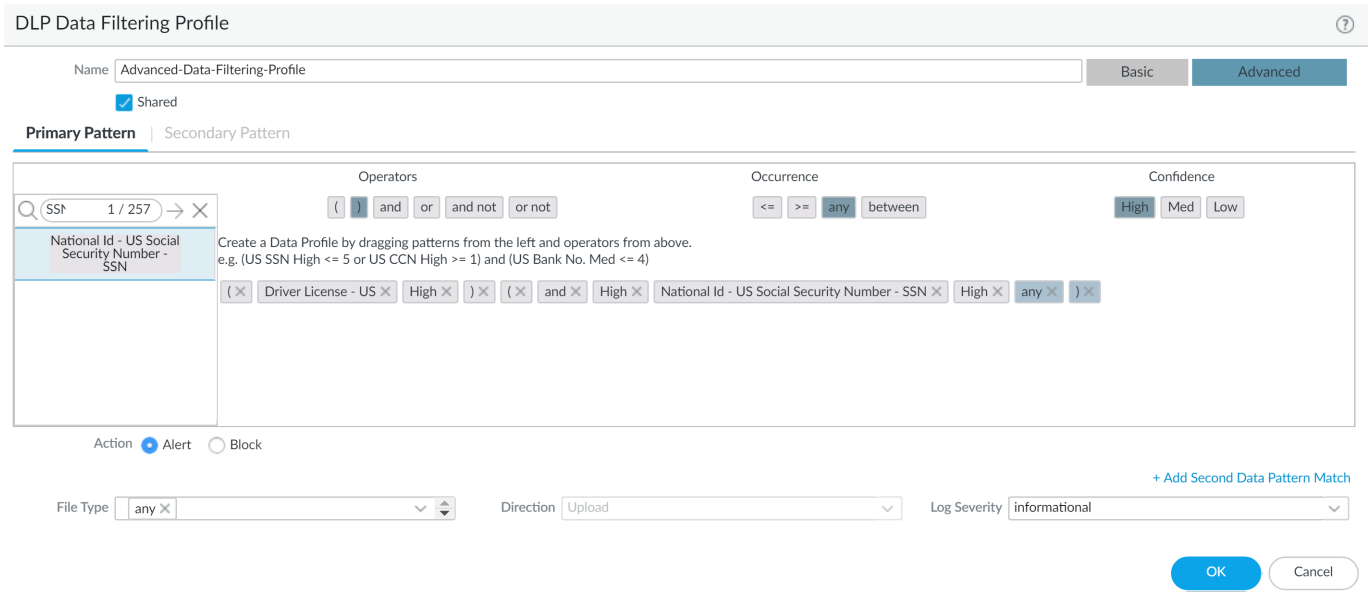
  たとえば、あるファイルに3回以上登場するパターンを照合するには、**Operator**（演算子）で**more_than_or_equal_to**を、**Threshold**（しきい値）で**3**を選択します。
- **Confidence**（確実度）—作成したデータパターンに指定した近接キーワードと一緒にこれを使用します。Confidence に**Low**（低）を指定すると、マネージドファイアウォールは近接キーワードを使用しません。Confidence に **High (高)** を指定すると、マネージドファイアウォールは、ファイル内のデータパターンが一致すると見なされる前に、パターン内の正規表現から 200 文字以内のパターン内の近接キーワードを検索します。



- **Advanced**（詳細）オプションを選択した場合、データパターン、**Confidence**（確実度）レベル、**Operators**（演算子）、および**Occurrence**（頻度）値を、ページ中央にあるフィールドにドラッグ アンド ドロップして式を作成します。

  次のスクリーンショットに記載されている順序で値を指定します（データパターン、 **Confidence**、および**Operator**または**Occurrence**の値）。

© 2019 Palo Alto Networks, Inc.



STEP 6 | ファイルに対して実施するAction（アクション）（Alert（アラート）またはBlock（ブロック））を選択します。

STEP 7 | File Type（ファイルタイプ）を指定します。

任意のサポートされているファイルタイプと一致するように、ファイルタイプはany（任意）を選択します。

STEP 8 | Direction（方向）でupload（アップロード）を選択します。

ダウンロードサポートされていません。

STEP 9 | （任意）このルールにマッチするファイルに対して記録するLog Severity（ログの重大度）を設定します。

デフォルトの重大度は、Informational（情報）です。

STEP 10 | OK をクリックして、設定の変更を保存します。

STEP 11 | データフィルタリングプロファイルをセキュリティポリシー ルールに添付します。

1. Policies (ポリシー) > Security (セキュリティ) を選択し、Device Group (デバイス グループ) を指定します。
2. データ フィルタリング プロファイル に追加したいセキュリティ ポリシー ルールを選択します。
3. Actions （アクション） を選択して Profile Type (プロファイル タイプ) を Profiles (プロファイル) に設定します。
4. 以前に作成した Data Filtering (データ フィルタリング) プロファイルを選択します。
5. OK をクリックして、設定の変更を保存します。

STEP 12 | コミットを実行し、設定の変更内容をエンタープライズ DLP を活用するマネージド ファイアウォールへの設定の変更にプッシュします。

© 2019 Palo Alto Networks, Inc.

Commit and Push (コミットしてプッシュ) の実行がサポートされる間は、エンタープライズ *DLP* 設定の変更は推奨されません。また、プッシュ スコープの選択で影響を受けるテンプレートとマネージド ファイアウォールを手動で選択する必要があります。

1. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、設定変更を **Commit**（コミット）します。
2. **Commit**（コミット）> **Push to Devices**（デバイスへのプッシュ）の順に選択し、**Edit Selections**（選択内容の編集）を行います。
3. **Device Groups** (デバイス グループ) を選択して、（ **Include Device and Network Templates** ネットワークのテンプレートを含める) を実行します。
4. **OK** をクリックします。
5. 設定の変更をマネージドファイアウォールに **Push** (プッシュ) します。

エンタープライズ データ漏洩防止 (DLP) の有効化

これらの手順を実行して、エンタープライズデータ漏洩防止 (DLP) を正常に利用するようにマネージドファイアウォールを設定します。

STEP 1 | Panorama Web インターフェースにログインします。

STEP 2 | (ハードウェア ファイアウォールのみ) サービス ルートを作成して、ファイアウォールがインターネットに接続できるようにします。

これらのファイアウォール プラットフォームでエンタープライズ DLP を正常に利用するには、サービス ルートを設定する必要があります。

PAN-OS 10.0 以降のリリースを実行するすべてのサポートされている ファイアウォールモデルにサービス ルートを作成します。

1. **Device** (デバイス) > **Setup** (セットアップ) > **Services** (サービス) を選択し、エンタープライズ DLP 設定を含むテンプレートを選択する
2. **Service Features** (サービス機能) 内の **Service Route Configuration** (サービス ルート設定) をクリックし、**Customize** (カスタマイズ) を選択します。
3. **Dataplane** (データプレーン) をクリックして、**Source Interface** (送信元インターフェース) と **Source Address** (送信元インターフェイス) を設定します。

   送信元インターフェースにはインターネット接続が必要です。送信元インターフェースとアドレスの作成の詳細情報については、Configure Interfaces (インターフェースの設定) と Create an Address Object (アドレス オブジェクトの作成) を参照してください。
4. **Dataplane** (データプレーン) を選択 (チェック) し、**OK** をクリックして、設定の変更を保存します。
5. **Device** (デバイス) > **Setup** (セットアップ) > **Content-ID** (コンテンツID) を選択し、**Service URL Setting** (サービス **URL** 設定) セクション内の **Public Cloud Server** (パブリッククラウド サーバー) FQDN をコピーします。
6. **Policies** (ポリシー) > **Security** (セキュリティ) を選択し、送信元インターフェースからパブリック クラウド サーバー FQDN へのトラフィックを許可する セキュリティ ポリシー ルールを **Add** (追加) します。

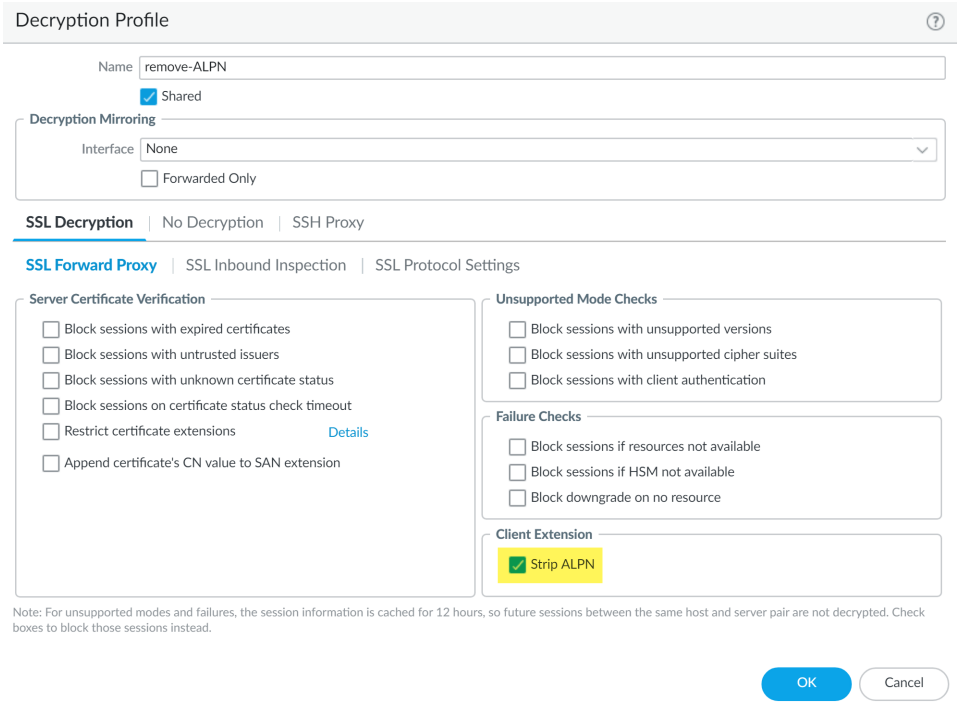
STEP 3 | 復号プロファイルを作成して、アプリケーションレイヤーアプロトコル ネゴシエーション (ALPN) ヘッダーをアップロード済みファイルから削除します。

エンタープライズ DLP は HTTP/1.1 をサポートします。デフォルトで、SharePointやOneDriveなど、一部のアプリケーションは、アップロード向けにHTTP/2をサポートしています。HTTP/2を使ってア

© 2019 Palo Alto Networks, Inc.

プリケーションからアップロードされたファイルと、エンタープライズ DLP との互換性を保つには、以下の手順に従ってください。

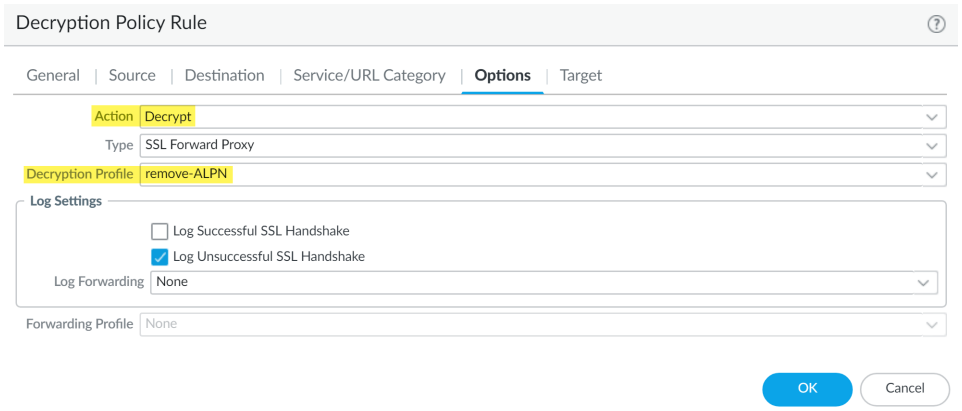
1. **Objects (オプション)** > **Decryption (復号化)** > **Decryption Profile (復号プロファイル)** を選択し、**Device Group (デバイス グループ)** を指定します。
2. 新しい復号化プロファイルを **Add (追加)**します。
3. 分かりやすい **Name** (名前) を入力します。
4. (任意) この復号プロファイルをすべてのデバイス グループで使用可能にするには、**Shared (共有)** を有効化 (チェック) します。
5. **SSL Decryption (SSL復号化)** > **SSL Forward Proxy (SSLフォワード プロキシ)** を選択して、**Client Extension (クライアント拡張)** 内の **Strip ALPN (ストリップ ALPN)** を有効化 (チェック) します。
6. **OK** をクリックして、設定の変更を保存します。



STEP 4 | アップロードされたファイルから ALPN ヘッダーを削除するポリシー ルールを作成します。

1. **Policies (ポリシー)** > **Decryption (復号化)** を選択し、**Device Group (デバイス グループ)** を指定します。
2. 必要に応じて新しい復号ポリシー ルールを**Add (追加)** して設定します。
3. **Options (オプション)**を選択します。
4. **Action (アクション)** に対して、**Decrypt (復号)** を選択します。
5. 作成した **Decryption Profile (復号プロファイル)** を選択します。
6. **OK** をクリックして、設定の変更を保存します。

© 2019 Palo Alto Networks, Inc.



STEP 5 | QUIC プロトコルを無効にし、ポート 80 と 443 上のトラフィックを拒否します。

Gmail など、Webアプリケーションの多くは、エンタープライズ DLP を正常に動作させるためにQUICプロトコルを無効にする必要があります。

1. **Policies** (ポリシー) > **Security** (セキュリティ) を選択し、**Device Group** (デバイス グループ) を指定します。
2. **quic** アプリケーションを使用するトラフィックを拒否するセキュリティポリシーを **Add** (追加) します。
3. **Objects** (オブジェクト) > **Services** (サービス)を選択して、**Device Group** (デバイス グループ) を指定します。
4. 2 つのサービスを **Add** (追加) します。1つは、ポート 80 のUDP、もう1つはポート 443 のUDPです。

   新しいバージョンのQUICは、**unknown-udp**と誤って識別されることがあります。このために、UDP ポート 80 および UDP ポート 443 向けのサービスを追加して、それらのポートへの UDP トラフィックを拒否するセキュリティポリシーを作成することを推奨します。
5. **Policies** (ポリシー) > **Security** (セキュリティ) を選択し、**Device Group** (デバイス グループ) を指定します。
6. UDP ポート 80 および 443 へのトラフィックを拒否するために作成した、サービスを含むセキュリティポリシー ルールを**Add** (追加) します。

   完了すると、2 つのセキュリティ ポリシーが作成され、1 つは QUIC プロトコルをブロックし、もう 1 つは UDP ポート 80 および 443 のトラフィックをブロックします。

STEP 6 | データ パターンの作成.

STEP 7 | データ フィルタリング プロファイルの作成.

STEP 8 | データフィルタリングプロファイルをセキュリティポリシー ルールにアタッチします。

新しいセキュリティ ポリシー ルールの作成に関する詳細情報は、Create a Security Policy Rule (セキュリティ ポリシー ルール) を参照してください。

Panorama 管理サーバーから旧 *PAN-OS* バージョンにダウングレードするには、セキュリティ ポリシー ルールで参照されているすべてのエンタープライズ *DLP* データ パターンとデータ フィルタリング プロファイルを削除する必要があります。エンタープライズ *DLP* データ パターンとフィルタリング プロファイルを参照するポリシー ルールを作成および整理するときは、こちらを考慮してください。

例えば、エンタープライズ *DLP* データ パターンとフィルタリング プロファイルのレファレンスを含んだすべてのセキュリティ ポリシー ルールを含むデバイス グループを

© 2019 Palo Alto Networks, Inc.

作成するとします。これにより、*Panorama PAN-OS* バージョンをダウングレードする必要がある場合に、関連するポリシー ルールをすばやく変更できます。

1. **Policies (ポリシー)** > **Security (セキュリティ)** > **Pre Rules (プレ ルール)** を選択し、**Device Group (デバイス グループ)** を指定します。
2. データ フィルタリング プロファイル に追加したいセキュリティ ポリシー ルールを選択します。
3. **Actions**（アクション）を選択して **Profile Type (プロファイル タイプ)** を **Profiles (プロファイル)** に設定します。
4. 作成した **Data Filtering (データ フィルタリング)** プロファイルを選択します。
5. **OK** をクリックして、設定の変更を保存します。

STEP 9 | コミットを実行し、設定の変更内容をエンタープライズ DLP を利用するマネージド ファイアウォールへの設定の変更にプッシュします。

Commit and Push (コミットしてプッシュ) の実行がサポートされる間は、エンタープライズ *DLP* 設定の変更は推奨されません。また、プッシュ スコープの選択で影響を受けるテンプレートとマネージド ファイアウォールを手動で選択する必要があります。

1. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、設定変更を **Commit**（コミット）します。
2. **Commit**（コミット）> **Push to Devices**（デバイスへのプッシュ）の順に選択し、**Edit Selections**（選択内容の編集）を行います。
3. **Device Groups (デバイス グループ)** を選択して、（ **Include Device and Network Templates** ネットワークのテンプレートを含める) を実行します。
4. **OK** をクリックします。
5. 設定の変更をマネージドファイアウォールに **Push (プッシュ)** します。

エンタープライズ データ消失防止 (DLP) のログ詳細を見る

マネージドファイアウォールがファイルのアップロード時に機密コンテンツを検出し、Alert（アラート）またはBlock（ブロック）アクションを作成している場合、データ フィルタリング ログが生成されます。検出したトラフィックの詳細なログ データをフィルタリングし、ポリシー ルール情報、トラフィックの送信元と宛先、関連のあるデータ パターンのデータ プロファイルなどを表示することが可能です。さらに、詳細ログ ビューには、トラフィックが一致した特定のデータ パターンが表示され、データ パターンが一致した一意の合計発生数と合計発生数が表示されます。詳細ログの表示は Panorama でのみ使用可能です。

マネージドファイアウォールがファイルのアップロード時に機密コンテンツを検出し、Alert（アラート）またはBlock（ブロック）アクションを作成している場合、ログが生成されます。その後Data Filtering（データフィルタリング）ログから、スニペットと呼ばれる機密コンテンツを参照することができます。スニペットは、パターンマッチングに関連する証拠または識別可能な情報となります。たとえば、クレジットカード番号のデータパターンを指定した場合、マネージドファイアウォールはユーザーの社会保障番号を一致したスニペットとして返します。デフォルトでは、マネージドファイアウォールはスニペットを返します。

マネージドファイアウォールはデータマスキングを使って、スニペット内のデータをマスクします。デフォルトでは、データ フィルタリング ログでは、値の下4桁が平文で表示されます（一部マスキング）。たとえば、データ フィルタリング ログには、クレジットカード番号のスニペットが`XXXX-XXXX-XXXX-1234`のように表示されます。データ全体を平文で表示するように指定したり、データを完全にマスキングして、すべての値を非表示にするように指定したりできます。

ファイルのスニペットも含め、DLP固有のログを表示するには、以下の手順に従ってください。

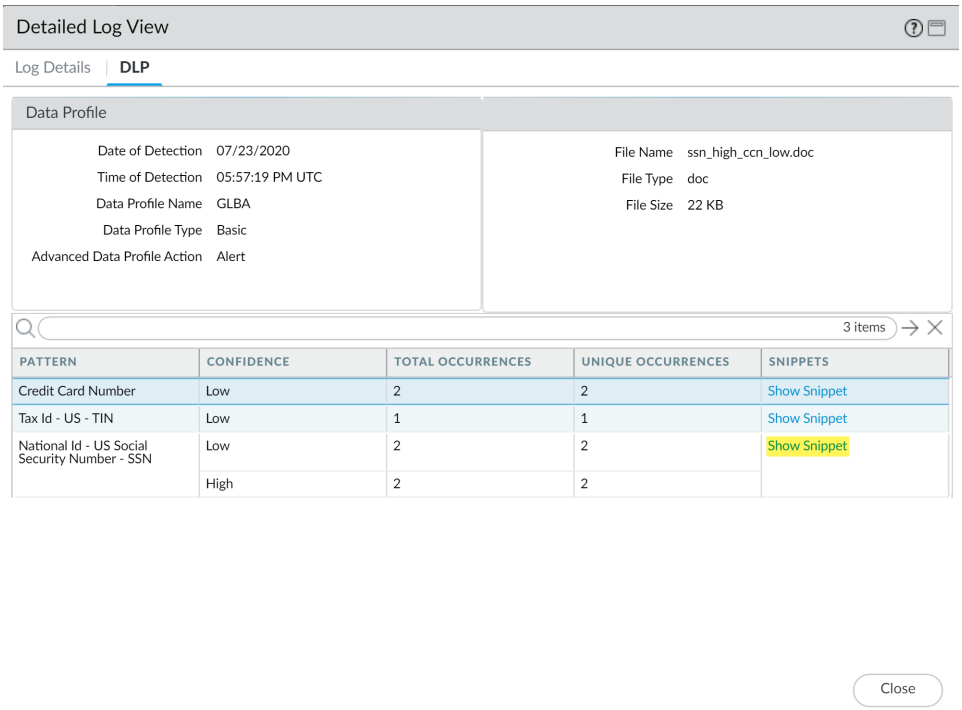
STEP 1 | エンタープライズ データ漏洩防止 (DLP) の有効化 .

© 2019 Palo Alto Networks, Inc.

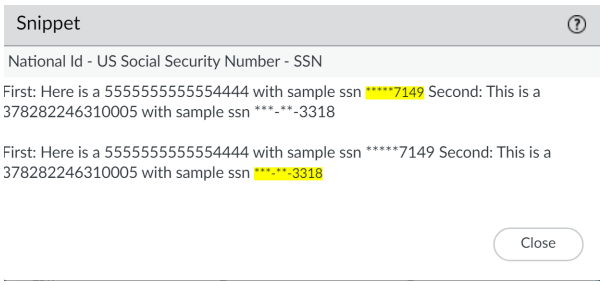
STEP 2 | **Monitor (監視) > Logs (ログ) > Data Filtering (データ フィルタリング)** の順に選択し、`( subtype eq dlp )` と入力することでデータ フィルタリング ログを**Filter (フィルタ)**します。

STEP 3 | ファイル スニペットを含めて、ファイルに関する詳細情報を表示します。

1. 詳細を表示するには、特定のログエントリの左側の拡大鏡 ( ) をクリックします。
2. **DLP** を選択して、パターン詳細を表示します。
3. 特定のデータ パターンに一致したデータのスニペットを表示するには、**Show Snippet (スニペットを表示)** を選択します。



4. マスクされたスニペットを確認して、検出されたデータを理解します。



既存のデータ パターンの有効化とプロファイルのフィルタリングの有効化

エンタープライズ データ漏洩防止 (DLP) プラグインを正常にインストールすると、既存のデータ パターンとフィルタリング プロファイルは表示されなくなりますが、セキュリティ ポリシー ルールで参照できます。DLP プラグインのインストール後に編集する必要のある、既存の データ フィルタリング パターンと設定済みのプロファイルがある場合は、Panorama Web インターフェース内でそれらをもう一度表示させることができます。

© 2019 Palo Alto Networks, Inc.

STEP 1 | Panorama CLI へのログインを行います。

STEP 2 | 既存のデータ パターンの有効化とプロファイルのフィルタリングを有効化します。

```
admin> request plugins dlp hide-old-config no
```

Panorama は `pass`（合格）を返し、データ パターンとフィルタリング プロファイルが現在表示されていることを確認します。

既存のデータ パターンとフィルタリング プロファイルを表示しないようにするには、次のコマンドを入力します。

```
admin> request plugins dlp hide-old-config yes
```

STEP 3 | Panorama Web インターフェースにログインします。

STEP 4 | 既存のデータ パターンの有効化とプロファイルのフィルタリングを編集します。

1. **Objects (オブジェクト)** > **Custom Objects (カスタム オブジェクト)** > **Data Patterns (データ パターン)** を選択してデータ パターンを編集します。
2. **Objects (オブジェクト)** > **Security Profiles (セキュリティ プロファイル)** > **Data Filtering (データ フィルタリング)** を選択し、データ フィルタリング プロファイルを編集します。

STEP 5 | **Policies (プロファイル)** > **Security (セキュリティ)** を選択し、**Device Group (デバイス グループ)** を選択して、必要に応じてセキュリティ ポリシー ルール を変更します。

STEP 6 | コミットを実行し、設定の変更内容をエンタープライズ DLP を利用するマネージド ファイアウォールへの設定にプッシュします。

Commit and Push (コミットしてプッシュ) の実行がサポートされる間は、エンタープライズ *DLP* 設定の変更は推奨されません。また、プッシュ スコープの選択で影響を受けるテンプレートとマネージド ファイアウォールを手動で選択する必要があります。

1. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、設定変更を **Commit**（コミット）します。
2. **Commit**（コミット）> **Push to Devices**（デバイスへのプッシュ）の順に選択し、**Edit Selections**（選択内容の編集）を行います。
3. **Device Groups (デバイス グループ)** を選択して、（ **Include Device and Network Templates** ネットワークのテンプレートを含める) を実行します。
4. **OK** をクリックします。
5. 設定の変更をマネージドファイアウォールに **Push (プッシュ)** します。

エンタープライズ データ消失防止 (DLP) の設定の編集

エンタープライズ データ消失防止 (DLP) の設定を編集して、ファイル スキャンのクラウド コンテンツ設定を編集し、データ フィルタリング設定を設定し、DLP スニペットでマスクされる機密データの量を設定します。

- クラウド コンテンツの設定の編集
- エンタープライズ データ消失防止 (DLP) のデータ フィルタリング設定の編集
- エンタープライズ データ消失防止 (DLP) のスニペット設定の編集

© 2019 Palo Alto Networks, Inc.

クラウド コンテンツの設定の編集

デフォルトでは、クローゼットのクラウドサービス サーバーに自動的に解決され、エンタープライズ DLP ファイルがスキャンされるエンタープライズ データ損失防止 (DLP) は完全修飾ドメイン名(FQDN) で設定されます。特定のデータ常駐要件がある場合は、クラウド コンテンツの FQDN を編集して、スキャン用にエンタープライズ データ損失防止 (DLP) ファイルを送信することにより、地域のクラウド サービス サーバーを指定できます。

STEP 1 | Panorama Web インターフェースにログインします。

STEP 2 | **Device (デバイス) > Setup (セットアップ) > Content-ID** を選択し、エンタープライズ DLP を活用するマネージドファイアウォールと関連する **Template (テンプレート)** を選択します。

STEP 3 | クラウド コンテンツ FQDN を編集します。

1. **Cloud Content Settings (クラウド コンテンツの設定)** を編集します。
2. データ常駐要件に基づいて、**Public Cloud Server (パブリック クラウド サーバー)** を変更します。
   - **APAC (アジア太平洋地域)**—`apac.hawkeye.services-edge.paloaltonetworks.com`
   - **Europe (欧州)**—`eu.hawkeye.services-edge.paloaltonetworks.com`
   - **United States (米国)**—`us.hawkeye.services-edge.paloaltonetworks.com`
3. **OK** をクリックして、設定の変更を保存します。

STEP 4 | コミットを実行し、設定の変更内容をエンタープライズ DLP を活用するマネージド ファイアウォールへの設定の変更にプッシュします。

Commit and Push (コミットしてプッシュ) の実行がサポートされる間は、エンタープライズ *DLP* 設定の変更は推奨されません。また、プッシュ スコープの選択で影響を受けるテンプレートとマネージド ファイアウォールを手動で選択する必要があります。

1. **Commit (コミット) > Commit to Panorama (Panorama へのコミット)** の順に選択し、設定変更を **Commit (コミット)** します。
2. **Commit (コミット) > Push to Devices (デバイスへのプッシュ)** の順に選択し、**Edit Selections (選択内容の編集)** を行います。
3. **Device Groups (デバイス グループ)** を選択して、(**Include Device and Network Templates** ネットワークのテンプレートを含める) を実行します。
4. **OK** をクリックします。
5. 設定の変更をマネージドファイアウォールに **Push (プッシュ)** します。

エンタープライズ データ消失防止 *(DLP)* のデータ フィルタリング設定の編集

エンタープライズ データ損失防止(DLP) クラウドサービスにスキャンされるファイルのネットワーク設定を構成し、エンタープライズ DLP を利用するファイアウォールが実行するアクションを指定します。

STEP 1 | Panorama Web インターフェースにログインします。

STEP 2 | **Device (デバイス) > Setup (セットアップ) > DLP** を選択し、エンタープライズ DLP を活用するマネージドファイアウォールと関連する **Template (テンプレート)** を選択します。

STEP 3 | データフィルタリング設定を編集する

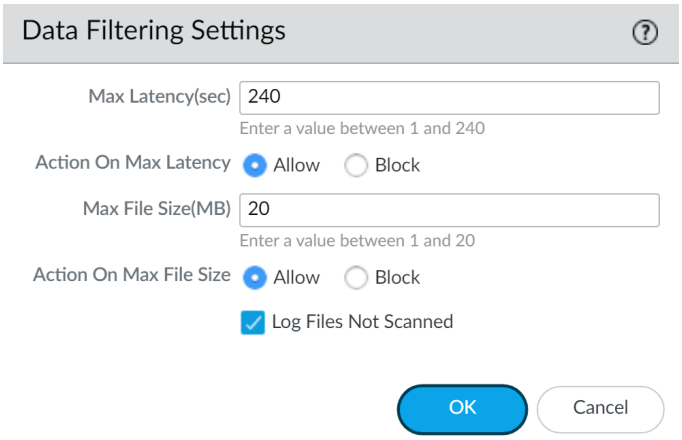
1. ファイアウォールによって実行されるアクションのファイルアップロード用の **Max Latency (sec) (最大遅延 (秒))** を指定します。

© 2019 Palo Alto Networks, Inc.

2. DLP クラウド サービスに保存するためにスキャンされたファイルが、設定されたMax Latency (最大遅延)に達したときに、ファイアウォールが取る Action on Max Latency (最大遅延でのアクション) を (Block (ブロック) または Allow (許可)) に指定します。

   Block (ブロック) の選択は、ファイルをブロックするように設定された エンタープライズ DLP データ フィルタリング プロファイルにのみ適用されます。この設定は、機密データを含むトラフィックがスキャンされたときにアラートを出すように設定されたエンタープライズ *DLP* フィルタリング プロファイルに影響を与えません。
3. **Max File Size (最大ファイルサイズ) (MB)** を指定して、DLP クラウド サービスに保存されるファイルの最大ファイル サイズを適用します。
4. DLP クラウド サービス用にスキャンされたファイルが、設定されたMax File Size (最大ファイルサイズ)に達したときに、ファイアウォールが取る Action on Max File Size (最大ファイルサイズでのアクション) を (Block (ブロック) または Allow (許可)) に指定します。

   Block (ブロック) の選択は、ファイルをブロックするように設定された エンタープライズ DLP データ フィルタリング プロファイルにのみ適用されます。この設定は、機密データを含むトラフィックがスキャンされたときにアラートを出すように設定されたエンタープライズ *DLP* フィルタリング プロファイルに影響を与えません。
5. **Log Files Not Scanned (ログ ファイル未スキャン)** をチェック (有効化) すると、ファイルを DLP クラウドサービスにスキャンできない場合、データ フィルタリング ログにアラートを生成します。
6. **OK** をクリックして、設定の変更を保存します。



STEP 4 | コミットを実行し、設定の変更内容をエンタープライズ DLP を活用するマネージド ファイアウォールへの設定の変更にプッシュします。

Commit and Push (コミットしてプッシュ) の実行がサポートされる間は、エンタープライズ *DLP* 設定の変更は推奨されません。また、プッシュ スコープの選択で影響を受けるテンプレートとマネージド ファイアウォールを手動で選択する必要があります。

1. **Commit** (コミット) > **Commit to Panorama** (**Panorama** へのコミット) の順に選択し、設定変更を **Commit** (コミット) します。
2. **Commit** (コミット) > **Push to Devices** (デバイスへのプッシュ) の順に選択し、**Edit Selections** (選択内容の編集) を行います。
3. **Device Groups (デバイス グループ)** を選択して、 (**Include Device and Network Templates** ネットワークのテンプレートを含める) を実行します。
4. **OK** をクリックします。
5. 設定の変更をマネージドファイアウォールに **Push (プッシュ)** します。

© 2019 Palo Alto Networks, Inc.

エンタープライズ データ消失防止 (DLP) のスニペット設定の編集

ファイアウォールが DLP クラウド サービス内のエンタープライズ DLP データ パターンに一致する機密データのスニペットを保存するように設定し、また、保存されている場合、機密データをマスクする方法を設定します。

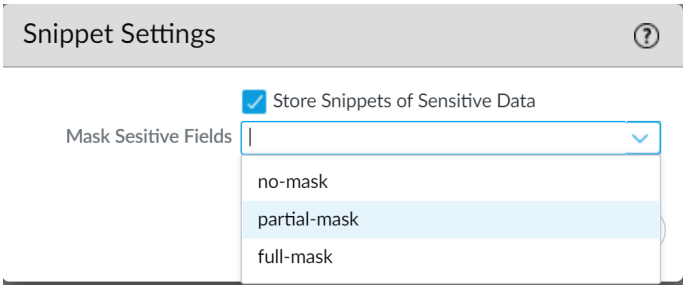
STEP 1 | Panorama Web インターフェースにログインします。

STEP 2 | **Panorama** > **DLP** > **Configuration** (設定) を選択し、スニペット設定を編集します。

STEP 3 | **Store Snippets of Sensitive Data** (機密データのスニペットを保存) をチェック (有効化) して、DLP クラウド サービス内の エンタープライズ DLP データ パターン に一致する機密データのスニペットを保存します。

STEP 4 | DLP クラウド サービス内の保存用に、**Mask Sensitive Field** (機密フィールドのマスク化) 方法を設定します。

- **no-mask** (マスクなし) – 一致した機密データ スニペットは、DLP クラウド サービスに保存されたときにマスクされず、完全に表示されます。
- **partial-mask** (一部をマスク) – 一致した機密データ スニペットは部分的にマスクされ、DLP クラウドサービスに保存されると 4 文字のみが表示されます。
- **full-mask** (完全マスク) – 一致した機密データ スニペットは、DLP クラウド サービスに保存されたときにすべてマスクされます。



STEP 5 | **OK** をクリックして、設定の変更を保存します。

STEP 6 | コミットを実行し、設定の変更内容をエンタープライズ DLP を活用するマネージド ファイアウォールへの設定の変更にプッシュします。

Commit and Push (コミットしてプッシュ) の実行がサポートされる間は、エンタープライズ *DLP* 設定の変更は推奨されません。また、プッシュ スコープの選択で影響を受けるテンプレートとマネージド ファイアウォールを手動で選択する必要があります。

1. **Commit** (コミット) > **Commit to Panorama** (**Panorama** へのコミット) の順に選択し、設定変更を **Commit** (コミット) します。
2. **Commit** (コミット) > **Push to Devices** (デバイスへのプッシュ) の順に選択し、**Edit Selections** (選択内容の編集) を行います。
3. **Device Groups** (デバイス グループ) を選択して、 (**Include Device and Network Templates** ネットワークのテンプレートを含める) を実行します。
4. **OK** をクリックします。
5. 設定の変更をマネージドファイアウォールに **Push** (プッシュ) します。

© 2019 Palo Alto Networks, Inc.

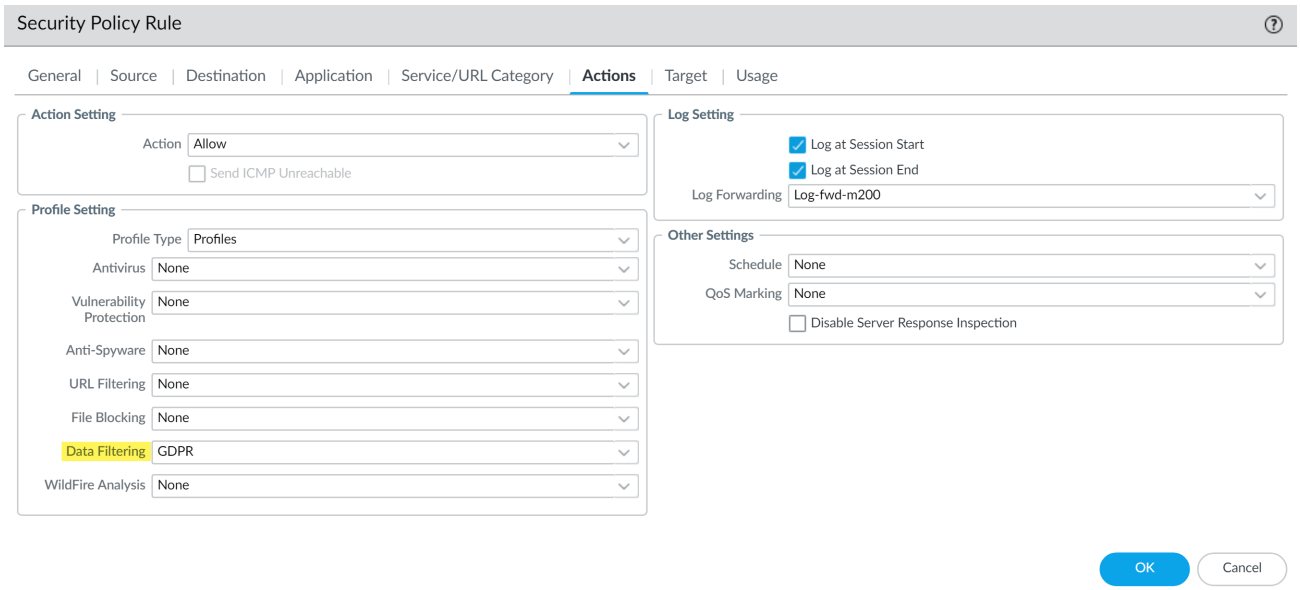
エンタープライズ データ消失防止 (DLP) プラグインのアンインストール

エンタープライズ データ損失防止 (DLP) プラグインをアンインストールするには、Panorama™ 管理サーバーとマネージドファイアウォールのプラグインをアンインストールが可能になる前に、すべてのセキュリティ ポリシー ルールからすべてのエンタープライズ データ損失防止 (DLP) データ フィルタリング プロファイルのリファレンスを削除する必要があります。プラグインを正常にアンインストールした後は、Panorama とマネージドファイアウォールのダウングレードを続行することができます。

STEP 1 | Panorama Web インターフェースにログインします。

STEP 2 | **Policies (ポリシー)** > **Security (セキュリティ)** を選択し、セキュリティ ポリシー ルールからすべてのエンタープライズ DLP データ フィルタリング プロファイルを削除します。

このステップは、エンタープライズ DLP プラグインをアンインストールするために必要です。



STEP 3 | コミットを実行し、設定の変更内容をエンタープライズ DLP を活用するマネージド ファイアウォールへの設定の変更にプッシュします。

Commit and Push (コミットしてプッシュ) の実行がサポートされる間は、エンタープライズ *DLP* 設定の変更は推奨されません。また、プッシュ スコープの選択で影響を受けるテンプレートとマネージド ファイアウォールを手動で選択する必要があります。

1. **Commit** (コミット) > **Commit to Panorama** (**Panorama** へのコミット) の順に選択し、設定変更を **Commit** (コミット) します。
2. **Commit** (コミット) > **Push to Devices** (デバイスへのプッシュ) の順に選択し、**Edit Selections** (選択内容の編集) を行います。
3. **Device Groups (デバイス グループ)** を選択して、(**Include Device and Network Templates** ネットワークのテンプレートを含める) を実行します。
4. **OK** をクリックします。
5. 設定の変更をマネージドファイアウォールに **Push (プッシュ)** します。

STEP 4 | マネージドファイアウォールからエンタープライズ DLP プラグインをアンインストールします。

© 2019 Palo Alto Networks, Inc.

1. マネージドファイアウォール CLI にアクセスします。
2. 次のコマンドを使用してエンタープライズ DLP プラグインをアンインストールします。

```
admin> request plugins uninstall dlp
```

   エンタープライズ DLP プラグインのアンインストールを確定する時は、**y** を入力します。

STEP 5 | Panorama から DLP プラグインをアンインストールします。

1. Panorama Web インターフェースにログインします。
2. **Panorama** > **Plugins (プラグイン)** を選択し、エンタープライズ DLP プラグインを **Uninstall (アンインストール)** します。

STEP 6 | コミットを実行し、設定の変更内容をエンタープライズ DLP を活用するマネージド ファイアウォールへの設定の変更にプッシュします。

Commit and Push (コミットしてプッシュ) の実行がサポートされる間は、エンタープライズ *DLP* 設定の変更は推奨されません。また、プッシュ スコープの選択で影響を受けるテンプレートとマネージド ファイアウォールを手動で選択する必要があります。

1. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、設定変更を **Commit**（コミット）します。
2. **Commit**（コミット）> **Push to Devices**（デバイスへのプッシュ）の順に選択し、**Edit Selections**（選択内容の編集）を行います。
3. **Device Groups (デバイス グループ)** を選択して、（ **Include Device and Network Templates** ネットワークのテンプレートを含める) を実行します。
4. **OK** をクリックします。
5. 設定の変更をマネージドファイアウォールに **Push (プッシュ)** します。

© 2019 Palo Alto Networks, Inc.

データをマネージドファイアウォールに再配信する

すべてのファイアウォールがポリシーを適用し、ポリシー ルールに必要なデータと認証タイムスタンプを含むレポートを生成することを確認するために、Panorama インフラストラクチャを活用して、マッピングとタイムスタンプを再配信できます。

- データを再配信するように Panorama 管理サーバーを設定します。
  1. ファイアウォール、仮想システムまたは Windows User-ID エージェントを再配信エージェントとして Panorama に追加します。
     1. **Panorama** > **Data Redistribution** (データ再配信)の順に選択し、各再配信ポイントを **Add**（追加）します。
     2. 再配信エージェントを識別するための **Name**（名前）を入力します。
     3. エージェントが **Enabled** (有効) になっていることを確認します。
     4. ファイアウォールの MGT インターフェイスの **Host**（ホスト）名または IP アドレスを入力します。
     5. ファイアウォールがデータ再配信のクエリを受け付ける **Port**（ポート）番号を入力します（デフォルトは 5007）。
     6. 再配信エージェントがファイアウォールまたは仮想システムである場合は、**Collector Name**（コレクタ名）と **Collector Pre-Shared Key**（コレクタの事前共有鍵）を入力します。
     7. 再配信する **Data type** (データ タイプ) を選択します。すべてのデータ タイプを選択できますが、次のデータ タイプの少なくとも 1 つを選択する必要があります。
        - **IP User Mappings** (IP ユーザー マッピング)
        - **IP Tags** (IP タグ)
        - **User Tags** (ユーザー タグ)
        - **HIP**
        - **Quarantine List** (検疫リスト)
     8. **OK** をクリックして設定を保存します。
  2. Panorama の MGT インターフェイスが、ファイアウォールからのデータ再配信クエリに応答できるようにします。

     Pnorama 管理サーバーが高可用性（*HA*）構成である場合は、各 *HA* ピアでこの手順を実行し、*Panorama* がフェイルオーバーしても再配信が継続できるようにすることをお薦めします。

     1. **Panorama** > **Setup**（セットアップ）> **Interfaces**（インターフェイス）の順に選択し、**Management**（管理）を選択します。
     2. Network Services（ネットワーク サービス）セクションで **User-ID**（ユーザー **ID**）を選択し、**OK** をクリックします。
  3. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を Panorama で有効にします。

- Panorama が再配信するデータを受信するために、ファイアウォールを設定します。
  1. **Device** (デバイス) > **Data Redistribution** (データの再配信) > **Agents** (エージェント) を選択してから、ファイアウォールが割り当てられる **Template** (テンプレート) を選択します。
  2. エージェントを **Add** (追加) し、**Name** (名前)を入力します。
  3. エージェントの追加方法を選択します。

© 2019 Palo Alto Networks, Inc.

- **Serial Number (シリアル番号)**—リストから使用する Panorama の**Serial Number (シリアル番号)** を選択します。
  - **panorama**—アクティブまたは単独の Panorama
  - **panorama2**—(HA のみ) パッシブ Panorama
- **Host and Port (ホストとポート)**—以下の情報を指定します。
  - ファイアウォールの MGT インターフェイスの **Host**（ホスト）名または IP アドレスを選択します。
  - ホストが **LDAP Proxy (LDAP プロキシ)** であるかどうかを選択します。
  - ファイアウォールがデータ再配信のクエリを受け付ける **Port**（ポート）番号を入力します（デフォルトは 5007）。
  - 再配信エージェントがファイアウォールまたは仮想システムである場合は、**Collector Name**（コレクタ名）と **Collector Pre-Shared Key**（コレクタの事前共有鍵）を入力します。
  - 再配信する **Data type (データ タイプ)** を選択します。

4. エージェントが **Enabled (有効)** であることを確認して、**OK** をクリックして設定を保存します。
5. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）を選択し、Panorama で変更を有効にしてファイアウォールにプッシュします。

- Panorama、ファイアウォールが、再配信されたデータを受信することを確認します。
  1. エージェントの統計 (**Panorama** > **Data Redistribution (データ再配信)** > **Agents (エージェント)**)を表示し 、**Status (ステータス)**を選択すると、クライアントのファイアウォールが受信したマッピングの数など、再配信エージェントのアクティビティの概要が表示されます。
  2. ファイアウォールが再配信エージェントからマッピングを受信したことを検証するには、User-ID ログ (**Monitor (監視)** > **Logs (ログ)** > **User-ID**) で**Source Name (ソース名)** を確認します。
  3. クライアント ファイアウォールがデータを受信していることを確認するには、IP-Tag ログ (**Monitor** > **Logs** > **IP-Tag**) を表示します。
  4. Access the CLI（CLI へのアクセス）に従い、データを再配信するファイアウォール、Panorama 管理サーバーの CLI にアクセスします。
  5. 以下のコマンドを入力し、すべてのユーザー マッピングを表示します。

```
> show user ip-user-mapping all
```

  6. 1 つのユーザー名に関連する IP アドレスを記録します。
  7. 再配信されるデータを受信するファイアウォールまたは Panorama 管理サーバーの CLI にアクセスします。
  8. 記録した *<IP-address>* のマッピング情報と認証タイムスタンプを表示します。

```
> show user ip-user-mapping ip <IP-address>
IP address:     192.0.2.0 (vsys1)
User:           corpdomain\username1
From:           UIA
Idle Timeout:   10229s
Max. TTL:       10229s
MFA Timestamp: first(1) - 2016/12/09 08:35:04
Group(s):       corpdomain\groupname(621)
```



この出力例では、認証要求（要因）に対する応答のタイムスタンプが表示されています。多要素認証（MFA）を使用する認証ルールでは、複数のタイムスタンプが出力に表示されます。

© 2019 Palo Alto Networks, Inc.

ファイアウォールを Panorama 管理に移行

これまで Palo Alto Networks ファイアウォールを導入し、ローカルに設定していて、新たに Panorama を使用した一元管理を行う場合、移行前の計画を行う必要があります。この移行作業には、ファイアウォールの設定を Panorama にインポートし、移動後にファイアウォールが適切に機能していることを確認する作業が含まれます。個々のファイアウォールに固有の設定がある場合、継続してそのファイアウォールにアクセスして固有の設定を管理することができます。Panorama から値をプッシュする、あるいはファイアウォールのローカルで設定を行うことによってあらゆるファイアウォールの設定を管理できますが、Panorama およびファイアウォールの両方を通して設定を管理することはできません。特定のファイアウォールの設定を Panorama 管理から除外する場合は次のいずれかが可能です。

- ファイアウォールの設定全体を移行してから、ファイアウォールのローカルで管理したい設定を Panorama で削除します。また、Panorama の設定を削除する代わりに、Panorama がファイアウォールにプッシュするテンプレート設定のオーバーライドを行うこともできます。
- Panorama を使用して管理する設定だけを含んだファイアウォールの一部の設定を読み込みます。



Panorama 管理に移行する際、ファイアウォールのログは無くなりません。

- Panorama 管理への変更を計画
- ファイアウォールを Panorama 管理に移行
- ファイアウォール HA ペアを Panorama 管理に移行
- ファイアウォールの設定の一部を Panorama に読み込む

Panorama 管理への変更を計画

次のタスクは、ファイアウォールをPanorama管理に移行する際に必要な計画を高レベルにまとめたものです。

- ☐ 移行するファイアウォールを決定します。
- ☐ メンテナンス時間枠を計画し、Panorama またはファイアウォールで保留中の設定変更がないことを確認します。
- ☐ 移行する前に、既知の動作中の Panorama とファイアウォール設定を保持します。
  - ファイアウォールのデバイスのステータスをエクスポートします。
  - Panorama 設定を実行中の 名前付きの Panorama 設定スナップショットをエクスポートします。
- ☐ Panoramaおよびファイアウォールのソフトウェア、コンテンツ バージョン、を行う方法を決定します。重要な詳細事項についてはPanorama、ログ コレクタ、ファイアウォール、および WildFire のバージョン互換性を参照してください。
- ☐ Panorama のデプロイ計画URL フィルタリング データベース (BrightCloud あるいは PAN-DB) 、ログ収集、管理ロールについて。
- ☐ 共通設定を管理する方法を計画します。

  冗長性を抑え、すべてのファイアウォールあるいは一連のファイアウォールで共有する設定を合理的に管理できるようなデバイス グループ階層、テンプレートおよびテンプレート スタックを計画します。移行の際、次の例外を除き、ファイアウォールの共有領域からオブジェクトを Panorama の Shared (共有) にインポートするかどうかを選択できます。

  - 共有ファイアウォール オブジェクトの名前と値が既存の共有 Panorama オブジェクトと同じである場合、インポートではそのファイアウォール オブジェクトは除外されます。
  - 共有ファイアウォール オブジェクトの名前または値が既存の共有 Panorama オブジェクトと異なる場合、Panorama はインポート用に新しく作成された各デバイス グループにそのファイアウォール オブジェクトをインポートします。

© 2019 Palo Alto Networks, Inc.

- テンプレートにインポートされた設定が共有ファイアウォール オブジェクトを参照する、あるいはテンプレートにインポートされた設定を共有ファイアウォール オブジェクトが参照する場合、**Import devices' shared objects into Panorama's shared context**（デバイスの共有オブジェクトを**Panorama**の共有コンテクストにインポート）するチェックボックスを選択するかどうかに関わらず、Panoramaはすべてのオブジェクトを共有オブジェクトとしてインポートします。

- Panoramaに同様の要素がすでに含まれている、あるいはその要素がファイアウォール固有（例えばタイムゾーンの設定）でありPanoramaを使用して管理を行わないためにインポートしたくない設定要素（ポリシー、オブジェクト、およびその他の設定）がファイアウォールにあるかどうか判断します。グローバル検索を実行し、Panoramaに類似の要素があるかどうか確認できます。
- デバイス グループごとに共通のゾーンを決定します。これには、各デバイス グループ内のファイアウォールと仮想システムに共通のゾーン名を命名する方法が含まれます。たとえば、支店 LAN と WAN というゾーンがある場合、Panorama は、ポート/メディア タイプ、モデル、論理アドレス スキーマの違いを意識せずに、それらのゾーンを参照するポリシー ルールをプッシュできます。
- 移行後のテスト計画を作成します。

  テスト計画を使用し、移行後もファイアウォールが効率よく稼働することを検証します。この計画には次のようなタスクが含まれる場合があります。

  - 移行後、少なくとも24時間ファイアウォールを監視する。
  - Panoramaおよびファイアウォールのログで異常の有無を監視する。
  - Panoramaへの管理者ログインをチェックする。
  - 複数のソースからの様々な種類のトラフィックをテストする。例えば、帯域幅のグラフ、セッション カウント、拒否ルールのトラフィック ログの項目をチェックします（Panorama を使用した可視化を参照）。このテストは、代表的なポリシー設定のサンプルに対して行う必要があります。
  - ユーザーが報告した問題があるかどうか、ネットワーク オペレーションセンター（NOC）およびセキュリティ オペレーションセンター（SOC）とともに確認します。
  - ファイアウォールの機能を検証する上で役立つその他のテスト指標をすべて盛り込みます。

ファイアウォールを Panorama 管理に移行

ファイアウォールの設定をインポートする際、Panorama は自動的にテンプレートを作成し、インポートしたネットワークおよびデバイスの設定を盛り込みます。インポートしたポリシーおよびオブジェクトを含めるために、Panorama は各ファイアウォールに対して単一のデバイス グループを、あるいはマルチ vsys ファイアウォールの各仮想システム（vsys）に対して単一のデバイス グループを自動的に作成します。

次の作業を行う際、Panorama がファイアウォールの設定全体をインポートします。あるいは、ファイアウォールの設定の一部を Panorama に読み込むこともできます。

Panorama は、*PAN-OS 5.0* 以降のリリースを実行するファイアウォールから設定をインポートしたり、設定をそれらのファイアウォールにプッシュ送信したりできます。例外として、*Panorama 6.1* 以降のリリースでは、*PAN-OS 6.0.0 ~ 6.0.3* を実行しているファイアウォールに設定をプッシュできません。

Panorama はすでに管理対象のデバイスになっているファイアウォールから設定をインポートできますが、これはまだデバイス グループあるいはテンプレートに割り当てられていない場合にのみ可能です。

STEP 1 | 移行計画を立てます。

Panorama管理への変更を計画のチェックリストをご覧ください。

STEP 2 | 管理対象デバイスとしてファイアウォールを追加します。

管理対象デバイスとしてのファイアウォールの追加を行います。

© 2019 Palo Alto Networks, Inc.

1. Panorama にログインし、**Panorama** > **Managed Devices** (管理対象デバイス) > **Summary** (サマリー) の順に選択し、**Add** (追加) をクリックします。
2. ファイアウォールのシリアル番号を入力して **OK** をクリックします。

   複数のファイアウォールの設定をインポートする場合、各シリアル番号を行を分けて入力します。任意で、*Microsoft Excel* のワークシートからシリアル番号をコピー & ペーストすることもできます。
3. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

STEP 3 | ファイアウォールから Panorama への接続を確立させます。

1. ファイアウォールにログインし、**Device**（デバイス）> **Setup**（セットアップ）の順に選択して Panorama 設定を編集します。
2. **Panorama Servers**（**Panorama** サーバー）フィールドに Panorama 管理サーバーの IP アドレスを入力します。
3. **OK**、**Commit** (コミット) の順にクリックします。

STEP 4 | ファイアウォール設定を Panorama にインポートします。



後でファイアウォールの設定を再度インポートする場合、まずは最初にファイアウォールデバイス グループと、それがメンバーになっているテンプレートを削除します。デバイス グループとテンプレートの名前がファイアウォールのホスト名と同じ場合、ファイアウォール構成を再インポートする前にデバイス グループとテンプレートを削除するか、*Device Group Name Prefix* (デバイス グループ名のプレフィックス) フィールドを使用して、再インポートして作成したデバイス グループとテンプレートの新しい名前を定義できます。さらに、ファイアウォールをデバイス グループまたはテンプレートから削除しても、ログが失われることはありません。

1. Panoramaで**Panorama** > **Setup** > **Operations** (Panorama > セットアップ > 操作)を選択し、**Import device configuration to Panorama** (Panoramaにデバイス設定をインポート)を選択してさらに**Device** (デバイス)を選択します。

   Panorama は、既存のデバイス グループあるいはテンプレートに割り当てられているファイアウォールから設定をインポートすることはできません。
2. (任意) **Template Name** (テンプレート名) を編集します。デフォルト値はファイアウォール名です。既存のテンプレートまたはテンプレート スタックの名前は使用できません。
3. （任意）**Device Group**（デバイス グループ）の名前を編集します。マルチ vsys ファイアウォールの場合、各デバイス グループにはデフォルトで vsys 名が付いているため、それぞれの Device Group Name Prefix（デバイス グループ名の接頭辞）となる文字列を追加します。そうでない場合、デフォルト値はファイアウォール名になります。既存のデバイス グループ名を使用することはできません。

   Import devices' shared objects into Panorama's shared context（デバイスの共有オブジェクトを *Panorama* の共有コンテクストにインポート）チェック ボックスはデフォルトでオンになっています。つまり、*Panorama* は、ファイアウォールの *Shared*（共有）領域に属するインポート オブジェクトを *Panorama* の *Shared*（共有）と比較します。インポートしたオブジェクトがファイアウォールの *Shared*（共有）コンテキストに存在しない場合、インポートする各デバイス グループに適用されます。このチェック ボックスをオフにすると、*Panorama* のコピーはインポートしたオブジェクトを比較せず、*Shared*（共有）ではなくすべての共有ファイアウォール オブジェクトをインポートするデバイス グループに適用します。これにより重複するオブジェクトが生成される可能性があるため、大抵の場合はチェック ボックスをオンにしておくことが推奨されます。共有あるいは重複オブジェクトを *Panorama* に

© 2019 Palo Alto Networks, Inc.

インポートするとどうなるのかということについては「共通設定を管理する方法を計画」をご覧ください。

4. インポートされたポリシールールの**Rule Import Location** (ルールのインポート先)を次の中から選択します。**Pre Rulebase** (プレ ルールベース)あるいは**Post Rulebase** (ポスト ルールベース)。選択内容に関係なく、Panorama はデフォルトのセキュリティ ルール (intrazone-default および interzone-default) をポスト ルールベースにインポートします。

   Panorama に、インポートするファイアウォール ルールと同じ名前のルールがある場合、*Panorama* には両方のルールが表示されます。*Panorama* でコミットを実行する前にいずれかのルールを削除し、コミットが失敗しないようにします。

5. **OK** をクリックします。インポートのステータス、結果、選択内容の詳細、インポートされた項目の詳細、警告が Panorama に表示されます。**Close** (閉じる) をクリックします。
6. **Commit** (コミット) > **Commit to Panorama** (**Panorama** へのコミット) の順に選択し、変更を **Commit** (コミット) します。

STEP 5 | Panorama から新しく追加されたデバイスに構成をプッシュします。

ルール名またはオブジェクト名の重複を防ぐには、デバイス グループ設定を Panorama からファイアウォールにプッシュして、コミットエラーを回避します。

この手順は、ファイアウォール管理を *Panorama* 管理サーバーに正常に移行するために必要です。この手順に失敗すると、構成エラーおよびコミットエラーが発生します。

1. **Panorama** > **Setup (セットアップ)** > **Operations (操作)** の順に選択し、**Export or push device config bundle (デバイス設定バンドルをエクスポートあるいはプッシュ)** をクリックします。Panorama Web インターフェイスへのログイン
2. **Export or push device config bundle (デバイス設定バンドルをエクスポートあるいはプッシュ)** をクリックし、ドロップダウンメニューから **Device (デバイス)** を選択して **OK** をクリックします。
3. 設定のインポート元である**Device** (デバイス)を選択し、**OK**、次に**Push & Commit** (プッシュしてコミット)をクリックします。Panorama がバンドルをプッシュし、ファイアウォール上でのコミットを開始します。
4. プッシュが正常にコミットされたら **Close (閉じる)** をクリックします。
5. ファイアウォールの Web インターフェイスを起動 し、構成が正常にコミットされたことを確認します。確認できない場合は、ファイアウォールで変更をローカルに **Commit (コミット)** します。
6. Panorama Web インターフェイスで、**Panorama** > **Managed Devices (管理対象デバイス)** > **summary (サマリー)** の順に選択し、デバイス グループとテンプレート スタックがパッシブ ファイアウォールと同期されていることを確認します。パッシブ ファイアウォールのポリシー ルール、オブジェクト、ネットワーク設定がアクティブ ファイアウォールに一致することを確認します。ファイアウォールの Web インターフェイスで、設定オブジェクトが緑の歯車 (.) を表示していることを確認します。これは、設定オブジェクトが Panorama からプッシュされたことを示します。
7. **Commit** (コミット) > **Commit to Panorama** (**Panorama** へのコミット) の順に選択し、変更を **Commit** (コミット) します。

STEP 6 | インポートされた設定の微調整を行います。

1. Panorama で**Panorama** > **Config Audit** (Panorama > 設定監査)を選択し、**Running config** (実行中の設定)および比較対象の**Candidate config** (候補設定)を選択し、**Go** (実行)をクリックして結果を確認します。
2. 設定監査、およびインポート後に Panorama が表示した警告に従って必要に応じてデバイス グループおよびテンプレートの設定を更新します。以下に例を示します。
   - 冗長なオブジェクトおよびポリシー ルールを削除します。
   - ポリシー ルールあるいはオブジェクトを別のデバイス グループに移動/コピーします。
   - ファイアウォールを別のデバイス グループあるいはテンプレートに移動させます。

© 2019 Palo Alto Networks, Inc.

- インポート時にPanoramaが作成したデバイスグループを別の親デバイスグループに移動させます。**Panorama** > **Device Groups** (Panorama > デバイスグループ)を選択し、移動させるデバイスグループを選択し、さらに新しい**Parent Device Group** (親デバイスグループ)を選択して**OK**をクリックします。

STEP 7 | ファイアウォールの設定バンドルをファイアウォールにプッシュし、ローカルの設定からすべてのポリシー ルールおよびオブジェクトを削除します。

ルールあるいはオブジェクト名が重複することにより、次のステップで Panorama からファイアウォールにデバイス グループの設定をプッシュする際にコミット エラーが発生するのを避けるためにこのステップが必要になります。

1. Panorama で **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。
2. **Panorama** > **Setup**（セットアップ）> **Operations**（操作）の順に選択し、**Export or push device config bundle**（デバイス設定バンドルをエクスポートあるいはプッシュ）をクリックします。
3. 設定のインポート元である**Device** (デバイス)を選択し、**OK**、次に**Push & Commit** (プッシュしてコミット)をクリックします。Panorama がバンドルをプッシュし、ファイアウォール上でのコミットを開始します。

STEP 8 | デバイス グループおよびテンプレートの設定をプッシュし、一元管理への移行を完了させます。

複数のファイアウォールを移行させている場合、次に進む前に各ファイアウォールに対して上記の全ステップ（このステップを含む）を実施します。

1. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択し、Push Scope（プッシュ スコープ）で **Edit Selections**（選択内容の編集）を行います。
2. **Device Groups**（デバイス グループ）を選択し、インポートしたファイアウォール設定を含むデバイス グループを選択します。
3. **Merge with Device Candidate Config**（デバイス候補設定にマージ）、**Include Device and Network Templates**（デバイスおよびネットワーク テンプレートを含める）、および **Force Template Values**（テンプレートの値を適用）を選択します。
4. **OK** をクリックして、プッシュ スコープに対する変更を保存します。
5. 変更を **Commit and Push**（コミットしてプッシュ）します。

STEP 9 | インポートされたすべてのファイアウォールの設定を統合します。

複数のファイアウォールを移行している場合、このステップが必須になります。

1. ファイアウォールの設定をすべてインポートした後、必要に応じてデバイス グループおよびテンプレートを更新して冗長性を無くし、設定の管理を合理化します (インポートされた設定の微調整を行うを参照)。（ファイアウォール設定バンドルを再度プッシュする必要はありません）
2. ファイアウォール固有の設定を構成します。

   ファイアウォールにローカル ゾーンをもたせる場合はデバイス グループあるいはテンプレートをコミットする前に作成しておく必要があります。Panorama はファイアウォールに対してゾーン名あるいはゾーン設定をポーリングすることはできません。後にローカルのファイアウォール ルールを使用する場合、それらの名前が一意になっていることを確認します（Panorama で重複なし）。必要に応じて、ファイアウォール固有値でテンプレートまたはテンプレートスタック値のオーバーライドを行うことができます。
3. 変更をコミットしてプッシュします。
   1. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択し、Push Scope（プッシュ スコープ）で **Edit Selections**（選択内容の編集）を行います。

© 2019 Palo Alto Networks, Inc.

2. **Device Groups**（デバイス グループ）を選択し、変更したデバイス グループを選択して、**Include Device and Network Templates**（デバイスおよびネットワーク テンプレートを含める）作業を実行します。
3. **OK** をクリックして、プッシュ スコープに対する変更を保存します。
4. 変更を **Commit and Push**（コミットしてプッシュ）します。

STEP 10 | 移行後のテスト計画を実行します。

移行計画を立てる際に決定した検証作業を行い、Panorama がプッシュした設定を使用しても元のローカル構成の時と同じように効率よくファイアウォールが稼働することを確認します (移行後のテスト計画を作成を参照)。

ファイアウォール HA ペアを Panorama 管理に移行

Panorama を使用して管理する HA 設定のファイアウォールのペアがある場合、設定やポリシーを再作成せずに、ファイアウォール HA ペアに対してローカルな設定を Panorama にインポートすることもできます。デバイス グループとテンプレート作成に使用されるファイアウォール設定を最初に Panorama にインポートします。ファイアウォールに対するデバイス グループとテンプレートの特殊な設定のプッシュを実行し、ローカル ファイアウォール設定を上書きして、ファイアウォールを Panorama と同期します。

STEP 1 | 移行計画を立てます。

Panorama管理への変更を計画のチェックリストをご覧ください。

STEP 2 | HA ピア間の設定の同期を無効にします。

HA ペアの両方のファイアウォールでこの手順を実行します。

1. 各ファイアウォールの Web インターフェイスにログインして、**Device**（デバイス）> **High Availability**（高可用性）> **General**（全般）の順に選択し、Setup（セットアップ）セクションを編集します。
2. **Enable Config Sync**（設定の同期を有効化）をオフにして **OK** をクリックします。
3. 各ファイアウォールで設定変更を **Commit**（コミット）します。

STEP 3 | 各ファイアウォールを Panorama に接続します。

Panorama でこれらのファイアウォールからすでにログを受信している場合、このステップを実行する必要はありません。ステップ 5 に進みます。

HA ペアの両方のファイアウォールでこの手順を実行します。

1. 各ファイアウォールの Web インターフェイスにログインして、**Device**（デバイス）> **Setup**（セットアップ）> **Management**（管理）の順に選択し、Panorama Settings（Panorama 設定）を編集します。
2. **Panorama Servers**（**Panorama** サーバー）フィールドに、Panorama 管理サーバーの IP アドレスを入力し、**Panorama Policy and Objects**（**Panorama** ポリシーとオブジェクト）と **Device and Network Template**（デバイスとネットワーク テンプレート）が有効になっていることを確認して、**OK** を選択します。
3. 各ファイアウォールで設定変更を **Commit**（コミット）します。

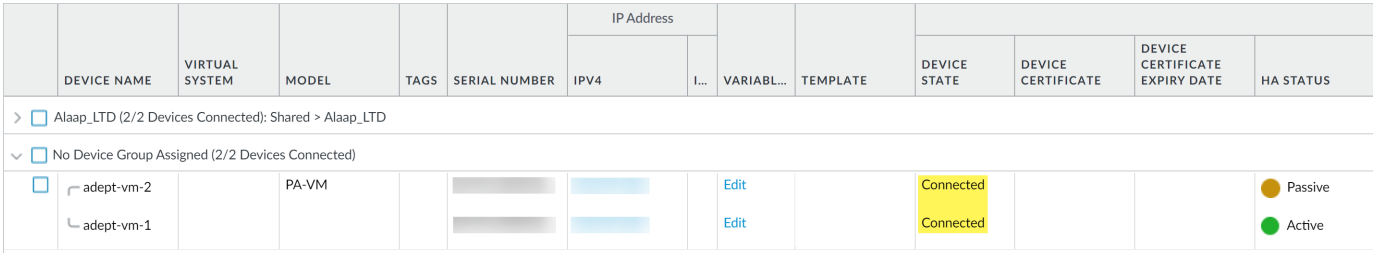
STEP 4 | 管理対象デバイスとして各ファイアウォールを追加します。

Panorama でこれらのファイアウォールからすでにログを受信している場合、このステップを実行する必要はありません。ステップ 5 に進みます。

管理対象デバイスとしてのファイアウォールの追加を行います。

© 2019 Palo Alto Networks, Inc.

1. Panorama Web インターフェイスへのログイン，**Panorama** > **Managed Devices** (管理対象デバイス) の順に選択し、**Add** (追加) をクリックします。
2. ファイアウォールのシリアル番号を入力し、**OK** をクリックします。
3. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。
4. 各ファイアウォールの Device State（デバイス状態）が Connected（接続済み）であることを確認します。



STEP 5 | 各ファイアウォール設定を Panorama にインポートします。

この手順では、デバイス グループまたはテンプレート スタック設定をマネージドファイアウォールにプッシュしないでください。この手順でデバイス グループとテンプレート スタックの設定をプッシュすると、次の手順でローカル ファイアウォールの *HA* 設定が消去されます。

後でファイアウォールの設定を再度インポートする場合、まずは最初にファイアウォールデバイス グループと、それがメンバーになっているテンプレートを削除します。デバイス グループとテンプレートの名前がファイアウォールのホスト名と同じ場合、ファイアウォール構成を再インポートする前にデバイス グループとテンプレートを削除するか、*Device Group Name Prefix (デバイス グループ名のプレフィックス)* フィールドを使用して、再インポートにより作成したデバイス グループとテンプレートの新しい名前を入力できます。さらに、ファイアウォールをデバイス グループまたはテンプレートから削除しても、ログが失われることはありません。

1. Panoramaで**Panorama** > **Setup** > **Operations** (Panorama > セットアップ > 操作)を選択し、**Import device configuration to Panorama** (Panoramaにデバイス設定をインポート)を選択してさらに**Device** (デバイス)を選択します。

   Panorama は、既存のデバイス グループあるいはテンプレート スタックに割り当てられているファイアウォールから設定をインポートすることはできません。
2. (任意) **Template Name (テンプレート名)** を編集します。デフォルト値はファイアウォール名です。既存のテンプレートまたはテンプレート スタックの名前は使用できません。
3. （任意）**Device Group**（デバイス グループ）の名前を編集します。マルチ vsys ファイアウォールの場合、各デバイス グループにはデフォルトで vsys 名が付いているため、それぞれの Device Group Name Prefix（デバイス グループ名の接頭辞）となる文字列を追加します。そうでない場合、デフォルト値はファイアウォール名になります。既存のデバイス グループ名を使用することはできません。

   Imported devices' shared objects into Panorama's shared context（デバイスの共有オブジェクトを *Panorama* の共有コンテキストにインポート済み）チェック ボックスはデフォルトでオンになっています。つまり、*Panorama* は、ファイアウォールの *Shared*（共有）領域に属するインポート オブジェクトを *Panorama* の *Shared*（共有）と比較します。インポートしたオブジェクトがファイアウォールの *Shared*（共有）コンテキストに存在しない場合、インポートする各デバイス グループに適用されます。このチェック ボックスをオフにすると、*Panorama* のコピーはインポートし

© 2019 Palo Alto Networks, Inc.

たオブジェクトを比較せず、*Shared*（共有）ではなくすべての共有ファイアウォール オブジェクトをインポートするデバイス グループに適用します。これにより重複するオブジェクトが生成される可能性があるため、大抵の場合はチェック ボックスをオンにしておくことが推奨されます。共有あるいは重複オブジェクトを *Panorama* にインポートするとどうなるのかということについては「共通設定を管理する方法を計画」をご覧ください。

4. **Commit to Panorama**（**Panorama** へのコミット）によってコミットします。
5. **Panorama** > **Setup (セットアップ)** > **Operations (操作)** の順に選択し、**Export or push device config bundle (デバイス設定バンドルをエクスポートあるいはプッシュ)** します。**Device (デバイス)**を選択し、**OK** を選択してから、設定を **Push & Commit (プッシュしてコミット)** します。

   ステップ 2 の *Config Sync (設定の同期)* を有効にする設定は、デバイス グループとテンプレート スタックをプッシュする前に両方のファイアウォールで無効にする必要があります。
6. ファイアウォール HA ピアの Web インターフェイスを起動し、以前のステップでプッシュされた設定が正常にコミットされたことを確認します。確認できない場合は、ファイアウォールで変更をローカルに **Commit (コミット)** します。
7. 2 つ目のファイアウォールで上記のステップ 1 ~ 6 を繰り返します。このプロセスにより、各ファイアウォールごとのデバイス グループとテンプレート スタックが作成されます。

STEP 6 | HA ファイアウォール ペアを同じデバイス グループとテンプレート スタックに追加します。

HA ファイアウォールペアがアクティブ/アクティブ設定の場合、この手順はスキップしてください。

1. **Panorama** > **Device Group**（デバイス グループ）の順に選択し、2 つ目のファイアウォールのデバイス グループを選択して、**Delete**（削除）します。
2. 最初のファイアウォールのデバイス グループを選択し、2 つ目のファイアウォールを選択して、**OK** をクリックし、**Commit to Panorama**（**Panorama** へのコミット）を行って HA ピアと同じデバイス グループに追加します。
3. **Panorama** > **Templates (テンプレート)** の順に選択し、2 つ目のファイアウォールのテンプレート スタックを選択して、**Delete (削除)** します。
4. 最初のファイアウォールのテンプレート スタックを選択し、2 つ目のファイアウォールを追加してから **OK** を選択し、**Commit to Panorama (Panorama** へのコミット**)** を行って HA ピアと同じテンプレート スタックに追加します。
5. 新しく移行されたファイアウォールに関連付けられているテンプレートの HA 設定を削除します。
   1. **Device (デバイス)** > **Setup (セットアップ)** > **High Availability (高可用性)** の順に選択します
   2. **Remove All (すべて削除)** を選択します。
   3. **Commit to Panorama**（**Panorama** へのコミット）によってコミットします。
6. デバイス グループとテンプレート スタックの設定をマネージドファイアウォールにプッシュします。

   最初にデバイス グループとテンプレート スタック設定をパッシブ *HA* ピアにプッシュし、次にアクティブ *HA* ピアにプッシュします。

   1. **Commit**（コミット）> **Push to Devices**（デバイスへのプッシュ）の順に選択し、**Edit Selections**（選択内容の編集）を行います。
   2. **Merge with Device Candidate Config**（デバイス候補設定にマージ）、**Include Device and Network Templates**（デバイスおよびネットワーク テンプレートを含める）、および **Force Template Values**（テンプレートの値を適用）を有効化 (選択) します。
   3. **OK** をクリックします。
   4. マネージドファイアウォールに **Push (プッシュ)** します。

© 2019 Palo Alto Networks, Inc.

5. アクティブな HA ピア の Launch the Web Interface (Web インターフェースを起動) して、**Device** (デバイス) > **High Availability** (高可用性) > **Operational Commands** (運用コマンド) で **Suspend local device** (ローカル デバイスの一時停止) を選択します。

   アクティブな HA ピアを変更する前に、パッシブ HA ピアにフェイルオーバーして、設定の移行を完了している間、セキュリティ体制を維持します。
6. 現在のパッシブ HA ピアに対してステップ1～4 を繰り返します。
7. 現在アクティブな HA ピア の Launch the Web Interface (Web インターフェースを起動) して、**Device** (デバイス) > **High Availability** (高可用性) > **Operational Commands** (運用コマンド) で **Suspend local device** (ローカル デバイスの一時停止) を選択します。

   これにより、元のアクティブ/パッシブ HA ピアのロールが復元されます。

7. **Panorama** > **Managed Devices** (管理対象デバイス) > **Summary** (サマリー) の順に選択し、パッシブ ファイアウォールについてはデバイス グループとテンプレートが同期されていることを確認します。パッシブ ファイアウォールのポリシー ルール、オブジェクト、ネットワーク設定がアクティブ ファイアウォールに一致することを確認します。

STEP 7 | HA ピア間の設定同期を有効にします。

同期する必要があるローカル設定を保持する予定にしている場合は、HA ペアの両方のファイアウォールでこの手順を実行します。

1. 各ファイアウォールの Web インターフェイスにログインして、**Device**（デバイス）> **High Availability**（高可用性）> **General**（全般）の順に選択し、Setup（セットアップ）セクションを編集します。
2. **Enable Config Sync**（設定の同期を有効化）をオンにして **OK** をクリックします。
3. 各ファイアウォールで設定変更を **Commit**（コミット）します。

ファイアウォールの設定の一部を Panorama に読み込む

他のファイアウォールと共通の設定がある場合、その設定をPanoramaに読み込んだ後、他のすべてのファイアウォールあるいは特定のデバイスグループおよびテンプレートのファイアウォールにプッシュすることができます。

設定を Panorama 管理サーバにロードするには、完全なコミットが必要であり、スーパーユーザーが実行しなければなりません。完全なコミットは、設定スナップショットの復元やロードなどの特定の Panorama 操作を実行するときに必要であり、カスタム管理者ロールプロファイルではサポートされていません。

STEP 1 | Panoramaへの移行計画を立てます。

Panorama管理への変更を計画のチェックリストをご覧ください。

STEP 2 | Panoramaにおける名前とファイアウォールでの名前が同じである重複した設定を管理する方法を決定します。

部分的なファイアウォールの設定を読み込む前の時点で、Panoramaとそのファイアウォールがすでに重複した設定を持っている可能性があります。ファイアウォールの設定を読み込むと、他の管理対象のファイアウォールの設定と重複している設定もPanoramaに追加される可能性があります。

*Panorama*にファイアウォールのものと同じ名前のポリシールールあるいはオブジェクトがある場合、ファイアウォールにデバイスグループ設定をプッシュしようとした際にコミット エラーが発生します。*Panorama*にファイアウォールのものと同じ名前のテンプレート設定がある場合、テンプレートをプッシュする際にファイアウォールの値がテンプレートの値で上書きされます。

1. Panoramaでグローバル検索を実行し、重複した設定があるかどうか確認します。

© 2019 Palo Alto Networks, Inc.

2. Panoramaで設定を管理する場合は重複した設定をファイアウォールから削除あるいは名称変更します。ファイアウォールで設定を管理する場合は重複した設定をPanoramaから削除あるいは名称変更します。デバイスあるいはネットワーク設定をファイアウォールで管理する場合、重複した設定を Panorama で削除あるいは名称変更する代わりに、Panorama から設定をプッシュし（ステップ 6）、ファイアウォール上でファイアウォール固有の値でテンプレートまたはテンプレートスタック値のオーバーライドを行うこともできます。

STEP 3 | ファイアウォールの設定全体をローカルのコンピューターにエクスポートします。

1. ファイアウォールで、**Device**（デバイス）> **Setup**（セットアップ）> **Operations**（操作）の順に選択します。
2. **Save named configuration snapshot**（名前を付けて設定スナップショットを保存）をクリックし、設定を識別できる **Name**（名前）を入力して **OK** をクリックします。
3. **Export named configuration snapshot**（名前を付けて設定スナップショットを保存）をクリックし、先ほど保存した設定の**Name**（名前）を選択して**OK**をクリックします。ファイアウォールは設定をXMLファイルとしてエクスポートします。

STEP 4 | ファイアウォール設定スナップショットをPanoramaにインポートします。

1. Panoramaで**Panorama** > **Setup** > **Operations**(Panorama > セットアップ > 操作) の順に選択します。
2. **Import named Panorama configuration snapshot**（名前を付けて保存した **Panorama** 設定スナップショットをインポート）をクリックし、コンピューターにエクスポートしたファイアウォールの設定ファイルを**Browse**（参照）し、**OK**をクリックします。

このオプションを使用してファイアウォールの設定ファイルをインポートした後は、*Panorama*の*Web*インターフェイスを使用してそれを読み込むことができなくなります。次のステップで説明するように、*XML*、*API*、あるいは*CLI*を使用する必要があります。

STEP 5 | ファイアウォールの設定の任意の部分をPanoramaに読み込みます。

設定の一部（例：すべてのアプリケーション オブジェクト）を指定する際、次の項目を提示する必要があります。

- ソースxpath—読み込み元であるファイアウォールの設定ファイルのXMLノード。
- 宛先xpath—読み込み先であるPanorama設定のノード。

XML、API、あるいはCLIを使用して設定の一部を指定・読込：

1. ファイアウォールのXML、API、あるいはCLIを使用してソースxpathを指定します。

   例えば、ファイアウォールのvsys1のアプリケーション オブジェクトのxpathは：

```
/config/devices/entry[@name='localhost.localdomain']/vsys/
entry[@name='vsys1']/application
```

2. PanoramaのXML、API、あるいはCLIを使用して宛先xpathを指定します。

   例えば、US-Westという名前のデバイスグループにアプリケーション オブジェクトを読み込む場合、xpathは：

```
/config/devices/entry[@name='localhost.localdomain']/device-group/
entry[@name='US-West']/application
```

3. Panorama CLIを使用して設定を読み込み、変更をコミットします。

```
# load config partial mode [append|merge|replace] from-xpath <source-
xpath> to-xpath <destination-xpath> from <filename>
```


© 2019 Palo Alto Networks, Inc.

```
# commit
```

例えば、次のように入力し、インポートしたfw1-config.xmlという名前のファイアウォールの設定のvsys1から、PanoramaのUS-Westという名前のデバイスグループにアプリケーション オブジェクトを読み込みます。

```
# load config partial mode merge from-xpath devices/
entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/application
 to-xpath /config/devices/entry[@name='localhost.localdomain']/device-
group/entry[@name='US-West']/application from fw1-config.xml
# commit
```

STEP 6 | 設定の一部をPanoramaからファイアウォールにプッシュし、一元管理への移行を完了させます。

1. Panoramaのものと同じ名前のルールあるいはオブジェクトをすべてファイアウォールから削除します。Panoramaのものと重複しているルールあるいはオブジェクトがそのファイアウォール用のデバイスグループに存在する場合、それらのファイアウォール上でこのステップも実行します。詳細は、ステップ 2 を参照してください。
2. Panorama で、設定の一部をファイアウォールにプッシュします。
    1. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択し、Push Scope（プッシュ スコープ）で **Edit Selections**（選択内容の編集）を行います。
    2. **Device Groups**（デバイス グループ）を選択し、インポートしたファイアウォール設定を含むデバイス グループを選択します。
    3. **Merge with Device Candidate Config**（デバイス候補設定にマージ）、**Include Device and Network Templates**（デバイスおよびネットワーク テンプレートを含める）、および **Force Template Values**（テンプレートの値を適用）を選択します。
    4. **OK** をクリックして、プッシュ スコープに対する変更を保存します。
    5. 変更を **Commit and Push**（コミットしてプッシュ）します。
3. Panorama で管理しないデバイスあるいはネットワーク設定がファイアウォールにある場合、ファイアウォールでテンプレートまたはテンプレートスタック値のオーバーライドを行います。

STEP 7 | 移行後のテスト計画を実行します。

移行計画を立てる際に決定した検証作業を行い、Panoramaがプッシュした設定を使用しても元のローカル構成の時と同じように効率よくファイアウォールが稼働することを確認します（移行後のテスト計画を作成を参照）。

© 2019 Palo Alto Networks, Inc.

Panoramaでのデバイスモニタリング

ファイアウォールを追加してポリシー ルールを設定した後、正常性状態を監視して、ファイアウォールが健全なパラメータ内で動作していることを確認できます。ポリシー ルールの場合は、ルールのトラフィックの一致を監視して、トラフィックの執行のニーズに一致するルールを特定します。

- デバイス健康状態の監視
- ポリシー ルール使用状況のモニター

デバイス健康状態の監視

管理対象のファイアウォールの正常性情報を監視して、ネットワーク セキュリティに影響を与える前にハードウェアの問題を特定し解決します。Panorama™ と管理対象のファイアウォールの両方が PAN-OS® 8.1 以降のリリースを実行している必要がありますが、ファイアウォールは、サマリー セッション、ロギング、リソース、および環境パフォーマンスを監視するために、デバイス グループまたはテンプレート スタックの一部である必要はありません。Panorama には管理対象のファイアウォールの正常性監視統計情報が過去 90 日間保存されているため、ファイアウォールを選択すると、セッション、環境、インターフェイス、ログ、リソース、および高可用性のパフォーマンスに関するグラフが表示されます。Panorama は、7 日間の平均と標準偏差を使用して、各メトリックのベースライン パフォーマンスを計算し、特定のファイアウォールの正常な動作範囲を決定します。ベースラインを追跡し、時間トレンドのパフォーマンスを比較するだけでなく、どのファイアウォールがメトリックを逸脱しているのかを確認し、パフォーマンスに関連する問題がネットワークに影響を及ぼす前に特定することができます。Panorama は、メトリックが通常の操作範囲外であることを認識すると、メトリックをマークし、逸脱デバイス タブに偏差のあるファイアウォールを設定します。

健康状態監視データは Panorama に保存され、ファイアウォールが削除された場合に保存されます。Panorama 管理からファイアウォールを削除すると、健康状態監視データは表示されなくなりますが、90 日間は保存されます。90 日後に、削除されたファイアウォールのすべての正常性監視データが Panorama から削除されます。ファイアウォールが Panorama 管理に追加されると、ファイアウォールが削除されたときの最新の健康状態監視データが表示されます。

STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | **Panorama** > **Managed Devices**（管理対象デバイス）> **Health**（健康状態）を選択して、管理対象のファイアウォールの健康状態を監視します。

すべての管理対象のファイアウォールと監視対象の健康状態メトリクスを見るには、**All Devices**（すべてのデバイス）を表示します。個々のファイアウォールを選択して、詳細なデバイス ビューを表示し、時間トレンドのグラフと監視対象のメトリックのテーブルを表示します。

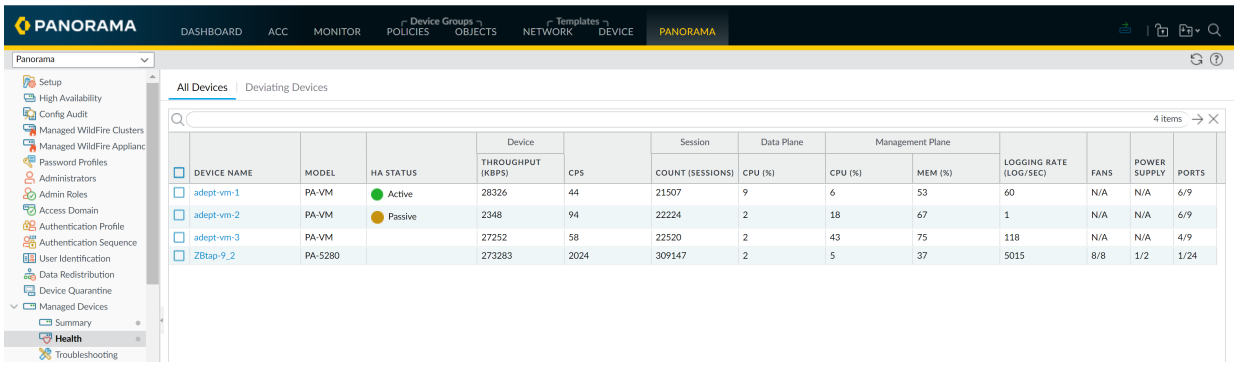


図 **12**：管理対象のファイアウォールの健康状態監視

© 2019 Palo Alto Networks, Inc.

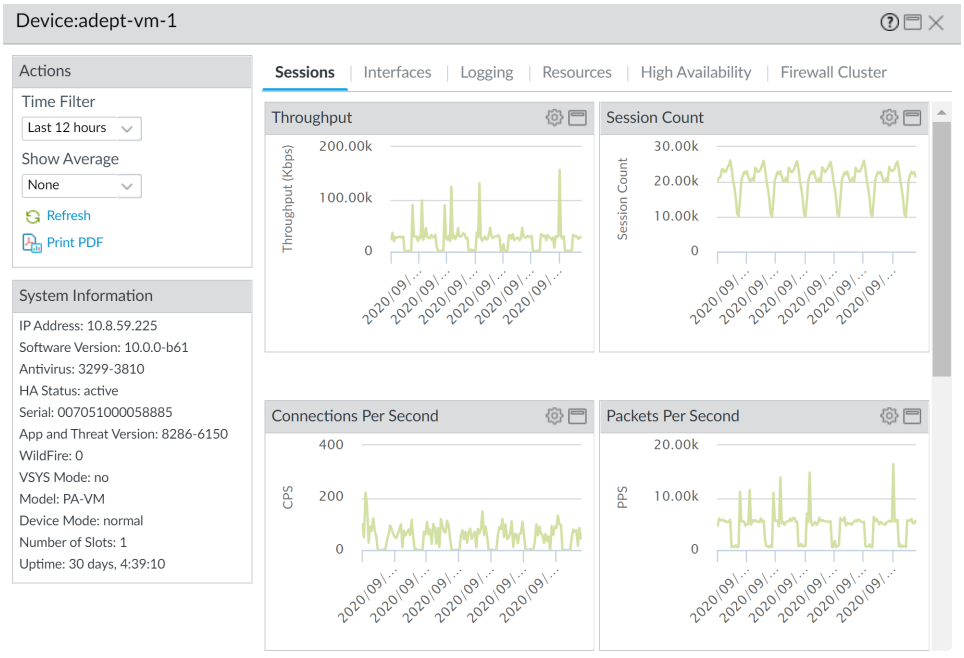
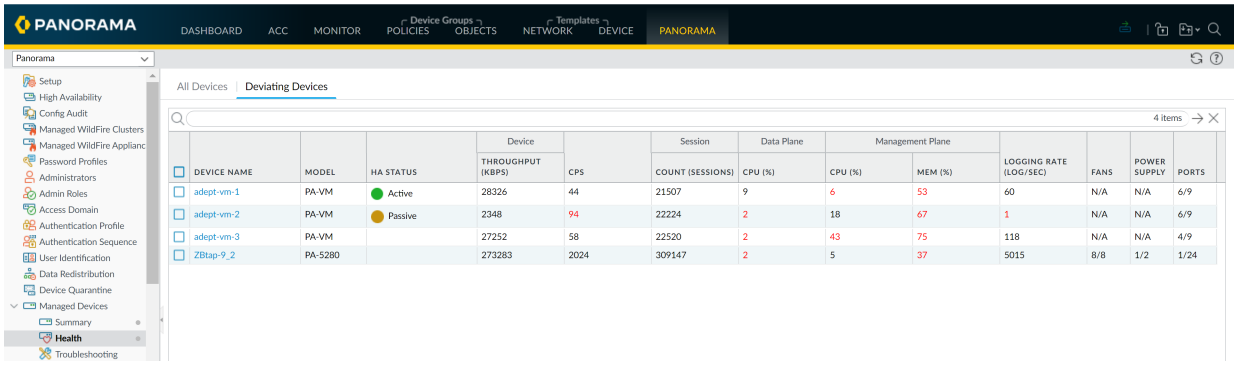


図 **13** : 詳細ログ ビュー

STEP 3 | **Deviating Devices**（逸脱しているデバイス）を選択して、計算されたベースライン外で逸脱した健康状態メトリクスを持つファイアウォールを表示します。

Panorama には、計算されたベースラインから外れたメトリックを報告しているすべてのファイアウォールと、逸脱したメトリックが赤色で表示されます。



ポリシー ルール使用状況のモニター

ポリシーは変更されるため、Panorama のルールの使用状況を追跡することで、ポリシーの実装が施行ニーズに引き続き適合しているかどうかを評価することができます。このように可視性が得られることで、未使用のルールを識別して除去し、セキュリティリスクを軽減し、ポリシー ルールベースを整理しやすくなります。さらに、ルールの使用状況を追跡することにより、新しいルールの追加やルールの変更を迅速に検証し、操作やトラブルシューティングのタスクのルールの使用状況を監視することができます。Panorama では、ポリシーをプッシュしたデバイス グループ内のファイアウォールのルール使用状況を表示して、デバイス グループ内のすべてのファイアウォールで、全体のヒット数のみを監視するのではなく、ファイアウォールの全部、一部でトラフィックがマッチするか、まったくマッチしないかを判断します。カスタマイズ可能な時間枠内であれば、作成日や変更日などのルール使用状況データを使用してルールをすばやくフィルタリングすることができます。表示されるルールの使用情報は、再起動、データプレーンの再起動、およびアップグレードの後も維持されます。

© 2019 Palo Alto Networks, Inc.

Panorama では、PAN-OS 8.1 以降のリリースを実行しており、ポリシー ルール ヒット カウントが有効（デフォルト）であり 、デバイス グループを使用してポリシー ルールを定義およびプッシュした管理対象ファイアウォールのルール使用の詳細を表示できます。Panorama ではファイアウォールでローカルに設定されたポリシー ルールのルール使用状況の詳細を取得できないため、ローカルに設定されたルールのルール使用情報を表示するには、ファイアウォールにログインしなければなりません。

ポリシー ルールベースをフィルタリングした後、管理者は、ポリシー オプティマイザから直接ポリシー ルールを削除、無効化、有効化、およびタグ付けするアクションを実行できます。たとえば、未使用のルールをフィルタリングし、レビュー用にタグを付けて、それらを安全に削除できるか、ルールベースに保持できるかを判断できます。管理者がポリシー オプティマイザから直接アクションを実行することを有効化するには、ルールのライフサイクル管理をさらに簡素化するために必要な管理諸経費を削減し、ファイアウォールが過剰にプロビジョニングされないようにします。

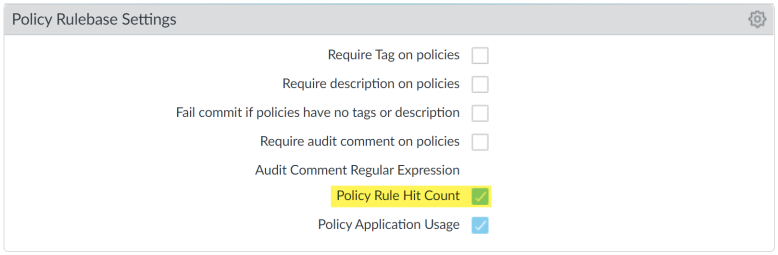
ポリシールール使用状況データは、Policy Optimizer を使用して、最初にどのルールを移行、あるいはクリーンアップするかを優先させる場合にも役立ちます。

共有ルールまたは特定のデバイスグループのルールの使用状況を表示するには、次の手順を実行します。

STEP 1 | Panorama Web インターフェイスへのログイン.

STEP 2 | ポリシールールのヒット数が有効になっていることを確認します。

1. ポリシールールベース設定には、**Panorama**（**Panorama**）> **Setup**（セットアップ）> **Management**（管理）の順に移動します。
2. **Policy Rule Hit Count** (ポリシールールのヒット数) が有効になっていることを確認します。



STEP 3 | ルールを表示するには、**Policies** (ポリシー) > <*policy rule*> を選択します。

STEP 4 | デバイス グループ コンテキストを **Shared**（共有中）または表示する特定のデバイス グループに変更します。

STEP 5 | ルールが使用されているかどうかを確認します（ルールの使用状況）。ポリシー ルールの使用状況は、次のいずれかです。

ルールの使用状況を判断するには、Panorama のポリシー ルール ヒット カウントを有効にして、ファイアウォールで PAN-OS 8.1 以降のリリースを実行する必要があります。

- 使用中–ポリシー ルールをプッシュしたデバイス グループ内のすべてのファイアウォールで、ポリシー ルールに一致するトラフィックが発生した場合。
- 部分的に使用–デバイスグループ内の一部のファイアウォール（ポリシー ルールをプッシュしたもの）に、ポリシー ルールに一致するトラフィックがあります。
- 不使用–ポリシー ルールをプッシュしたデバイス グループ内のファイアウォールで、ポリシー ルールに一致するトラフィックが発生していません。
- emダッシュ (–)–ポリシー ルールをプッシュしたデバイス グループ内のファイアウォールがない場合は、ポリシー ルール ヒット カウントを有効にするか、Panorama でルールの使用状況を判断することができます。
- 編集–ポリシールールを最後に編集した日時です。

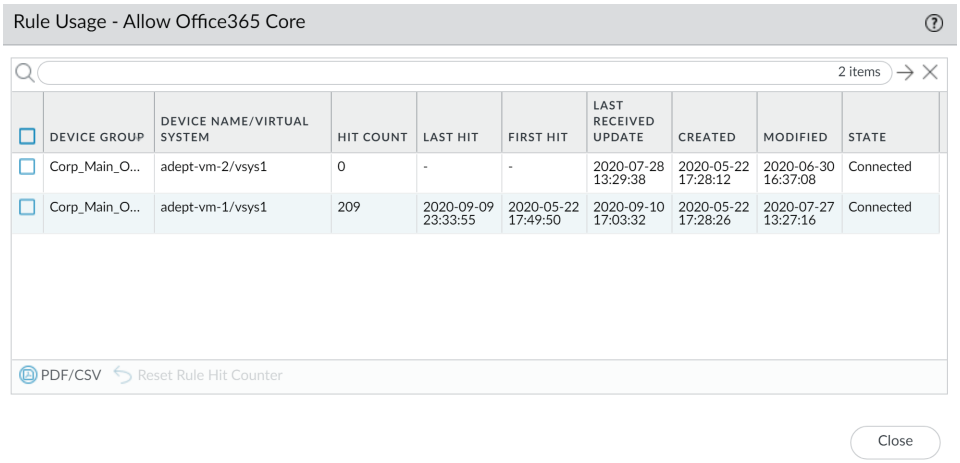
© 2019 Palo Alto Networks, Inc.

- 作成–ポリシールールが作成された日時です。

Panorama で *PAN-OS 8.1* を実行し、ポリシー ルール ヒット カウント設定が有効になっているときにルールが作成された場合、*PAN-OS 9.0* 以降のリリースへのアップグレード時に作成された日時として、最初のヒットが日時として使用されます。ポリシー ルール ヒット カウントの設定が無効なときに *PAN-OS 8.1* でルールを作成した場合、または *Panorama* で *PAN-OS 8.0* 以前のリリースを実行しているときにルールが作成された場合、ルールの作成日は、*Panorama*を*PAN-OS9.0*以降のリリースに正常にアップグレードした日時になります。

Rule Usage		DAYS WITH NO NEW APPS	MODIFIED	CREATED
RULE USAGE	APPS SEEN			
Used	6	150	2020-06-24 10:34:...	2020-04-09 11:34:03
Unused	0	-	2020-06-24 10:34:...	2020-04-16 11:42:46
Used	11	57	2020-06-24 10:34:...	2020-04-16 11:42:46
Partially Used	3	111	2020-06-24 10:34:...	2020-05-22 17:26:44
Unused	0	-	2020-06-24 10:34:...	2020-05-22 22:45:53

STEP 6 | ルールの使用状況のステータスをクリックすると、ルールを使用するファイアウォールの一覧と、各ファイアウォールのルールに一致するトラフィックのヒット数データが表示されます。



STEP 7 | （ 任意 ）デバイス グループ内の個々のファイアウォールのポリシー ルール ヒット カウント データを表示します。

1. **Preview Changes**（変更をプレビュー）をクリックします。
2. デバイス コンテキストから、ポリシー ルールの使用状況データを表示するファイアウォールを選択します。

STEP 8 | **Policies**（ポリシー）を選択し、Policy Optimizer ダイアログで **Rule Usage**（ルールの使用状況）フィルターを表示します。

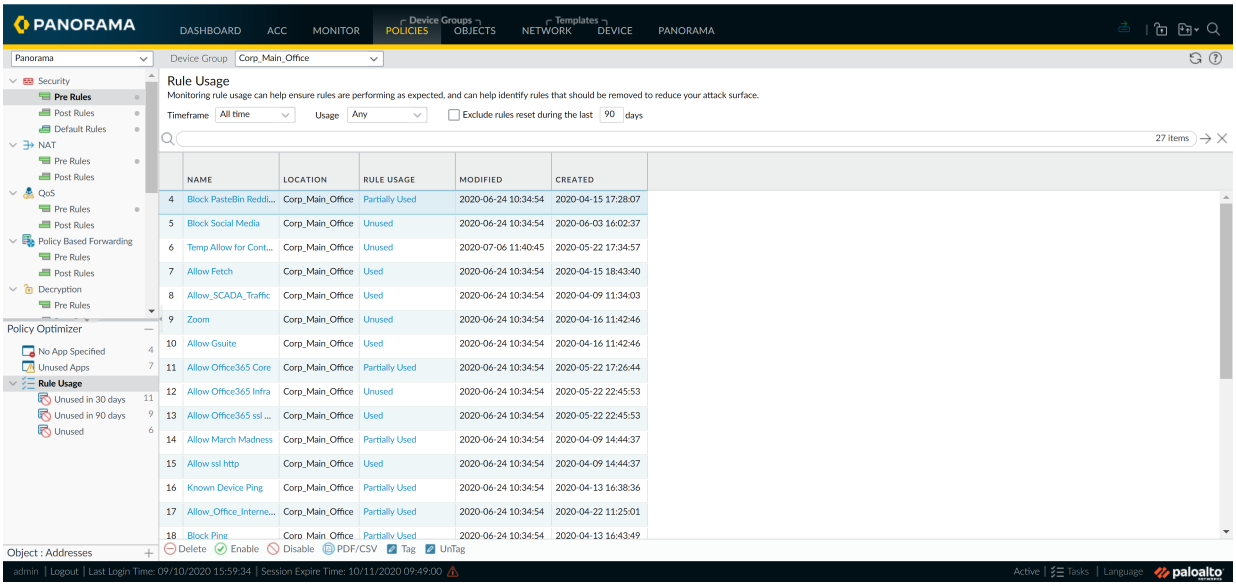
STEP 9 | 選択したルールベースのルールをフィルタリングします。

© 2019 Palo Alto Networks, Inc.

Panorama からファイアウォールにプッシュされたルールのルール使用状況をフィルタリングできます。Panorama は、ファイアウォール上でローカルに設定されたルールのルール使用状況をフィルタリングできません。

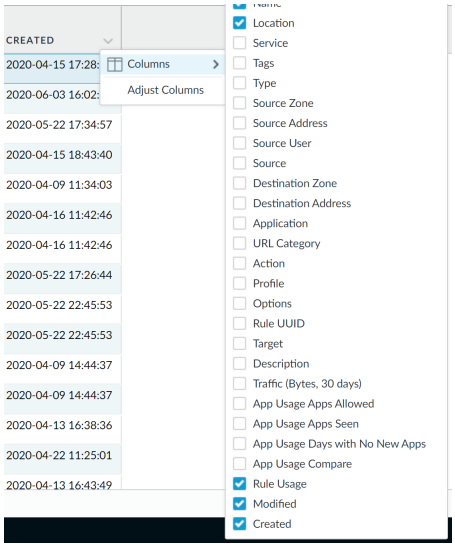
ルール使用状況のフィルタを使用し、特定の期間でルール使用状況を評価します。たとえば、過去 *30* 日間の *Unused* (未使用) ルールを選択したルールベースでフィルタリングします。作成日や変更日など、他のルール属性を使用してルールの使用状況を評価することもできます。これにより、確認する一連の正しいルールをフィルタリングできます。ルールのライフサイクルを管理し、ネットワークへの攻撃の入り口を減らすためにルールを削除する必要があるかどうかを判断するためにこのデータを使用することができます。

1. フィルタリングする **Timeframe**（時間枠）を選択するか、**Custom**（カスタム）の時間枠を指定します。
2. フィルタするルールの **Usage**（使用状況）を選択します。
3. （任意）いずれかのルールのルール使用状況データをリセットした場合は、過去 <日数> 日の間にリセットされた除外ルールを確認し、ルールがリセットされてから指定した日数に基づいて、いつルールを除外するかを決定します。指定した日数より前にリセットされたルールのみが、フィルタリング結果に含まれます。

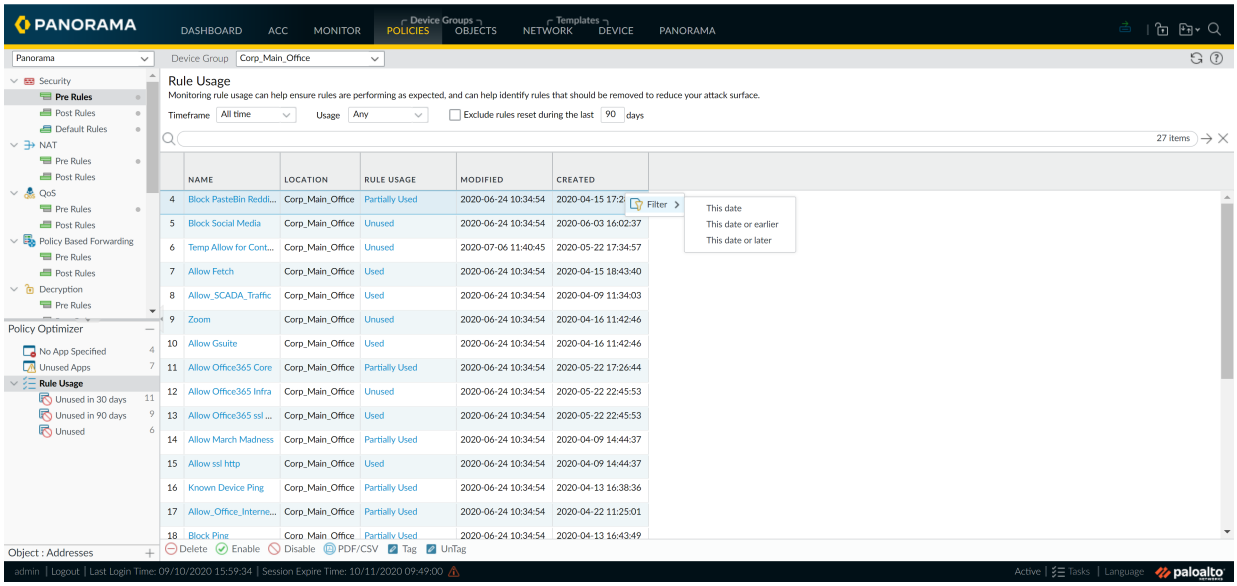


4. (任意) ルールの使用方法以外の追加のルールデータに基づいて検索フィルタを指定します。
   1. マウスを列見出しの上に移動して、ドロップダウンから **Columns** (列) を選択します。
   2. フィルタをかけたり表示したりする列を追加します。

© 2019 Palo Alto Networks, Inc.



3. フィルタリングしたい列データの上にマウスを移動して、ドロップダウンから **Filter** (フィルタ) を選択します。日付を含むデータの場合は、**This date** (現在の日付)、**This date or earlier** (現在の日付以前)、または **This date or later** (現在の日付以降) の内どれを使用してフィルタリングするかを選択します。
4. **Apply Filter** (フィルタの適用) (→) をクリックします。



STEP 10 | 1つ以上の未使用のポリシー ルールへのアクションを実行します。

1. 1つ以上の未使用のポリシー ルールを選択します。
2. 以下のいずれかのアクションを実行します。
   - **Delete** (削除)—選択した1つ以上のポリシー ルールを削除します。
   - **Enable** (有効化)—無効にしたときに、1つ以上の選択したポリシー ルールを有効にします。
   - **Disable** (無効化)—選択した1つ以上のポリシー ルールを無効にします。
   - **Tag** (タグ)—1つ以上のグループ タグを1つ以上の選択したポリシー ルールに適用します。ポリシー ルールにタグを付けるには、グループ タグがすでに存在している必要があります。
   - **Untag** (タグ外し)—1つ以上のグループ タグを1つ以上の選択したポリシー ルールから削除します。

© 2019 Palo Alto Networks, Inc.

3. 変更内容の **Commit** (コミット)および**Commit and Push** (コミットおよびプッシュ)を選択します。

© 2019 Palo Alto Networks, Inc.

「ユース ケース：Panorama を使用してファイアウォールを構成

Panorama を 高可用性設定で使用して、ネットワーク上の 12 台のファイアウォールを管理するとします。6 つの支店にファイアウォール 6 台、2 つのデータセンターそれぞれに高可用性設定のファイアウォールを 2 台ずつ、2 つの地域本部にファイアウォール 1 台ずつがデプロイされています。

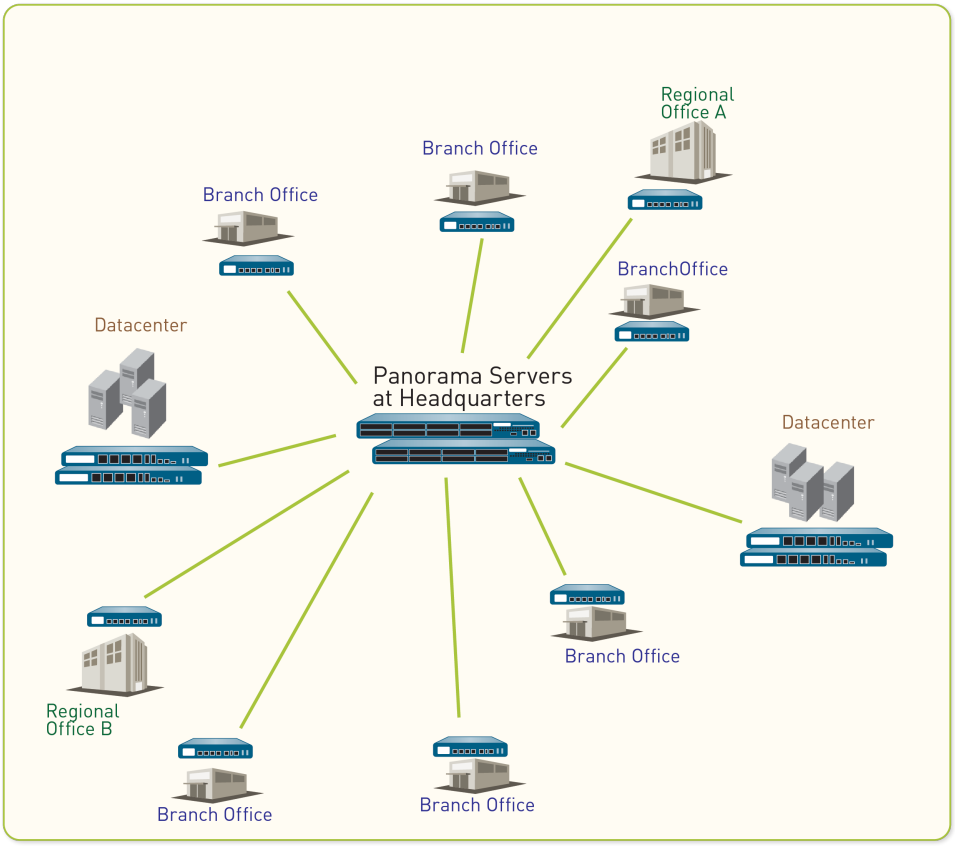


図 **14 :** ファイアウォール分散の例

中央管理戦略を作成するための最初のステップでは、ファイアウォールをデバイス グループとテンプレートにグループ化して Panorama から設定を効率よくプッシュする方法を決定します。グループ化の基準は、ファイアウォールの業務上の機能、地理的な場所、または管理ドメインにすることができます。この例では、2 つのデバイス グループと 3 つのテンプレートを作成し、Panorama を使用してファイアウォールを管理します。

- このユース ケースにおけるデバイス グループ
- このユース ケースのテンプレート
- 中央管理設定とポリシーのセットアップ

このユース ケースにおけるデバイス グループ

「「ユース ケース：Panorama を使用してファイアウォールを構成」では、ファイアウォールが実行する機能に基づいて、以下の 2 つのデバイス グループを定義する必要があります。

© 2019 Palo Alto Networks, Inc.

- DG_BranchAndRegional には、支店と地域本部でセキュリティ ゲートウェイとして機能するファイアウォールをグループ化します。類似の機能を持つデバイスには類似のポリシー ルールベースが必要であるため、支店のファイアウォールと地域本部のファイアウォールは同じデバイス グループに入れます。
- DG_DataCenter には、データセンターのサーバーを保護するファイアウォールをグループ化します。

これで、両方のデバイス グループ間の共有ポリシールールと、地域本部グループと支店グループの個別のデバイス グループ ルールを管理できます。柔軟性を高めるために、地域本部または支店のローカル管理者は、特定の送信元、宛先、およびサービス フローに一致するローカル ルールを作成して、そのオフィスで必要なアプリケーションとサービスにアクセスすることができます。この例では、以下のセキュリティ ルールの階層を作成します。他のルールベースにも類似の方法を使用できます。

Device Groups	DG_BranchAndRegional		DG_DataCenter
Rules	**Regional**	**Branch**	**Datacenter**
Shared pre-rule	Allow DNS and SNMP services.		
	Acceptable use policy that denies access to specified URL categories and peer-to-peer traffic that is of risk level 3, 4, and 5.		
Device Group pre-rule	Allow Facebook to all users in the marketing group in the regional offices only.		Allow access to the Amazon cloud application for the specified hosts/servers in the datacenter.
Local rules on a device	None		
Device Group post-rule	None		
Shared post-rule	To enable logging for all Internet-bound traffic on your network, create a rule that allows or denies all traffic from the trust zone to the untrust zone.		

図 **15 :** セキュリティ ルールの階層

このユース ケースのテンプレート

ファイアウォールをテンプレートにグループ化する場合は、ネットワーキング設定の違いを考慮に入れる必要があります。たとえば、インターフェイス設定が異なる場合、つまり、インターフェイスのタイプ、使用するインターフェイスの採番体系やリンク機能、ゾーン インターフェイス間のマッピングが異なる場合、ファイアウォールは別のテンプレートに分ける必要があります。さらに、ファイアウォールは地理的に広範囲にわたって設置されているため、ネットワーク リソースへのアクセス設定も異なる場合があります。たとえば、ファイアウォールがアクセスする DNS サーバー、Syslog サーバー、ゲートウェイが異なる可能性があります。そのため、「「ユース ケース：Panorama を使用してファイアウォールを構成」で最適な基本設定を可能にするには、ファイアウォールを以下のように個別のテンプレートに分ける必要があります。

- 支店のファイアウォールは T_Branch
- 地域本部のファイアウォールは T_Regional
- データセンターのファイアウォールは T_DataCenter

© 2019 Palo Alto Networks, Inc.

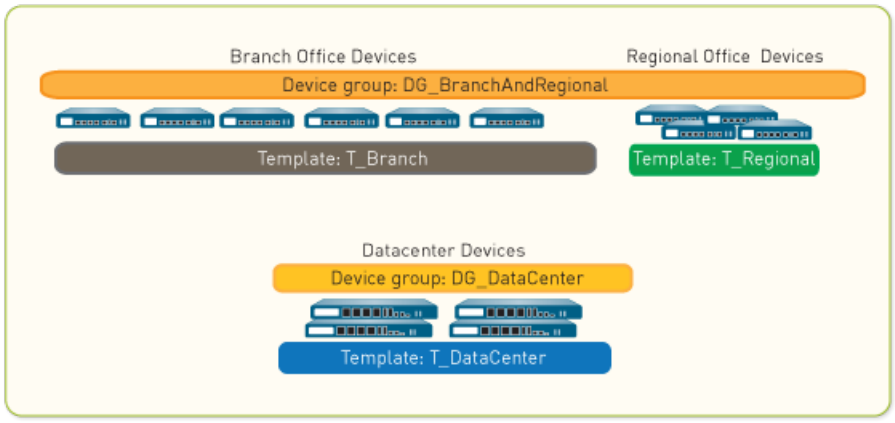


図 **16 :** デバイス グループの例

ファイアウォールをアクティブ/アクティブの *HA* 設定でデプロイする計画の場合は、*HA* ペアの各ファイアウォールを個別のテンプレートに割り当てます。これにより、ピアごとに個別のネットワーク設定を柔軟にセットアップできます。たとえば、ピアごとにテンプレートを分けてネットワーク設定を管理し、それぞれが北方向ルーターと南方向ルーターに個別に接続したり、異なる *OSPF* または *BGP* ピア設定を使用したりできます。

中央管理設定とポリシーのセットアップ

「「ユース ケース : Panorama を使用してファイアウォールを構成」では、次の作業を行い、ファイアウォールを一元的にデプロイし、管理する必要があります。

- 管理対象のファイアウォールを追加して更新をデプロイ
- テンプレートを使用した基本設定の管理
- デバイス グループを使用したポリシー ルールのプッシュ
- ルールのプレビューと変更のコミット

管理対象のファイアウォールを追加して更新をデプロイ

「「ユース ケース : Panorama を使用してファイアウォールを構成」の最初の作業は、管理対象デバイスとしてファイアウォールを追加し、コンテンツ更新と PAN-OS ソフトウェア更新をそれらのファイアウォールにデプロイすることです。

STEP 1 | Panorama で管理するファイアウォールごとに「管理対象デバイスとしてのファイアウォールの追加」を行います。

この例ではファイアウォールを 12 台追加します。

STEP 2 | コンテンツ更新をファイアウォールにデプロイします。脅威防御サブスクリプションを購入している場合は、コンテンツ データベースとアンチウイルス データベースを使用できます。最初に、**Applications**（アプリケーション）または**Applications and Threats**（アプリケーションおよび脅威）データベースをインストールし、次に **Antivirus**（アンチウイルス）をインストールします。

Panorama で実行されるすべてのタスクの状態または進捗をレビューする方法については、「Panorama タスク マネージャの使用」を参照してください。

© 2019 Palo Alto Networks, Inc.

1. **Panorama** > **Device Deployment**（デバイスのデプロイ）> **Dynamic Updates**（ダイナミック更新）を選択します。
2. **Check Now**（今すぐチェック）をクリックして最新の更新があるかどうか確認します。Action（アクション）列の値が **Download**（ダウンロード）の場合は、入手可能な更新があることを示します。
3. **Download**（ダウンロード）をクリックします。ダウンロードが完了すると、Action（アクション）列の値が **Install**（インストール）になります。
4. **Action**（アクション）列で **Install**（インストール）をクリックします。この更新をインストールする管理対象ファイアウォールを選択するには、フィルタまたはユーザー定義タグを使用します。
5. **OK** をクリックし、各ファイアウォールのコンテンツ更新の状態、進捗状況、および結果をモニターします。**Result**（結果）列には、インストールの成功または失敗が表示されます。

STEP 3 | ソフトウェア更新をファイアウォールにデプロイします。

1. **Panorama** > **Device Deployment**（デバイスのデプロイ）> **Software**（ソフトウェア）を選択します。
2. **Check Now**（今すぐチェック）をクリックして最新の更新があるかどうか確認します。Action（アクション）列の値が **Download**（ダウンロード）の場合は、入手可能な更新があることを示します。
3. 各ハードウェア モデルに必要なバージョンを見つけ、**Download**（ダウンロード）をクリックします。ダウンロードが完了すると、Action（アクション）列の値が **Install**（インストール）になります。
4. Action（アクション）列で **Install**（インストール）リンクをクリックします。このバージョンをインストールする管理対象ファイアウォールを選択するには、フィルタまたはユーザー定義タグを使用します。
5. **Reboot device after install**（インストール後にデバイスを再起動）または **Upload only to device (do not install)**（デバイスへのアップロードのみ（インストールしない））チェック ボックスをオンにして、**OK** をクリックします。**Results**（結果）列には、インストールの成功または失敗が表示されます。

テンプレートを使用した基本設定の管理

ユースケースの2番目のタスク：Panorama を使用してファイアウォールを構成の2番目の作業は、基本設定をファイアウォールにプッシュするために必要なテンプレートを作成することです。

STEP 1 | 使用するテンプレートごとにテンプレートの追加を行い、適切なファイアウォールを各テンプレートに割り当てます。

この例では、T_Branch、T_Regional、および T_DataCenter という名前のテンプレートを作成します。

STEP 2 | DNS サーバー、NTP サーバー、Syslog サーバー、およびログイン バナーを定義します。各テンプレートでこの手順を繰り返します。

1. **Device**（デバイス）タブで、ドロップダウンから **Template**（テンプレート）を選択します。
2. DNS サーバーと NTP サーバーを定義します。
   1. **Device** > **Setup** > **Services** > **Global**(デバイス > セットアップ > サービス > グローバル) の順に選択し、Services (サービス)を編集します。
   2. **Services**（サービス）タブで **Primary DNS Server**（プライマリ **DNS** サーバー）の IP アドレスを入力します。

      仮想システム（*vsys*）が *1* つ以上あるすべてのファイアウォールについて、各 *vsys* で DNS サーバー プロファイルをテンプレートに追加します（*Device*（デバイス）> *Server Profiles*（サーバー プロファイル）> *DNS*）。
   3. **NTP** タブで**Primary DNS Server**（プライマリ **NTP** サーバー）の IP アドレスを入力します。

© 2019 Palo Alto Networks, Inc.

4. **OK** をクリックして変更内容を保存します。

3. ログイン バナーを追加し、**Device** > **Setup** > **Management**(デバイス > セットアップ > 管理) の順に選択し、General Settings (一般設定)を編集します。このセクションで、**Login Banner**(ログイン バナー) のテキストを入力し、**OK** をクリックします。
4. Syslog サーバー プロファイルを設定します（**Device** > **Server Profiles** > **Syslog**(デバイス > サーバー プロファイル > Syslog)）。

STEP 3 | 管理対象ファイアウォールの管理インターフェイスへの HTTPS、SSH、および SNMP アクセスを有効にします。各テンプレートでこの手順を繰り返します。

1. **Device**（デバイス）タブで、ドロップダウンから **Template**（テンプレート）を選択します。
2. **Setup** > **Management**(セットアップ > 管理) の順に選択し、Management Interface Settings (管理インターフェイス設定) を編集します。
3. Services（サービス）で、**HTTPS**、**SSH**、および **SNMP** のチェック ボックスをオンにして、**OK** をクリックします。

STEP 4 | データセンター テンプレート（T_DataCenter）に含まれるファイアウォールのゾーン プロテクション プロファイルを作成します。

1. **Network**（ネットワーク）タブを選択し、**Template**（テンプレート）ドロップダウンで T_DataCenter を選択します。
2. **Network Profiles>Zone Protection**[ネットワーク プロファイル] > [ゾーン プロテクション] > の順に選択し、**Add**[追加] をクリックします。
3. この例では、SYN フラッドに対する保護を有効にします。有効にするには、**(**フラッド プロテクション**)** タブで **(SYN)** チェック ボックスをオンにし、**(**アクション**)** を **(SYN Cookie)** に、**(**アラート**)** パケット/秒を **(100)** に、**(**アクティベーション**)** パケット/秒を **(1000)** に、および **(**最大**)** パケット/秒を **(10000)** に設定します。
4. この例では、アラートを有効にします。有効にするには、**Reconnaissance Protection**（偵察行為防御）タブで、**TCP Port Scan**（**TCP** ポート スキャン）、**Host Sweep**（ホスト スイープ）、および **UDP Port Scan**（**UDP** ポート スキャン）の **Enable**（有効化）チェック ボックスをオンにします。Action（アクション）の値が **alert**（アラート）（デフォルト値）に設定されていることを確認します。
5. **OK** をクリックしてゾーン プロテクション プロファイルを保存します。

STEP 5 | データセンター テンプレート（T_DataCenter）でインターフェイスとゾーンの設定を行い、作成したゾーン プロテクション プロファイルを添付します。



この手順を実行する前に、まずファイアウォール上でインターフェイスをローカルに設定しておく必要があります。少なくとも、各インターフェイスに対してインターフェイス タイプを定義し、必要に応じてそのタイプを仮想ルーターに割り当て、セキュリティ ゾーンを適用しておく必要があります。

1. **Network**（ネットワーク）タブを選択し、**Template**（テンプレート）ドロップダウンで T_DataCenter を選択します。
2. **[Network]** > [インターフェイス] > の順に選択し、[インターフェイス] 列でインターフェイス名をクリックします。
3. ドロップダウンから **Interface Type**（インターフェイス タイプ）を選択します。
4. **Virtual Router**（仮想ルーター）ドロップダウンから **New Virtual Router**（新規仮想ルーター）を選択します。ルーターを定義するときには、**Name**（名前）がファイアウォールで定義されている名前と確実に一致するようにします。
5. **Security Zone**（セキュリティ ゾーン）ドロップダウンで、**New Zone**（新規ゾーン）をクリックします。ゾーンを定義するときには、**Name**（名前）がファイアウォールで定義されている名前と確実に一致するようにします。
6. **OK** をクリックして、インターフェイスに対する変更を保存します。

© 2019 Palo Alto Networks, Inc.

7. **[Network]** > [ゾーン] の順に選択し、作成したゾーンを選択します。ゾーンに正しいインターフェイスが適用されていることを確認します。
8. **Zone Protection Profile**（ゾーン プロテクション プロファイル）ドロップダウンで、作成したプロファイルを選択し、**OK** をクリックします。

STEP 6 | テンプレートの変更をプッシュします。

1. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択し、Push Scope（プッシュ スコープ）で **Edit Selections**（選択内容の編集）を行います。
2. **Templates**（テンプレート）を選択し、変更を行ったテンプレートに割り当てられたファイアウォールを選択します。
3. Panorama 設定およびテンプレートに加えた変更を **Commit and Push**（コミットしてプッシュ）します。

デバイス グループを使用したポリシー ルールのプッシュ

ユースケースの3番目のタスク：Panorama を使用してファイアウォールを構成の3番目の作業は、ファイアウォール上でポリシールールを管理するデバイスグループを作成することです。

STEP 1 | デバイス グループを作成し、適切なファイアウォールを各デバイス グループに割り当てます（「デバイス グループの追加」を参照）。

この例では、DG_BranchAndRegional および DG_DataCenter という名前のデバイス グループを作成します。

DG_BranchAndRegional デバイス グループを設定する際、**Master**（マスター）ファイアウォールを割り当てる必要があります。これはデバイス グループ内でポリシー評価のためにユーザーおよびグループ マッピング情報を収集する唯一のファイアウォールです。

STEP 2 | DNS および SNMP サービスを許可するための共有プレ ルールを作成します。

1. DNS および SNMP サービスの共有アプリケーション グループを作成します。
    1. **Objects** > **Application Group**(オブジェクト > アプリケーション グループ) の順に選択し、**Add**(追加)をクリックします。
    2. 共有アプリケーション グループ オブジェクトを作成するには、**Name**（名前）を入力し、**Shared**（共有）チェック ボックスをオンにします。
    3. **(追加)** をクリックし、「**DNS**」と入力し、リストから **(dns)** を選択します。SNMP についても繰り返し、**snmp**、**snmp-trap** を選択します。
    4. **OK** をクリックしてアプリケーション グループを作成します。
2. 共有ルールを作成します。
    1. **Policies**（ポリシー）タブを選択し、**Device Group**（デバイス グループ）ドロップダウンで **Shared**（共有）を選択します。
    2. **Security** > **Pre-Rules** (セキュリティ > プレルール)ルールベースの順に選択します。
    3. **Add**（追加）をクリックし、セキュリティ ルールの **Name**（名前）にポリシー名を入力します。
    4. ルールの **Source**（送信元）タブと **Destination**（宛先）タブで、**Add**（追加）をクリックし、トラフィックの **Source Zone**（送信元ゾーン）と **Destination Zone**（宛先ゾーン）を入力します。
    5. **Applications**（アプリケーション）タブで、**Add**（追加）をクリックし、作成したアプリケーション グループ オブジェクトの名前を入力し、ドロップダウンからその名前を選択します。
    6. **Actions**（アクション）タブで、**Action**（アクション）を **Allow**（許可）に設定して、**OK** をクリックします。

STEP 3 | すべてのオフィスに適用される会社の有効な使用ポリシーを定義します。この例では、一部の URL カテゴリへのアクセスを制限し、リスク レベルが 3、4、5 のピアツーピア トラフィックへのアクセスを拒否する、共有ルールを作成します。

© 2019 Palo Alto Networks, Inc.

1. **Policies**（ポリシー）タブを選択し、**Device Group**（デバイス グループ）ドロップダウンで **Shared**（共有）を選択します。
2. **Security** > **Pre-Rules**(セキュリティ > プレルール) の順に選択し、**Add** (追加)をクリックします。
3. **General**（全般）タブで、セキュリティルールの **Name**（名前）を入力します。
4. **Source**（送信元）タブと **Destination**（宛先）タブで、**Add**（追加）をクリックし、トラフィックの **Source Zone**（送信元ゾーン）と **Destination Zone**（宛先ゾーン）として **any**（いずれか）を選択します。
5. **Application**（アプリケーション）タブでアプリケーション フィルターを定義します。
   1. **Add**（追加）をクリックし、ドロップダウン リストのフッター領域にある **New Application Filter**（新規アプリケーション フィルター）をクリックします。
   2. **Name**（名前）を入力し、**Shared**（共有）チェック ボックスをオンにします。
   3. Risk（リスク）列で、レベル **3**、**4**、および **5** を選択します。
   4. Technology（テクノロジ）列で、**peer-to-peer**（ピアツーピア）を選択します。
   5. **OK** をクリックして新しいフィルタを保存します。
6. **Service/URL Category**（サービス/**URL** カテゴリ）タブの URL Category（URL カテゴリ）セクションで、**Add**（追加）をクリックし、ブロックするカテゴリ（**streaming-media**、**dating**、**online-personal-storage** など）を選択します。
7. デフォルトの URL フィルタリング プロファイルを適用することもできます。**Actions**（アクション）タブの Profile Setting（プロファイル設定）セクションで、**Profile Type**（プロファイル タイプ）のオプションとして **Profiles**（プロファイル）を選択し、**URL Filtering**（**URL** フィルタリング）のオプションとして **default**（デフォルト）を選択します。
8. **OK** をクリックしてセキュリティ プレルールを保存します。

STEP 4 | 地方支社でのみ、マーケティング グループの全ユーザーに Facebook を許可します。

ユーザーおよびグループに基づいてセキュリティ ルールを有効にする場合、次のような前提条件があります。

- ファイアウォールで User-ID を設定します。
- 識別したいユーザーを含む各ゾーンの User-ID を有効にします。
- DG_BranchAndRegional デバイス グループ用のマスター ファイアウォールを定義します（ステップ 1 を参照）。

1. **Policies**（ポリシー）タブを選択し、**Device Group**（デバイス グループ）ドロップダウンで DG_BranchAndRegional を選択します。
2. **Security** > **Pre-Rules** (セキュリティ > プレルール)ルールベースの順に選択します。
3. **Add**（追加）をクリックし、セキュリティ ルールの **Name**（名前）にポリシー名を入力します。
4. **Source**（送信元）タブでマーケティング グループ ユーザーを含む送信元ゾーンを **Add**（追加）します。
5. **Destination**（宛先）タブで宛先ゾーンを **Add**（追加）します。
6. **User**（ユーザー）タブでマーケティング ユーザー グループをソース ユーザーのリストに**Add**（追加）します。
7. **(**アプリケーション**)** タブで、**(**追加**)** をクリックし、「**`Facebook`**」と入力して、ドロップダウンから (Facebook) を選択します。
8. **Action**（アクション）タブで、**Action**（アクション）を **Allow**（許可）に設定します。
9. **Target**（ターゲット）タブで、地域本部のファイアウォールを選択し、**OK** をクリックします。

STEP 5 | データセンターの指定されたホスト/サーバーに Amazon クラウド アプリケーションのへのアクセスを許可します。

1. Amazon クラウド アプリケーションへのアクセスが必要なデータセンターのサーバー/ホストのアドレス オブジェクトを作成します。

© 2019 Palo Alto Networks, Inc.

1. **Objects** > **Addresses** (オブジェクト > アドレス)を選択し、**Device Group**(デバイス グループ) ドロップダウンリストでDG_DataCenterを選択します。
2. **Add**（追加）をクリックし、アドレス オブジェクトの **Name**（名前）を入力します。
3. **Type**（タイプ）を選択し、IP アドレスおよびネットマスク（**IP Netmask**（**IP** ネットマスク）、IP アドレスの範囲（**IP Range**（**IP** 範囲））、あるいは **FQDN** を指定します。
4. **OK** をクリックしてオブジェクトを保存します。

2. Amazon クラウド アプリケーションへのアクセスを許可するセキュリティ ルールを作成します。
   1. **Policies** > **Security** > **Pre-Rules** (ポリシー > プレルール)を選択し、**Device Group**(デバイス グループ) ドロップダウンリストでDG_DataCenterを選択します。
   2. **Add**（追加）をクリックし、セキュリティ ルールの **Name**（名前）にポリシー名を入力します。
   3. **Source**（送信元）タブを選択し、データセンターの送信元ゾーンを**Add**（追加）し、先ほど定義したアドレス オブジェクト（ソース アドレス）を**Add**（追加）します。
   4. **Destination**（宛先）タブを選択し、宛先ゾーンを **Add**（追加）します。
   5. **Application**(アプリケーション) タブを選択し、**Add**(追加) をクリックし、「`amazon`」と入力して、一覧から Amazon アプリケーションを選択します。
   6. **Action**（アクション）タブを選択し、**Action**（アクション）を **Allow**（許可）に設定します。
   7. **OK** をクリックしてルールを保存します。

STEP 6 | ネットワーク上のインターネット方向へのトラフィックすべてのロギングを有効にするには、Trust ゾーンから Untrust ゾーンに一致するルールを作成します。

1. **Policies**（ポリシー）タブを選択し、**Device Group**（デバイス グループ）ドロップダウンで **Shared**（共有）を選択します。
2. **Security** > **Pre-Rules** (セキュリティ > プレルール)ルールベースの順に選択します。
3. **Add**（追加）をクリックし、セキュリティ ルールの **Name**（名前）にポリシー名を入力します。
4. ルールの **Source**(送信元) タブと **Destination**(宛先) タブで、送信元ゾーンとして`trust_zone`を、宛先ゾーンとして`untrust_zone`を**Add**(追加) します。
5. **Action**（アクション）タブで、**Action**（アクション）を **Deny**（拒否）に設定し、**Log Setting**（ログ設定）を **Log at Session end**（セッション終了時にログ）に設定して、**OK** をクリックします。

ルールのプレビューと変更のコミット

「「ユース ケース：Panorama を使用してファイアウォールを構成」の最後の作業は、ルールを確認し、Panorama、デバイス グループ、およびテンプレートに行った変更をコミットすることです。

STEP 1 | ルールをプレビューします。

このプレビューでは、特定のルールベースについて、ルールがどのようにレイヤー化されているかを視覚的に評価できます。

1. **Policies**（ポリシー）および **Preview Rules**（ルールのプレビュー）を選択します。
2. **Rulebase**（ルールベース）、**Device Group**（デバイス グループ）、**Device**（デバイス）を選択します。
3. 完了したらプレビュー ダイアログを閉じます。

STEP 2 | 設定変更をコミットしてプッシュします。

1. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択し、Push Scope（プッシュ スコープ）で **Edit Selections**（選択内容の編集）を行います。
2. **Device Groups**（デバイス グループ）を選択し、追加したデバイス グループを選択して **Include Device and Network Templates**（デバイスおよびネットワーク テンプレートを含める）によってデバイスとネットワーク テンプレートを含めます。
3. **OK** をクリックして、プッシュ スコープに対する変更を保存します。
4. 変更を **Commit and Push**（コミットしてプッシュ）します。

© 2019 Palo Alto Networks, Inc.

STEP 3 | Panorama によってテンプレートとポリシーの設定が適用されたことを確認します。

1. Panorama のヘッダーで、**Context**（コンテクスト）をファイアウォールに設定し、その Web インターフェイスにアクセスします。
2. テンプレートとポリシーの設定を確認し、変更が適用されていることを確認します。

大規模なファイアウォールのデプロイを管理

Panorama™ は、大規模なファイアウォールのデプロイメントを管理するための複数のオプションを提供します。すべての管理機能を統合するために、Panorama は M-600 アプライアンスを管理専用モードで使用して、最大 5,000 のファイアウォールの管理をサポートするか、Panorama バーチャル アプライアンスを管理専用モードで使用して、最大 2,500 のファイアウォールの管理をサポートします。5,000 を超える大規模なファイアウォールのデプロイメント、および運用管理を簡素化する場合、Panorama Interconnect プラグインを使用すれば、単一の anorama Controller から複数の Panorama 管理サーバーノードを管理することができます。

- 最適な大規模ファイアウォールのデプロイソリューションを決定
- M-600 および Panorama バーチャル アプライアンスのデバイス管理能力の強化
- Panorama Interconnect

最適な大規模ファイアウォールのデプロイソリューションを決定

大規模なファイアウォールのデプロイメント設定を管理する運用上の負担を軽減するため、Palo Alto Networks は、デプロイメントシナリオに最適なさまざまなファイアウォール管理オプションを提供しています。

大規模なファイアウォールのデプロイメントが 1 つまたはごく少数の Panorama 管理サーバで構成されている場合、M-600 アプライアンスをデプロイして最大 5,000 のファイアウォールを管理するか、Panorama バーチャル アプライアンスをデプロイして最大 2,500 のファイアウォールを管理して、単一の Panorama 管理サーバから すべての Panorama の機能を活用します。複数の Panorama 管理サーバをデプロイしてより少ないファイアウォールを管理するのではなく、1 つの Panorama 管理サーバから多数のファイアウォールを管理する垂直スケーリング展開には、M-600 および Panorama バーチャル アプライアンスのデバイス管理能力の強化が最適です。

類似の設定を共有する複数の Panorama 管理サーバで大規模なファイアウォールのデプロイメントを設定している場合、Panorama Interconnectプラグインを使用すれば、1 つの Panorama Controller から複数の Panorama ノードを管理することができます。このプラグインにより単一の Panorama Controller からポリシーや設定を一元的に管理できるようになるため、大規模なファイアウォールのデプロイ環境でデプロイメントや運用の管理が簡単になります。デバイス グループとテンプレート スタックの構成は、Panorama Controller から Panorama ノードに同期され、管理対象デバイスにプッシュされます。Panorama Interconnect プラグインは、複数の分散 Panorama 管理サーバを備えた水平スケーリングのファイアウォール展開に最適です。

© 2019 Palo Alto Networks, Inc.

M-600 および Panorama バーチャル アプライアンスのデバイス管理能力の強化

管理専用モードの M-600 アプライアンスは、最大 5,000 のファイアウォールを管理でき、また管理専用モードの Panorama バーチャル アプライアンスは、最大 2,500 のファイアウォールを管理できるため、大規模なファイアウォール デプロイメントの管理負荷を低減できます。

- デバイス管理能力要件の強化
- Panorama をデプロイしてデバイス管理を強化

デバイス管理能力要件の強化

単一の管理専用モードの M-600 アプライアンスを使用して最大 5,000 のファイアウォールを管理でき、また単一の管理専用モードの Panorama バーチャル アプライアンスを使用して最大 2,500 のファイアウォールを管理できます。このような大規模なデプロイメントを単一の Panorama 管理サーバで管理することにより、構成管理の運用上の複雑性が軽減され、複数の Panorama 管理サーバを管理することによるセキュリティとコンプライアンスのリスクが軽減されます。

ログ収集に関しては、単一の Panorama 管理サーバを使用することにより、個々の Panorama 管理サーバにアクセスする必要がなくなり、管理対象デバイスから収集したログデータを一元化された場所で表示および分析することができるため、理想的です。システムやネットワークの障害が発生した場合に備えて冗長性を提供するため、Palo Alto Networks では、2 つの Panorama™ 管理サーバーを高可用性 (HA) 構成でデプロイすることをお勧めしています。

事前定義されたレポートを生成するには、Panorama が事前定義されたレポートで Panorama データを使用できるようにする必要があります。Panorama または専用ログ コレクタは既に収集されたログデータを使用して事前定義されたレポートを生成するため、レポート生成時のリソースの使用率を削減します。この設定の有効化は必須です。有効化しない場合、Panorama のパフォーマンスに影響を及ぼし、応答しなくなる可能性があります。

Panorama 管理サーバーで最大 5,000 のファイアウォールを管理するには、以下の最低要件を満たす必要があります：

要件	M-Series アプライアンス	Panoramaバーチャル アプライアンス
Model	M-600	サポートされているすべての Panorama ハイパーバイザ。詳細は、「Panorama モデル」を参照してください。
Panoramaモード	管理のみ	管理のみ
管理対象ファイアウォール数	5,000	2,500
システム ディスク	240GB SSD—オペレーティングシステムファイルとシステムログの保存に使用されます。	• 81GB—オペレーティングシステムファイルとシステムログの保存に使用されます。 • 最低 90GB の容量の追加ディスク。

© 2019 Palo Alto Networks, Inc.

要件	M-Series アプライアンス	Panoramaバーチャル アプライアンス
コア	28（ハイパースレッド）	28（ハイパースレッド）
メモリ	256GB	250GB
ログ収集	ローカル ログ収集はサポートされていません。 ログ収集のセットアップについては専用のログ コレクタを使用する Panorama のデプロイを参照してください。	ローカル ログ収集はサポートされていません。 ログ収集のセットアップについては専用のログ コレクタを使用する Panorama のデプロイを参照してください。
ロギングおよびレポート	**Use Panorama Data for Pre-Defined Reports (事前定義済みレポートに Panorama データを使用) する設定を有効にします (Panorama > Setup (セットアップ) > Management (管理) > Logging and Reporting Settings (ロギングおよびレポート設定) > Log Export and Reporting (ログのエクスポートとレポート))**	**Use Panorama Data for Pre-Defined Reports (事前定義済みレポートに Panorama データを使用) する設定を有効にします (Panorama > Setup (セットアップ) > Management (管理) > Logging and Reporting Settings (ロギングおよびレポート設定) > Log Export and Reporting (ログのエクスポートとレポート))**

Panorama をデプロイしてデバイス管理を強化

デバイス管理を強化するために Panorama を展開するには、デプロイメント シナリオを決定し、以下の手順に従います。

- Panorama をインストールしてデバイス管理能力を強化
- Panorama をアップグレードしてデバイス管理能力を強化

Panorama をインストールしてデバイス管理能力を強化

デバイス管理ライセンスをアクティブ化して、単一の M-600 Panorama™ 管理サーバ、または単一の Panorama バーチャル アプライアンスから 1,000 台以上のファイアウォールを管理します。

STEP 1 | Palo Alto Networks の販売代理店にお問い合わの上、最大 5,000 のファイアウォールを管理できる Panorama デバイス管理ライセンスを取得します。

- M-600 アプライアンスをデプロイする場合は、`PAN-M-600-P-1K` デバイス管理ライセンスを取得します。
- Panorama バーチャル アプライアンスをデプロイする場合は、`PAN-PRA-1000` デバイス管理ライセンスを取得します。

STEP 2 | Panorama 管理サーバーをセットアップします。

- （M-600 アプライアンスのみ）M-Series アプライアンスのセットアップ。

or

- Panorama バーチャル アプライアンスのセットアップ.

STEP 3 | Panorama 管理サーバが管理専用モードになっていない場合は、管理専用モードに変更します。

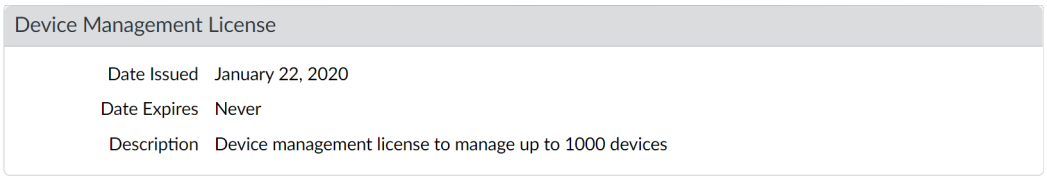
© 2019 Palo Alto Networks, Inc.

- ステップ 5 から開始して 管理専用モードの M-Series アプライアンスのセットアップします。
- 管理専用モードの Panorama バーチャル アプライアンスのセットアップ.

STEP 4 | Panorama 管理サーバーを登録し、ライセンスをインストールします。

1. Panorama の登録.
2. Panorama サポート ライセンスのアクティベーション.
3. Panorama 管理サーバーでデバイス管理ライセンスをアクティブ化します。
   - M-Series アプライアンスにおけるファイアウォール管理ライセンスのアクティベーション/取得.
   - Panorama バーチャル アプライアンスがインターネットに接続していない時のファイアウォール管理ライセンスのアクティベーション/取得.
   - Panorama バーチャル アプライアンスがインターネットに接続している時のファイアウォール管理ライセンスのアクティベーション/取得.

STEP 5 | **Panorama** > **Licenses**を選択し、デバイス管理ライセンスが正常にアクティブ化されていることを確認します。



Panorama で新規デバイス管理ライセンスをアクティブ化する場合、*M-600* アプライアンスで最大 *5,000* のファイアウォール、または *Panorama* バーチャル アプライアンスで最大 *2,500* のファイアウォールを管理できますが、説明には引き続き `Device management license to manage up to 1000 devices or more` と表示されます。

Panorama をアップグレードしてデバイス管理能力を強化

PAN-OS 9.1 以降のリリースにアップグレードして、M-600 アプライアンスの既存のデバイス管理ライセンスを使用して、最大 5,000 のファイアウォールを管理するか、Panorama™ バーチャル アプライアンスを使用して、最大 2,500 のファイアウォールを管理します。

STEP 1 | Panorama バーチャル アプライアンスの CPU およびメモリを増やす パノラマ バーチャル アプライアンスが、デバイス管理を強化するための最小リソース要件をまだ満たしていない場合。

アップグレードする前に、デバイス管理能力要件の強化 を確認して、既存のパノラマ バーチャル アプライアンスが最小要件を満たしているかどうかを確認します。

STEP 2 | Panorama CLI へのログイン.

STEP 3 | Panorama が管理専用モードになっていない場合は変更します。

- （M-600 アプライアンスのみ）ステップ 5 から 管理専用モードの M-Series アプライアンスのセットアップまで。

or

- 管理専用モードの Panorama バーチャル アプライアンスのセットアップ.

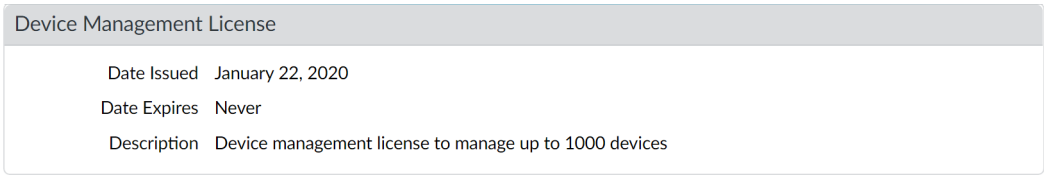
STEP 4 | Panorama Web インターフェイスへのログイン.

STEP 5 | Panorama 管理サーバーをアップグレードします。

© 2019 Palo Alto Networks, Inc.

- Panorama からインターネットに接続できる場合の更新のインストール.
- Panorama からインターネットに接続できない場合の更新のインストール.
- HA 設定の Panorama に更新をインストール.

STEP 6 | **Panorama** > **Licenses**を選択し、デバイス管理ライセンスが正常にアクティブ化されていることを確認します。



デバイス管理ライセンスをアクティブ化してから *PAN-OS 9.1* 以降のリリースにアップグレードした場合、*M-600* アプライアンスでは最大 *5,000* のファイアウォール、または *Panorama* バーチャル アプライアンスでは最大 *2,500* のファイアウォールを管理できますが、説明には引き続き *Device management license to manage up to 1000 devices or more*（最大*1000*台以上のデバイスを管理するためのデバイス管理ライセンス）と表示されます。

© 2019 Palo Alto Networks, Inc.

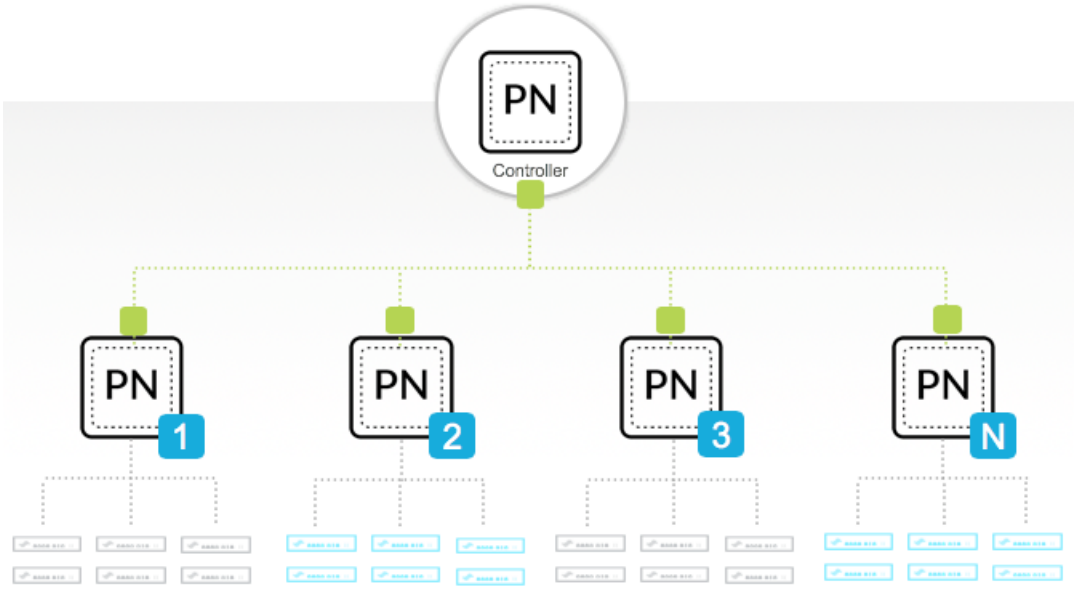
Panorama Interconnect

Panorama™ Interconnect を使用して、大規模なファイアウォールのデプロイメントの設定を管理します。Panorama Interconnect は、複数の Panorama 管理サーバーを同じ構成で管理する際に便利です。

- Panorama Interconnect の概要
- Panorama Interconnect の要件
- Panorama Controller およびノード間の認証を有効化
- Panorama Interconnect プラグインのセットアップ
- Panorama Interconnect の同期
- Panorama Interconnect でファイアウォールを管理
- Panorama Interconnect プラグインのアップグレード

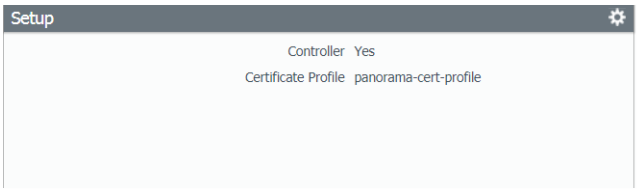
Panorama Interconnect の概要

単一の Panorama インスタンスの管理能力を超える大量のファイアウォールで一様な設定を使用する場合、あるいは複数の Panorama™ 管理サーバーをデプロイした場合、Panorama 上で Interconnect プラグインを使用して運用負荷を減らすことができます。Interconnect プラグインを使用すれば、最大 64 の Panorama ノードを管理できる Panorama Controller をセットアップし、ネットワーク上の Panorama アプライアンスや管理対象のファイアウォールに対して共通で使用する設定やポリシーを効率化できます。例えば、Panorama ノードの管理者ロールなどの Panorama 固有の設定と、すべてのファイアウォールを管理するのに使用する Panorama ノードにプッシュする共通のテンプレート スタックおよびデバイスグループのあらゆる設定の両方を一元的に管理するよう、Panorama Controller をセットアップできます。次の図は Panorama Interconnect の階層構造を示しています。ここでは、Panorama Controller が複数の Panorama ノードを管理、つまり複数のデバイスを管理します。

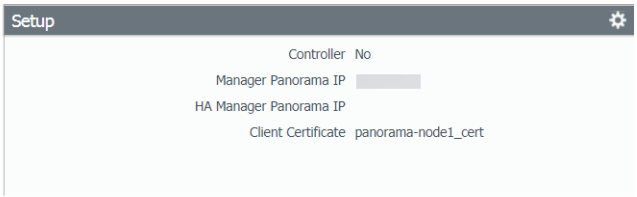


次の図は、設定完了後の Panorama Controller および Panorama ノード用の Panorama Interconnect **Setup** (セットアップ)ページの例です。

© 2019 Palo Alto Networks, Inc.



Panorama Controller



Panorama Node

Panorama Interconnect プラグインをセットアップするには、次の各作業を完了させる必要があります：

タスク	詳細
次をレビューPanorama Interconnect の要件	Panorama 管理サーバーとファイアウォールがシステムおよび運用の要件を満たしていなければ、Panorama Interconnect を正常にデプロイできません。 これには、ライセンスのインストールおよびアクティベート、Panorama 管理サーバーの登録が含まれます。
Panorama Controller およびノード間の認証を有効化	認証局を生成あるいはインポートし、ノード用の証明書を発行し、証明書プロファイルを構成して Panorama Controller および Panorama ノード間の通信を保護します。
Panorama Interconnect プラグインのセットアップ	Panorama Controller および Panorama ノード上で Panorama Interconnect プラグインをダウンロード、インストール、セットアップします。
Panorama Controller が構成を管理対象のファイアウォールにプッシュするための準備を行います	Panorama Controller でデバイス グループの追加およびテンプレート スタックの設定を行ってポリシールール、オブジェクト、設定を構成し、ファイアウォールがネットワーク上で稼働できるようにします。
Panorama Interconnect の同期	Panorama 固有の設定、テンプレート スタックおよびデバイスグループの設定を Panorama Controller から Panorama ノードにプッシュします。
Panorama Interconnect でファイアウォールを管理	ファイアウォールを一つあるいは複数追加し、同期済みの設定を Panorama ノードから管理対象のデバイスにプッシュします。

Panorama Interconnect の要件

Panorama 管理サーバーで Panorama™ Interconnect プラグインを正常にデプロイするための要件を計画・確認します。

- Panorama Interconnect のデプロイ計画
- Panorama Interconnect のシステム要件
- Panorama Interconnect の証明書要件

© 2019 Palo Alto Networks, Inc.

Panorama Interconnect のデプロイ計画

Panorama 管理サーバーで Panorama™ Interconnect プラグインを正常にデプロイするためには：

- Panorama Interconnect のシステム要件を確認します。

  Panorama とマネージドファイアウォールが最小のリソース要件を満たしており、ファイアウォールが single-vsys ファイアウォールであることを確認します。
- Panorama Node とマネージドファイアウォールのデバイス グループとテンプレート スタック設定を計画します。

  設定管理は Panorama Controller で一元化され、Panorama Controller により管理されるすべての Panorama Node に複製されます。この設定がシンプル、コンパクト、かつすべての Panorama Node でほぼ同一であることを確認してください。

  相互接続は、オブジェクト、ポリシー、ファイアウォール、およびネットワーク設定を含むデバイス グループとテンプレートに基づく一元化された設定をサポートします。NSX、SD-WAN、Prisma Access などの Panorama Integration プラグインにより追加された増分機能は、相互接続デプロイメントでサポートされません。

  Panorama Node 設定は、*Panorama Controller* からのみ管理できます。*Panorama Node* で行われた設定変更は、Panorama Node と Panorama Controller を同期 すると上書きされます。
- Panorama Controller および Panorama ノードを Management Only（管理専用）モードに設定します。Panorama 管理サーバーのモードを変える詳細な方法については、管理専用モードの M-Series アプライアンスのセットアップあるいは管理専用モードの Panorama バーチャル アプライアンスのセットアップを参照してください。

  ローカルでログ収集を行う *Panorama* モードの *Panorama Controller* あるいは *Panorama* ノードに *Panorama Interconnect* をデプロイすると、管理プロセスやログ収集プロセスで多くのリソースが必要になるため、パフォーマンスが低下するおそれがあります。
- Panorama の登録とライセンスのインストール（Panorama Controller および Panorama ノードの場合）。
- ログ収集を行うための専用ログコレクタを一つあるいは複数デプロイします。Log Collection（ログ収集）モードで Panorama 管理サーバーをデプロイするためのログ保持要件と流れの詳細については、Panorama のセットアップを参照してください。

  ログとレポートの生成は、Panorama Node からのみ利用可能です。
- プラグインをインストールする前に、Panorama Controller およびすべての Panorama ノードが Operational（運用）モードであることを確認してください。Panorama Interconnect プラグインは FIPS モードの Panorama 管理サーバーをサポートしていないため、Panorama 管理サーバーが反応しなくなるおそれがあります。
- 認証局（CA）を取得して Panorama Controller CA が署名した Panorama ノード証明書を発行し、Panorama Controller および Panorama ノード間の通信を保護します。詳細は、「Panorama Controller およびノード間の認証を有効化」を参照してください。
- ファイアウォールの Web インターフェイスおよび Panorama Web インターフェイスへのログインを行えるよう、Panorama Controller、Panorama ノード、管理対象のファイアウォールの HTTPS アクセスを有効化します。Panorama Interconnect は CLI および API アクセスをサポートしていません。

Panorama Interconnect のシステム要件

Panorama Interconnect プラグインを正しくインストールして大規模なファイアウォールのデプロイメントを管理できるよう、Panorama™ 管理サーバーおよびファイアウォールが次のシステム要件を満たしていることを確認します。

- Panorama Interconnect は 1 つの VSYS ファイアウォールのみを管理することができます

© 2019 Palo Alto Networks, Inc.

要件	Panorama Controller およびノード	ファイアウォール
モード	管理専用（推奨）	N/A
CPU とメモリ	16 CPU と 32GB メモリ	N/A
システム ディスク	81GB	N/A
サポートされている OS	PAN-OS 8.1.3 以降のリリース	PAN-OS 7.1 以降のリリース
サポートされているモデル	• **M-Series** アプライアンス—M-600 • **Panorama** バーチャル アプライアンス—サポートされているすべての Panorama バーチャル アプライアンスのモデルについては、Panorama モデルを参照してください。	• 物理的ファイアウォール—サポートされているすべての物理的ファイアウォールのモデルについては、ファイアウォールのモデルを参照してください。 • **VM-Series** ファイアウォール—サポートされているすべての VM-Series ファイアウォールについては、VM-Series モデルを参照してください。

Panorama Interconnect の証明書要件

Panorama™ Controller および Panorama ノード間の通信を保護するために、使用する証明書が次の要件を満たしていることを確認してください：

- Panorama ノードに証明書を発行した認証局（CA）が Panorama Controller で必須になっていなければなりません。自己署名ルート CA 証明書の作成を行うか、あるいは証明書および秘密鍵をインポートして署名します。Interconnect プラグインをセットアップするには、**Panorama**タブで CA 証明書を設定しておかなければなりませんので、ご注意ください。
- 各 Panorama ノードに対して証明書をインポートするか、一意の証明書を生成します。Panorama Controller 上の CA 証明書が、ノードで使用する証明書を発行する必要があります。
  - 証明書を Panorama ノードにインポートする場合は、証明書の**Common Name** (共通名)が Panorama ノードのシリアル番号になっていることを確認してください。
  - 証明書が PKCS12 あるいは PEM 形式であり、かつ秘密鍵が含まれていなければ、Panorama ノードが認証に失敗します。

Panorama Controller およびノード間の認証を有効化

Panorama™ Controller および Panorama ノード間の通信を保護する証明書プロファイルを作成します。

- Panorama Controller 用の CA 証明書を取得
- Panorama ノード証明書の生成
- Panorama ノードを認証するための証明書プロファイルを作成

Panorama Controller 用の *CA* 証明書を取得

インターネット接続を保護するために、Panorama™ ノードに証明書を反抗する信頼できる認証局（CA）を作成します。大規模なファイアウォールのデプロイメントで使用する Panorama をセットアップする際に、信頼できる CA が必要になります。

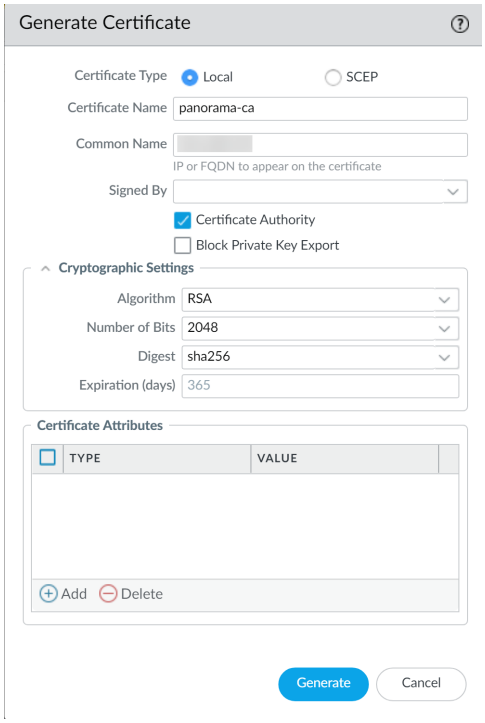
STEP 1 | Panorama Web インターフェイスへのログイン（Panorama Controller の）。

© 2019 Palo Alto Networks, Inc.

STEP 2 | 認証局の証明書を作成します。

- 新しい **CA** 証明書を生成

1. **Panorama** > **Certificate Management**（証明書の管理）> **Certificates** (証明書)の順に選択し、新しい証明書を**Generate** (生成)します。
2. **Certificate Type** (証明書タイプ)は**Local** (ローカル)を選択します。
3. **Certificate Name** (証明書名)に`panorama-CA`などを入力します。名前は大文字小文字を区別し、最大 31 文字を使用できます。英字、数字、ハイフン、およびアンダースコアのみを使用し、一意である必要があります。
4. **Common Name** (共通名) フィールドに、Panorama Controller の IP アドレスまたは FQDN を入力します。
5. **Signed By**[署名者] フィールドは空白のままにし、証明書を自己署名として指定します。
6. **Certificate Authority**（認証局）チェックボックスをオンにします。
7. CA 証明書を **Generate** (生成)します。

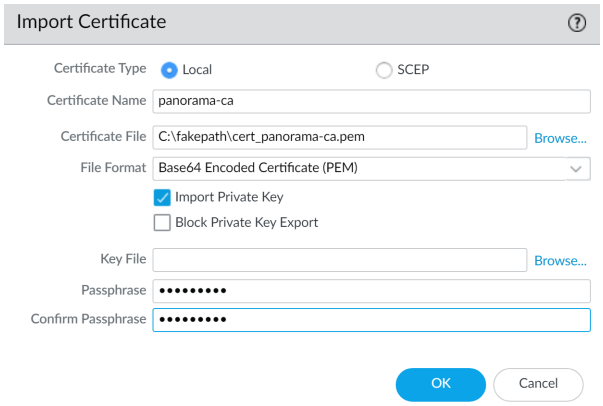


- 既存の **CA** 証明書をインポート

1. **Panorama** > **Certificate Management**（証明書の管理）> **Certificates** (証明書)の順に選択し、CA 証明書を**Import** (インポート)します。
2. **Certificate Name** (証明書名)に`panorama-CA`などを入力します。名前は大文字小文字を区別し、最大 31 文字を使用できます。英字、数字、ハイフン、およびアンダースコアのみを使用し、一意である必要があります。
3. **Certificate File** (証明書ファイル)を**Browse** (参照)します。
4. 以下の **File Format**[ファイル 形式] を選択します。
   - **Base64 Encoded Certificate (PEM)**[Base64 エンコード済み証明書（PEM）] – 証明書とは別にキーをインポートする必要があります。**Import Private Key** (秘密鍵のインポート)のチェックボックスを選択し、**Key File** (鍵ファイル)を**Browse** (参照)します。
   - **Encrypted Private Key and Certificate (PKCS12)**[暗号化された秘密鍵と証明書（PKCS12）] – 一般的な形式であり、キーおよび証明書が単一のコンテナに（**Certificate File**[証明書ファイル]）格納されています。
5. キーの暗号化に使用する **Passphrase** (パスフレーズ) に入力して、再入力（確認）します。

© 2019 Palo Alto Networks, Inc.

6. **OK** をクリックします。インポートした CA 証明書が Certificates (証明書) ページに表示されます。



STEP 3 | **Commit (コミット)**および**Commit to Panorama (Panoramaにコミット)**をクリックします。

Panorama ノード証明書の生成

Panorama™ Controller に各 Panorama ノードを認証させるために、各 Panorama ノードが使用する一意のクライアント証明書を作成します。Panorama Controller およびノードは、証明書ベースの認証を使用してお互いに安全に通信を行います。一意の Panorama ノード証明書を生成する豆に、Panorama Controller 用の CA 証明書を取得を行います。

Panorama ノードが高可用性 (HA) 設定の場合は、両方の Panorama ノードの Panorama ノード証明書を作成して、HA 設定の各ピアにインポートしなければなりません。

STEP 1 | Panorama Web インターフェイスへのログイン (Panorama Controller の) 。

STEP 2 | **Panorama** > **Certificate Management** (証明書の管理) > **Certificates (証明書)**の順に選択し、新しい証明書を**Generate (生成)**します。

1. **Certificate Type (証明書タイプ)**は**Local (ローカル)**を選択します。

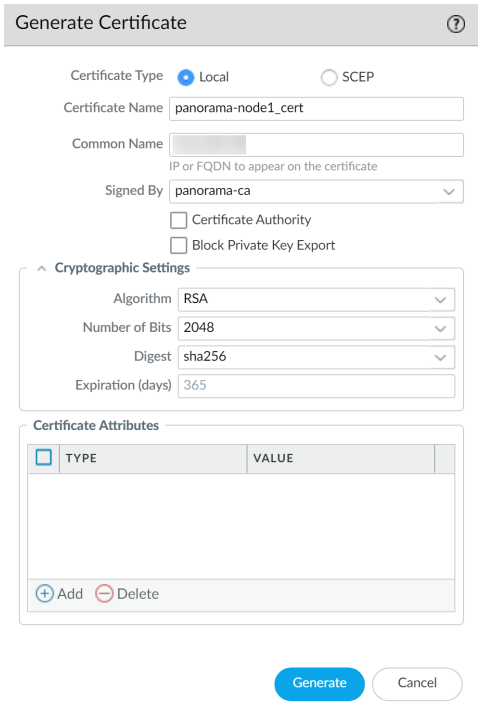
   SCEP は現在サポートされていません。

2. **Certificate Name (証明書名)**に`panorama-node1_cert`などを入力します。名前は大文字小文字を区別し、最大 31 文字を使用できます。英字、数字、ハイフン、およびアンダースコアのみを使用し、一意である必要があります。
3. **Common Name (共通名)** フィールドに、Panorama ノードのシリアル番号を入力します。

   Panorama Controller および *Panorama* ノード間の通信の認証を行うために、*Common Name (共通名)*フィールドにシリアル番号を入力する必要があります。このフィールドにシリアル番号が入力されていない場合、*Panorama* ノードは *Panorama Controller* に接続できません。

4. **Signed By** (署名者) フィールドで CA 証明書を選択します。
5. 証明書を **Generate**[生成] します。

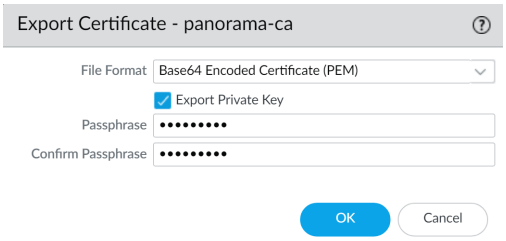
© 2019 Palo Alto Networks, Inc.



STEP 3 | **Commit (コミット)**および**Commit to Panorama (Panoramaにコミット)**をクリックします。

STEP 4 | ステップ2で生成された各 Panorama ノードの証明書をエクスポートします。

1. **Panorama** > **Certificate Management (証明書管理)** > **Certificates (証明書)**の順に移動して証明書を選択し、**Export Certificate (証明書をエクスポート)**します。
2. **File Format (ファイル形式)**を選択します：
   - **Base64** エンコード済み証明書（**PEM**） - 証明書と秘密鍵を別々にエクスポートできます。エクスポートされたファイルに秘密鍵を含める場合は、**Export Private Key** [秘密鍵のエクスポート]チェック ボックスをオンにします。
   - 暗号化された秘密鍵と証明書（**PKCS12**） - 証明書と秘密鍵を 1 つのファイルにエクスポートします。
3. **Export private key (秘密鍵のエクスポート)**ボックスにチェックを入れます。
4. 秘密鍵を暗号化するための**Passphrase**（パスフレーズ）および**Confirm Passphrase**（パスフレーズの確認）を入力します。このパスフレーズは、証明書のキーを Panorama ノードにインポートする際に使用します。
5. **OK** をクリックして、証明書/キー ファイルをコンピュータに保存します。



6. インポート対象の Panorama ノードが見つけやすくなるよう、分かりやすいファイル名を入力して証明書を**Save (保存)**します。

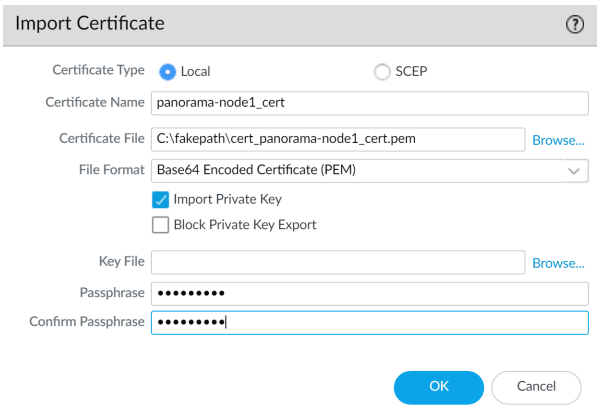
STEP 5 | 証明書を各 Panorama ノードにインポートします。

1. Panorama Web インターフェイスへのログイン（Panoramaノードの）。

© 2019 Palo Alto Networks, Inc.

2. **Panorama** > **Certificate Management**（証明書の管理）> **Certificates** (証明書)の順に選択し、証明書を**Import** (インポート)します：
   1. **Certificate Type** (証明書タイプ)は**Local** (ローカル)を選択します。

      SCEP は現在サポートされていません。
   2. 同じ**Certificate Name** (証明書名)を入力します。名前は大文字小文字を区別し、最大 31 文字を使用できます。英字、数字、ハイフン、およびアンダースコアのみを使用し、一意である必要があります。
   3. ステップ4でエクスポートした証明書を**Browse** (参照)します。
   4. **Import private key** (秘密鍵のインポート)ボックスにチェックを入れます。
   5. 秘密鍵を暗号化するために使用する**Passphrase**（パスフレーズ）および**Confirm Passphrase**（パスフレーズの確認）を入力します。
   6. **[OK]** をクリックして、証明書をインポートします。



3. **Commit** (コミット)および**Commit to Panorama** (**Panorama**にコミット)をクリックします。

Panorama ノードを認証するための証明書プロファイルを作成

証明書プロファイルは、Panorama™ コントローラと Panorama ノード間の通信を保護し、Panorama ノードの失効ステータスを確認するために使用される、Panorama ノード証明書の確認に使用する認証局（CA）証明書を定義します。大規模なファイアウォール展開で Panorama をセットアップする場合、証明書プロファイルが必要です。

STEP 1 | Panorama Web インターフェイスへのログイン（Panorama Controller の）。

STEP 2 | Panorama Controller 用の CA 証明書を取得.

STEP 3 | Panorama ノード証明書の生成Panorama Controller および Panorama ノード間の通信を保護するために使用します。すべての Panorama ノードに対してこのステップを繰り返します。

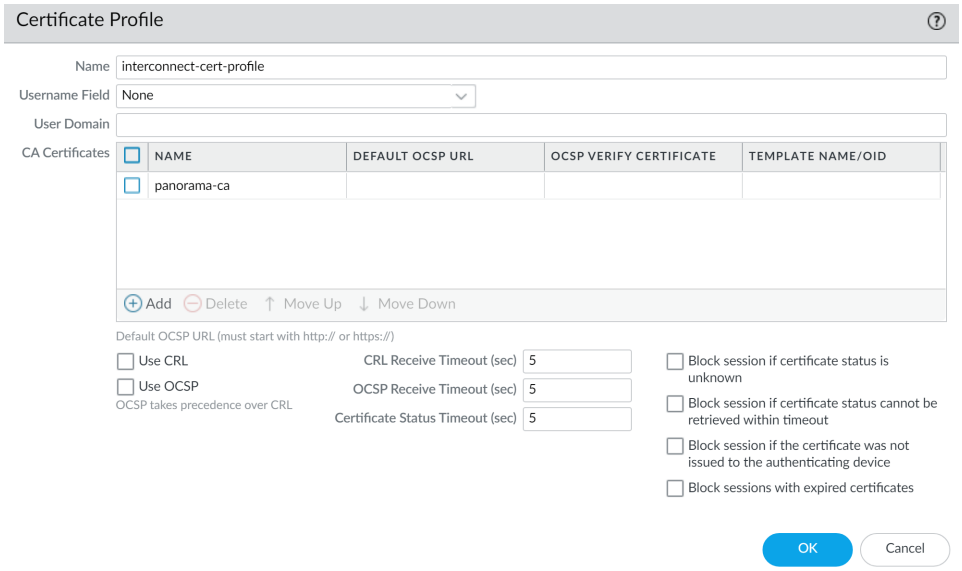
STEP 4 | 証明書プロファイルを作成します。

*CRL*および*OCSP*は現在サポートされていません。

1. **Panorama** > **Certificate Management**（証明書の管理）> **Certificate Profile**（証明書プロファイル）の順に選択し、新しい証明書プロファイルを **Add**(追加)します。
2. 証明書プロファイルの**Name**（名前）を入力します。
3. ステップ2で作成した CA 証明書を**Add** (追加)します。

© 2019 Palo Alto Networks, Inc.

4. **OK** をクリックして、証明書プロファイルの追加を完了させます。



STEP 5 | **Commit (コミット)**および**Commit to Panorama (Panoramaにコミット)**をクリックします。

Panorama Interconnect プラグインのセットアップ

Panorama™ Interconnect を使って大規模なファイアウォールのデプロイメント環境でテンプレート スタックおよびデバイスグループの管理を一元的に行い、Panorama Controller から Panorama ノードに複製した設定をプッシュし、必ずファイアウォールの設定およびセキュリティ ポリシーの間で一貫性が保たれるようにします。Panorama Interconnect を使用すれば、ファイアウォールを管理して設定をプッシュする Panorama ノードを管理する目的で使用する Panorama Controller を構築できます。これにより、単一の場所から大規模なファイアウォールのデプロイメントの設定を管理し、複数の Panorama 管理サーバーを素早く構成したり、設定ミスがあった場合のセキュリティの脆弱性を減らしたりすることができます。Panorama 管理サーバー上で Panorama Interconnect プラグインをセットアップする前に、Panorama Interconnect の要件を確認してください。

Panorama ノードが高可用性（HA）設定になっている場合は、両方の Panorama HA ピアに Panorama Interconnect プラグインを設定する必要があります。

STEP 1 | Panorama Interconnect プラグインをインストールします。Panorama Controller およびすべての Panorama ノードにプラグインをインストールする必要があります。

1. Panorama Web インターフェイスへのログイン.
2. **Panorama** > **Plugins (プラグイン)**を選択して`Interconnect`を検索します。
3. Panorama Interconnect プラグインを**Download (ダウンロード)**して**Install (インストール)**します。
4. **Commit (コミット)** > **Commit to Panorama (Panorama にコミット)**をクリックし、Panorama Interconnect プラグインのインストールを完了させます。

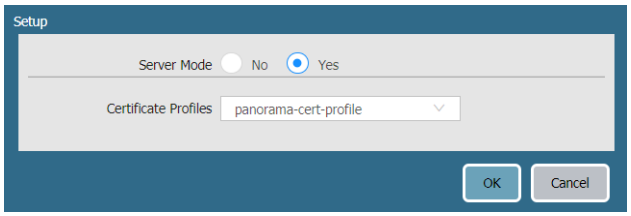
STEP 2 | （Panorama Controller および Panorama ノード間の認証を保護するためPanorama Controller およびノード間の認証を有効化）。

STEP 3 | Panorama Controller 上でプラグインをセットアップします。Panorama Controller が HA 構成である場合、高可用性ピアでこのステップを繰り返します。

© 2019 Palo Alto Networks, Inc.

Panorama Controller として構成した *Panorama* は、*Panorama* ノードとして再構成できなくなります。続行する前に、正しい *Panorama* 管理サーバーを *Panorama Controller* として構成しようとしているか確認してください。

1. **Panorama** > **Interconnect** > **Setup** (セットアップ)を選択して**Interconnect Plugin Setup** (**Interconnect** プラグインのセットアップ)を編集します：
2. **Server Mode** (サーバーモード)フィールドで**Yes** (はい)を選択します。
3. **Certificate Profile** (証明書プロファイル)で、ステップ 2 で作成したプロファイルを選択します。
4. **OK** をクリックして設定を保存します。

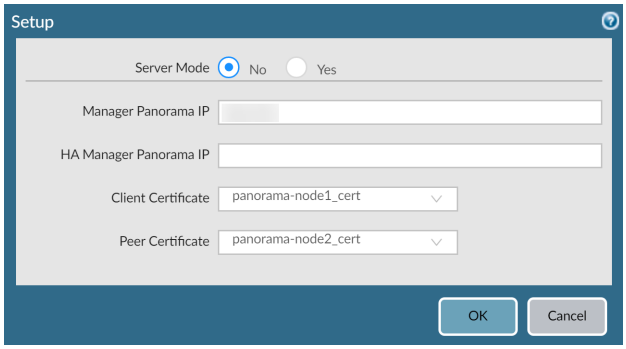


5. **Commit** (コミット)および**Commit to Panorama** (**Panorama**にコミット)をクリックします。

STEP 4 | Panorama ノード上でプラグインをセットアップします。すべての Panorama ノードに対してこのステップを繰り返します。

Panorama ノードが高可用性（*HA*）設定になっている場合、各ピアで*Panorama Interconnect* プラグインを設定するときに、各 *Panorama* ノード*HA*ピアにインポートした *Panorama* ノード証明書を選択しなければなりません。

1. **Panorama** > **Interconnect** > **Setup** (セットアップ)を選択して**Interconnect Plugin Setup** (**Interconnect** プラグインのセットアップ)を編集します：
   1. **Server Mode** (サーバーモード)フィールドで**No** (いいえ)を選択します。
   2. **Manager Panorama IP** (マネージャー **Panorama IP**)—Panorama Controller の管理 IP アドレスを入力します。
   3. **HA Manager IP** (**HA** マネージャー **IP**)—Panorama Controller が高可用性構成である場合、HA Panorama Controller ピアの管理 IP アドレスを入力します。
   4. ステップ2でインポートした Panorama ノード証明書を選択します。
   5. （HA のみ）ステップ 2 でインポートしたピア Panorama ノード証明書を選択します。
2. **OK** をクリックして設定を保存します。



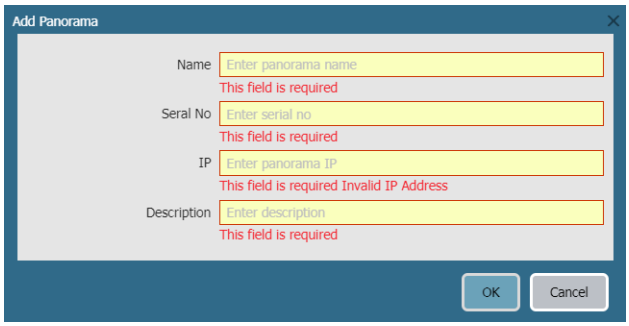
3. **Commit** (コミット)および**Commit to Panorama** (**Panorama** にコミット)をクリックし、Panorama ノード上のプラグインのセットアップを完了させます。

STEP 5 | Panorama ノードを Panorama Controller に追加します。

© 2019 Palo Alto Networks, Inc.

1. **Panorama** > **Interconnect** > **Panorama Nodes (Panorama** ノード)を選択して Panorama ノードを**Add** (追加)します。
    1. Panorama ノードの **Name** (名前) を入力します。これは、Panorama 管理サーバーで設定されている Device Name (デバイス名) と同じでなくても構いません。

        Panorama ノードの*Name* (名前)にはピリオド (.) を使用できません。
    2. Panorama ノードの**Serial No** (シリアル番号)を入力します。
    3. Panorama ノードの **IP** アドレスを入力します。Panorama Controller がアクセスできる IP アドレスでなければなりません。
    4. Panorama ノードの**Description** (説明)を入力します。
2. **OK**をクリックして Panorama ノードを追加します。



3. **Commit** (コミット)および**Commit to Panorama** (**Panorama** にコミット)をクリックし、Panorama ノードの追加を完了させます。

STEP 6 | 新たに追加した Panorama ノードが`Connected` (接続済み) であることを確認します。

1. **Panorama** > **Interconnect** > **Panorama Nodes (Panorama** ノード)を選択します。
2. 追加した Panorama ノードを探し、Connection Status (接続ステータス) 列に`Connected` (接続済み) と表示されていることを確認します。

	Name	Description	IP Address	Serial Number	Connection Status	Host Name
	panorama-node1	Panorama Node 1			connected	

STEP 7 | プラグインを正常に Panorama Controller および Panorama ノードにインストールしたら、次のステップを行って Panorama Interconnect のセットアップを完了させます：

1. Panorama Controller でデバイス グループの追加を行います。このステップを繰り返し、デバイス グループを必要な数だけ作成します。
2. Panorama Controller でテンプレート スタックの設定を行います。このステップを繰り返しテンプレート スタックを必要な数だけ作成します。
3. （Panorama 固有の設定、テンプレート スタックおよびデバイスグループの設定を Panorama Controller から Panorama ノードにプッシュするためPanorama Interconnect の同期）。
4. Panorama Controller で、Panorama ノードが管理するファイアウォールを一つあるいは複数追加します。
    - ファイアウォールを Panorama ノードに追加
    - 複数のファイアウォールを Panorama ノードにインポート
5. Panorama ノードの設定を管理対象のデバイスにプッシュ.

© 2019 Palo Alto Networks, Inc.

Panorama Interconnect の同期

Panorama™ テンプレート スタックおよびデバイスグループの設定を Panorama Controller からプッシュするには、Panorama™ ノードの設定を Panorama Controller と同期し、すべての Panorama 固有の設定を同期して Panorama ノードが設定を管理対象のデバイスにプッシュできるようにします。

- 一般的な Panorama 設定をPanorama ノードにプッシュ
- Panorama ノードとPanorama Controller の同期

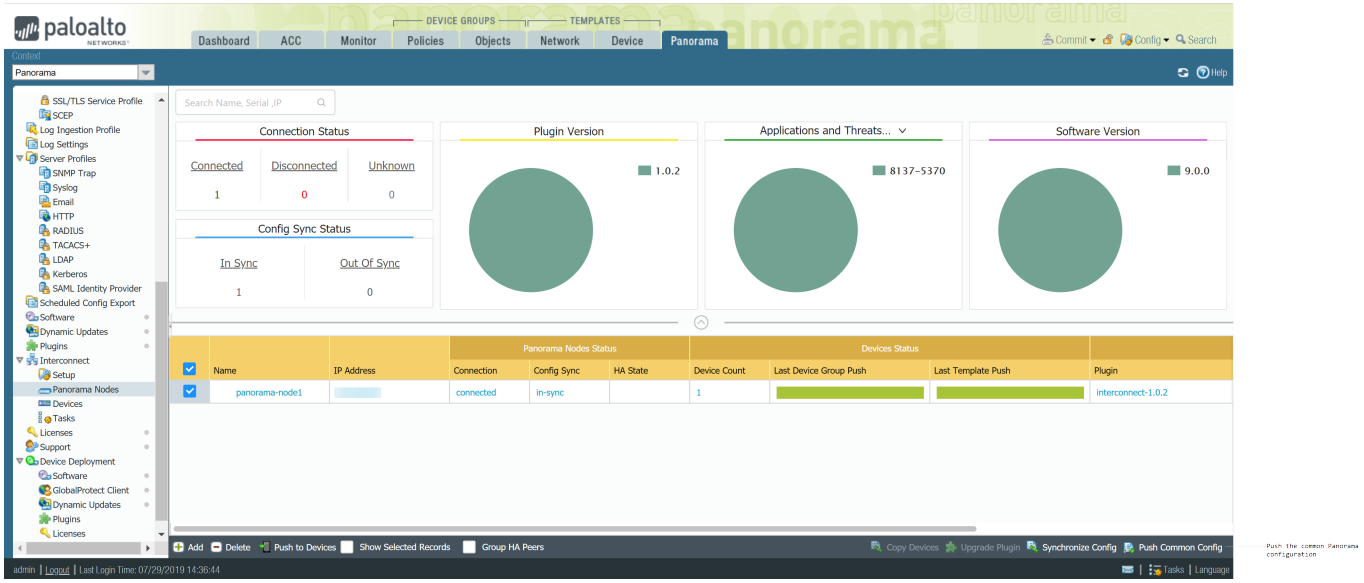
一般的な *Panorama* 設定を*Panorama* ノードにプッシュ

Panorama™ Controller の共通の設定を Panorama ノードにプッシュし、Panorama 固有の設定を Panorama ノードに適用します。テンプレート スタックおよびデバイスグループの設定を同期して管理対象のデバイスにプッシュする方法については、Panorama ノードとPanorama Controller の同期を参照してください。

STEP 1 | Panorama Web インターフェイスへのログイン（Panorama Controller の）。

STEP 2 | **Panorama** > **Interconnect** > **Panorama Nodes (Panorama** ノード)を選択し、設定をプッシュするためにファイアウォールを管理している Panorama ノードを選択します。

STEP 3 | **Push Common Config** (共通の設定をプッシュ)し、Panorama 固有の設定を Panorama ノードにプッシュします。



Panorama ノードと*Panorama Controller* の同期

Panorama™ Controller の設定を Panorama ノードと同期し、Panorama ノードがテンプレート スタックおよびデバイスグループの設定を管理対象のデバイスにプッシュできるようにします。

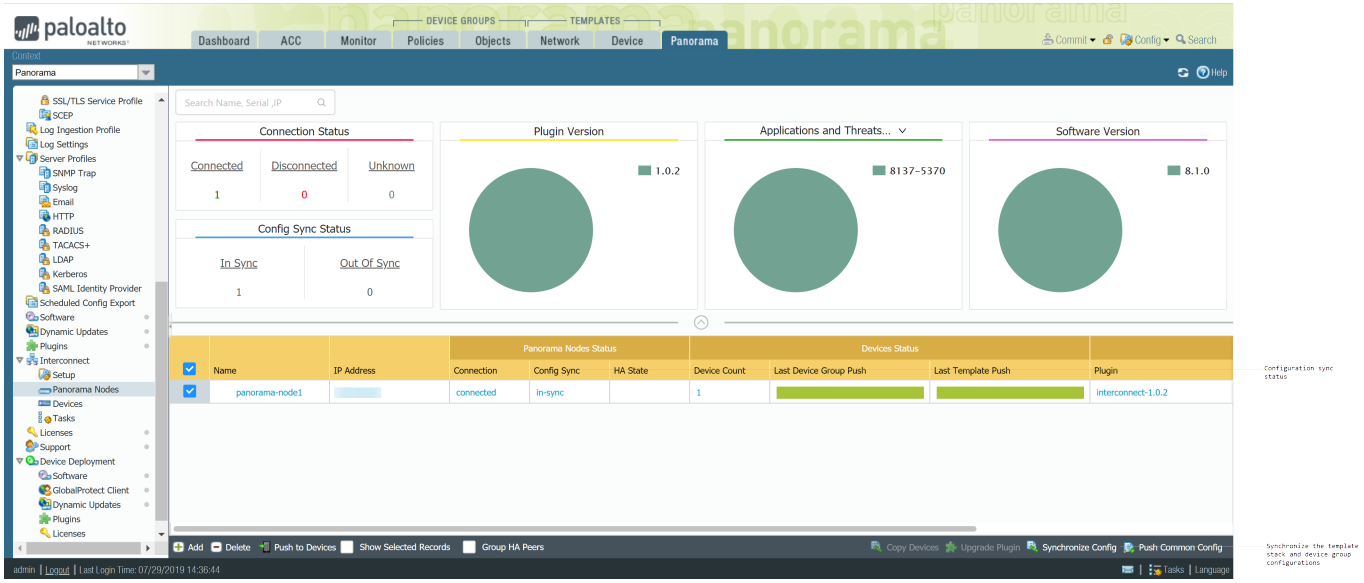
STEP 1 | Panorama Web インターフェイスへのログイン（Panorama Controller の）。

STEP 2 | **Panorama** > **Interconnect** > **Panorama Nodes (Panorama** ノード)を選択し、Panorama Controller と同期させる Panorama ノードを選択します。

STEP 3 | **Synchronize Config** (設定を同期)し、デバイスグループおよびテンプレート スタックの設定を Panorama ノードにプッシュします。管理対象デバイスに設定をプッシュするために、これが必要になります。

© 2019 Palo Alto Networks, Inc.

STEP 4 | Sync Status (同期ステータス) 列で、Panorama ノードが**in-sync** (同期中) であることを確認します。



Panorama Interconnect でファイアウォールを管理

Panorama™ ノードで管理する単一のファイアウォールを追加、あるいは複数のデバイスを一括インポートします。

-
-
-
-
-

ファイアウォールを *Panorama* ノードに追加

Panorama™ ノードが管理する単一のファイアウォールを追加し、単一の Panorama Controller からテンプレート スタックおよびデバイス グループ設定を一元的に管理できるようにします。複数のファイアウォールを一括インポートする方法については、複数のファイアウォールを Panorama ノードにインポートを参照してください。

STEP 1 | Panorama ノードと通信するようにファイアウォールを設定します。

1. ファイアウォールで初期設定を行い、ネットワーク経由でアクセスし、Panorama と通信できるようにします。
2. Panorama ノードの IP アドレスをファイアウォールに追加します。
   1. **[Device]** > [セットアップ] > [管理] の順に選択し、[Panorama 設定] を編集します。
   2. 先頭のフィールドに Panorama の IP アドレスを入力します。
   3. (任意) Panorama で高可用性ペアをセットアップした場合は、2 番目のフィールドにセカンダリ Panorama の IP アドレスを入力します。
   4. **OK** をクリックします。
3. **Commit** (コミット) を選択し、変更内容を **Commit** (コミット) します。

STEP 2 | Panorama Web インターフェイスへのログイン (Panorama Controller の) 。

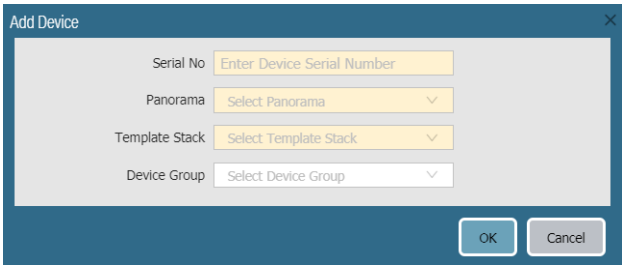
© 2019 Palo Alto Networks, Inc.

STEP 3 | **Panorama** > **Interconnect** > **Devices** (デバイス)を選択してファイアウォールを**Add** (追加)します。

STEP 4 | ファイアウォールの情報を入力します。

- ファイアウォールの**Serial No** (シリアル番号)を入力します。
- ファイアウォールを管理する**Panorama**ノードを選択します。
- ファイアウォールの設定を管理するために使用する**Template Stack** (テンプレート スタック)を選択します。
- ファイアウォールを関連付ける**Device Group** （ デバイス グループ ）を選択します。

STEP 5 | **OK**をクリックして管理対象デバイスとしてファイアウォールを追加します。

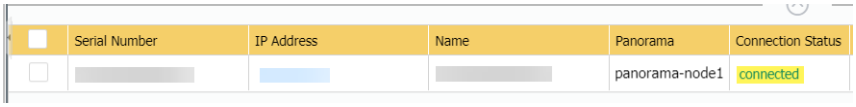


STEP 6 | **Commit** (コミット)および**Commit to Panorama** (**Panorama** にコミット)をクリックし、ファイアウォールを追加する作業を完了させます。

STEP 7 | **Panorama** > **Interconnect** > **Panorama Nodes** (**Panorama** ノード)、さらに**Synchronize Config** (設定の同期)を選択します。

STEP 8 | 新たに追加したファイアウォールが`Connected` (接続済み) であることを確認します。

1. **Panorama** > **Interconnect** > **Panorama Nodes** (**Panorama** ノード)を選択します。
2. 追加したファイアウォールを探し、Connection Status (接続ステータス) 列に`Connected` （接続済み）と表示されていることを確認します。



複数のファイアウォールを *Panorama* ノードにインポート

インポート作業の間に入手できる CSV テンプレートを使用すれば、Panorama™ ノードが管理する複数のファイアウォールをインポートできます。一度に複数のファイアウォールをインポートすることで、素早く複数のファイアウォールを Panorama ノードに追加し、それらをテンプレート スタックおよびデバイス グループに割り当てて設定管理を一元化することができます。

複数のファイアウォールをインポートする際、異なる Panorama ノード、テンプレート スタックおよびデバイスグループにファイアウォールを追加できます。例えば、それぞれが 2 つのテンプレート スタックと 2 つのデバイスグループを持つ Panorama ノード A と Panorama ノード B をデプロイしたとします。100 件のファイアウォールをインポートする場合、それらを次の方法でインポートできます：

- 50 件のファイアウォールを Panorama ノード A に追加します：
  - 25 件のファイアウォールをテンプレート スタック A1 および デバイスグループ A1 に割り当てます。
  - 25 件のファイアウォールをテンプレート スタック A2 および デバイスグループ A2 に割り当てます。
- 50 件のファイアウォールを Panorama ノード B に追加します：

© 2019 Palo Alto Networks, Inc.

- 30 件のファイアウォールをテンプレート スタック B1 および デバイスグループ B1 に割り当てます。
- 20 件のファイアウォールをテンプレート スタック B2 および デバイスグループ B2 に割り当てます。

単一のファイアウォールを追加する場合は、ファイアウォールを Panorama ノードに追加を参照してください。

STEP 1 | Panorama ノードと通信するようにファイアウォールを設定します。

Interconnect プラグインを使用して Panorama が管理するすべてのファイアウォールに対してこのステップを繰り返します。

1. ファイアウォールで初期設定を行い、ネットワーク経由でアクセスし、Panorama と通信できるようにします。
2. Panorama ノードの IP アドレスをファイアウォールに追加します。
   1. **[Device]** > [セットアップ] > [管理] の順に選択し、[Panorama 設定] を編集します。
   2. 先頭のフィールドに Panorama の IP アドレスを入力します。
   3. （任意）Panorama で高可用性ペアをセットアップした場合は、2 番目のフィールドにセカンダリ Panorama の IP アドレスを入力します。
   4. **OK** をクリックします。
3. **Commit**（コミット）を選択し、変更内容を **Commit**（コミット）します。

STEP 2 | Panorama Web インターフェイスへのログイン（Panorama Controller の）。

STEP 3 | **Commit (コミット)**をクリックし、保留中の Panorama Controller の変更内容を**Commit to Panorama (Panorama** にコミット)します。Panorama Controller に対する保留中の変更がある場合は複数のファイアウォールをインポートできず、インポートが失敗します。

STEP 4 | **Panorama** > **Interconnect** > **Devices (デバイス)**を選択してファイアウォールを**Import (インポート)**します。

STEP 5 | **Download Sample CSV (サンプル CSV** のダウンロード)をクリックし、複数のファイアウォールのアップロードに使用する、正しい書式の CSV ファイルのテンプレートをダウンロードします。

STEP 6 | ダウンロードした CSV に入力を行います。**serial (シリアル)**、**panorama**、**device-group (デバイス グループ)**、および **template-stack (テンプレート スタック)** の各フィールドに適切な値を入力します。ファイアウォールをインポートする前に Panorama ノード、デバイスグループ、テンプレート スタックを Panorama Controller 上で追加・作成しておく必要があり、ファイアウォールを正しく追加するためにはこれらが必要になります。ファイアウォールの情報を入力し終えたら、ファイルを**Save (保存)**します。

また、ファイアウォールをコンテンツ スケジュールに割り当てることもできます。ファイアウォールのインポートについては、これらは不要です。

CSV 列の順序を変えることはできません。列の順序を変えると、ファイアウォールのインポートが失敗します。

STEP 7 | Panorama Web インターフェイスに戻り、**Select File (ファイル選択)**でファイアウォールの情報が含まれている CSV ファイルを参照・選択します。

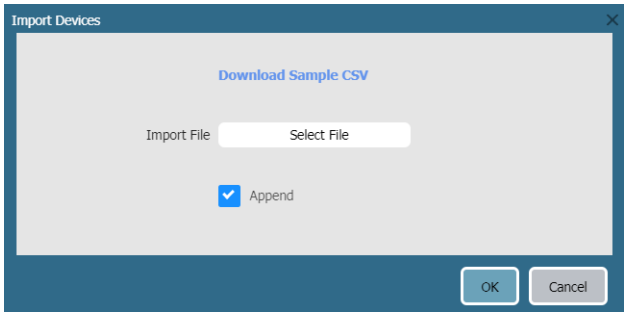
© 2019 Palo Alto Networks, Inc.

一括インポートの際にファイアウォールの必要な情報が不足していると、インポート全体が失敗します。エラーが発生した場合、インポートファイルのエラーか所を示すエラーメッセージが表示されます。

STEP 8 | 新しいデバイスを**Append** (アペンド)し、**Devices** (デバイス)のリストの最後に追加します。インポートされるデバイスがすべて新しいデバイスでなければなりません。インポート対象のいずれかのデバイスが、Panorama Controller 上で実行中の設定の一部である場合、インポートが失敗します。

リストに含まれている既存のデバイスを削除する場合は*Append* (アペンド)のボックスを選択解除し、対象の新しいデバイスを追加します。

STEP 9 | **OK**をクリックして管理対象デバイスとしてファイアウォールを追加します。

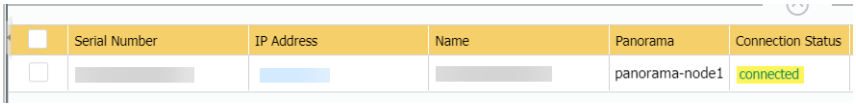


STEP 10 | **Commit** (コミット)および**Commit to Panorama** (Panorama にコミット)をクリックし、ファイアウォールを追加する作業を完了させます。

STEP 11 | **Panorama** > **Interconnect** > **Panorama Nodes** (Panorama ノード)、さらに**Synchronize Config** (設定の同期)を選択します。

STEP 12 | 新たにインポートしたファイアウォールが`Connected` (接続済み) であることを確認します。

1. **Panorama** > **Interconnect** > **Panorama Nodes** (Panorama ノード)を選択します。
2. インポートしたファイアウォールを探し、Connection Status (接続ステータス) 列に`Connected` (接続済み) と表示されていることを確認します。



テンプレート スタックの変数をインポート

ファイアウォール構成内の IP アドレス、IP 範囲、FQDN、IKE、VPN、HA 構成内のインターフェイス、グループ ID を置換するには、テンプレート スタックの変数を使用します。変数を使用すると、管理する必要のあるテンプレートとテンプレート スタックの総数を減らすことができ、ファイアウォール固有の値は保持できます。

テンプレート スタックの変数をインポートすることで、既存の複数の変数を上書きできます。インポート時に新しいテンプレート スタックの変数を作成することはできません。新しいテンプレートあるいはテンプレート スタックの変数を作成する方法については、テンプレートまたはテンプレートスタック変数の設定を参照してください。

STEP 1 | 既存のテンプレート スタックの変数をエクスポートします。

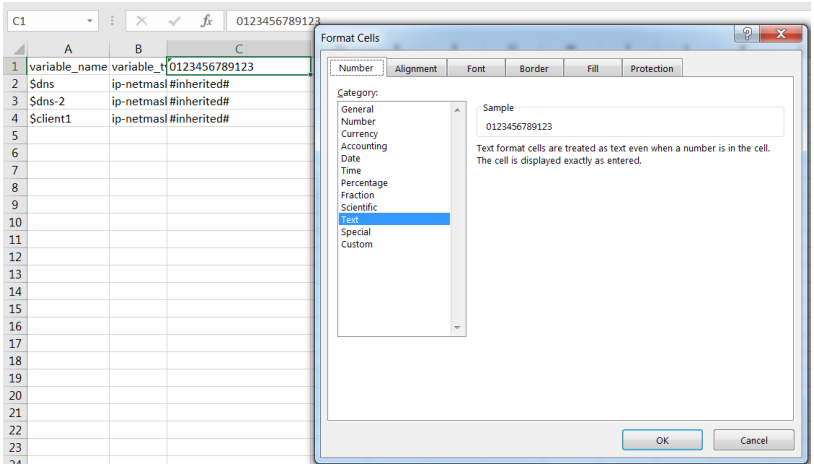
© 2019 Palo Alto Networks, Inc.

1. Panorama Controller のPanorama Web インターフェイスにログインします。
2. **Panorama** > **Interconnect** > **Devices** (デバイス)を選択して**Export Variables** (変数をエクスポート)します。
3. ドロップダウンリストからテンプレート スタックの**Name** (名前)を選択します。
4. **OK**をクリックして CSV ファイルを保存します。

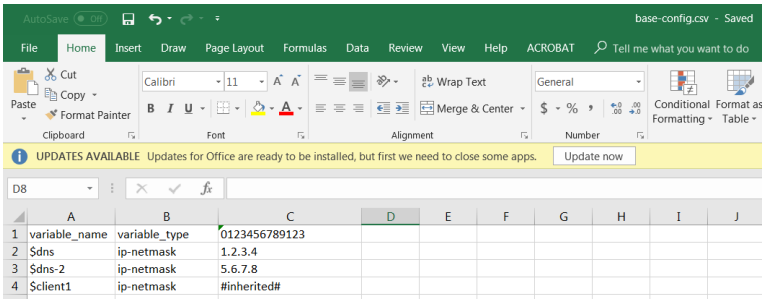
STEP 2 | Panorama Interconnect にインポートするテンプレート スタックの変数を含む CSV ファイルを、次の書式で編集します：

`#inherited#`として表示される値は、テンプレート スタックで定義されている値です。

1. ファイアウォールのシリアル番号を含むセルの番号を修正します。CSV ファイルに含まれるすべてのファイアウォールに対してこのステップを繰り返します。
   1. ファイアウォールのシリアル番号が含まれるセルを右クリックし、**Format Cells** (セルのフォーマット)を選択します。
   2. **Number** (数値) > **Text** (テキスト)を選択して**OK**をクリックします。
   3. シリアル番号の頭に0を追加します。



2. 適切なテンプレート変数の値を新たに入力します。
3. **File** (ファイル) > **Save As** (次として保存)を選択して**CSV UTF-8**形式でファイルを保存します。

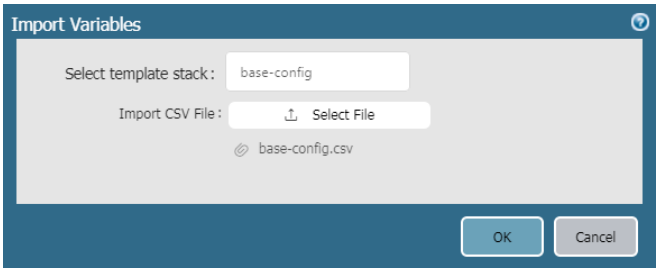


STEP 3 | CSV ファイルをテンプレート スタックにインポートします。

1. Panorama Controller のPanorama Web インターフェイスにログインします。
2. **Panorama** > **Interconnect** > **Devices** (デバイス)を選択して**Import Variables** (変数をインポート)します。
3. **Select template stack** (テンプレート スタックの選択)ドロップダウンリストで、変数をインポートするテンプレート スタックを選択します。
4. **Import CSV File** (CSV ファイルのインポート)のところで、テンプレート スタックの変数が含まれる**Select File** (ファイルの選択)をクリックします。

© 2019 Palo Alto Networks, Inc.

5. **OK**をクリックしてテンプレート スタックの変数をインポートします。



6. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

STEP 4 | Panorama ノードとPanorama Controller の同期.

STEP 5 | Panorama ノードの設定を管理対象のデバイスにプッシュ.

Panorama Interconnect でマスターキーを管理

Panorama、ファイアウォール、ログ コレクタ、および WF-500 アプライアンスは、マスター キーを使用して構成内の機密要素を暗号化し、パスワードと構成要素を暗号化するために使用するデフォルトのマスター キーがあります。

標準のセキュリティ慣行の一環として、マスター キーの有効期限が切れた際は個々のファイアウォール、ログ コレクタ、WildFire アプライアンス、および Panorama でキーを更新する必要があります。管理デバイスにデプロイされるマスター キーは、Panorama Controller、Panorama ノード、および管理対象デバイスが構成を正常にプッシュするために同一のものでなければなりません。キーを同じようにデプロイするには、新しいマスター キーをデプロイするか、期限切れになるマスター キーを Panorama から直接、複数のファイアウォール、ログ コレクタ、WF-500 アプライアンスで更新します。Panorama Interconnect を使用する場合、1 回の手順で Panorama Controller、すべての Panorama ノード、および管理対象デバイスに同じマスター キーを設定してデプロイする必要があります。マスター キーを管理対象デバイスにデプロイするには、各 Panorama ノードでマスター キーを設定し、そのノードで管理されるすべてのデバイスにそれらをデプロイする必要があります。詳細についてはマスター キーの構成を参照してください。

STEP 1 | Panorama Controller でマスター キーを構成します。

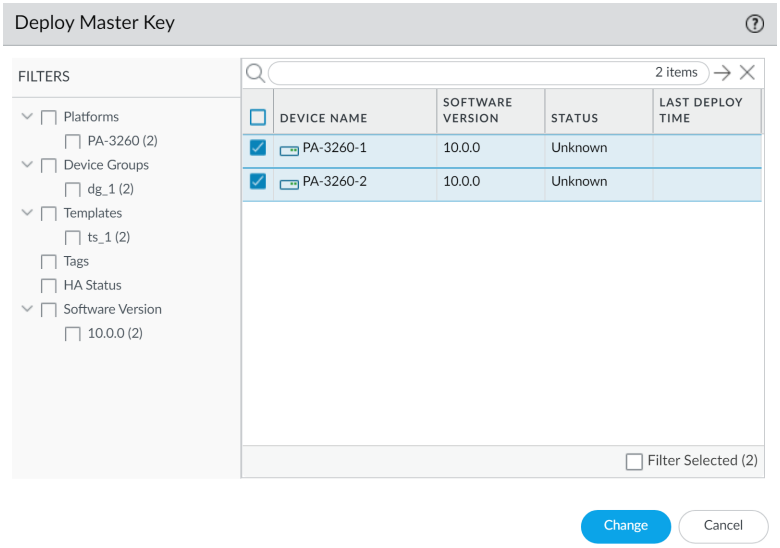
1. Panorama Web インターフェイスへのログインPanorama Controller の Panorama Web インターフェイスにログインします。
2. **Panorama** > **Master Key and Diagnostics** (マスター キーおよび診断) の順に選択し、マスター キーを構成します。
    1. マスター キーを更新する場合は、**Current Master Key** (現在のマスター キー) を入力します。デフォルトのマスター キーを新しいマスター キーに置き換える場合は、**Current Master Key** (現在のマスター キー) を指定しないでください。
    2. **New Master Key** (新規マスター キー) を設定し、**Confirm New Master** (マスター キーの確認) を行います。
    3. マスター キーの **Lifetime** (有効期間) と **Time for Reminder** (リマインダーの時間) を構成します。
    4. キーの有効期限が切れた後、指定された日数の間、**Auto Renew with Same Master Key** (同じマスター キーで自動更新) するように Panorama Controller を設定します。
    5. **OK** をクリックします。
3. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

STEP 2 | Panorama ノードで管理されているデバイスにマスター キーをデプロイします。

すべての Panorama ノードに対してこのステップを繰り返します。

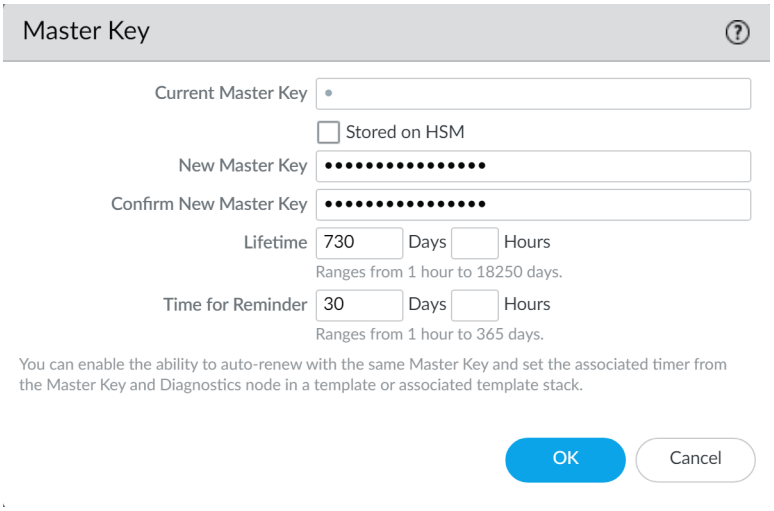
© 2019 Palo Alto Networks, Inc.

1. Panorama Web インターフェイスへのログインPanorama ノードの Panorama Web インターフェイスにログインします。
2. **Panorama** > **Master Key and Diagnostics** (マスター キーおよび診断) を選択してマスターキーを構成します。新しいマスターキーは、ステップ 1 で Panorama Controller に構成したキーと同じなければなりません。
   1. マスター キーを更新する場合は、**Current Master Key** (現在のマスター キー) を入力します。デフォルトのマスター キーを新しいマスター キーに置き換える場合は、**Current Master Key** (現在のマスター キー) を指定しないでください。
   2. **New Master Key** (新規マスター キー) を設定し、**Confirm New Master** (マスター キーの確認) を行います。
   3. マスター キーの **Lifetime** (有効期間) と **Time for Reminder** (リマインダーの時間) を構成します。
   4. キーの有効期限が切れた後、指定された日数の間、**Auto Renew with Same Master Key** (同じマスター キーで自動更新) するように Panorama Controller を設定します。
   5. **OK** をクリックします。
3. **Panorama** > **Managed Devices** (管理対象デバイス) > **Summary** (サマリー) を選択し、**Deploy Master Key** (マスター キーをデプロイ) します。
4. すべてのデバイスを選択し、マスター キーを **Change** (変更) します。



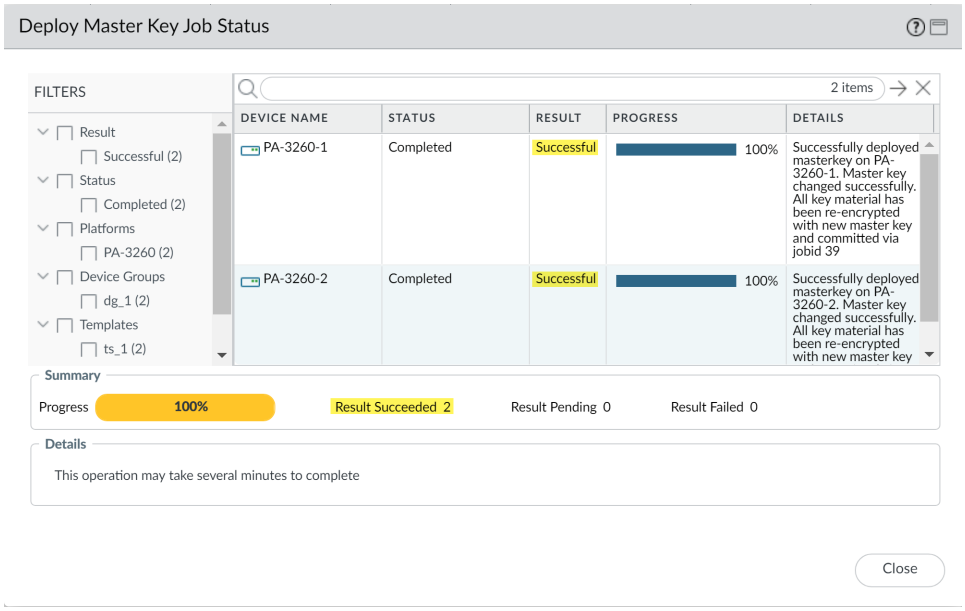
5. マスター キーを設定します。このキーは、ステップ 1 で構成したキーと同じでなければなりません。
   1. マスター キーを更新する場合は、**Current Master Key** (現在のマスター キー) を入力します。デフォルトのマスター キーを新しいマスター キーに置き換える場合は、**Current Master Key** (現在のマスター キー) を指定しないでください。
   2. **New Master Key** (新規マスター キー) を設定し、**Confirm New Master** (マスター キーの確認) を行います。
   3. マスター キーの **Lifetime** (有効期間) と **Time for Reminder** (リマインダーの時間) を構成します。
   4. **OK** をクリックします。

© 2019 Palo Alto Networks, Inc.



6. 選択したすべてのデバイスにマスター キーが正常にデプロイされたことを確認します。

   Panorama から新しいマスター キーをデプロイすると、システムログが生成されます。



STEP 3 | マスター キーをログ コレクタにデプロイします。

すべての Panorama ノードに対してこのステップを繰り返します。新しいマスターキーは、ステップ 1 で構成したものと同じでなければなりません。

1. **Panorama** > **Managed Collectors** (管理対象コレクタ) を選択し、**Deploy Master Key** (マスター キーをデプロイ)します。
2. すべてのデバイスを選択し、マスター キーを **Change** (変更) します。
3. マスター キーを次のように構成します。
   1. マスター キーを更新する場合は、**Current Master Key** (現在のマスター キー) を入力します。デフォルトのマスター キーを新しいマスター キーに置き換える場合は、**Current Master Key** (現在のマスター キー) を指定しないでください。
   2. **New Master Key** (新規マスター キー) を指定し、**Confirm New Master** (マスター キーの確認) を行います。
   3. マスター キーの **Lifetime** (有効期間) と **Time for Reminder** (リマインダーの時間) を構成します。

© 2019 Palo Alto Networks, Inc.

4. **OK** をクリックします。

4. 選択したすべてのデバイスにマスター キーが正常にデプロイされたことを確認します。

   Panorama から新しいマスター キーをデプロイすると、システムログが生成されます。

STEP 4 | マスター キーを管理対象の WildFire アプライアンスにデプロイします。

すべての Panorama ノードに対してこのステップを繰り返します。新しいマスターキーは、ステップ 1 で構成したものと同じでなければなりません。

1. **Panorama** > **Managed WildFire Appliances** (管理対象 **WildFire** アプライアンス) を選択し、**Deploy Master Key** (マスター キーをデプロイ)します。
2. すべてのデバイスを選択し、マスター キーを **Change** (変更) します。
3. マスター キーを次のように構成します。
   1. マスター キーを更新する場合は、**Current Master Key** (現在のマスター キー) を入力します。デフォルトのマスター キーを新しいマスター キーに置き換える場合は、**Current Master Key** (現在のマスター キー) を指定しないでください。
   2. **New Master Key** (新規マスター キー) を指定し、**Confirm New Master** (マスター キーの確認) を行います。
   3. マスター キーの **Lifetime** (有効期間) と **Time for Reminder** (リマインダーの時間) を構成します。
   4. **OK** をクリックします。
4. 選択したすべてのデバイスにマスター キーが正常にデプロイされたことを確認します。

   Panorama から新しいマスター キーをデプロイすると、システムログが生成されます。

Panorama ノードの設定を管理対象のデバイスにプッシュ

Panorama ノードとPanorama Controller の同期、テンプレート スタックおよびデバイスグループの設定を行ったら、テンプレート スタックおよびデバイスグループの設定を管理対象のデバイスにプッシュします。

STEP 1 | Panorama Web インターフェイスへのログイン (Panorama Controller の) 。

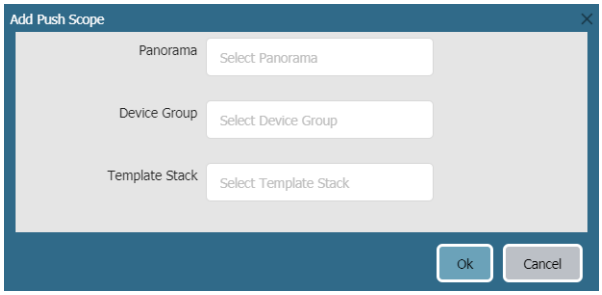
STEP 2 | **Panorama** > **Interconnect** > **Panorama Nodes (Panorama** ノード)を選択します。

STEP 3 | **Push to Devices** (デバイスにプッシュ)し、同期済みの設定を Panorama ノードから管理対象のデバイスにプッシュします。

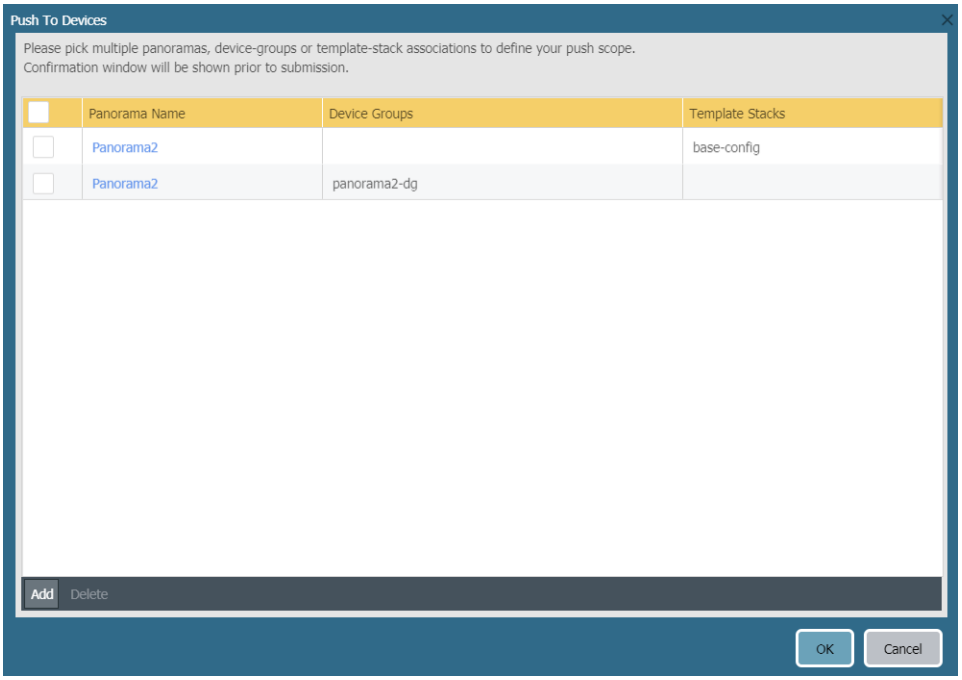
STEP 4 | 設定のプッシュ先であるデバイスを管理している Panorama ノードを**Add** (追加)します。このステップを繰り返し、必要に応じて複数の Panorama ノード、デバイスグループ、あるいはテンプレートにプッシュします：

1. **Panorama**ノードを選択します。
2. **Device Group** (デバイスグループ)を選択してデバイスグループおよびテンプレート スタックの設定を両方ともプッシュするか、**Template Stack** (テンプレート スタック)を選択してテンプレート スタックの設定だけをプッシュします。
3. **OK** をクリックして、プッシュ スコープの定義を完了させます。

© 2019 Palo Alto Networks, Inc.



STEP 5 | **OK**をクリックして管理対象デバイスに設定をプッシュします。



STEP 6 | Device Group Push Status (デバイスグループのプッシュ状態) 列および Template Stack Push Status (テンプレート スタックのプッシュ状態) 列で、プッシュが**in-sync (同期中)**であることを確認します。

Panorama Interconnect プラグインのアップグレード

次の各作業を行い、Panorama Controller および Panorama ノード上の Panorama™ Interconnect プラグインをアップグレードします。Panorama Interconnect プラグインをアップグレードする際、Panorama ノードを Controllerと同じプラグイン バージョンにアップグレードする前に、Panorama Controller をアップグレードする必要があります。Panorama Controller および選択した Panorama ノードのプラグインのバージョンを必ず同じに保つために、ダウンロードして Panorama ノードにインストールする新しいプラグインのバージョンが、Panorama Controller にインストールされているプラグインのバージョンと同じでなければなりません。

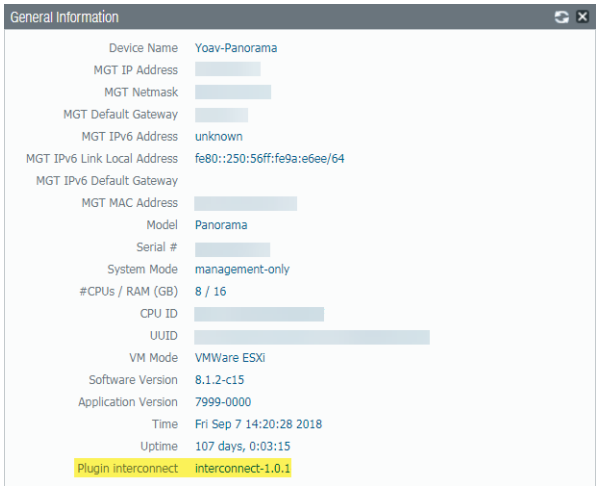
ここで初めてプラグインをインストールする場合は、Panorama Interconnect プラグインのセットアップを参照してください。

STEP 1 | Panorama Web インターフェイスへのログイン (Panorama Controller の) 。

STEP 2 | Panorama Controller 上の Panorama Interconnect プラグインをアップグレードします。

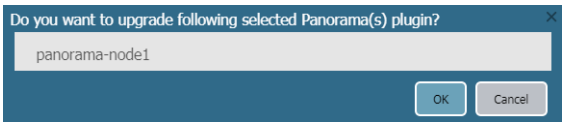
© 2019 Palo Alto Networks, Inc.

1. **Panorama** > **Plugins** (プラグイン)を選択して`Interconnect`を検索します。
2. 新しいバージョンの Interconnect プラグインを**Download** (ダウンロード)して**Install** (インストール)します。インストールが完了したら、そのことを知らせるプロンプトが表示されます。
3. 新たにインストールした Interconnect プラグインのバージョンが**Dashboard** (ダッシュボード)に表示されていることを確認します。

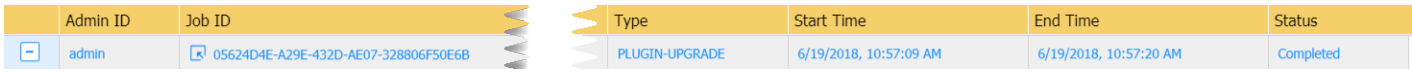


STEP 3 | Panorama ノード上の Panorama Interconnect プラグインをアップグレードします。

1. **Panorama** > **Interconnect** > **Panorama Nodes** (Panorama ノード)を選択し、単一あるいは複数の Panorama ノードを選択して**Upgrade Plugin** (プラグインをアップグレード)します。
2. 選択済みの Panorama ノードを確認し、**OK**をクリックしてプラグインのアップグレードを開始します。



3. プラグインのアップグレード ジョブが`Completed` (完了)になるまで待ちます。**Panorama** > **Interconnect** > **Tasks** (タスク)をクリックしてジョブの進行状況を表示します。



4. アップグレードが正常に完了したら、**Panorama** > **Interconnect** > **Panorama Nodes** (Panorama ノード)を選択し、選択した Panorama ノードの**Plugin** (プラグイン)バージョンが正しいことを確認します。



© 2019 Palo Alto Networks, Inc.

ログ収集の管理

Palo Alto Networks のすべてのファイアウォールでは、ファイアウォール アクティビティの監査証跡となるログを生成できます。ログとレポートの中央管理については、ファイアウォールで生成されたログを、Panorama™ 管理サーバまたはログ コレクタを含むオンプレミス インフラストラクチャに転送するか、ログをクラウド ベースの Cortex Data Lake に送信する必要があります。その後、必要に応じて、ログを外部のロギング宛先（Syslog サーバーなど）に転送するように Panorama を設定します。

レガシー モードの Panorama バーチャル アプライアンスにログを転送する場合、ロギングを有効にするために追加のタスクを実行する必要はありません。ログをログ コレクタに転送する場合は、ログ コレクタを管理対象コレクタとして設定して、コレクタ グループに割り当てる必要があります。管理対象のコレクタは、M-Series アプライアンスのローカルにすることも、Panorama モードの Panorama バーチャル アプライアンスにすることもできます。さらに、M-Series アプライアンス、またはログ コレクタモードの Panorama バーチャル アプライアンスは、専用ログ コレクタにすることができます。これらのタイプの管理対象コレクタの一方をデプロイするのか、それとも両方をデプロイするのかを決定するには、ローカルおよび分散ログ収集を参照してください。

Panorama でローカルに生成されるシステム ログおよび設定ログを管理する方法については、Panorama のモニタリングを参照してください。

> 管理対象コレクタの設定
> 専用のログ コレクタの認証の設定
> コレクタ グループの管理
> Panorama へのログ転送の設定
> 外部の宛先への syslog 転送の設定
> ログの Cortex Data Lake への転送
> Panorama へのログ転送の確認
> ログ転送とバッファのデフォルトの変更
> Panorama から外部の宛先へのログ転送を設定
> ログ収集のデプロイメント

管理対象コレクタの設定

Panorama 管理サーバーでログ コレクタを管理できるようにするには、管理対象コレクタとして追加する必要があります。2 つのタイプの管理対象コレクタを追加できます。

- 専用ログ コレクタ – 新しい M-600、M-500、M-200 アプライアンスまたは Panorama バーチャル アプライアンスをログ コレクタとしてセットアップする、あるいは既存の M-Series アプライアンスまたは Panorama バーチャル アプライアンスを Panorama モードからログ コレクタ モードに切り替えるには、「M-Series アプライアンスをログ コレクタとしてセットアップ」を参照してください。Panorama モードからログ コレクタ モードに切り替えると、Panorama モードの M-Series アプライアンスで事前定義されたローカル ログ コレクタが削除されるのでご注意ください。
- ローカル ログ コレクタ – ログ コレクタは、 M-600、M-500、M-200 アプライアンス、または Panorama モードの Panorama バーチャル アプライアンスで設定できます。M-Series アプライアンスではログ コレクタが事前定義済みであり、バーチャル アプライアンスではログ コレクタを追加する必要があります。Panorama 管理サーバーが高可用性 (HA) 設定の場合、各 HA ピアがローカル ログ コレクタを持つことができます。ただし、プライマリ Panorama の場合と異なり、セカンダリ Panorama のログ コレクタはローカルではなくリモートです。そのため、セカンダリ Panorama でログ コレクタを使用するには、手動でプライマリ Panorama に追加する必要があります (詳細は、「ローカル ログ コレクタを使用する Panorama M-Series アプライアンスのデプロイ」または「ローカル ログ コレクタを使用する Panorama バーチャル アプライアンスのデプロイ」を参照)。ローカル ログ コレクタを削除した場合、後から追加し直すことができます。以下の手順は、ローカル ログ コレクタの追加方法を示しています。



管理対象が専用ログ コレクタであるかどうかにかかわらず、ローカル ログ コレクタおよびコレクタ グループを *Panorama* 管理サーバー上に保持することをお勧めします。



Panorama バーチャル アプライアンスがレガシー モードの場合、*Panorama* モードに切り替えてログ コレクタを作成する必要があります。詳細は、「ローカル ログ コレクタを使用する Panorama バーチャル アプライアンスのセットアップ」を参照してください。

STEP 1 | ログ コレクタのシリアル番号を控えておきます。

これは、ログ コレクタを管理対象コレクタとして追加するときに必要になります。

1. Panorama Web インターフェイスにアクセスします。
2. **Dashboard** (ダッシュボード) を選択し、General Information (一般情報) セクションの **Serial #** (シリアル番号) を記録します。

STEP 2 | ログ コレクタを管理対象コレクタとして追加します。

1. **Panorama** > **Managed Collectors** (管理対象コレクタ) の順に選択し、新しいログ コレクタを **Add** (追加) します。
2. **General** (全般) 設定で、ログ コレクタについて記録したシリアル番号 (**Collector S/N** (コレクタ シリアル番号)) を入力します。
3. **OK** をクリックして変更内容を保存します。
4. **Commit** (コミット) > **Commit to Panorama** (**Panorama** にコミット) を選択します。

STEP 3 | (任意) ログ コレクタの管理者認証を構成します。

1. **Panorama** > **Managed Collectors** (管理対象コレクタ) の順に選択し、その名前をクリックしてログ コレクタを編集します。
2. ログ コレクタの管理者パスワードを構成します。
    1. パスワードの **Mode (モード)** を選択します。

© 2019 Palo Alto Networks, Inc.

2. **Password** (パスワード) モードを選択した場合は、プレーンテキストの **Password** (パスワード) と **Confirm Password** (パスワードを確認) を入力します。**Password Hash** (パスワード ハッシュ) モードを選択した場合は、ハッシュされたパスワード文字列 (最大 63 文字) を入力します。
3. 管理ログインのセキュリティ要件を構成します。

   Failed Attempts (試行失敗回数) を *0* 以外の値にしながら、*Lockout Time* (ロックアウト時間) を *0* のままにしている場合、別の管理者がロックアウトされた管理者を手動でロック解除するまで、管理者ユーザーは無期限にロックアウトされます。他の管理者が作成されていない場合は、*Panorama* で *Failed Attempts* (試行失敗回数) および *Lockout Time* (ロックアウト時間) の設定を再構成し、構成変更をログ コレクタにプッシュする必要があります。管理者がロックアウトされないようにするには、*Failed Attempts* (試行失敗回数) および *Lockout Time* (ロックアウト時間) の両方にデフォルト値の *0* を使用します。

   1. ログイン **Failed Attempts** (試行失敗回数) の値を入力します。範囲はデフォルト値 0 から最大 10 までです。ここで値 0 は無制限のログイン試行を指定します。
   2. デフォルト値 0 から最大 60 分で **Lockout Time** (ロックアウト時間) の値を入力します。
4. **OK** をクリックして変更内容を保存します。

STEP 4 | ロギング用ディスクを有効にします。

1. **Panorama** > **Managed Collectors** (管理対象コレクタ) の順に選択し、その名前をクリックしてログ コレクタを編集します。

   ログ コレクタ名は、Panorama 管理サーバーのホスト名と同じ値です。
2. **Disks** (ディスク) を選択し、各ディスク ペアを **Add** (追加) します。
3. **OK** をクリックして変更内容を保存します。
4. **Commit** (コミット) > **Commit to Panorama** (**Panorama** にコミット) を選択します。

STEP 5 | (任意) デプロイメントで Panorama と管理対象デバイス間の認証にカスタム証明書を使用している場合、カスタム クライアント デバイス証明書をデプロイします。詳細は、「カスタム証明書を使用する認証のセットアップ」を参照してください。

1. **Panorama** > **Certificate Management** (証明書の管理) > **Certificate Profile** (証明書プロファイル) の順に選択し、ドロップダウンから証明書プロファイルを選択するか、**New Certificate Profile** (新しい証明書プロファイル) をクリックして作成します。
2. **Panorama** > **Managed Collectors** (管理対象コレクタ) の順に選択し、新しいログ コレクタを **Add** (追加) するか、既存のログ コレクタを選択します。**Communication** (通信) を選択します。
3. Type (タイプ) ドロップダウンからデバイス証明書のタイプを選択します。
   - ローカル デバイス証明書を使用している場合、それぞれのドロップダウン リストから **Certificate** (証明書) および **Certificate Profile** (証明書プロファイル) を選択します。
   - デバイス証明書として SCEP を使用している場合、それぞれのドロップダウンから **SCEP Profile** (**SCEP** プロファイル) および **Certificate Profile** (証明書プロファイル) を選択します。
4. **OK** をクリックします。

STEP 6 | (任意) ログ コレクタで **Secure Server Communication** (保護されたサーバー通信) を設定します。詳細は、「カスタム証明書を使用する認証のセットアップ」を参照してください。

1. **[Panorama]** > **[管理対象コレクタ]** の順に選択し、**[追加]** をクリックします。**Communication** (通信) を選択します。
2. **Custom Certificate Only** (カスタム証明書のみ) チェック ボックスがオフになっていることを確認します。これにより、カスタム証明書への移行中もすべてのデバイスの管理を続行できます。

© 2019 Palo Alto Networks, Inc.

Custom Certificate Only（カスタム証明書のみ）チェック ボックスをオンにしていると、ログ コレクタは事前定義済みの証明書を使用したデバイスからのログを認証せず、受信することができません。

3. **SSL/TLS Service Profile**（**SSL/TLS** サービス プロファイル）ドロップダウンから SSL/TLS サービス プロファイルを選択します。この SSL/TLS サービス プロファイルは、ログ コレクタとログを送信するデバイス間のすべての SSL 接続に適用されます。
4. **Certificate Profile**（証明書プロファイル）ドロップダウンから証明書プロファイルを選択します。
5. **Authorize Client Based on Serial Number**（シリアル番号に基づいてクライアントを承認）を選択し、サーバーが管理対象デバイスのシリアル番号と照合してクライアントをチェックするようにします。クライアント証明書では、シリアル番号に基づいて認証するために CN として特殊なキーワード $UDID を設定する必要があります。
6. **Disconnect Wait Time (min)**（切断待機時間（分））に、Panorama が管理対象デバイスとの接続を切断して再開するまで待機する分数を入力します。このフィールドはデフォルトで空白であり、範囲は 0 ~ 44,640 分です。

   切断待機時間は、新しい設定をコミットするまでカウント ダウンを開始しません。

7. （任意）認証リストを設定します。
   1. Authorization List（承認リスト）で **Add**（追加）をクリックします。
   2. 識別子タイプとして **Subject**（サブジェクト）または **Subject Alt Name**（サブジェクト代替名）を選択します。
   3. 選択したタイプの識別子を入力します。
   4. **OK** をクリックします。
   5. **Check Authorization List**（承認リストのチェック）を選択して認証リストを適用します。
8. **OK** をクリックします。
9. **Commit**（コミット）> **Commit to Panorama**（**Panorama** にコミット）を選択します。

STEP 7 | 変更を検証します。

1. **Panorama** > **Managed Collectors**Panorama > 管理対象コレクタ) ページで、追加したログ コレクタが表示されていることを確認します。Connected（接続済み）列には、ログ コレクタが Panorama に接続されていることを示すチェック マークが表示されます。更新された接続ステータスがページに表示されるまで、数分かかる場合があります。

   コレクタ グループの設定を行ってコレクタ グループに設定変更をプッシュするまで、*Configuration Status (*設定ステータス*)* 列には *Out of Sync (*非同期*)*、*Run Time Status (*ランタイム ステータス*)* 列には *disconnected (*未接続*)* と表示され、***show interface all*** の *CLI* コマンドを実行するとインターフェイスが *down* 状態だと表示されます。

2. 最後の列にある **Statistics**（統計）をクリックし、ロギング用ディスクが有効になっていることを確認します。

STEP 8 | 次のステップ...

ログ コレクタがファイアウォールのログを受信できるようにするには、予め次の作業が必要になります。

1. Panorama への ログ転送の設定
2. コレクタ グループの設定— M-Series アプライアンスではデフォルトのコレクタ グループが事前定義済みであり、すでにローカル ログ コレクタがメンバーとして含まれています。Panorama バーチャル アプライアンスでは、コレクタ グループを追加してローカル ログ コレクタをメンバーとして追加する必要があります。どちらのモデルでも、ログ転送のためにファイアウォールをローカル ログ コレクタに割り当てます。

© 2019 Palo Alto Networks, Inc.

専用のログ コレクタの認証の設定

きめ細かな認証パラメータが設定されたローカルの管理者ユーザーを設定する、ならびに承認および認証用の RADIUS、TACAS+、または LDAP を活用することにより、専用のログ コレクタ用に強化された認証を作成し、設定します。

Panorama から管理者を設定してプッシュする際は、専用のログ コレクタの既存の管理者を、Panorama で設定した管理者で上書きします。

- 専用のログ コレクタの管理者アカウントの設定
- 専用のログ コレクタの RADIUS 認証の設定
- 専用のログ コレクタの TACACS+ 認証を設定する
- 専用のログ コレクタの LDAP 認証の設定

専用のログ コレクタの管理者アカウントの設定

Panorama™ 管理サーバーから管理する専用のログ コレクタ サーバーの詳細な認証パラメーターを使用して1人以上の管理者を作成します。さらに、専用のログ コレクタの CLI で直接設定可能な Panorama からローカル管理者を設定できます。ただし、新しい構成の変更を専用のログ コレクタにプッシュすると、既存のローカル管理者が専用のログ コレクタ用に設定された管理者で上書きされます。

STEP 1 | Panorama Web インターフェイスへのログイン.

STEP 2 | 管理対象コレクタの設定.

STEP 3 | (任意) 認証プロファイルを設定して、専用のログ コレクタ CLI にアクセスする管理者のログイン資格情報を検証する認証サービスを定義します。

STEP 4 | 必要に応じて、1つ以上の管理者アカウントを設定します。

Panorama で作成された管理者アカウントは、後で専用のログ コレクタにインポートされ、Panorama で管理されます。

STEP 5 | 専用のログ コレクタの認証を設定します。

1. **Panorama** > **Managed Collectors** (管理対象コレクタ) を選択し、以前に追加した専用のログ コレクタを選択します。
2. (任意) 前のステップで設定した **Authentication Profile** (認証プロファイル) を選択します。
3. 専用のログ コレクタの認証 **Timeout Configuration** (タイムアウト設定) を設定します。
    1. ユーザーが専用のログ コレクタ CLI からロックアウトされるまでの **Failed Attempt** (試行失敗回数) の数を入力します。
    2. **Lockout Time** (ロックアウト時間) を分単位で入力します。専用のログ コレクタは、ユーザーが設定された数の試行失敗回数に達すると、ユーザー アカウントをロックアウトします。
    3. アクティブではないユーザー アカウントが自動的にログアウトされるまでの時間である、**Idle Timeout** (待機タイムアウト) を分単位で入力します。
    4. 専用のログ コレクタに同時にアクセスできるユーザー アカウントの数を設定するには、**Max Session Count** (最大セッション カウント) を入力します。
    5. 管理者が自動的にログアウトする前にログインできる**Max Session Time** (最大セッション時間) を入力します。
4. 専用のログ コレクタの管理者を追加します。

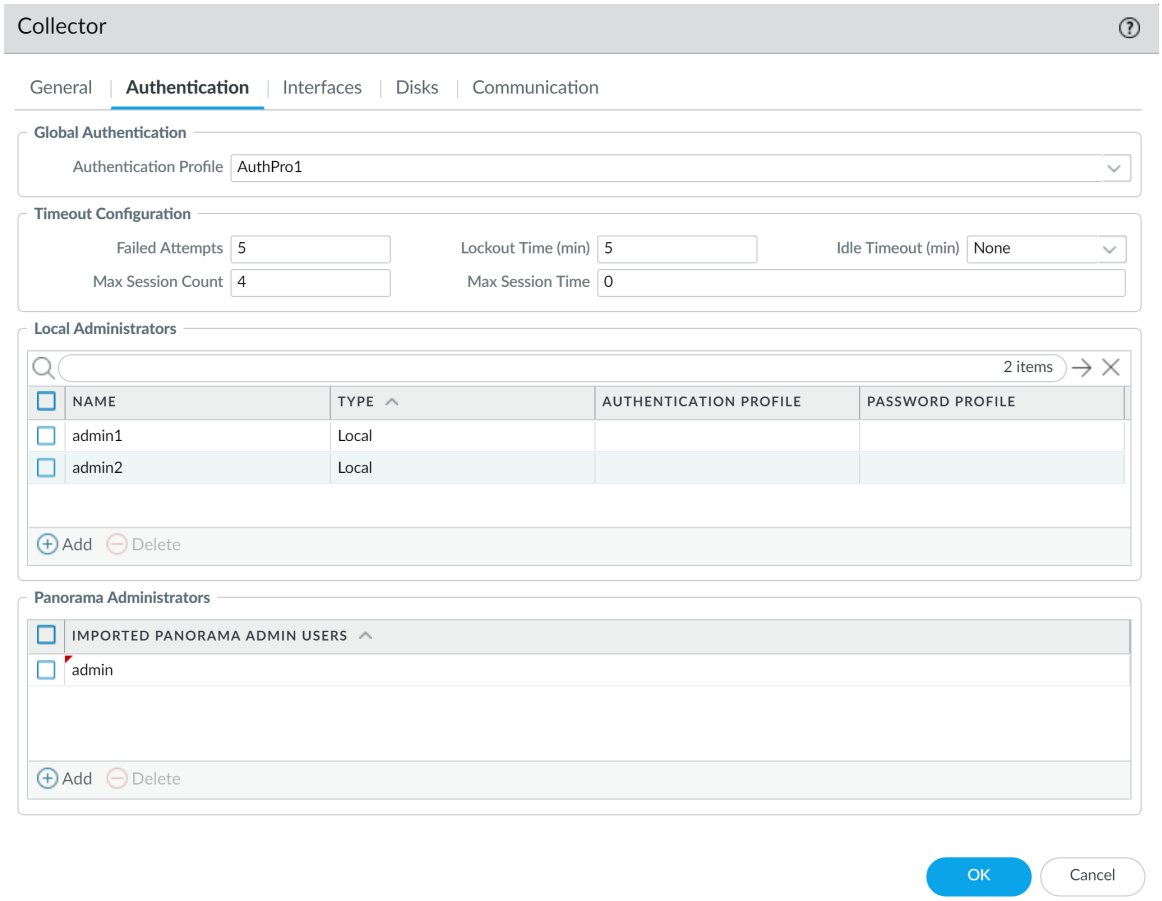
    管理者は、ローカル管理者またはインポートされた Panorama 管理者のいずれかとして追加できますが、両方を追加することはできません。ローカル管理者とインポートされた Panorama 管理者

© 2019 Palo Alto Networks, Inc.

の両方として同じ管理者を追加することはサポートされておらず、Panorama コミットが失敗します。例えば、**admin1** をローカル管理者と Panorama 管理者の両方として追加する場合、Panorama へのコミットは失敗します。

1. 専用のログ コレクタに固有の新しい管理者を**Add** (追加) して設定します。これらの管理者は、それらが作成された専用ログ コレクタに固有であり、この表からこれらの管理者を管理します。
2. Panorama で設定された管理者を **Add** (追加) します。これらの管理者は Panorama で作成され、専用のログ コレクタにインポートされます。

5. **OK** をクリックすると、専用のログ コレクタ認証設定を保存します。



STEP 6 | 設定の変更を **Commit** (コミット) してから、**Commit and Push** (コミットしてプッシュ) します。

STEP 7 | 専用のログ コレクタのPanorama CLI へのログインを使用して、ローカル管理者ユーザーによって専用ログ コレクタに正常にアクセスできることを確認します。

専用のログ コレクタの RADIUS 認証の設定

RADIUS サーバーを使用して、専用のログ コレクタ CLI への管理アクセスを認証します。RADIUS サーバーでベンダー固有属性 (VSA) を定義し、管理者認証を管理することもできます。VSA を使用すれば、ディレクトリ サービスを介してロール、アクセス ドメイン、管理者のユーザー グループをすばやく変更できます。この方法は多くの場合、Panorama™ 管理サーバーで設定し直すよりも簡単です。

© 2019 Palo Alto Networks, Inc.

Palo Alto Networks RADIUS ディクショナリーを *RADIUS* サーバーにインポートして、*Panorama* と *RADIUS* サーバー間の通信に必要な認証属性を定義することができます。

STEP 1 | Panorama Web インターフェイスへのログイン.

STEP 2 | 管理対象コレクタの設定.

STEP 3 | RADIUS 認証を設定します。

1. RADIUS サーバー プロファイルを追加します。

   このプロファイルは、専用のログ コレクタが RADIUS サーバーに接続する方法を定義します。

   1. **Panorama** > **Server Profiles**（サーバー プロファイル）> **RADIUS** の順に追加し、プロファイルを **Add**（追加）します。
   2. サーバー プロファイルを識別する **Profile Name**（プロファイル名）を入力します。
   3. 認証要求がタイムアウトするまでの**Timeout (**タイムアウト**)** 時間を秒単位で入力します（デフォルトは 3、範囲は1 ~ 20）。
   4. 専用のログ コレクタが RADIUS サーバーに認証するために使用する **Authentication Protocol**（認証プロトコル）（デフォルトは **CHAP**）を選択します。

      RADIUS サーバーがサポートする場合は *CHAP* を選択します。このプロトコルは *PAP* よりも安全です。

   5. 各 RADIUS サーバーを **Add**（追加）して、以下を入力します。
      1. サーバーを識別するための**Name**（名前）。
      2. **RADIUS Server**（**RADIUS** サーバー）の IP アドレス あるいは FQDN。
      3. **Secret**（シークレット）/**Confirm Secret**（再入力 シークレット）（ユーザー名とパスワードを暗号化するための鍵）。
      4. 認証要求用のサーバー **Port**（ポート）（デフォルトは1812）。
   6. **OK** をクリックしてサーバー プロファイルを保存します。
2. RADIUS サーバー プロファイルを認証プロファイルに割り当てます。

   認証プロファイルにより、一連の管理者に共通の認証設定が定義されます。

   1. **Panorama** > **Authentication Profile**（認証プロファイル）の順に選択し、プロファイルを **Add**（追加）します。
   2. 認証プロファイルを識別する **Name**（名前）を入力します。
   3. **Type**（タイプ）を **RADIUS** に設定します。
   4. 設定した **Server Profile**（サーバー プロファイル）を選択します。
   5. **Retrieve user group from RADIUS**（**RADIUS** からユーザー グループを取得）を選択して、RADIUS サーバーで定義された VSA からユーザー グループ情報を収集します。

      Panorama は、グループ情報を認証プロファイルの Allow List（許可リスト）で指定したグループと照合します。
   6. **Advanced**（詳細）を選択し、Allow List（許可リスト）で、この認証プロファイルで認証することが許可された管理者を **Add**（追加）します。
   7. **OK** をクリックして認証プロファイルを保存します。

STEP 4 | 専用のログ コレクタの認証を設定します。

1. **Panorama** > **Managed Collectors (**管理対象コレクタ**)** を選択し、以前に追加した専用のログ コレクタを選択します。
2. 前のステップで設定した **Authentication Profile (**認証プロファイル**)** を選択します。

© 2019 Palo Alto Networks, Inc.

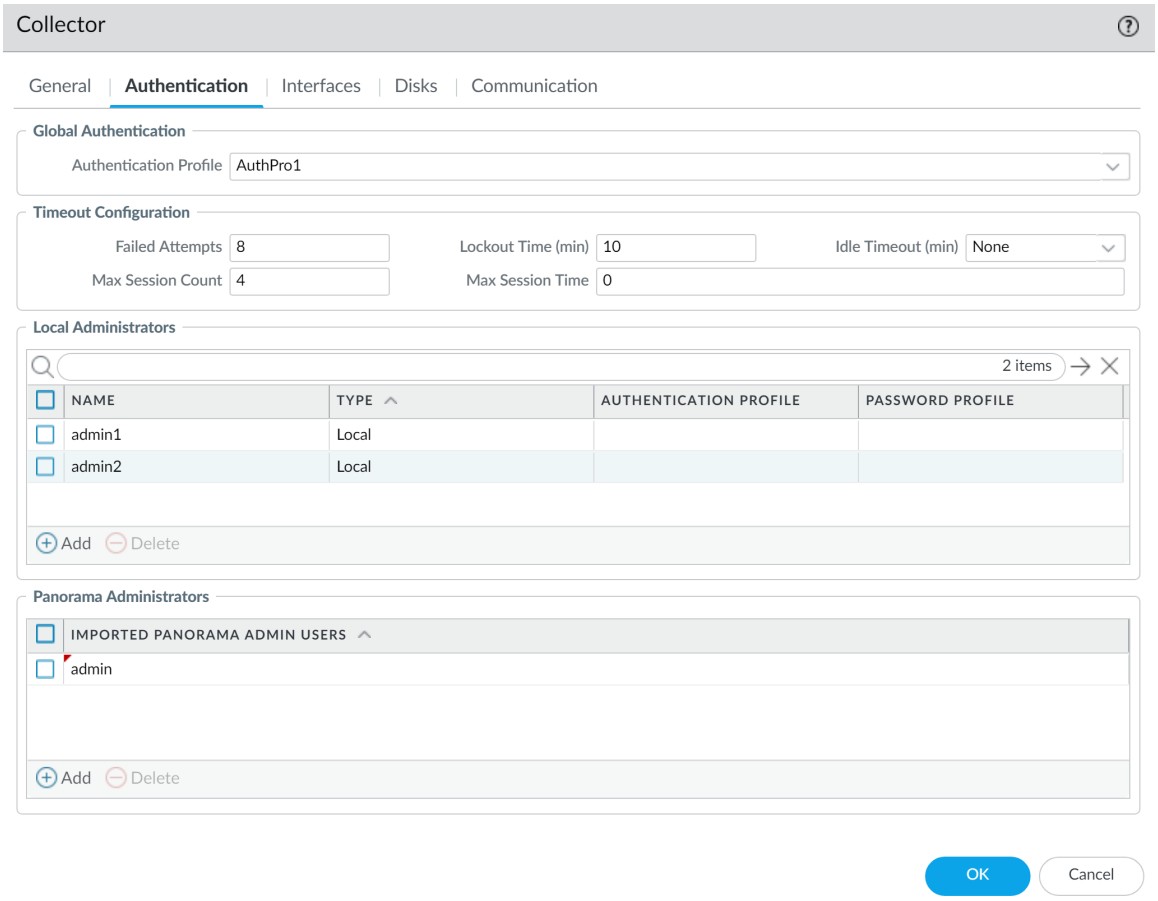
グローバル認証プロファイルが割り当てられていない場合は、リモート認証を活用するために、個々のローカル管理者に認証プロファイルを割り当てる必要があります。

3. 専用のログ コレクタの認証 **Timeout Configuration** (タイムアウト設定) を設定します。
    1. ユーザーが専用のログ コレクタ CLI からロックアウトされるまでの **Failed Attempt** (試行失敗回数) の数を入力します。
    2. **Lockout Time** (ロックアウト時間) を分単位で入力します。専用のログ コレクタは、ユーザーが設定された数の試行失敗回数に達すると、ユーザー アカウントをロックアウトします。
    3. アクティブではないユーザー アカウントが自動的にログアウトされるまでの時間である、**Idle Timeout** (待機タイムアウト) を分単位で入力します。
    4. 専用のログ コレクタに同時にアクセスできるユーザー アカウントの数を設定するには、**Max Session Count** (最大セッション カウント) を入力します。
    5. 管理者が自動的にログアウトする前にログインできる**Max Session Time** (最大セッション時間) を入力します。
4. 専用のログ コレクタの管理者を追加します。

    管理者は、ローカル管理者またはインポートされた Panorama 管理者のいずれかとして追加できますが、両方を追加することはできません。ローカル管理者とインポートされた Panorama 管理者の両方として同じ管理者を追加することはサポートされておらず、Panorama コミットが失敗します。例えば、`admin1` をローカル管理者と Panorama 管理者の両方として追加する場合、Panorama へのコミットは失敗します。

    1. 専用のログ コレクタに固有の新しい管理者を**Add** (追加) して設定します。これらの管理者は、それらが作成された専用ログ コレクタに固有であり、この表からこれらの管理者を管理します。
    2. Panorama で設定された管理者を **Add** (追加) します。これらの管理者は Panorama で作成され、専用のログ コレクタにインポートされます。
5. **OK** をクリックすると、専用のログ コレクタ認証設定を保存します。

© 2019 Palo Alto Networks, Inc.



STEP 5 | 設定の変更を **Commit** (コミット) してから、**Commit and Push** (コミットしてプッシュ) します。

STEP 6 | 専用のログ コレクタのPanorama CLI へのログインを使用して、ローカル管理者ユーザーを使用して専用ログ コレクタに正常にアクセスできることを確認します。

専用のログ コレクタの TACACS+ 認証を設定する

TACACS+ サーバーを使用して、専用のログ コレクタ CLI への管理アクセスを認証することができます。TACACS+ サーバーでベンダー固有属性 (VSA) を定義し、管理者認証を管理することもできます。VSA を使用すれば、ディレクトリ サービスを介してロール、アクセス ドメイン、管理者のユーザー グループをすばやく変更できます。この方法は多くの場合、Panorama で設定し直すよりも簡単です。

STEP 1 | Panorama Web インターフェイスへのログイン.

STEP 2 | 管理対象コレクタの設定.

STEP 3 | TACACS+ 認証を設定します。

1. TACACS+サーバー プロファイルを追加します。

   このプロファイルは、専用のログ コレクタが TACACS+ サーバーに接続する方法を定義します。

   1. **Panorama** > **Server Profiles** (サーバー プロファイル) > **TACACS+** の順に選択し、プロファイルを **Add** (追加) します。
   2. サーバー プロファイルを識別する **Profile Name** (プロファイル名) を入力します。

© 2019 Palo Alto Networks, Inc.

3. 認証要求がタイムアウトするまでの**Timeout** (タイムアウト) 時間を秒単位で入力します (デフォルトは 3、範囲は1 ~ 20) 。
4. Panorama が TACACS+ サーバーに認証するために使用する **Authentication Protocol** (認証プロトコル) (デフォルトは **CHAP**) を選択します。
5. TACACS+ サーバーがサポートする場合は **CHAP** を選択します。このプロトコルは **PAP** よりも安全です。
6. 各 TACACS+ サーバーを **Add** (追加) して、以下を入力します。
    1. サーバーを識別するための**Name** (名前) 。
    2. **TACACS+ Server** (**TACACS+** サーバー) の IP アドレス あるいは FQDN。
    3. **Secret** (シークレット) **/Confirm Secret** (再入力 シークレット) (ユーザー名とパスワードを暗号化するための鍵) 。
    4. 認証要求用のサーバー **Port** (ポート) (デフォルトは49) 。
7. **OK** をクリックしてサーバー プロファイルを保存します。

2. TACACS+ サーバー プロファイルを認証プロファイルに割り当てます。

   認証プロファイルにより、一連の管理者に共通の認証設定が定義されます。

    1. **Panorama** > **Authentication Profile** (認証プロファイル) の順に選択し、プロファイルを **Add** (追加) します。
    2. プロファイルを識別する **Name** (名前) を入力します。
    3. **Type** (タイプ) を **TACACS+** に設定します。
    4. 設定した **Server Profile** (サーバー プロファイル) を選択します。
    5. **Retrieve user group from TACACS+** (**TACACS+** からユーザー グループを取得) を選択して、TACACS+ サーバーで定義された VSA からユーザー グループ情報を収集します。

       Panorama は、グループ情報を認証プロファイルの Allow List (許可リスト) で指定したグループと照合します。
    6. **Advanced** (詳細) を選択し、Allow List (許可リスト) で、この認証プロファイルで認証することが許可された管理者を **Add** (追加) します。
    7. **OK** をクリックして認証プロファイルを保存します。

STEP 4 | 専用のログ コレクタの認証を設定します。

1. **Panorama** > **Managed Collectors** (管理対象コレクタ) を選択し、以前に追加した専用のログ コレクタを選択します。
2. 前のステップで設定した **Authentication Profile** (認証プロファイル) を選択します。

   グローバル認証プロファイルが割り当てられていない場合は、リモート認証を活用するために、個々のローカル管理者に認証プロファイルを割り当てる必要があります。
3. 専用のログ コレクタの認証 **Timeout Configuration** (タイムアウト設定) を設定します。
    1. ユーザーが専用のログ コレクタ CLI からロックアウトされるまでの **Failed Attempt** (試行失敗回数) の数を入力します。
    2. **Lockout Time** (ロックアウト時間) を分単位で入力します。専用のログ コレクタは、ユーザーが設定された数の試行失敗回数に達すると、ユーザー アカウントをロックアウトします。
    3. アクティブではないユーザー アカウントが自動的にログアウトされるまでの時間である、**Idle Timeout** (待機タイムアウト) を分単位で入力します。
    4. 専用のログ コレクタに同時にアクセスできるユーザー アカウントの数を設定するには、**Max Session Count** (最大セッション カウント) を入力します。
    5. 管理者が自動的にログアウトする前にログインできる**Max Session Time** (最大セッション時間) を入力します。
4. 専用のログ コレクタの管理者を追加します。

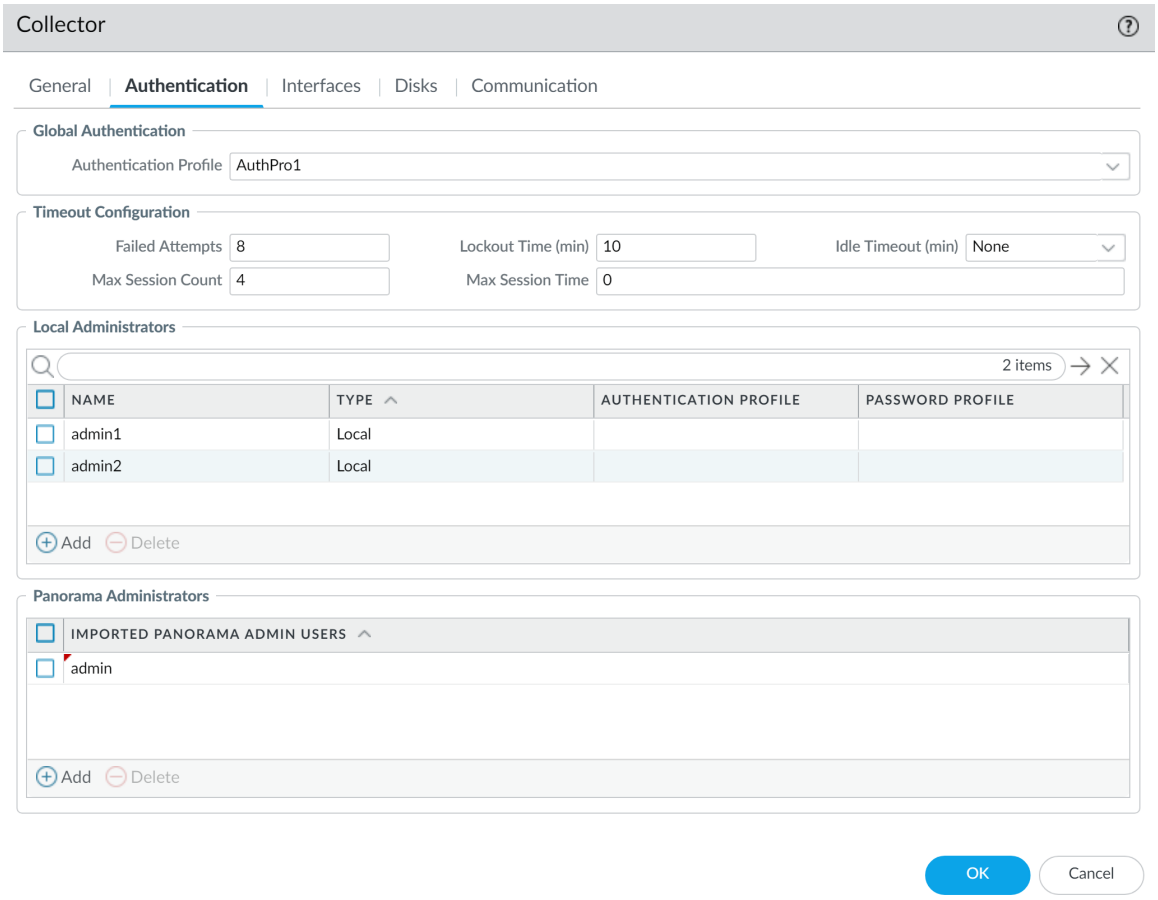
   管理者は、ローカル管理者またはインポートされた Panorama 管理者のいずれかとして追加できますが、両方を追加することはできません。ローカル管理者とインポートされた Panorama 管理者

© 2019 Palo Alto Networks, Inc.

の両方として同じ管理者を追加することはサポートされておらず、Panorama コミットが失敗します。例えば、**admin1** をローカル管理者と Panorama 管理者の両方として追加する場合、Panorama へのコミットは失敗します。

1. 専用のログ コレクタに固有の新しい管理者を**Add** (追加) して設定します。これらの管理者は、それらが作成された専用ログ コレクタに固有であり、この表からこれらの管理者を管理します。
2. Panorama で設定された管理者を **Add** (追加) します。これらの管理者は Panorama で作成され、専用のログ コレクタにインポートされます。

5. **OK** をクリックすると、専用のログ コレクタ認証設定を保存します。



STEP 5 | 設定の変更を **Commit** (コミット) してから、**Commit and Push** (コミットしてプッシュ) します。

STEP 6 | 専用のログ コレクタのPanorama CLI へのログインを使用して、ローカル管理者ユーザーを使用して専用ログ コレクタに正常にアクセスできることを確認します。

専用のログ コレクタの LDAP 認証の設定

LDAP を使用して、専用のログ コレクタ Web インターフェースにアクセスするエンド ユーザーを認証できます。

STEP 1 | Panorama Web インターフェイスへのログイン.

STEP 2 | 管理対象コレクタの設定.

© 2019 Palo Alto Networks, Inc.

STEP 3 | LDAP サーバー プロファイルを追加します。

このプロファイルは、専用のログ コレクタが LDAP サーバーに接続する方法を定義します。

1. **Panorama** > **Server Profiles**（サーバー プロファイル）> **LDAP**を選択し、サーバー プロファイルを **Add**（追加）します。
2. サーバー プロファイルを識別する **Profile Name**（プロファイル名）を入力します。
3. LDAP サーバーを **Add** (追加) します（最大 4 件）。各サーバーについて、**Name** (名前) (サーバーを識別するため）、**LDAP Server** (サーバー) の IP アドレスあるいは FQDN、およびサーバーの **Port** (ポート) (デフォルトは 389）を入力します。

   FQDN アドレス オブジェクトを使用してサーバーを識別し、後でアドレスを変更する場合は、変更をコミットし、新しいサーバー アドレスを有効にする必要があります。
4. サーバーの **Type** (タイプ) を選択します。
5. **Base DN**（ベース **DN**）を選択します。

   ディレクトリのベース DN を識別するには、**Active Directory Domains and Trusts(Active Directory** ドメインと信頼関係)Microsoft 管理コンソールスナップインを開き、トップレベル ドメインの名前を使用します。
6. **Bind DN** と **Password**（パスワード）を入力して、ファイアウォールを認証するための認証サービスを有効にします。

   Bind DN (バインド DN) アカウントには、*LDAP* ディレクトリを参照する権限が必要です。
7. **Bind Timeout** (バインドのタイムアウト) および **Search Timeout** (検索タイムアウト) を秒単位で入力します（デフォルトはどちらも 30）。
8. **Retry Interval**（再試行間隔）を秒単位で入力します（デフォルトは 60）。
9. （LDAP のみ）ディレクトリサーバーとの保護された接続のためにエンドポイントで SSL または TLS を使いたい場合は、 **Require SSL/TLS secured connection**（**SSL/TLS** で保護された接続を要求）オプションを有効にしてください（デフォルトで有効）。サーバー ポートによってエンドポイントが使用するプロトコル：
   - 389（デフォルト）– TLS（具体的には、専用のログ コレクタは StartTLS 操作を使用して、最初のプレーンテキスト接続を TLS にアップグレードします）
   - 636 – SSL
   - その他の任意のポート – 専用のログ コレクタはまず TLS を使用します。ディレクトリ サーバーで TLS がサポートされていない場合は、専用のログ コレクタは SSL にフォールバックします。
10. （LDAP のみ）保護を強化するには、**Verify Server Certificate for SSL sessions**（**SSL** セッションのサーバー証明書を確認）オプションを有効化します。すると、エンドポイントは SSL/TLS 接続にディレクトリサーバーが提示する証明書を確認します。この検証を有効にする場合は、**Require SSL/TLS secured connection**（**SSL/TLS**で保護された接続を要求）オプションを有効化する必要があります。進めるための確認において、証明書は次のいずれかの条件に合う必要があります。
    - 以下はPanorama 証明書のリストにあります：**Panorama** > **Certificate Management**（証明書の管理）> **Certificates**（証明書）> **Device Certificates**（デバイス証明書）。必要に応じて、証明書を Panorama にインポートします。
    - 証明書の署名者は信頼できる証明機関のリストにあること：**Panorama** > **Certificate Management (Panorama 証明書管理)** > **Certificates (証明書)**。
11. **OK** をクリックしてサーバー プロファイルを保存します。

STEP 4 | 専用のログ コレクタの認証を設定します。

1. **Panorama** > **Managed Collectors** (管理対象コレクタ) を選択し、以前に追加した専用のログ コレクタを選択します。
2. 専用のログ コレクタの認証 **Timeout Configuration** (タイムアウト設定) を設定します。

© 2019 Palo Alto Networks, Inc.

1. ユーザーが専用のログ コレクタ CLI からロックアウトされるまでの **Failed Attempt** (試行失敗回数) の数を入力します。
2. **Lockout Time** (ロックアウト時間) を分単位で入力します。専用のログ コレクタは、ユーザーが設定された数の試行失敗回数に達すると、ユーザー アカウントをロックアウトします。
3. アクティブではないユーザー アカウントが自動的にログアウトされるまでの時間である、**Idle Timeout** (待機タイムアウト) を分単位で入力します。
4. 専用のログ コレクタに同時にアクセスできるユーザー アカウントの数を設定するには、**Max Session Count** (最大セッション カウント) を入力します。
5. 管理者が自動的にログアウトする前にログインできる**Max Session Time** (最大セッション時間) を入力します。

3. 専用のログ コレクタの管理者を追加します。

   管理者は、ローカル管理者またはインポートされた Panorama 管理者のいずれかとして追加できますが、両方を追加することはできません。ローカル管理者とインポートされた Panorama 管理者の両方として同じ管理者を追加することはサポートされておらず、Panorama コミットが失敗します。例えば、`admin1` をローカル管理者と Panorama 管理者の両方として追加する場合、Panorama へのコミットは失敗します。

   - ローカルの管理者を設定します。

     専用のログ コレクタに固有の新しい管理者を設定します。これらの管理者は、それらが作成された専用ログ コレクタに固有であり、この表からこれらの管理者を管理します。

     1. 1名以上のローカル管理者を **Add** (追加) します。
     2. ローカル管理者の **Name** (名前) を入力します。
     3. 前に作成した **Authentication Profile** (認証プロファイル) を割り当てます。

        LDAP 認証プロファイルは、個々のローカル管理者に対してのみサポートされます。

     4. **Use Public Key Authentication (SSH)** (公開キーの認証 (SSH) の使用) を 有効化 (チェックを入れる) して、認証用の公開キー ファイルをインポートします。
     5. **Password Profile** (パスワードのプロファイル) を選択して、有効期限パラメータをセットします。
   - 既存の Panorama 管理者をインポートする

     Panorama で設定された既存の管理者を インポートします。これらの管理者は Panorama で設定、管理され、専用のログ コレクタにインポートされます。

     1. 既存の Panorama 管理者を **Add** (追加) する
4. **OK** をクリックすると、専用のログ コレクタ認証設定を保存します。

STEP 5 | 専用のログ コレクタの認証を設定します。

1. **Panorama** > **Managed Collectors** (管理対象コレクタ) を選択し、以前に追加した専用のログ コレクタを選択します。
2. 前のステップで設定した **Authentication Profile** (認証プロファイル) を選択します。
3. 専用のログ コレクタの認証 **Timeout Configuration** (タイムアウト設定) を設定します。
   1. ユーザーが専用のログ コレクタ CLI からロックアウトされるまでの **Failed Attempt** (試行失敗回数) の数を入力します。
   2. **Lockout Time** (ロックアウト時間) を分単位で入力します。専用のログ コレクタは、ユーザーが設定された数の試行失敗回数に達すると、ユーザー アカウントをロックアウトします。
   3. アクティブではないユーザー アカウントが自動的にログアウトされるまでの時間である、**Idle Timeout** (待機タイムアウト) を分単位で入力します。
   4. 専用のログ コレクタに同時にアクセスできるユーザー アカウントの数を設定するには、**Max Session Count** (最大セッション カウント) を入力します。

© 2019 Palo Alto Networks, Inc.

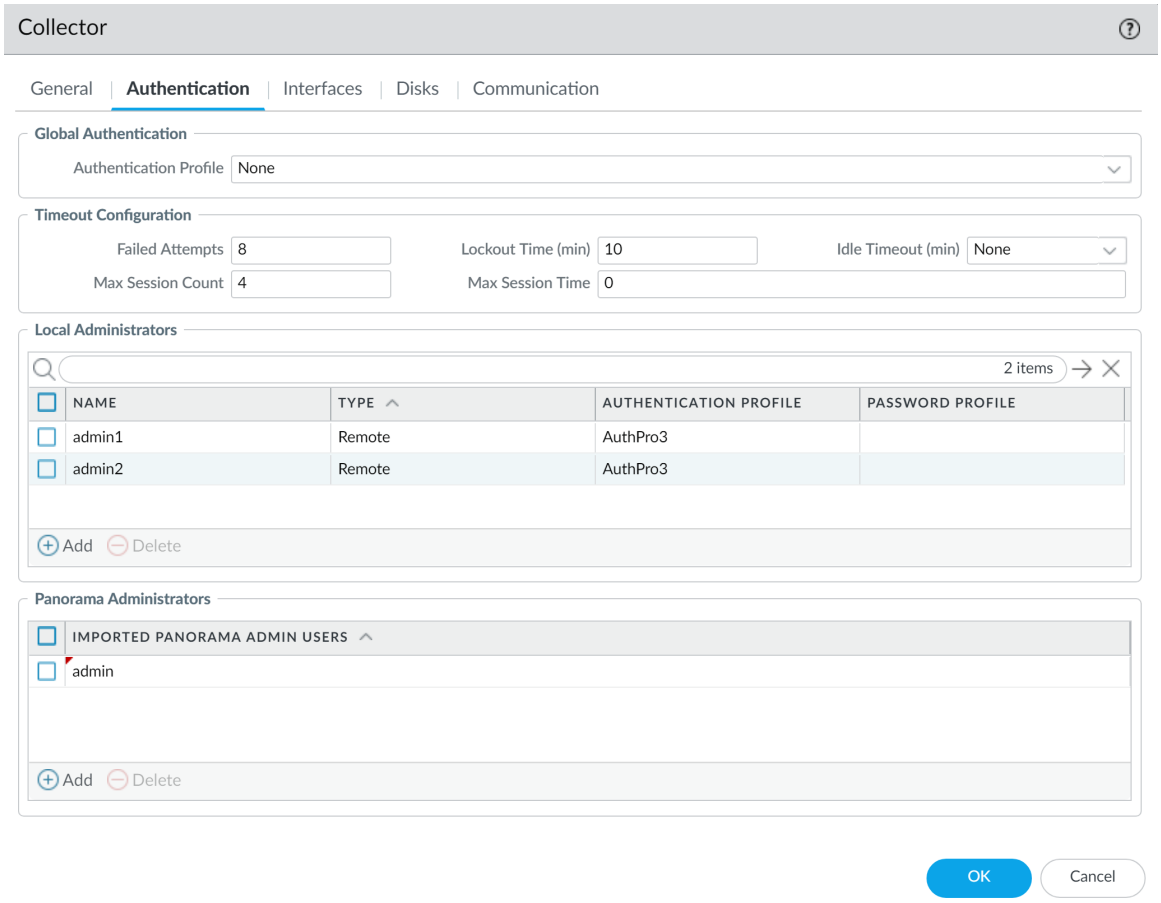
5. 管理者が自動的にログアウトする前にログインできる**Max Session Time** (最大セッション時間) を入力します。

4. 専用のログ コレクタの管理者を追加します。

   管理者 (`admin`) はローカル管理者またはインポートされた Panorama 管理者のいずれかとして追加する必要がありますが、両方を追加することはできません。管理者が追加されていない場合、または管理者がローカル管理者とインポートされた Panorama 管理者の両方として追加されている場合、管理対象コレクタへのプッシュは失敗します。

   1. 専用のログ コレクタに固有の新しい管理者を**Add** (追加) して設定します。これらの管理者は、それらが作成された専用ログ コレクタに固有であり、この表からこれらの管理者を管理します。
   2. Panorama で設定された管理者を **Add** (追加) します。これらの管理者は Panorama で作成され、専用のログ コレクタにインポートされます。

5. **OK** をクリックすると、専用のログ コレクタ認証設定を保存します。



STEP 6 | 設定の変更を **Commit** (コミット) してから、**Commit and Push** (コミットしてプッシュ) します。

STEP 7 | 専用のログ コレクタのPanorama CLI へのログインを使用して、ローカル管理者ユーザーを使用して専用ログ コレクタに正常にアクセスできることを確認します。

© 2019 Palo Alto Networks, Inc.

コレクタ グループの管理

コレクタ グループとは、単一の論理ユニットとしてファイアウォール ログを収集する 1 から 16 個のログ コレクタの集まりです。ファイアウォールがログをログ コレクタに正常に送信するには、1 個以上のログ コレクタをコレクタ グループに割り当てる必要があります。コレクタ グループが設定されていない場合、またはログ コレクタがコレクタ グループに割り当てられていない場合は、ファイアウォール ログが廃棄されます。複数のログ コレクタを持つコレクタ グループを定義し、ログの冗長性を確保する、あるいは単一のログ コレクタのキャパシティを超えるロギング レートを達成することができます（「Panorama モデル」を参照）。「複数のログ コレクタを含むコレクタ グループに関する注意事項」を参照し、リスクおよび推奨される移行についての情報をご確認ください。

Panorama モードの M-600、M-500、および M-200 アプライアンスには、定義済みのローカル ログ コレクタを含む定義済みのコレクタ グループがあります。定義済みのコレクタ グループは、名前を除くすべての設定を編集できます（デフォルト）。

コレクタ グループを削除すると、ログが失われます。

Palo Alto Networks は、*Panorama* が専用のログ コレクタも管理するかどうかに関わらず、定義済みのログ コレクタとコレクタ グループを *Panorama* 管理サーバー上に保持することをお勧めします。

M-Series アプライアンスを *Panorama* モードからログ コレクタ モードに切り替えると、定義済みのコレクタ グループとログ コレクタが失われます。そのときは、M-Series アプライアンスをログ コレクタとしてセットアップし、管理対象コレクタとして *Panorama* に追加した後、そのコレクタを含むようにコレクタ グループを設定する必要があります。

- コレクタ グループの設定
- ログ コレクタ間でのカスタム証明書を用いる認証の設定
- ログ コレクタを別のコレクタ グループに移動
- コレクタ グループからのファイアウォールの削除

コレクタ グループの設定

コレクタ グループを設定する前に、各グループに単一のログ コレクタを含めるか、複数のログ コレクタ（最大 16 個）を含めるかを決定します。複数のログ コレクタが含まれるコレクタ グループは、より高いロギング速度とログの冗長性をサポートしますが、以下の要件があります。

- 単一のコレクタ グループでは、すべてのログ コレクタ、すべての M-600 アプライアンス、すべての M-500 アプライアンス、すべての M-200 アプライアンス、すべての Panorama バーチャル アプライアンスは同じ Panorama モデルで動作する必要があります。
- 各ログ コレクタのロギング用ディスク数が同じ場合にのみ、ログの冗長化が可能になります。ディスクをログ コレクタに追加するには、「M-Series アプライアンスのストレージの拡張」を参照してください。
- (ベストプラクティス) 同じコレクタ グループ内のすべてのログ コレクタは、同じローカルエリアネットワーク (LAN) 内にある必要があります。同じまたは異なるワイドエリアネットワーク (WAN) のログ コレクタを同じコレクタ グループに追加することは避けてください。ネットワークの中断はより一般的に発生するため、ログデータの損失につながる可能性があります。さらに、必要に応じて Panorama がログ コレクタをすばやく照会できるよう、同じコレクタ グループ内のログ コレクタを物理的に近接させることをお勧めします。

STEP 1 | コレクタ グループを定義する前に次の作業を行います。

1. コレクタ グループに割り当てる各ファイアウォールに対して管理対象デバイスとしてのファイアウォールの追加を行います。

© 2019 Palo Alto Networks, Inc.

2. コレクタ グループに割り当てる各ログ コレクタに対して管理対象コレクタの設定を行います。

STEP 2 | コレクタ グループを追加します。

1. Panorama Web インターフェイスにアクセスし、**Panorama** > **Collector Groups**（コレクタ グループ）の順に選択して、コレクタ グループを **Add**（追加）するか、既存のものを編集します。
2. 追加する場合は、コレクタ グループの **Name**（名前）を入力します。

   既存のコレクタ グループの名前は変更できません。
3. コレクタ グループがファイアウォール ログを保持する **Minimum Retention Period**（最小保持期間）の日数（1 ~ 2,000）を入力します。

   デフォルトでは、このフィールドは空白（コレクタ グループが無期限にログを保持する）です。
4. ログ コレクタ（1 ~ 16 個）を Collector Group Members（コレクタ グループ メンバー）リストに **Add**（追加）します。
5. （推奨）複数のログ コレクタを単一のコレクタ グループに追加する場合、**Enable log redundancy across collectors**（コレクタ間のログ冗長性の有効化）を行います。

   冗長性により、いずれかのログ コレクタが利用できなくなった際にログが失われるのを防ぎます。各ログのコピーが 2 つ作成され、それぞれ異なるログ コレクタに保存されます。たとえば、コレクタグループに 2 つのログ コレクタがある場合、ログは両方のログコレクタに書き込まれます。

   冗長性を有効にすると、作成されるログが多くなるため、より大きなストレージ容量が必要になり、ストレージのキャパシティが半減します。コレクタ グループの容量が不足すると、古いログが削除されます。また、冗長性の有効化を行うとコレクタ グループ内のログ処理トラフィックが 2 倍になり、最大ロギング レートが半分になります。各ログ コレクタが、受信する各ログのコピーを配信する必要があるためです。

STEP 3 | コレクタ グループにログ コレクタおよびファイアウォールを割り当てます。

1. **Device Log Forwarding**（デバイス ログ転送）を選択し、ファイアウォールのログ転送設定リストを **Add**（追加）します。

   ログデータは別の TCP チャネル経由で転送されます。ログ転送の設定を追加することで、ログデータを転送するための個別の TCP 接続を作成できるようになります。

   preference list (設定リスト *- plist)* により、ログコレクタがファイアウォールからログを受信する順番が決定されます。ログ転送設定リストが割り当てられていない場合、以下のシナリオのいずれかが発生する可能性があります。

   - *Panorama* が管理専用モードの場合、*Panorama* はすべての受信ログを削除します。
   - *Panorama* が *Panorama* モードの場合、ローカルログコレクタが管理対象コレクタとして設定されていなければ、*Panorama* はすべての受信ログを削除します。
   - *Panorama* が *Panorama* モードの場合、ローカルログコレクタが管理対象コレクタとして構成されていなければ、受信ログは受信されますが、すべての管理対象ファイアウォールが、他の利用可能なログコレクタに再配信する前にまずローカルログコレクタにログを転送するため、*Panorama* が障害になる可能性があります。

   1. Devices（デバイス）セクションで、ファイアウォールのリストを **Modify**（変更）し、**OK** をクリックします。
   2. Collectors（コレクタ）セクションで、ログ コレクタを設定リストに **Add**（追加）します。

      手順 2 で、冗長性を有効にした場合は、少なくとも 2 つのログ コレクタを追加することをお勧めします。複数のログ コレクタを割り当てる場合、最初のログ コレクタがプライマリになります。プライマリが使用できなくなった場合、ファイアウォールはリスト内の次のログ コレクタ

© 2019 Palo Alto Networks, Inc.

にログを送信します。ログ コレクタの優先順位を変更するには、ログ コレクタを選択して、優先順位を上げる場合は **Move Up**（上へ）、下げる場合は **Move Down**（下へ）で移動させます。

3. **OK** をクリックします。

STEP 4 | 各ログ タイプのストレージ容量（ログ割り当て）および有効期間を定義します。

1. **General**（全般）タブに戻り、**Log Storage**（ログ保存エリア）の値をクリックします。

   フィールドに「*0MB*」が表示される場合は、ロギング用のディスク ペアを有効にし、変更をコミットしたことを確認します（「管理対象コレクタの設定」、*Disks*（ディスク）タブ参照）。

2. ログ タイプごとにログ ストレージ **Quota(%)**（割り当て **(%)**）を入力します。
3. 各ログ タイプの **Max Days**（最大日数）（有効期間）を入力します（1 ~ 2,000）。

   デフォルトではこのフィールドは空白（ログは無期限）です。

STEP 5 | 変更をコミットし、確認します。

1. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択し、変更を Panorama および設定したコレクタ グループに **Commit and Push**（コミットしてプッシュ）します。
2. **Panorama** > **Managed Collectors**（管理対象コレクタ）の順に選択し、コレクタ グループのログ コレクタが以下の状態であることを確認します。
   - **Panorama** に接続済み — Connected（接続済み）列には、ログ コレクタが Panorama に接続されていることを示すチェック マーク アイコンが表示されます。
   - **Panorama** と同期済み — Configuration Status（設定ステータス）列は、ログ コレクタが Panorama と `In Sync`（同期中）（緑色のアイコン）であるか `Out of Sync`（非同期）（赤色のアイコン）であるかを示します。

STEP 6 | ネットワーク リソースへの接続のトラブルシューティングファイアウォールがログ コレクタに正常に接続されていることを確認します。

STEP 7 | 次のステップ...

1. Panorama へのログ転送の設定

   Panorama に転送するようにファイアウォールを設定するまで、コレクタ グループはファイアウォール ログを受信しません。

2. （任意）Panorama から外部の宛先へのログ転送を設定します。

   各コレクタ グループはログを個別の宛先（Syslog サーバーなど）に転送するように設定することができます。

ログ コレクタ間でのカスタム証明書を用いる認証の設定

ログ コレクタ間の通信にカスタム証明書を設定するには、次の手順を実行します。サーバーとクライアントのロールが動的に選択されるため、コレクタ グループ内の各ログ コレクタで安全なサーバー通信とセキュリティ保護されたクライアント通信を設定する必要があります。カスタム証明書を使用して、ログ コレクタ グループのメンバー間の相互認証を保証する独自の信頼関係を作成します。

カスタム証明書の使用の詳細については、SSL/TLS 接続を相互に認証する方法を参照してください。

STEP 1 | 各ログ収集のためのキーペアと認証局（CA）証明書を取得します。

STEP 2 | コレクタ グループの各ログ コレクタのクライアント ログ コレクタ、サーバー キーペア、およびクライアント キーペアの ID を検証するために CA 証明書をインポートします。

© 2019 Palo Alto Networks, Inc.

1. **Panorama** > **Certificate Management**（ 証明書の管理 ） > **Certificates**（ 証明書 ） > **Import**を選択します。
2. CA 証明書、サーバー キーペア、およびクライアント キーペアをインポートします。
3. 各ログ コレクタに対して ステップを繰り返します。

STEP 3 | セキュア サーバー通信用のルート CA および中間 CA が含まれる証明書プロファイルを設定します。この証明書プロファイルは、ログ コレクタ間の認証を定義します。

1. **Panorama** > **Certificate Management**（証明書の管理 ） > **Certificate Profile**（証明書プロファイル ）の順に選択します。
2. 証明書プロファイルの設定を行います。

   証明書プロファイルの一部として中間 CA を設定する場合、ルート CA も含める必要があります。

STEP 4 | セキュア クライアント通信の証明書プロファイルを設定します。このプロファイルは、各クライアント ログ コレクタで個別に設定することも、Panorama™ から管理対象ログ コレクタにプッシュすることもできます。



クライアント証明書に *SCEP* を使用している場合は、証明書プロファイルの代わりにSCEP プロファイルを設定します。

1. **Panorama** > **Certificate Management**（証明書の管理 ） > **Certificate Profile**（証明書プロファイル ）の順に選択します。
2. 証明書プロファイルの設定を行います。

STEP 5 | SSL/TLS サービス プロファイルの設定を行います。

1. **Panorama** > **Certificate Management**（証明書の管理 ） > **SSL/TLS Service Profile**（**SSL/TLS** サービス プロファイル ）の順に選択します。
2. SSL/TLS プロファイルを設定し、ログ コレクタが SSL/TLS サービスに使用する証明書とプロトコルを定義します。

STEP 6 | すべてのログ コレクタにカスタム証明書をデプロイした後で、カスタム証明書認証を適用します。

1. **Panorama** > **Collector Groups**(Panorama > コレクタ グループ) の順に選択し、コレクタ グループを選択します。
2. 全般タブで、**Enable Secure Inter LC Communication**（セキュア インター **LC** 通信の有効化 ）を行います。

   セキュア インター LC 通信を有効化し、コレクタ グループがローカルのログ コレクタを追加している場合、**Log Collector on local Panorama is using the secure client configuration from Panorama** > **Secure Communication Settings**（ローカルの **Panorama** は **Panorama** セキュア通信設定からのセキュア クライアント 設定を使用しています ）を宣言するリンクが表示されるはずです。このリンクをクリックすると、セキュア通信設定ダイアログ ボックスが開き、そこからローカルのログ コレクタのセキュリティ保護されたクライアント設定が保護されます。
3. **OK** をクリックします。
4. 変更を **Commit** (コミット)します。

STEP 7 | 各ログ コレクタでセキュア サーバー通信を設定します。

1. 専用ログ コレクタの **Panorama** > **Managed Collectors**（管理対象のコレクタ ）または **Panorama** > **Setup**（セットアップ ） > **Management**（管理 ）を選択して、ローカルのログ コレクタのセキュア通信設定を **Edit**（変章 ）します。
2. 専用ログ コレクタの場合は、Log Collector をクリックし、 **Communications**（通信 ）を選択します。

© 2019 Palo Alto Networks, Inc.

3. **Customize Secure Server Communication**（セキュリティで保護されたサーバー通信のカスタマイズ）機能を有効にします。
4. **SSL/TLS Service Profile**（**SSL/TLS** サービス プロファイル）ドロップダウンから SSL/TLS サービス プロファイルを選択します。この SSL/TLS サービス プロファイルは、ログ コレクタ間のすべての SSL 接続に適用されます。
5. ドロップダウン リストから **Certificate Profile**（証明書プロファイル）を選択します。
6. **Custom Certificate Only**（カスタム証明書のみ）が無効（チェックボックスがオフ）になっていることを確認します。これにより、ログ コレクタ間通信で、カスタム証明書を構成する際に定義済みの証明書を使用し続けることができます。
7. 切断待機時間 - 他のログ コレクタとの接続を切断して再確立するまでにログ コレクタが待機する時間（分）を設定します。このフィールドはデフォルトで空白になっています（範囲は 0 ~ 44,640 分）。
8. （任意）認証リストを設定します。承認リストにより、証明書認証に新たなセキュリティの層が追加されます。承認リストは、クライアント証明書の Subject（サブジェクト）または Subject Alt Name（サブジェクト代替名）をチェックします。クライアント証明書で示されたサブジェクトまたはサブジェクト代替名が承認リストの識別子と一致しない場合、認証は拒否されます。
    1. Authorization List（承認リスト）を **Add**（追加）します。
    2. 識別子タイプとして証明書プロファイルで設定した **Subject**（サブジェクト）または **Subject Alt Name**（サブジェクト代替名）を選択します。
    3. 識別子が `Subject`の場合は Common Name（共通名（CN））を入力し、識別子が `Subject Alt Name` の場合は IP アドレス、ホスト名、または電子メール アドレスを入力します。
    4. **OK** をクリックします。
    5. **Check Authorization List**（承認リストのチェック）オプションを有効にして、Panorama が承認リストを適用するように設定します。
9. **OK** をクリックします。
10. 変更を **Commit (**コミット**)**します。

これらの変更をコミットすると、切断待機時間カウントダウンが開始されます。待機時間が終了すると、コレクタ グループのログ コレクタは、設定された証明書なしでは接続できません。

STEP 8 | 各ログ コレクタでクライアント サーバー通信を設定します。

1. 専用ログ コレクタの **Panorama** > **Managed Collectors**（管理対象のコレクタ）または **Panorama** > **Setup**（セットアップ） > **Management**（管理）を選択して、ローカルのログ コレクタのセキュア通信設定を **Edit**（変章）します。
2. 専用ログ コレクタの場合は、Log Collector をクリックし、 **Communications**（通信）を選択します。
3. セキュア クライアント設定で、それぞれのドロップダウン リストから **Certificate Type**（証明書タイプ）、**Certificates**（証明書）、**Certificate Profile**（証明書プロファイル）を選択します。
4. **OK** をクリックします。
5. 変更を **Commit (**コミット**)**します。

ログ コレクタを別のコレクタ グループに移動

M-600、M-500、M-200、および　Panorama バーチャル アプライアンスでは、各コレクタ グループに 1 つ以上のログ コレクタを含めることができます。コレクタ グループのロギング レートおよびログ保持要件に基づいて、ログ コレクタをコレクタ グループに割り当てます。コレクタ グループのレートと必要とされるストレージが増える場合は、M-Series アプライアンスのストレージの容量を増やすか、コレクタ グループの設定を行ってログコレクタを追加することが推奨されます。しかし一部の導入環境では、コレクタ グループ間でログコレクタを移動させる方が合理的な場合があります。

ログ コレクタが *Panorama* モードのアプライアンスの *M-600*、*M-500* または *M-200* のローカルにある場合、アプライアンスが高可用性 *(HA)* 構成のパッシブ ピアである場合のみ、ロ

© 2019 Palo Alto Networks, Inc.

グ コレクタを移動させます。*HA* 同期では、新しいコレクタ グループに関連付けられた構成を適用します。アクティブ *HA* ピアのローカルにあるログ コレクタは決して移動させないでください。

単一のコレクタ グループでは、すべてのログ コレクタ、すべての *M-600* アプライアンス、すべての *M-500* アプライアンス、すべての *M-200* アプライアンス、すべての *Panorama* バーチャル アプライアンスは同じ *Panorama* モデルで動作する必要があります。

各ログ コレクタのロギング用ディスク数が同じ場合にのみ、ログの冗長化が可能になります。ディスクをログ コレクタに追加するには、「M-Series アプライアンスのストレージの拡張」を参照してください。

STEP 1 | Panorama管理からログコレクタを削除します。

1. **Panorama** > **Collector Groups**（コレクタ グループ）を選択し、移動させるログ コレクタを含むコレクタ グループを選択します。
2. Collector Group Members（コレクタ グループ メンバー）リストでログ コレクタを選択して **Delete**（削除）します。
3. **Device Log Forwarding**（デバイス ログ転送）を選択し、ログ転送設定リストにて、移動させるログ コレクタに割り当てられている各ファイアウォールのセットに対して次の作業を行います。
   1. ログコレクタに割り当てられているファイアウォールのリンクを Devices（デバイス）列でクリックします。
   2. Collectors（コレクタ）列でログ コレクタを選択して **Delete**（削除）します。

      ファイアウォールを割り当てるには、ログの転送先となるログコレクタを新規に*Add*（追加）します。
   3. **OK** を2回クリックして変更内容を保存します。
4. **Panorama** > **Managed Collectors**（管理対象コレクタ）を選択し、移動するログ コレクタを選択して **Delete**（削除）します。

STEP 2 | コレクタ グループの設定

ログコレクタを新しいコレクタ グループに追加し、ファイアウォールをログコレクタに割り当てます。

変更をコレクタ グループの設定にプッシュする際、*Panorama* がログ コレクタ全体に再びログを配布し始めます。このプロセスは、*1*テラバイトのログの場合は数時間かかることがあります。再配信プロセス中は、最大ロギング率が低くなります。*Panorama* > *Collector Groups*（コレクタ グループ）ページの *Log Redistribution State*（ログ再配信状態）列には、プロセスの完了状況がパーセントで表示されます。

STEP 3 | Panorama への ログ転送の設定設定を行った新しいコレクタ グループで Panorama へのログ転送を設定します。

STEP 4 | **Commit (コミット)** > **Commit and Push (コミットしてプッシュ)** の順に選択し、Panorama に対する変更をコミットして、その変更をデバイス グループ、テンプレート、コレクタ グループにプッシュします (プッシュしていない場合)。

コレクタ グループからのファイアウォールの削除

レガシー モードの Panorama バーチャル アプライアンスを使用して専用ログ コレクタを管理する場合は、ファイアウォール ログをログ コレクタに転送する代わりに、Panorama に転送するという選択肢があります。この場合は、ファイアウォールをコレクタ グループから削除する必要があります。このようにすると、ファイアウォールは自動的にログを Panorama に転送します。

© 2019 Palo Alto Networks, Inc.

ファイアウォール上にあるログ転送設定リストを一時的に削除するには、ファイアウォールで *CLI* を使用して削除できます。ただし、*Panorama* のコレクタ グループ設定内の割り当てられたファイアウォールを削除する必要があります。削除しないと、次回コレクタ グループに変更をプッシュしたとき、ファイアウォールは割り当てられたログ コレクタにログを送信するように再設定されます。

STEP 1 | **Panorama** > **Collector Groups**（コレクタ グループ）の順に選択し、コレクタ グループを編集します。

STEP 2 | **Device Log Forwarding**（デバイス ログ転送）を選択し、デバイス リストでファイアウォールをクリックし、デバイス リストを **Modify**（変更）し、ファイアウォールのチェック ボックスをオフにして **OK** を 3 回クリックします。

STEP 3 | **Commit**（コミット） > **Commit and Push**（コミットしてプッシュ）を選択し、ファイアウォールを削除した Panorama とコレクタ グループに変更を **Commit and Push**（コミットしてプッシュ）します。

© 2019 Palo Alto Networks, Inc.

Panorama へのログ転送の設定

各ファイアウォールはデフォルトでログ ファイルをローカルで保存し、他のファイアウォールに保存されたログを表示できません。そのため、すべてのファイアウォールで監視するネットワーク アクティビティをグローバルに表示できるようにするには、すべてのファイアウォール ログを Panorama に転送して Panorama を使用した可視化を実現する必要があります。組織内の一部のチームで、業務に関連したログのみを監視することで効率を高められる場合、ログ属性（脅威タイプやソース ユーザーなど）に基づいて転送フィルタを作成できます。たとえば、マルウェア攻撃を調査するセキュリティ オペレーション アナリストの場合、タイプ属性が wildfire-virus に設定された脅威ログにしか関心を持たない可能性もあります。

以下の手順は、複数のファイアウォールを設定してログを転送するための Panorama テンプレートおよびデバイス グループの使用方法を示しています。

Panorama が *PAN-OS 7.0* 以前のソフトウェア バージョンで動作するファイアウォールを管理する場合、ファイアウォールが送信する *WildFire* サンプルに対する分析情報を *Panorama* が収集するのに使用する *WildFire*® サーバーを指定します。*Panorama* はこの情報を利用し、*PAN-OS 7.0* で導入されたフィールドの値が欠けている *WildFire* 送信ログを完成させます。それより古いバージョンのファイアウォールはこのフィールドを自動で埋めることはありません。サーバーを指定するには、*Panorama* > *Setup*（セットアップ）> *WildFire* を選択し、*General Settings*（一般設定）を編集して*WildFire Private Cloud*（*WildFire* プライベート クラウド）の名前を入力します。デフォルトの値は、米国でホストされている *WildFire* クラウドである *wildfire-public-cloud* です。

ファイアウォール ログを外部サービス（*Syslog* サーバーなど）に転送することもできます。詳細は、「ログ転送オプション」を参照してください。

STEP 1 | ログを転送するファイアウォールに対してデバイス グループの追加を行います。

Panorama は、デバイス グループがログ転送プロファイルをファイアウォールにプッシュ送信することを求めます。新しいデバイス グループを作成するか、既存のデバイス グループにファイアウォールを割り当てます。

STEP 2 | ログを転送するファイアウォールに対してテンプレートの追加を行います。

Panorama は、テンプレートがログ設定をファイアウォールにプッシュ送信することを求めます。新しいテンプレートを作成するか、既存のテンプレートにファイアウォールを割り当てます。

STEP 3 | ログ転送プロファイルを作成します。

プロファイルにより、トラフィック、脅威、WildFire への送信、URL フィルタリング、データ フィルタリング、トンネルおよび認証ログの宛先が定義されます。

1. **Objects** > **Log Forwarding** (オブジェクト > ログ転送)を選択し、さらにログを転送するファイアウォールの**Device Group** (デバイスグループ)を選択してプロファイルを**Add** (追加)します。
2. ログ転送プロファイルを識別する **Name**（名前）を入力します。
3. 1 つ以上の一致リスト プロファイルを **Add**（追加）します。

   プロファイルにより、ログ クエリ フィルター、転送先、タギングなどの自動アクションが指定されます。各一致リスト プロファイルについて、以下の手順を実行します。

   1. プロファイルを識別する **Name**（名前）を入力します。
   2. **Log Type**（ログ タイプ）を選択します。
   3. **Filter**（フィルター）ドロップダウンから **Filter Builder**（フィルター ビルダー）を選択します。以下を指定してから、各クエリを **Add**（追加）します。

© 2019 Palo Alto Networks, Inc.

Connector（条件式）のロジック（and/or）

ログの **Attribute**（属性）

包含または除外ロジックを定義する **Operator**（演算子）

クエリを一致させるための属性の **Value**（値）

4. **Panorama** を選択します。

4. **OK** をクリックして Log Forwarding（ログ転送）プロファイルを保存します。

STEP 4 | Log Forwarding（ログ転送）プロファイルをポリシー ルールおよびネットワーク ゾーンに割り当てます。

セキュリティ、認証、DoS 防御ルールはログ転送をサポートしています。この例では、プロファイルをセキュリティ ルールに割り当てます。

ログ転送をトリガーするルールごとに、以下の手順を実行します。

1. ルールベースを選択（たとえば、**Policies**（ポリシー）> **Security**（セキュリティ）> **Pre Rules**（プレ ルール））し、ログを転送するファイアウォールの **Device Group**（デバイス グループ）を選択し、さらにそのルールを編集します。
2. **Actions**（アクション）を選択し、作成した **Log Forwarding**（ログ転送）プロファイルを選択します。
3. **Profile Type**（プロファイル タイプ）を **Profiles**（プロファイル）または **Group**（グループ）に設定してから、以下のログの生成と転送をトリガーするために必要なセキュリティ プロファイルまたは **Group Profile**（グループ プロファイル）を選択します。
   - 脅威ログ — トラフィックは、そのルールに割り当てられたいずれかのセキュリティ プロファイルと一致する必要があります。
   - WildFire ログ — トラフィックは、ルールに割り当てられた WildFire 分析プロファイルに一致する必要があります。
4. トラフィック ログについては、**Log At Session Start**（セッション開始時にログ）かつ/または **Log At Session End**（セッション終了時にログ）を選択します。
5. **OK** をクリックしてルールを保存します。

STEP 5 | システム ログ、設定ログ、User-ID™ ログ、HIP マッチ ログの宛先を設定します。

Panorama は相関ログをファイアウォールから集約するのでなく、受信するファイアウォールログに基づいて相関ログを生成します。

1. **Device** > **Log Settings** (デバイス > ログ設定)を選択し、ログを転送するファイアウォールの**Template** (テンプレート)を選択します。
2. ファイアウォールが転送する各ログ タイプについては、1 つ以上の一致リスト プロファイルを追加するステップを参照してください。

STEP 6 | （PA-7000 シリーズ ファイアウォールのみ）ログ転送を実行するようにログ カード インターフェイスを設定します。

ログ カード インターフェイスとして PA-7000 シリーズのネットワーク処理カード（NPC）のいずれかでデータ ポートを設定する場合、ファイアウォールは設定したロギング先へのログの転送をこのインターフェイスを使用して自動的に開始し、WildFire 分析用にファイルを転送します。設定したインターフェイスがログの転送先と WildFire クラウドまたは WildFire アプライアンス、またはその両方にアクセスできることを確認してください。

PA-7000 シリーズ ファイアウォールがログを *Panorama* に転送できるようになったため、*Panorama* は管理する *PA-7000* シリーズ ファイアウォールをログ コレクタとして扱わなくなります。ログを *Panorama* に転送するように *PA-7000* シリーズ ファイア

© 2019 Palo Alto Networks, Inc.

ウォールを設定していない場合、管理対象 *PA-7000* シリーズ ファイアウォールが生成するすべてのログはローカル ファイアウォールからのみ表示でき、*Panorama* からは表示できません。*PA-7000* シリーズ ファイアウォールからのロギング速度およびボリュームを扱うことができるログ転送インフラストラクチャがまだない場合、*PAN-OS 8.0.8* 以降では、ログを監視するときに *Panorama* で *PA-7000* シリーズ ファイアウォールを直接照会することができます。この機能を使用するには、*Panorama* と *PA-7000* シリーズ ファイアウォールの両方で *PAN-OS 8.0.8* 以降が実行されている必要があります。*Panorama CLI* から以下のコマンドを入力して、*Panorama* で *PA-7000* シリーズ ファイアウォールを直接照会できるようにします。

```
> debug reportd send-request-to-7k yes
```

このコマンドを実行すると、*Panorama* の *Monitor*（監視）タブで管理対象 *PA-7000* シリーズ ファイアウォールのログを表示できるようになります。さらに、すべての管理対象デバイスの場合と同じように、*Data Source*（データ ソース）として *Remote Device Data*（リモート デバイス データ）を選択することで、*PA-7000* シリーズ ログ データが含まれるレポートを生成することもできます。後から *PA-7000* シリーズ ファイアウォールでログを *Panorama* に転送できるようにする場合、最初に ***debug reportd send-request-to-7k no*** コマンドを使用してこのオプションを無効にする必要があります。

1. **Network**（ネットワーク）> **Interfaces**（インターフェイス）> **Ethernet**（イーサネット）の順に選択し、ログを転送するファイアウォールの **Template**（テンプレート）を選択して、**Add Interface**（インターフェイスの追加）を行います。
2. **Slot**（スロット）および **Interface Name**（インターフェイス名）を選択します。
3. **Interface Type**（インターフェイス タイプ）を **Log Card**（ログ カード）に設定します。
4. **IP Address**（IP アドレス）、**Default Gateway**（デフォルト ゲートウェイ）、および（IPv4 のみ）**Netmask**（ネットマスク）を入力します。
5. **Advanced**（詳細）を選択し、**Link Speed**（接続速度）、**Link Duplex**（リンクデュプレックス）、および **Link State**（リンク状態）を指定します。

   こうしたフィールドのデフォルトは*auto*（自動）で、ファイアウォールが接続に基づいて値を自動的に決定するように指定します。しかし、*Link Speed*（接続速度）は最低 *1000　Mbps* 以上に設定することをお勧めします。
6. **OK** をクリックして変更内容を保存します。

STEP 7 | ログを受信するように Panorama を設定します。

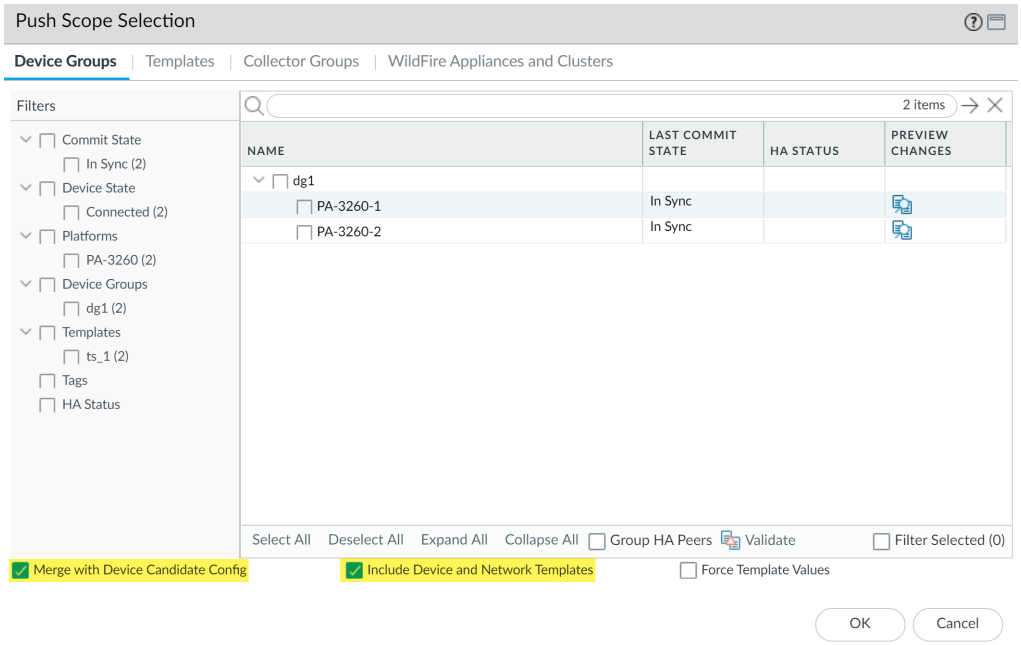
ログをレガシー モードの *Panorama* バーチャル アプライアンスに転送する場合、この手順はスキップできます。

1. ログを受信する各ログ コレクタに対して管理対象コレクタの設定を行います。
2. コレクタ グループの設定を行い、ログ転送のためにファイアウォールを特定のログ コレクタに割り当てます。

STEP 8 | 設定の変更をコミットします。

1. **Commit (コミット) > Commit and Push (コミットしてプッシュ)** を選択して **Edit Selections (選択内容の編集)** します。
2. **Merge with Device Candidate Config (デバイス候補構成にマージ)**、**Include Device and Network Templates (デバイスおよびネットワーク テンプレートを含める)**を選択して **OK** をクリックします。

© 2019 Palo Alto Networks, Inc.



3. Panorama に対する変更を **Commit and Push** (コミットしてプッシュ) し、コミットして、デバイス グループに対する変更とコレクタ グループに対する変更をプッシュします。
4. Panorama へのログ転送の確認を行い、設定が正しく完了したことを確認します。

Panorama にログを送信する際にファイアウォールが使用するログ転送モードを変更するために、ログ転送とバッファのデフォルトの変更が可能です。また、ログおよびレポートのストレージ割り当ておよび有効期間を管理することも可能です。

© 2019 Palo Alto Networks, Inc.

外部の宛先への syslog 転送の設定

ログ生成のレートが高いデプロイメントの場合、イーサネット インターフェースを介して syslog を転送して、ログの損失を防ぎ、管理インターフェースの負荷を軽減して、管理操作を最適化できます。

イーサネット インターフェースを使用する syslog 転送は、Panorama モードまたはログ コレクタ モードの Panorama™ 管理サーバーに対してのみサポートされます。また、Panorama が Panorama モードであるかログ コレクタ モードであるかに関係なく、単一のインターフェース上でのみ syslog を転送することができます。

STEP 1 | Panorama Web インターフェースにログインします。

STEP 2 | 管理対象コレクタの設定.

STEP 3 | コレクタ グループの設定.

M-Series アプライアンスではデフォルトのコレクタ グループが事前定義済みであり、すでにローカル ログ コレクタがメンバーとして含まれています。しかし、Panorama バーチャル アプライアンスでは、コレクタ グループを追加してローカル ログ コレクタをメンバーとして追加する必要があります。どちらの設定でも、ログ転送のためにファイアウォールをログ コレクタに割り当てる必要があります。

STEP 4 | Syslog サーバー プロファイルを設定します。

1. **Panorama** > **Server Profiles**（サーバー プロファイル）> **Syslog** の順に選択し、新しい syslog サーバー プロファイルを **Add**（追加）します。
2. syslog サーバー プロファイルの **Name** (名前) を入力します。
3. 各 syslog サーバーに対して、Panorama または専用のログ コレクタが接続のために要求する情報を **Add** (追加) します。
   - **Name** (名前)—syslog サーバーの一意の名前。
   - **Syslog Server**[Syslog サーバー] — Syslog サーバーの IP アドレスまたは完全修飾ドメイン名 (FQDN)。
   - **Transport** (転送)—syslog サーバーとの通信手段として、**UDP**、**TCP**、または **SSL** を選択します。
   - **Port** (ポート)—syslog メッセージを送信するときに経由するポート番号（デフォルトはポート 514 の UDP）。Panorama と専用のログ コレクタで同じポート番号を使用する必要があります。
   - **Format** [フォーマット]— 使用する Syslog メッセージ フォーマットを選択します。**BSD** (デフォルト) または **IETF**。従来、UDP 経由の場合は **BSD** フォーマット、TCP または SSL 経由の場合は **IETF** フォーマットが使用されています。
   - **Facility** (ファシリティ) - Syslog の標準値を選択します（デフォルトは **LOG_USER**）。実装されている Syslog サーバーの優先度（PRI）フィールドの計算で使用されます。PRI フィールドを使用して Syslog を管理する方法に対応する値を選択します。
4. (任意) Panorama または専用のログ コレクタが送信する syslog メッセージの形式をカスタマイズするには、**Custom Log Format** (カスタム ログ 形式)を選択します。さまざまなログ タイプのカスタム フォーマットの作成方法については、『Common Event Format Configuration Guide』（英語）を参照してください。
5. **OK** をクリックして syslog サーバー プロファイルを保存します。

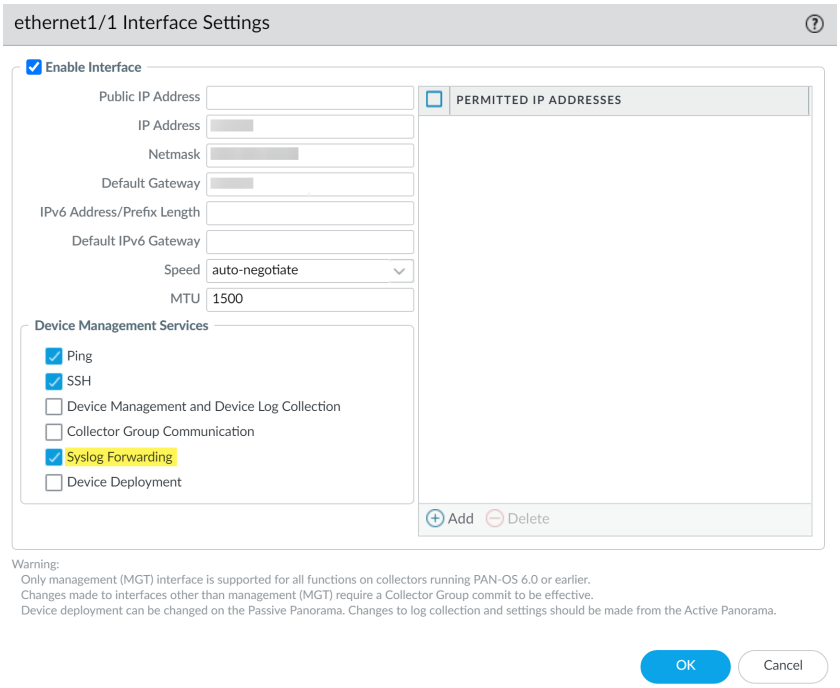
STEP 5 | 転送 syslog のイーサネット インターフェースを設定します。

デフォルトでは、syslog 転送は管理インターフェースで有効になっており、一度に1つのインターフェースでのみサポートされます。

© 2019 Palo Alto Networks, Inc.

- Panorama Web インターフェースからローカルのログ コレクタでイーサネット インターフェースを構成します。
  1. **Panorama** > **Setup**（セットアップ）> **Interfaces**（インターフェース）を選択し、イーサネット インターフェースをクリックします。
  2. **Enable Interface (インターフェースの有効化)** を実行します。
  3. Ethernet インターフェイスを適切に設定します。
  4. Device Management Services (デバイス管理サービス) セクションで **Syslog Forwarding (syslog 転送)** を有効化します。
  5. **Yes** を選択すると syslog 転送の変更内容を確定します。

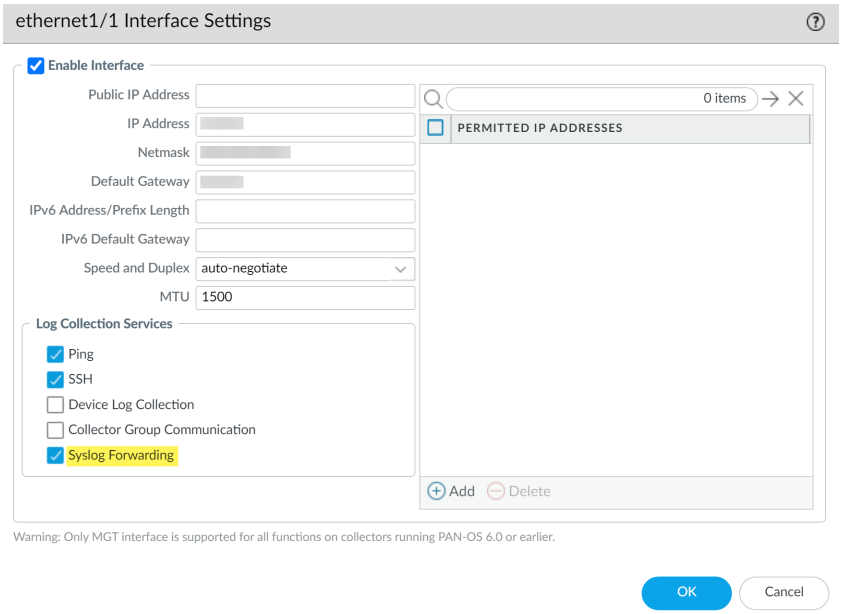
     ローカルのログ コレクタの単一のイーサネット インターフェースでのみ実行できます。
  6. **OK** をクリックして変更内容を保存します。
  7. 設定の変更を **Commit (コミット)** してから、**Commit and Push (コミットしてプッシュ)** します。



- 専用のログ コレクタのイーサネット インターフェースを設定します。
  1. **Panorama** > **Managed Collectors**(Panorama > 管理対象コレクタ) の順に選択し、専用のログ コレクタを選択します。
  2. **Enable Interface (インターフェースの有効化)** を実行します。
  3. Ethernet インターフェイスを適切に設定します。
  4. Log Collection Services (ログ収集サービス) セクションで **Syslog Forwarding (syslog 転送)** を有効化します。
  5. **Yes** を選択すると syslog 転送の変更内容を確定します。

     専用のログ コレクタの単一のイーサネット インターフェースでのみ実行できます。
  6. **OK** をクリックして変更内容を保存します。
  7. 設定の変更を **Commit (コミット)** してから、**Commit and Push (コミットしてプッシュ)** します。

© 2019 Palo Alto Networks, Inc.



- Panorama CLI からローカルのログ コレクタまたは専用のログ コレクタでイーサネット インターフェースを構成します。

  CLI からイーサネット インターフェースを介した syslog 転送を正常に設定するには、最初に管理インターフェースで syslog 転送を無効にしてから、CLI からイーサネット インターフェースで syslog 転送を有効にする必要があります。Panoramaは、CLIからイーサネットインターフェースのsyslog転送を有効にしても、管理インターフェイスを介したsyslog転送を自動的に無効にしないため、管理インターフェイスとイーサネットインターフェイスの両方で有効にした場合、syslog転送は管理インターフェイスを介して続行されます。

  1. Panorama CLI へのログイン
  2. 管理インターフェース上の syslog 転送を無効化する:

     ```
     admin@Panorama> configure
     ```

     ```
     admin@Panorama> set log-collector <Log Collector Serial Number>
      deviceconfig system service disable-syslog-forwarding yes
     ```
  3. 管理インターフェース上の syslog 転送を有効化する:

     ```
     admin@Panorama> configure
     ```

     ```
     admin@Panorama> set log-collector <Log Collector Serial Number>
      deviceconfig system eth<Interface Number>  service disable-syslog-
     forwarding no
     ```

     ```
     admin@Panorama> commit
     ```
  4. 設定の変更をコミットする:

     ```
     admin@Panorama> run commit-all log-collector-config log-collector-
     group <Collector Group name>
     ```

STEP 6 | Panorama へのログ転送の設定.

© 2019 Palo Alto Networks, Inc.

STEP 7 | Panorama から syslog サーバーへの syslog 転送を設定します。

© 2019 Palo Alto Networks, Inc.

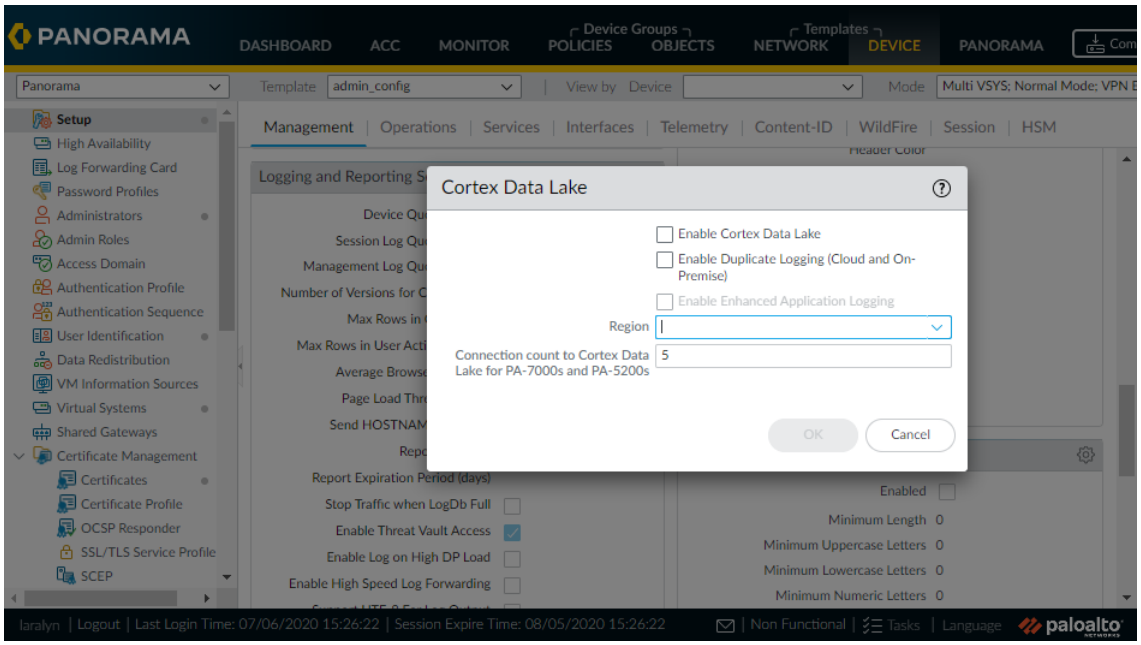
Cortex Data Lake へのログの転送

Cortex Data Lake は、Palo Alto Networks のクラウドベースのロギング インフラストラクチャです。Cortex Data Lake（旧名ロギング サービス）にログを送信するように管理対象ファイアウォールを設定する前に、デプロイメント内のログ容量に適したライセンスを購入し、クラウドサービス プラグインをインストールする必要があります。ログ コレクタを既に使用している場合は、Cortex Data Lake を使用して既存のセットアップを補完し拡張することができます。

STEP 1 | Panorama プラグインをインストールします。

STEP 2 | Cortex Data Lake にログを送信するようにファイアウォールを設定します。

PAN-OS 8.1 以降のリリースを実行しているファイアウォールの場合、ロギングの複製（クラウドおよびオンプレミス）を有効化を選択すると、Cortex Data Lake、ならびに Panorama およびオンプレミスのログコレクタの両方にログを送信することができます。有効にすると、選択したテンプレートに属するファイアウォールはログのコピーを両方の場所に保存します。**Enable Duplicate Logging (Cloud and On-Premise)** (ロギングの複製（クラウドおよびオンプレミス）を有効化) または **Enable Cortex Data Lake (Cortex Data Lake** の有効化) のいずれかを選択できますが、両方を選択することはできません。



© 2019 Palo Alto Networks, Inc.

Panorama へのログ転送の確認

Cortex Data Lake または Panorama へのログ転送を設定を行った後で、Panorama へのログ転送を確認して、設定が成功したことをテストします。

ログ コレクタへのログ転送を構成すると、管理対象ファイアウォールは、構成されたすべてのログ コレクタに対する TCP 接続を開きます。これらの接続は 60 秒ごとにタイムアウトし、ファイアウォールがログ コレクタへの接続を失ったことは示されません。サポートされているイーサネットインターフェースを介してローカルまたは専用ログ コレクタへのログ転送を設定すると、ファイアウォールがログ コレクターに正常に接続できるにもかかわらず、ファイアウォールトラフィックログに `incomplete` セッションと表示されます。管理ポートを介してログ転送を設定すると、`incomplete` セッションを示すトラフィックログは生成されません。`incomplete` セッションと表示されるトラフィックログは、PA-5200 および PA-7000 Series ファイアウォールを除くすべてのファイアウォールで生成されます。

STEP 1 | ファイアウォール CLI にアクセスします。

STEP 2 | ログ コレクタを設定したら、各ファイアウォールにログ転送設定リストがあることを検証します。

```
> show log-collector preference-list
```

コレクタ グループにログ コレクタが 1 つだけある場合、出力は次のようになります。

```
Forward to all: No
Log collector Preference List
Serial Number: 003001000024
IP Address: 10.2.133.48
IPV6 Address: unknown
```

STEP 3 | 各ファイアウォールがログを転送していることを確認します。

```
> show logging-status
```

転送が正常な場合、ログ転送エージェントがアクティブであるという内容が出力されます。

- Panorama バーチャル アプライアンスの場合、エージェントは `Panorama` になります。
- M-Series アプライアンスの場合、エージェントは `LogCollector` になります。
- Cortex Data Lake の場合、エージェントは `Log CollectionService` になります。さらに、以下のようになります。

```
'Log Collection log forwarding agent' is active and connected
 to <IP_address>.
```

STEP 4 | 平均ロギング率を表示します。直近 5 分間の平均ログ数/秒という形式で率が表示されます。

- ログコレクタがログを受信する場合、Panorama Webインターフェイスにアクセスし、 **Panorama** > **Managed Collectors** (Panorama > 管理対象コレクタ)を選択し、かなり右の方にある列の**Statistics** (統計情報)リンクをクリックします。
- レガシー モードの Panorama バーチャル アプライアンスがログを受信する場合は、Panorama CLI にアクセスして、次のコマンドを実行します。**`debug log-collector log-collection-stats show incoming-logs`**

© 2019 Palo Alto Networks, Inc.

このコマンドは *M-Series* アプライアンスでも有効です。

© 2019 Palo Alto Networks, Inc.

ログ転送とバッファのデフォルトの変更

ファイアウォールが Panorama へのログ送信に使用するログ転送モードを定義できます。高可用性（HA）設定に設定する場合は、どの Panorama ピアがログを受信するかを指定します。これらのオプションにアクセスするには、**Panorama** > **Setup**（セットアップ）> **Management**（管理）の順に選択し、Logging and Reporting Settings（ロギングおよびレポート設定）を編集して、**Log Export and Reporting**（ログのエクスポートとレポート）を選択します。

- ファイアウォールのログ転送モードを定義します。ファイアウォールは、バッファ済みログ転送モードか、ライブ モードログ転送モードのどちらかで、Panorama（M-Seriesアプライアンスと Panorama バーチャル アプライアンスの両方に関連）にログを転送できます。

ログ オプション	説明
(ベストプラクティス) **Buffered Log Forwarding from Device (デバイスから転送するバッファ済みログ)** デフォルト：有効	各管理対象ファイアウォールにログのバッファリングを許可し、30 秒間隔でログを Panorama に送信します（ユーザー設定不可）。 バッファ済みログ転送は、ファイアウォールから Panorama への接続が失われたときに、非常に役に立ちます。ファイアウォールは、ログ エントリをローカル ハード ディスクにバッファして、Panorama に最後に送信されたログ エントリを記録するためのポインタを保持します。接続が復元されると、ファイアウォールは、残りの先頭からログの転送を再開します。 バッファに使用できるディスク領域は、ファイアウォール モデルへのログ ストレージの割り当てと、まだ循環利用されていないログの量によって異なります。ファイアウォールが長時間切断され、最後に転送されたログが循環利用のために削除された場合は、再接続時にローカル ハード ディスクからすべてのログが Panorama に転送されます。ファイアウォールのローカル ハード ディスク上に使用可能な領域がなくなると、新しいイベントをロギングできるように最も古いエントリが削除されます。
デバイスからのライブ モード ログ転送 このオプションは、**Buffered Log Forwarding from Devic**（デバイスから転送するバッファ済みログ）チェック ボックスがオフの場合に有効になります。	ライブ モードでは、管理対象ファイアウォールがすべてのログ トランザクションをファイアウォール上に記録するのと同時に Panorama に送信します。

- 高可用性（HA）設定でデプロイされた、レガシー モードの Panorama バーチャル アプライアンス上にログ転送設定を定義します。
  - 仮想ディスクにロギングする場合、プライマリ Panorama ピアのローカル ディスクへのロギングのみを有効にします。デフォルトでは、HA 設定の Panorama ピアは両方ともログを受信します。

    5200 Series および *7000 Series* のファイアウォールでは、アクティブ ピアのみがログを受信します。
  - NFS にロギングする場合（ESXi サーバーのみ）、ファイアウォールが、フェイルオーバー後にプライマリに昇格したセカンダリ Panorama ピアに、新しく生成されたログのみを送信できるようにします。

© 2019 Palo Alto Networks, Inc.

ログ オプション	関連	説明
ローカル ディスクへのアクティブ プライマリ ログのみ デフォルト：無効	仮想ディスクにロギングしていて HA 構成でデプロイされている、レガシー モードの Panorama バーチャル アプライアンス。	プライマリ Panorama ピアのみがローカル ディスクにログを保存するように設定できます。
プライマリへの変換時に新規ログのみを取得 デフォルト：無効	ネットワーク ファイル システム（NFS）データストアにマウントされており、VMware ESXi サーバーで動作し、HA 構成でデプロイされている、レガシー モードの Panorama バーチャル アプライアンス	NFS ロギングを使用すると、Panorama サーバーのペアを高可用性設定にしている場合、プライマリ Panorama ピアのみが NFS データストアをマウントします。そのため、NFS データストアに書き込めるプライマリ Panorama ピアにのみ、ファイアウォールからログを送信できます。 **Get Only New Logs on Convert to Primary**（プライマリへの変換時に新規ログのみを取得）オプションをオンにすると、管理者は、HA フェイルオーバーが発生したときに、管理対象ファイアウォールが新しく生成されたログのみを Panorama に送信するように設定できます。このイベントは、アクティブ-セカンダリ Panorama がプライマリに昇格して、NFS へのロギングを開始できるようになると、トリガーされます。この動作を有効にするのは、通常、Panorama への接続が復元されるまで長時間かかったときに、ファイアウォールが大量のバッファ済みログを送信しないようにするためです。

© 2019 Palo Alto Networks, Inc.

Panorama から外部の宛先へのログ転送を設定

Panorama では、Syslog、電子メール、SNMP トラップ、HTTP ベースのサービスなど、外部サービスにログを転送できます。外部サービスを使用すると、重要なイベントに関するアラートの受信、専用の長期的なストレージを持つシステムへのモニターされた情報のアーカイブ、サードパーティのセキュリティ モニタリング ツールとの統合が可能になります。ファイアウォール ログの転送に加えて、Panorama 管理サーバーおよびログ コレクタが生成するログを転送できます。ログを転送する Panorama 管理サーバーまたはログ コレクタは、宛先に応じた形式 (Syslog メッセージ、電子メール通知、SNMP トラップ、または HTTP ペイロード) にログを変換します。



Panorama 管理サーバーがレガシー モードの *Panorama* バーチャル アプライアンスの場合、ログ コレクタを使用せずにログを変換して外部サービスに転送します。

ファイアウォールから外部サービスに直接ログを転送することもできます。「ログ転送オプション」を参照してください。

Panorama 5.1 以前のバージョンを実行している *Panorama* バーチャル アプライアンス上で、CLI から Secure Copy (SCP) コマンドを使用して、ログ データベース全体を *SCP* サーバーにエクスポートし、さらに別の *Panorama* バーチャル アプライアンスにインポートできます。ログ データベースのサイズが実際にエクスポートまたはインポートするには大きすぎるため、*Panorama 6.0* 以降のバージョンを実行している *Panorama* バーチャル アプライアンス、およびあらゆるバージョンの *M-Series* アプライアンスはこれらのオプションをサポートしていません。

ログを外部サービスに転送するには、最初にログを Panorama に転送するようにファイアウォールを設定します。次に、Panorama およびログ コレクタがサービスに接続する方法を定義するサーバー プロファイルを設定する必要があります。最後に、サーバー プロファイルを Panorama のログ設定とコレクタ グループに割り当てます。

STEP 1 | ファイアウォールが Panorama にログを転送するよう設定します。

Panorama へのログ転送の設定。

STEP 2 | ログ情報を受信する外部サービスごとにサーバー プロファイルを設定します。

1. **Panorama** > **Server Profiles** (Panorama > サーバープロファイル)を選択し、ログデータを受信するサーバーのタイプを選択します。**SNMP Trap (SNMPトラップ)**、**Syslog**、**Email** (電子メール アドレス) 、または **HTTP** です。
2. サーバー プロファイルを設定します。
   - SNMP トラップ サーバー プロファイルを設定します。SNMP がどのように Panorama およびログ コレクタと連携するのか、詳細は「SNMP サポート」を参照してください。
   - Syslog サーバー プロファイルを設定します。Syslogサーバーでクライアント認証が必要な場合、**Panorama** > **Certificate Management** > **Certificates** (Panorama > 証明書管理 > 証明書)ページを使用し、SSLを介してセキュアなsyslog通信を行うための証明書を作成します。
   - 電子メールサーバーのプロファイルを設定します。
   - HTTP サーバー プロファイルを設定します。

STEP 3 | 次の項目の宛先を設定します。

- Panorama 管理サーバーおよびログ コレクタが生成するログ。
- レガシー モードの Panorama バーチャル アプライアンスが収集するファイアウォール ログ。

1. **[Panorama]** > [ログ設定] > [設定] の順に選択します。
2. ログ タイプごとに 1 つ以上の一致リスト プロファイルを **Add** (追加) します。

© 2019 Palo Alto Networks, Inc.

プロファイルにより、ログ クエリ フィルター、転送先、タギングなどの自動アクションが指定されます。各一致リスト プロファイルについて、以下の手順を実行します。

1. プロファイルを識別する **Name**（名前）を入力します。
2. **Log Type**（ログ タイプ）を選択します。
3. **Filter**（フィルター）ドロップダウンから **Filter Builder**（フィルター ビルダー）を選択します。以下を指定してから、各クエリを **Add**（追加）します。

   Connector（条件式）のロジック（and/or）

   ログの **Attribute**（属性）

   包含または除外ロジックを定義する **Operator**（演算子）

   クエリを一致させるための属性の **Value**（値）
4. 各外部サービスについて設定したサービス プロファイルを **Add**（追加）します。
5. **OK** をクリックしてプロファイルを保存します。

STEP 4 | ログ コレクタが受信するファイアウォール ログの宛先を設定します。



各コレクタ グループはログを異なる宛先に転送することができます。ログ コレクタが *Panorama* 管理サーバーの高可用性（*HA*）ペアのローカルにある場合、各 *HA* ピアにログインし、そのコレクタ グループのログ転送を設定する必要があります。

1. **Panorama** > **Collector Groups**（コレクタ グループ）を選択し、ファイアウォール ログを受信するコレクタ グループを編集します。
2. （任意、SNMP トラップ転送のみ）**Monitoring**（監視）を選択して SNMP 設定を行います。
3. 必要に応じて**Collector Log Forwarding**（コレクタ ログ転送）を選択し、設定された一致リストプロファイルを **Add**（追加）します。
4. **OK** をクリックして、コレクタ グループに対する変更を保存します。

STEP 5 | （Syslog 転送のみ）Syslog サーバーでクライアント認証が必要であり、ファイアウォールが専用ログ コレクタにファイアウォール ログを転送する場合、SSL を介してセキュアな Syslog 通信を行うために使用する証明書を割り当てます。

各専用ログ コレクタごとに以下の手順を実行します。

1. **Panorama** > **Managed Collectors**(Panorama > 管理対象コレクタ) の順に選択し、ログ コレクタを編集します。
2. **Certificate for Secure Syslog**（保護された **Syslog** の証明書）を選択し、**OK** をクリックします。

STEP 6 | （SNMP トラップ転送のみ）SNMP マネージャを有効化して Traps を解釈します。

サポートされた MIB をロードし、必要に応じてコンパイルします。具体的な手順は、SNMP マネージャのドキュメントを参照してください。

STEP 7 | 設定変更をコミットし、確認します。

1. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択し、Panorama に対する変更をコミットして、変更をデバイス グループ、テンプレート、コレクタ グループにプッシュします。
2. 外部サービスがログ情報を受信していることを確認します。
   - 電子メール サーバー — 指定した受信者がログを電子メール通知として受信していることを確認します。
   - **Syslog** サーバー — Syslog サーバーが Syslog メッセージとしてログを受信していることを確認するには、Syslog サーバーのドキュメントを参照してください。

© 2019 Palo Alto Networks, Inc.

- **SNMP** マネージャ – SNMP トラップ サーバーが SNMP トラップとしてログを受信していることを確認するには、SNMP トラップのドキュメントを参照してください。
- **HTTP** サーバー – HTTP ベースのサーバーが適切なペイロード形式でログを受信していることを確認します。

© 2019 Palo Alto Networks, Inc.

ログ収集のデプロイメント

以下のトピックでは、最も一般的なデプロイ環境でログ収集を設定する方法について説明します。作業を始める前に、現在と将来のロギングの必要性に応じて、「Panorama のデプロイ計画」を行います。

以下のトピックのデプロイ環境は、すべて高可用性（*HA*）設定の *Panorama* を表しています。*HA*では設定バックアップの一部として保存されていないコンポーネントを自動で復元できる（サーバーの障害時など）ため、*Palo Alto Networks*は*HA*を推奨しています。*HA* デプロイ環境の場合、*Panorama* 管理サーバーでは、アクティブ/パッシブ設定のみがサポートされます。

- 専用のログ コレクタを使用する Panorama のデプロイ
- ローカル ログ コレクタを使用する Panorama M-Series アプライアンスのデプロイ
- ローカル ログ コレクタを使用する Panorama バーチャル アプライアンスのデプロイ
- ローカル ログ収集を使用するレガシー モードの Panorama バーチャル アプライアンスのデプロイ

専用のログ コレクタを使用する Panorama のデプロイ

以下の図は、分散ログ収集デプロイ環境における Panorama を示しています。これらの例では、Panorama 管理サーバは、アクティブ/パッシブ高可用性（HA）設定で展開された Panorama モードの 2 つの M-Series または Panorama バーチャル アプライアンスで構成されています。ファイアウォールは専用のログ コレクタ（ログ コレクタ モードの M-Series　またはバーチャル アプライアンス）にログを送信します。これは、ファイアウォールが 10,000 ログ/秒を超えるログを生成する場合に推奨される設定です

コレクタ グループに複数のログ コレクタを割り当てる場合は、「複数のログ コレクタを含むコレクタ グループに関する注意事項」を参照し、要件、リスク、および推奨される軽減策を理解してください。

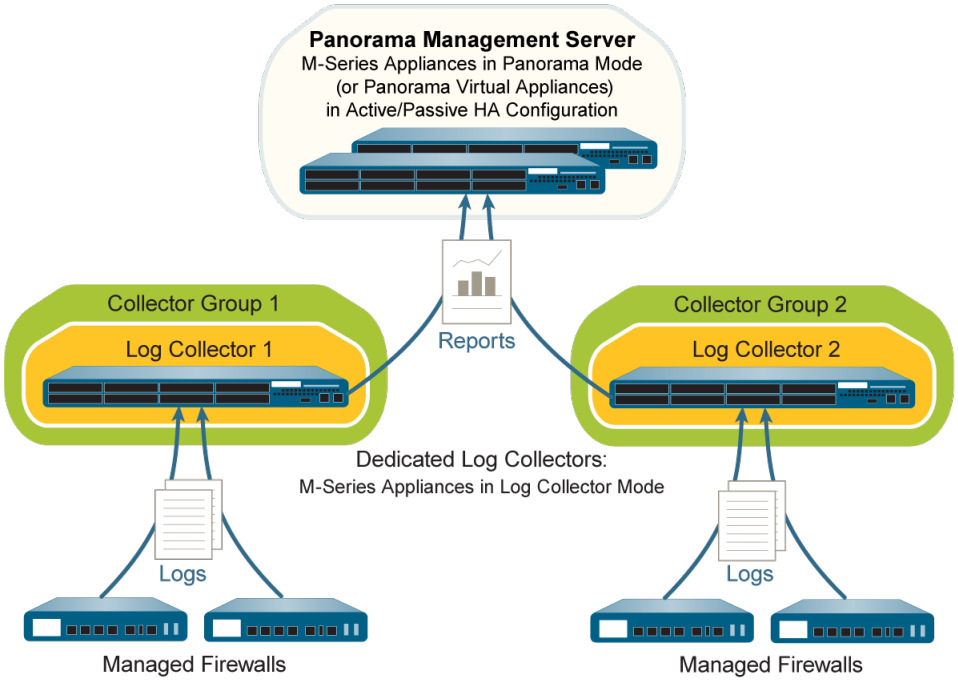


図 17 : コレクタ グループごとに 1 つの専用のログ コレクタ

© 2019 Palo Alto Networks, Inc.

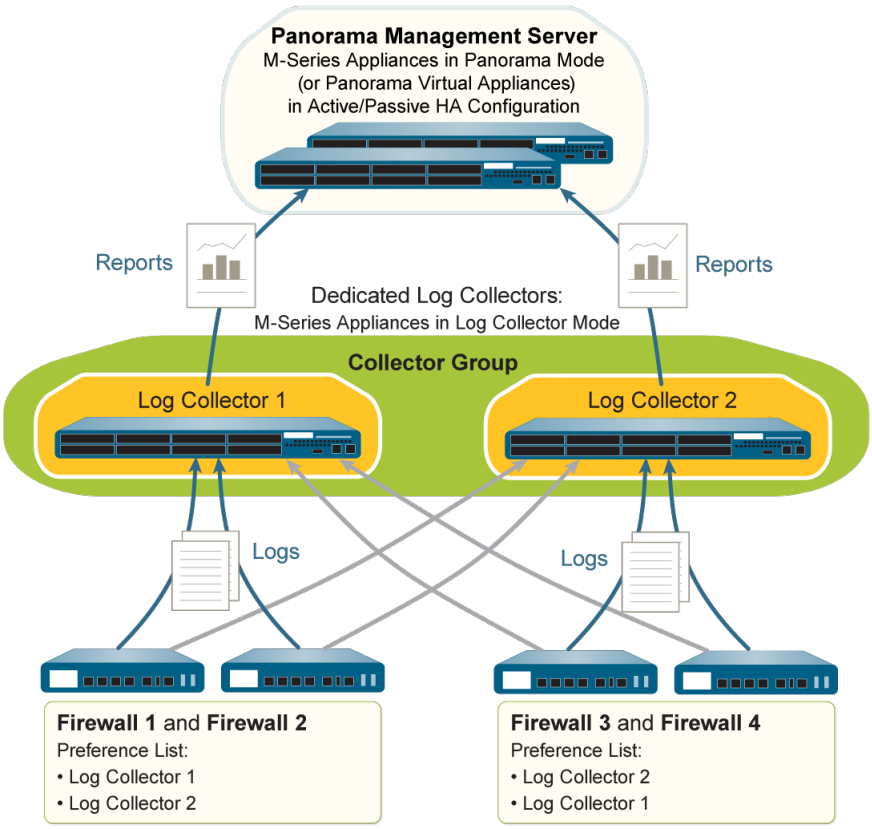


図 **18 :** コレクタ グループごとに複数の専用のログ コレクタ

専用のログ コレクタを使用する Panorama をデプロイするには、以下の手順を実行します。すでに実行したステップ (初期セットアップなど) は省略してください。

STEP 1 | Panorama 管理サーバー (バーチャル アプライアンスあるいは M-Series アプライアンス) および専用のログ コレクタの初期セットアップを実行します。

各 M-Series アプライアンスについて、以下の手順を実行します。

1. M-Series アプライアンスをラック マウントします。方法については、『M-Series のハードウェア リファレンス ガイド』を参照してください。
2. M-Series アプライアンスの初期設定を行います。

   Palo Alto Networks は、管理 (*MGT*) インターフェイスを *Panorama* への管理アクセス用に予約し、別の M-Series アプライアンス インターフェイスを他の *Panorama* サービス専用として使用することをお勧めします。
3. 各アレイを設定します。RAID ディスクを口ギングに使用できるようにするには、この作業が必要になります。必要に応じて、ディスクを追加して、M-Series アプライアンスのストレージの拡張を行えます。
4. Panorama の登録とライセンスのインストールを行います。
5. Panorama のコンテンツ更新とソフトウェア更新のインストールを行います。

各バーチャル アプライアンス (存在する場合) について、以下の手順を実行します。

1. Panorama バーチャル アプライアンスのインストールを行います。
2. Panorama バーチャル アプライアンスの初期設定の実行を行います。
3. Panorama の登録とライセンスのインストールを行います。
4. Panorama のコンテンツ更新とソフトウェア更新のインストールを行います。

© 2019 Palo Alto Networks, Inc.

Panorama 管理サーバー（バーチャル アプライアンスあるいは M-Series アプライアンス）の場合、Panorama での HA のセットアップも行う必要があります。

STEP 2 | 専用ログ コレクタになる各 Panorama 管理サーバー上で Panorama モードをログ コレクタ モードに切り替えます。

M-Series またはバーチャル アプライアンスのモードを変更すると、管理アクセス設定を除くすべての設定と既存のログ データが削除されます。モードを切り替えると、*M-Series* またはバーチャル アプライアンスは *CLI* にはアクセスできますが、*Web* インターフェイスにアクセスできなくなります。

1. 以下のいずれかの方法で Panorama に接続します。
   - （M-Series アプライアンスのみ）お使いのマシンから M-Series アプライアンスのコンソール ポートにシリアル ケーブルを接続します。次に、ターミナル エミュレーション ソフトウェア（9600-8-N-1）を使って接続を行います。
   - 初期設定時に Panorama 管理サーバの MGT インターフェイスとして指定した IP アドレスの SSH セッションを開くには、PuTTY などの端末エミュレーション ソフトウェアを使用します。
2. 指示に従って CLI にログインします。初期設定時に指定したパスワードとデフォルトの admin アカウントを使用します。
3. 次のコマンドを入力して、ログ コレクタ モードに切り替えます。

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

4. **y**を入力して、モード変更を確定します。Panorama 管理サーバーが再起動します。再起動処理によりターミナル エミュレーション ソフトウェアのセッションが終了した場合は、Panorama に再接続して、Panorama のログイン画面を表示します。

   CMS Login *(CMS*ログイン*)*画面が表示された場合は、ログコレクタが再起動をまだ完了させていないということです。入力を指示されたら、ユーザー名やパスワードは入力せずに *Enter* キーを押します。

5. CLI に再度ログインします。
6. ログ コレクタ モードへの切り替えが正しく完了したことを、次のコマンドで確認します。

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

モード変更が正しく完了した場合、出力は次のようになります。

```
system-mode: logger
```

STEP 3 | 各ログ コレクタおよび Panorama 管理サーバー間の接続を有効にします。

このステップを事前に行わなければ、ログ コレクタのロギング用ディスクを有効にすることができません。

ログコレクタのCLIで次のコマンド（適宜、*<IPaddress1>*は単独（非HA）あるいはアクティブ（HA）PanoramaのMGTインターフェイスのもの、*<IPaddress2>*はパッシブ（HA）PanoramaのMGTインターフェイスのもの）を入力します。

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


© 2019 Palo Alto Networks, Inc.

```
# exit
```

STEP 4 | 各ログ コレクタのシリアル番号を控えておきます。

Panorama 管理サーバーでログ コレクタを管理対象のコレクタとして追加する際、このシリアル番号が必要になります。

1. 各ログ コレクタの CLI で以下のコマンドを入力し、シリアル番号を表示します。

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

2. シリアル番号を控えておきます。

STEP 5 | 各ログ コレクタを管理対象コレクタとして追加します。

プライマリ Panorama 管理サーバー ピアの Web インターフェイスを使用して、管理対象コレクタの設定を行います。

1. **Panorama** > **Managed Collectors**(Panorama > 管理対象コレクタ) の順に選択し、管理対象コレクタを**Add** (追加)します。
2. すでに控えてあるログ コレクタのシリアル番号 (**Collector S/N** (コレクタ シリアル番号)) を**General** (全般) タブで入力します。
3. アクティブおよびパッシブ Panorama HA ピアの IP アドレスおよび FQDN を **Panorama Server IP** (**Panorama** サーバー **IP**) フィールドおよび **Panorama Server IP 2** (**Panorama** サーバー **IP 2**) フィールドにそれぞれ入力します。これらのフィールドは必須です。
4. **Interfaces** (インターフェイス) を選択し、**Management** (管理) をクリックした後、ネットワークの IP プロトコルに応じて MGT インターフェイス用に次のフィールドのセットのうちいずれか、あるいは両方の設定を行います。
   - IPv4 — **IP Address** (**IP** アドレス)、**Netmask** (ネットマスク)、および **Default Gateway** (デフォルト ゲートウェイ)
   - IPv6 — **IPv6 Address/Prefix Length** (**IPv6** アドレス/プレフィックス長) および **Default IPv6 Gateway** (デフォルト **IPv6** ゲートウェイ)
5. (任意) SNMP マネージャを使用してログ コレクタの統計を監視する場合は、**SNMP** を選択します。

   SNMP を使用するには、ログ コレクタを設定する以外に、追加のステップが必要です (「SNMP を使用して Panorama およびログ コレクタの統計を監視」を参照)。
6. **OK** をクリックして変更内容を保存します。
7. **Commit** (コミット) > **Commit to Panorama** (**Panorama** へのコミット) の順に選択し、変更を **Commit** (コミット) します。

   このステップを事前に行わなければ、ログ コレクタのロギング用ディスクを有効にすることができません。
8. **Panorama** > **Managed Collectors**Panorama > 管理対象コレクタ) ページで、追加したログ コレクタが表示されていることを確認します。Connected (接続済み) 列には、ログ コレクタが Panorama に接続されていることを示すチェック マークが表示されます。更新された接続ステータスがページに表示されるまで、数分かかる場合があります。

   この時点では、*Configuration Status* (設定ステータス) 列には *Out of Sync* (非同期)、*Run Time Status* (ランタイム ステータス) 列には *disconnected* (未接続) が表示されます。コレクタ グループを設定すると、このステータスは *In Sync* (同期) および *connected* (接続済み) に変わります (ステップ 9)。

STEP 6 | 各ログ コレクタのロギング用ディスクを有効にします。

© 2019 Palo Alto Networks, Inc.

プライマリ Panorama 管理サーバー ピアの Web インターフェイスを使用して、以下の手順を実行します。

1. **Panorama** > **Managed Collectors**(Panorama > 管理対象コレクタ) の順に選択し、ログ コレクタを編集します。
2. **Disks**（ディスク）を選択し、各ディスク ペアを **Add**（追加）して **OK** をクリックします。
3. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

STEP 7 | （推奨）ログ コレクタが **Device Log Collection**（デバイス ログ収集）（ファイアウォールからログを受信）および **Collector Group Communication**（コレクタ グループ通信）で **Ethernet1**、**Ethernet2**、**Ethernet3**、**Ethernet4**、および **Ethernet5** の各インターフェイスを使用する場合は、これらのインターフェイスを設定します。

デフォルトでは、ログ コレクタは、MGT インターフェイスを使用して、ログ収集とコレクタ グループ通信を行います。これらの機能に別のインターフェイスを割り当てると、MGT インターフェイスを管理トラフィック用に予約できます。ログ トラフィックが大量に発生する環境の場合は、10Gbps のインターフェイス（**Ethernet4** と **Ethernet5**）を M-500 アプライアンスで使用して、ログ収集とコレクタ グループ通信を行うことを検討してください。トラフィックのロギングの負荷を複数のインターフェイスで分散するには、それらのインターフェイスで **Device Log Collection**（デバイス ログ収集）を有効にします。

プライマリ Panorama 管理サーバー ピアの Web インターフェイスを使用して、各ログ コレクタに対して以下の手順を実行します。

1. **Panorama** > **Managed Collectors**（管理対象コレクタ）の順に選択し、ログ コレクタを編集して、**Interfaces**（インターフェイス）を選択します。
2. インターフェイスごとに以下のステップを実行します。
   1. インターフェイスの名前をクリックして、インターフェイスを編集します。
   2. **<interface-name>** を選択してインターフェイスを有効化します。
   3. ネットワークの IP プロトコルに合わせて、以下のいずれか、あるいは両方のフィールドを入力します。

      IPv4 — **IP Address**（**IP** アドレス）、**Netmask**（ネットマスク）、および **Default Gateway**（デフォルト ゲートウェイ）

      IPv6 — **IPv6 Address/Prefix Length**（**IPv6** アドレス/プレフィックス長）および **Default IPv6 Gateway**（デフォルト **IPv6** ゲートウェイ）
   4. インターフェイスでサポートされるデバイス管理サービスを選択します。

      Device Log Collection（デバイス ログ収集）— インターフェイスを 1 つ以上割り当てることができます。

      Collector Group Communication（コレクタ グループ通信）— インターフェイスを 1 つのみ割り当てることができます。
   5. **OK** をクリックして、インターフェイスに対する変更を保存します。
3. **OK** をクリックして、ログ コレクタに対する変更を保存します。
4. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、Panorama 設定に対して、変更内容を **Commit**（コミット）します。

STEP 8 | 管理対象デバイスとしてのファイアウォールの追加を行います。

プライマリ Panorama 管理サーバー ピアの Web インターフェイスを使用して、ログ コレクタにログを転送するファイアウォールごとに、このタスクを実行します。

STEP 9 | コレクタ グループを設定します。

© 2019 Palo Alto Networks, Inc.

各コレクタ グループに 1 つのログ コレクタを持たせる場合、コレクタ グループごとにこのステップを繰り返してから次に進みます。

すべてのログ コレクタを 1 つのコレクタ グループに割り当てる場合は、このステップを一度だけ実施します。

プライマリ Panorama 管理サーバー ピアの Web インターフェイスを使用して、コレクタ グループの設定を行います。

1. **Panorama** > **Collector Groups**(Panorama > コレクタ グループ) の順に選択し、コレクタ グループを**Add**(追加)します。
2. コレクタ グループを識別するための **Name**（名前）を入力します。
3. Collector Group Members（コレクタ グループ メンバー）リストに 1 つ以上のログ コレクタを **Add**（追加）します。

   単一のコレクタ グループでは、すべてのログ コレクタ、すべての *M-600* アプライアンス、すべての *M-500* アプライアンス、すべての *M-200* アプライアンス、すべての *Panorama* バーチャル アプライアンスは同じ *Panorama* モデルで動作する必要があります。
4. （推奨設定）1 つのコレクタ グループに複数のログ コレクタを追加する場合は、**Enable log redundancy across collectors**（コレクタ間のログ冗長性の有効化）を選択します。このオプションでは、各ログ コレクタのロギング用ディスクの数が同じでなければなりません。
5. （任意）ログ コレクタの統計情報および Traps の監視に SNMP を使用する場合は、**Monitoring**（監視）を選択して設定を行います。
6. **Device Log Forwarding**（デバイス ログ転送）を選択し、Log Forwarding Preferences（ログ転送設定）リストを設定します。このリストでは、どのファイアウォールがどのログ コレクタにログを転送するかが定義されています。このコレクタ グループのログ コレクタ数に基づいてファイアウォールを割り当てます。
   - 単一 – 「コレクタ グループごとに 1 つの専用のログ コレクタ」のように、ログ コレクタにログを転送するファイアウォールを割り当てます。
   - 複数 – 各ファイアウォールを両方のログ コレクタに割り当てて冗長性を確保します。この設定を行う場合、「コレクタ グループごとに複数の専用のログ コレクタ」のように、半分のファイアウォールでログ コレクタ 1 を最優先にし、もう半分のファイアウォールでログ コレクタ 2 を最優先にします。
7. **OK** をクリックして、コレクタ グループに対する変更を保存します。
8. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択してから、Panorama および追加したコレクタ グループに対して、変更内容を **Commit and Push**（コミットしてプッシュ）します。
9. **Panorama** > **Managed Collectors** (Panorama > 管理対象コレクタ)を選択し、ログコレクタの構成がPanoramaと同期していることを確認します。

   Configuration Status（設定ステータス）列には In Sync（同期）、Run Time Status（ランタイム ステータス）列には connected（接続済み）が表示されている必要があります。

STEP 10 | ファイアウォールから Panorama へのログ転送を設定します。

プライマリ Panorama 管理サーバー ピアの Web インターフェイスを使用して、以下を行います。

1. Panorama へのログ転送の設定
2. Panorama へのログ転送の確認
3. （任意）Panorama から外部の宛先へのログ転送を設定します。

© 2019 Palo Alto Networks, Inc.

ローカル ログ コレクタを使用する Panorama M-Series アプライアンスのデプロイ

以下の図は、一元的なログ収集デプロイ環境の Panorama を示しています。これらの例では、Panorama 管理サーバーは、アクティブ/パッシブ高可用性（HA）設定でデプロイされた 2 つの Panorama モードの M-Series アプライアンスで構成されています。ファイアウォールは、各 Panorama M-Series アプライアンスの事前設定された（デフォルト）ローカル ログ コレクタにログを送信します。これは、ファイアウォールが最大 10,000 ログ/秒でログを生成する場合に推奨されるデプロイ方法です。

コレクタ グループに複数のログ コレクタを割り当てる場合は、「複数のログ コレクタを含むコレクタ グループに関する注意事項」を参照し、要件、リスク、および推奨される軽減策を理解してください。

この導入環境を実装した後で、ロギング レートが増加して *10,000* ログ/秒を超えるようになった場合は、「専用のログ コレクタを使用する Panorama のデプロイ」の説明に従って、専用のログ コレクタ（ログ コレクタ モードの *M-Series* アプライアンス）を追加することをお勧めします。このような拡張を行う場合、必要に応じてローカル ログ コレクタから専用のログ コレクタにファイアウォールを再割り当てします。

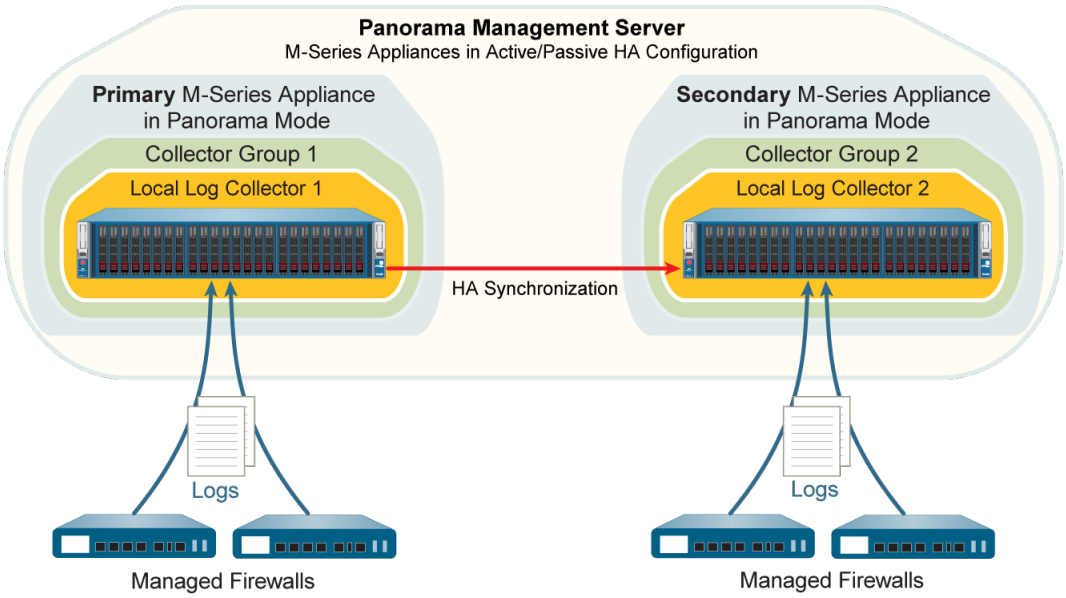


図 **19 :** コレクタ グループごとに **1** つのローカル ログ コレクタ

© 2019 Palo Alto Networks, Inc.

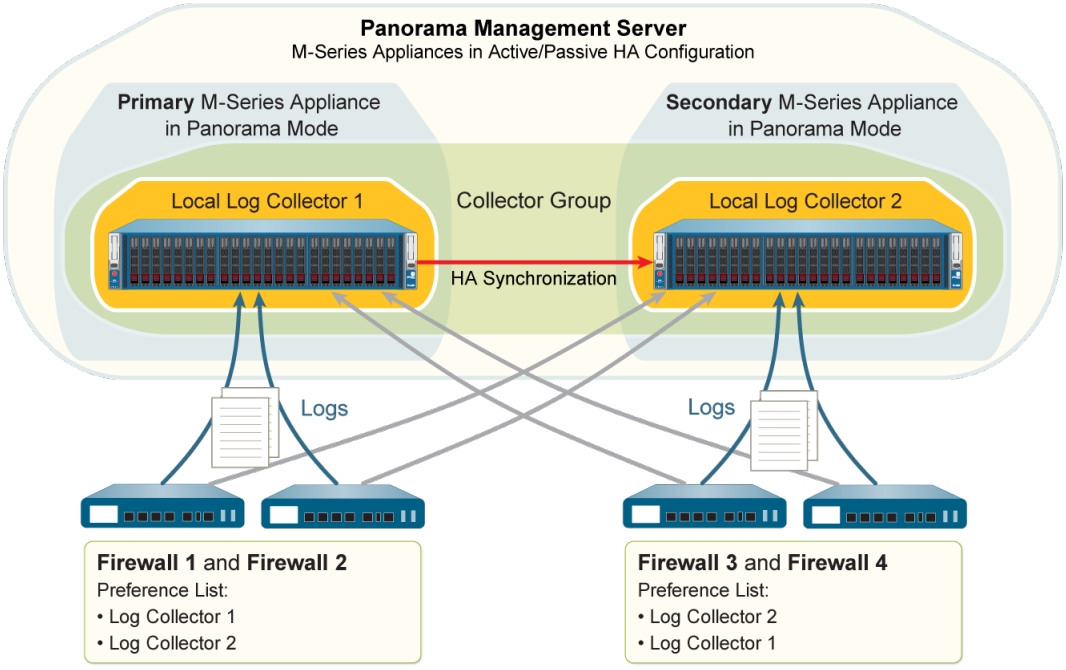


図 **20 :** コレクタ グループごとに複数のローカル ログ コレクタ

ローカル ログ コレクタを使用する Panorama をデプロイするには、以下のステップを実行します。すでに実行したステップ (初期セットアップなど) は省略してください。

STEP 1 | 各 M-Series アプライアンスの初期セットアップを実行します。

1. M-Series アプライアンスをラック マウントします。方法については、『M-Series のハードウェア リファレンス ガイド』を参照してください。
2. M-Series アプライアンスの初期設定を行います。

   Palo Alto Networks は、管理 (*MGT*) インターフェイスを *Panorama* への管理アクセス用に予約し、別の M-Series アプライアンス インターフェイスを他の *Panorama* サービス専用として使用することをお勧めします。
3. 各アレイを設定します。RAID ディスクを口ギングに使用できるようにするには、この作業が必要になります。必要に応じて、ディスクを追加して、M-Series アプライアンスのストレージの拡張を行えます。
4. Panorama の登録とライセンスのインストールを行います。
5. Panorama のコンテンツ更新とソフトウェア更新のインストールを行います。
6. Panorama での HA のセットアップを行います。

STEP 2 | 次の作業を行って Panorama のログ収集を準備します。

1. 以下のいずれかの方法でプライマリ Panorama に接続します。
   - お使いのパソコンからプライマリ Panorama のコンソール ポートにシリアル ケーブルを接続します。次に、ターミナル エミュレーション ソフトウェア (9600-8-N-1) を使って接続を行います。
   - 初期設定時にプライマリ Panorama の MGT インターフェイス用に指定した IP アドレスに対して SSH セッションを開くには、PuTTY などの端末エミュレーション ソフトウェアを使用します。
2. 指示に従って CLI にログインします。初期設定時に指定したパスワードとデフォルトの admin アカウントを使用します。
3. 以下のコマンド (*<IPaddress2>*はセカンダリ Panorama のMGTインターフェイス) を入力し、プライマリ Panorama がセカンダリ Panoramaに接続できるようにします。

© 2019 Palo Alto Networks, Inc.

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

4. セカンダリ Panorama の CLI にログインします。
5. 以下のコマンド（*<IPaddress1>*はプライマリ Panorama のMGTインターフェイス）を入力し、セカンダリ Panorama がプライマリ Panoramaに接続できるようにします。

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

6. セカンダリ Panorama の CLI で以下のコマンドを入力し、シリアル番号を表示してそれを控えておきます。

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

セカンダリ Panorama のログ コレクタを管理対象のコレクタとしてプライマリ Panorama に追加する際、このシリアル番号が必要になります。

STEP 3 | プライマリ Panorama のローカル ログ コレクタを編集します。

以下のステップではプライマリ Panorama の Web インターフェイスを使用します。

1. **[Panorama]** > [管理対象コレクタ] の順に選択し、defaultログ コレクタを選択します。
2. **Disks**（ディスク）を選択し、各ロギング用ディスク ペアを **Add**（追加）します。
3. **OK** をクリックして変更内容を保存します。

STEP 4 | セカンダリ Panorama のローカル ログ コレクタを設定します。



このログ コレクタはプライマリ *Panorama* のローカルにはないため、*Panorama* はこれをリモートとして扱います。そのため、これはプライマリ *Panorama* に手動で追加する必要があります。

プライマリ Panorama の Web インターフェイスを使用して、管理対象コレクタの設定を行います。

1. **Panorama** > **Managed Collectors**(Panorama > 管理対象コレクタ) の順に選択し、ログ コレクタを**Add**(追加)します。
2. セカンダリ Panorama のログ コレクタ用に控えておいたシリアル番号（**Collector S/N**（コレクタ シリアル番号））を入力します。
3. プライマリおよびセカンダリ Panorama HA ピアの IP アドレスおよび FQDN を **Panorama Server IP**（**Panorama** サーバー**IP**）フィールドおよび **Panorama Server IP 2**（**Panorama Server IP 2**）フィールドにそれぞれ入力します。

   これらのフィールドは両方とも必須です。
4. **Interfaces**（インターフェイス）を選択し、ログ コレクタが使用する各インターフェイスを設定します。**Management**（管理）インターフェイスは必須です。インターフェイスごとに以下のステップを実行します。
   1. インターフェイス名をクリックします。
   2. ネットワークの IP プロトコルに基づいて、以下のいずれか、あるいは両方のフィールドを設定します。

© 2019 Palo Alto Networks, Inc.

IPv4 — **IP Address**（**IP** アドレス）、**Netmask**（ネットマスク）、および **Default Gateway**（デフォルト ゲートウェイ）

IPv6 — **IPv6 Address/Prefix Length**（**IPv6** アドレス/プレフィックス長）および **Default IPv6 Gateway**（デフォルト **IPv6** ゲートウェイ）

3. （管理インターフェイスのみ）SNMP マネージャを使用してログ コレクタの統計を監視する場合は、**SNMP** を選択します。

   SNMP を使用するには、ログ コレクタを設定する以外に、追加のステップが必要です（「SNMP を使用して Panorama およびログ コレクタの統計を監視」を参照）。
4. **OK** をクリックして、インターフェイスに対する変更を保存します。
5. **OK** をクリックして、ログ コレクタに対する変更を保存します。
6. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

   このステップを事前に行わなければ、ロギング用ディスクを有効にすることができません。
7. ログ コレクタの名前をクリックして、ログ コレクタを編集します。
8. **Disks**（ディスク）を選択し、各 RAID ディスク ペアを **Add**（追加）して **OK** をクリックします。
9. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

STEP 5 | 管理対象デバイスとしてのファイアウォールの追加を行います。

プライマリ Panorama の Web インターフェイスを使用して、ログ コレクタにログを転送するファイアウォールごとに、このタスクを実行します。

STEP 6 | プライマリ Panorama で定義済みのデフォルトのコレクタ グループを編集します。

プライマリ Panorama の Web インターフェイスを使用して、コレクタ グループの設定を行います。

1. **Panorama** > **Collector Groups**（コレクタ グループ）の順に選択し、**default**（デフォルト）のコレクタ グループを編集します。
2. 1 つのコレクタ グループに複数のログ コレクタを追加する場合は、セカンダリ Panorama のローカル ログ コレクタを Collector Group Members（コレクタ グループ メンバー）リストに **Add**（追加）します。デフォルトでは、プライマリ Panorama のローカル ログ コレクタがデフォルトのコレクタ グループに事前に割り当てられているため、リストには、このログ コレクタが表示されます。

   単一のコレクタ グループでは、すべてのログ コレクタ、すべての *M-600* アプライアンス、すべての *M-500* アプライアンス、すべての *M-200* アプライアンス、すべての *Panorama* バーチャル アプライアンスは同じ *Panorama* モデルで動作する必要があります。
3. （推奨設定）1 つのコレクタ グループに複数のログ コレクタを追加する場合は、**Enable log redundancy across collectors**（コレクタ間のログ冗長性の有効化）を選択します。このオプションでは、各ログ コレクタのロギング用ディスクの数が同じでなければなりません。
4. （任意）ログ コレクタの統計情報および Traps の監視に SNMP を使用する場合は、**Monitoring**（監視）を選択して設定を行います。
5. **Device Log Forwarding**（デバイス ログ転送）を選択し、Log Forwarding Preferences（ログ転送設定）リストを設定します。このリストでは、どのファイアウォールがどのログ コレクタにログを転送するかが定義されています。このコレクタ グループのログ コレクタ数に基づいてファイアウォールを割り当てます。
   - 単一 — 「コレクタ グループごとに 1 つのローカル ログ コレクタ」のように、プライマリ Panorama のローカル ログ コレクタに、ログを転送するファイアウォールを割り当てます。
   - 複数 — 各ファイアウォールを両方のログ コレクタに割り当てて冗長性を確保します。この設定を行う場合、「コレクタ グループごとに複数のローカル ログ コレクタ」のように、半分のファ

© 2019 Palo Alto Networks, Inc.

イアウォールでログ コレクタ 1 を最優先にし、もう半分のファイアウォールでログ コレクタ 2 を最優先にします。

6. **OK** をクリックして変更内容を保存します。

STEP 7 | セカンダリ Panorama のログ コレクタを含むコレクタ グループを設定します。

これは各コレクタ グループにログ コレクタが 1 つしかない場合に必須になります。

プライマリ Panorama の Web インターフェイスを使用して、コレクタ グループの設定を行います。

1. **Panorama** > **Collector Groups**(Panorama > コレクタ グループ) の順に選択し、コレクタ グループを**Add**(追加)します。
2. コレクタ グループを識別するための **Name**（名前）を入力します。
3. セカンダリ Panorama のローカル ログ コレクタを Collector Group Members（コレクタ グループ メンバー）リストに **Add**（追加）します。
4. （任意）ログ コレクタの統計情報および Traps の監視に SNMP マネージャを使用する場合は、**Monitoring**（監視）を選択して設定を行います。
5. **Device Log Forwarding**（デバイス ログ転送）を選択し、Log Forwarding Preferences（ログ転送設定）リストにエントリを **Add**（追加）します。
   1. Devices（デバイス）リストを **Modify**（変更）し、セカンダリ Panorama のローカル ログ コレクタにログを転送するファイアウォールを選択した後（「コレクタ グループごとに 1 つのローカル ログ コレクタ」を参照）、**OK** をクリックします。
   2. セカンダリ Panorama のローカル ログ コレクタを Collector（コレクタ）リストに **Add**（追加）して、**OK** をクリックします。
6. **OK** をクリックして変更内容を保存します。

STEP 8 | Panorama 設定およびコレクタ グループに、変更内容をコミットしてプッシュします。

プライマリ Panorama の Web インターフェイスで、**Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択してから、Panorama および追加したコレクタ グループに、変更内容を **Commit and Push**（コミットしてプッシュ）します。

STEP 9 | セカンダリ Panorama がアクティブになるように手動でフェイル オーバーします。

プライマリ Panorama の Web インターフェイスを使用して、以下の手順を実行します。

1. **[Panorama]** > **[高可用性]** の順に選択します。
2. Operational Commands（操作コマンド）セクションで **Suspend local Panorama**（ローカルの **Panorama** をサスペンド）をクリックします。

STEP 10 | セカンダリ Panorama で、プライマリ Panorama のローカル ログ コレクタのネットワークを設定します。

セカンダリ Panorama の Web インターフェイスを使用して、以下の手順を実行します。

1. Panorama Web インターフェイスで、**Panorama** > **Managed Collectors**（管理対象コレクタ）の順に選択し、プライマリ Panorama のローカル ログ コレクタを選択します。
2. プライマリおよびセカンダリ Panorama HA ピアの IP アドレスおよび FQDN を **Panorama Server IP**（**Panorama** サーバー**IP**）フィールドおよび **Panorama Server IP 2**（**Panorama Server IP 2**）フィールドにそれぞれ入力します。

   これらのフィールドは両方とも必須です。
3. **Interfaces**（インターフェイス）を選択した後、**Management**（管理）をクリックし、プライマリ Panorama の MGT インターフェイスの値を使用して、（ネットワークの IP プロトコルに応じて）以下のいずれかあるいは両方のフィールド セットを入力します。

© 2019 Palo Alto Networks, Inc.

- **IPv4** — **IP Address**（**IP** アドレス）、**Netmask**（ネットマスク）、および **Default Gateway**（デフォルト ゲートウェイ）
- **IPv6** — **IPv6 Address/Prefix Length**（**IPv6** アドレス/プレフィックス長）および **Default IPv6 Gateway**（デフォルト **IPv6** ゲートウェイ）

4. **OK** をクリックして変更内容を保存します。
5. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択してから、Panorama および追加したコレクタ グループに、変更内容を **Commit and Push**（コミットしてプッシュ）します。

STEP 11 | プライマリ Panorama がアクティブになるように手動でフェイルバックします。

セカンダリ Panorama の Web インターフェイスを使用して、以下の手順を実行します。

1. **[Panorama]** > [高可用性] の順に選択します。
2. Operational Commands（操作コマンド）セクションで **Suspend local Panorama**（ローカルの **Panorama** をサスペンド）をクリックします。

STEP 12 | ファイアウォールから Panorama へのログ転送を設定します。

プライマリ Panorama の Web インターフェイスを使用して、以下を行います。

1. Panorama へのログ転送の設定
2. Panorama へのログ転送の確認
3. （任意）Panorama から外部の宛先へのログ転送を設定します。



各 *Panorama HA* ピアに対して個別の外部サーバー プロファイルを割り当てることができます。たとえば、ピアごとに異なる *Syslog* サーバーへログを転送させたいことがあるかもしれません。*Panorama HA*ピアごとに異なる外部サービスへログを転送させる場合、各ピアの*Web*インターフェイスにログインし、*Panorama* > *Collector Groups (Panorama* > コレクタ グループ*)*を選択し、コレクタ グループを選択し、さらに*Collector Log Forwarding (*コレクタ ログ転送*)*を選択してサーバープロファイルを割り当て、*OK*をクリックします。

ローカル ログ コレクタを使用する Panorama バーチャル アプライアンスのデプロイ

Panorama モードの Panorama バーチャル アプライアンスでローカルに実行されるログ コレクタにログを送信するようにファイアウォールを設定できます。高可用性（HA）設定の場合、各 Panorama HA ピアがローカル ログ コレクタを持つことができます。以下の図に示すように、HA ピアのローカル ログ コレクタは、同じコレクタ グループに割り当てることも、個別のコレクタ グループに割り当てることもできます。Panorama バーチャル アプライアンスのセットアップ前提条件を参照して、ローカル ログ コレクタを備えた Panorama バーチャル アプライアンスを VMware 仮想インフラストラクチャに展開する際にサポートされる毎 秒あたりのログを確認してください。



コレクタ グループに複数のログ コレクタを割り当てる場合は、「複数のログ コレクタを含むコレクタ グループに関する注意事項」を参照し、要件、リスク、および推奨される軽減策を理解してください。

© 2019 Palo Alto Networks, Inc.

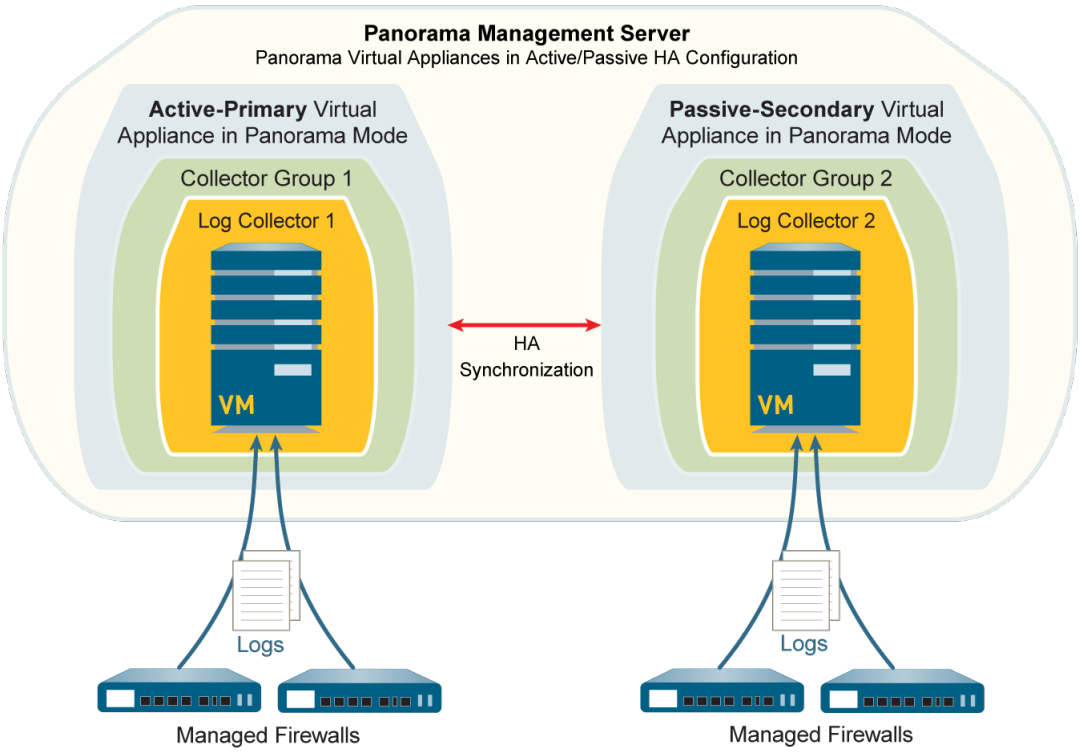


図 21 : コレクタ グループごとに 1 つのログ コレクタ

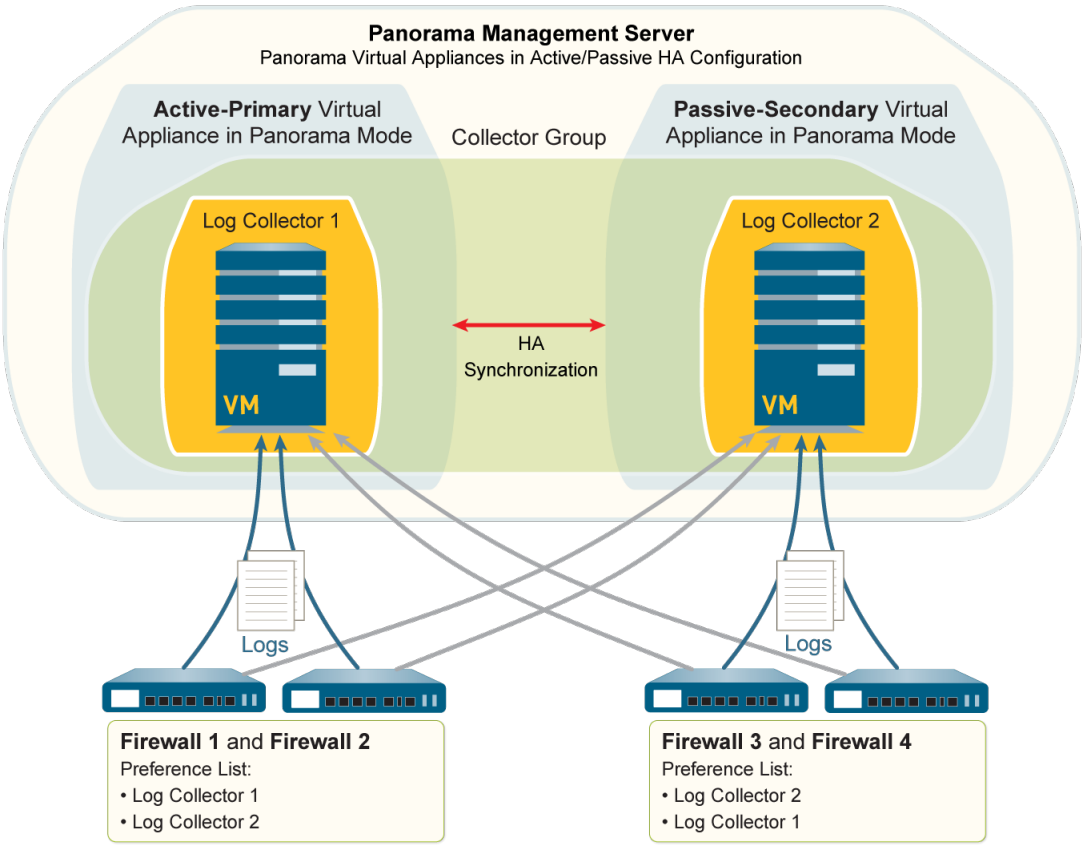


図 22 : コレクタ グループごとに複数のログ コレクタ

© 2019 Palo Alto Networks, Inc.

ローカル ログ コレクタを使用する Panorama をデプロイするには、以下のステップを実行します。すでに実行したステップ（初期セットアップなど）は省略してください。

STEP 1 | 各 Panorama バーチャル アプライアンスの初期セットアップを実行します。

1. Panorama バーチャル アプライアンスのインストールを行います。バーチャル アプライアンスが Panorama モードで起動するように以下のリソースを設定する必要があります。
   - 正確に 81GB のストレージを持つシステム ディスク。
   - Panorama が受信および保存するログの量に対して十分な CPU およびメモリ。
   - 2 – 24TB のストレージを持つ仮想ロギング ディスク。

   Panorama は、新しいディスクを *2TB* のパーティションに自動的に分割します。各パーティションは、個別の仮想ディスクとして機能します。
2. Panorama バーチャル アプライアンスの初期設定の実行を行います。
3. Panorama の登録とライセンスのインストールを行います。
4. Panorama のコンテンツ更新とソフトウェア更新のインストールを行います。

STEP 2 | Panorama バーチャル アプライアンスを HA 設定でセットアップします。

1. Panorama での HA のセットアップを行います。
2. Panorama HA フェイルオーバーのテストを行います。

STEP 3 | プライマリ Panorama のローカル ログ コレクタを追加します。

プライマリ Panorama 上で、以下を行います。

1. Panorama のシリアル番号をメモします。
   1. Panorama Web インターフェイスにアクセスします。
   2. **Dashboard**（ダッシュボード）を選択し、General Information（一般情報）セクションの **Serial #**（シリアル番号）を記録します。
2. ログ コレクタを管理対象コレクタとして追加します。
   1. **Panorama** > **Managed Collectors**（管理対象コレクタ）の順に選択し、新しいログ コレクタを **Add**（追加）します。
   2. Panorama 用に記録したシリアル番号（**Collector S/N**（コレクタ シリアル番号）を **General**（全般）設定に入力します。
   3. **OK** をクリックして変更内容を保存します。
   4. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択します。

      このステップを事前に行わなければ、仮想ロギング ディスクを追加できません。
3. 仮想ロギング ディスクを追加します。
   1. **Panorama** > **Managed Collectors**（管理対象コレクタ）の順に選択し、その名前をクリックしてログ コレクタを編集します。

      ログ コレクタ名の値は、プライマリ Panorama のホスト名と同じです。
   2. **Disks**（ディスク）を選択し、仮想ロギング ディスクを **Add**（追加）します。
   3. **OK** をクリックして変更内容を保存します。
   4. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択します。

STEP 4 | セカンダリ Panorama のローカル ログ コレクタを追加します。

このログ コレクタは、プライマリ *Panorama* でローカルに実行されないため、リモートとして扱われます。

1. セカンダリ Panorama のシリアル番号をメモします。

© 2019 Palo Alto Networks, Inc.

1. セカンダリ Panorama の Web インターフェイスにアクセスします。
2. **Dashboard**（ダッシュボード）を選択し、General Information（一般情報）セクションの **Serial #**（シリアル番号）を記録します。

2. プライマリ Panorama の Web インターフェイスにアクセスします。
3. **Panorama** > **Managed Collectors**(Panorama > 管理対象コレクタ) の順に選択し、ログ コレクタを**Add**(追加)します。
4. セカンダリ Panorama 用に記録したシリアル番号（**Collector S/N**（コレクタ シリアル番号）を **General**（全般）設定に入力します。
5. プライマリおよびセカンダリ Panorama HA ピアの IP アドレスおよび FQDN を **Panorama Server IP**（**Panorama** サーバーIP）フィールドおよび **Panorama Server IP 2**（**Panorama Server IP 2**）フィールドにそれぞれ入力します。

   これらのフィールドは両方とも必須です。
6. **OK** をクリックして、ログ コレクタに対する変更を保存します。
7. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

   このステップを事前に行わなければ、仮想ロギング ディスクを追加できません。
8. ログ コレクタの名前をクリックして、ログ コレクタを編集します。

   ログ コレクタ名の値は、セカンダリ Panorama のホスト名と同じです。
9. **Disks**（ディスク）を選択し、仮想ロギング ディスクを **Add**（追加）して **OK** をクリックします。
10. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

STEP 5 | 管理対象デバイスとしてのファイアウォールの追加を行います。

プライマリ Panorama を使用して、ログ コレクタにログを転送するファイアウォールごとに、このタスクを実行します。

STEP 6 | コレクタ グループを設定します。

両方のログ コレクタを同じコレクタ グループに割り当てる場合は、このステップを 1 回実行します。それ以外の場合は、ログ コレクタごとにコレクタ グループを設定します。

プライマリ Panorama 上で、以下を行います。

1. **Panorama** > **Collector Groups**（コレクタ グループ）の順に選択し、コレクタ グループを **Add**（追加）します。
2. 一方または両方のログ コレクタをコレクタ グループ メンバーとして **Add**（追加）します。

   単一のコレクタ グループでは、すべてのログ コレクタ、すべての *M-600* アプライアンス、すべての *M-500* アプライアンス、すべての *M-200* アプライアンス、すべての *Panorama* バーチャル アプライアンスは同じ *Panorama* モデルで動作する必要があります。
3. （推奨設定）1 つのコレクタ グループに複数のログ コレクタを追加する場合は、**Enable log redundancy across collectors**（コレクタ間のログ冗長性の有効化）を選択します。このオプションでは、各ログ コレクタの仮想ロギング ディスクの数が同じでなければなりません。

   冗長性を有効化すると、コレクタ グループのログとログ処理トラフィックの量が倍になります。必要に応じて、Panorama バーチャル アプライアンスでのログ ストレージ容量の拡張を行います。
4. **Device Log Forwarding**（デバイス ログ転送）を選択し、Log Forwarding Preferences（ログ転送設定）リストを設定します。このリストでは、どのファイアウォールがどのログ コレクタにログを転送するかが定義されています。このコレクタ グループのログ コレクタ数に基づいてファイアウォールを割り当てます。

© 2019 Palo Alto Networks, Inc.

- 単一 – 「コレクタ グループごとに 1 つのログ コレクタ」のように、プライマリ Panorama のローカル ログ コレクタに、ログを転送するファイアウォールを割り当てます。
- 複数 – 各ファイアウォールを両方のログ コレクタに割り当てて冗長性を確保します。この設定リストを設定する時に、「コレクタ グループごとに複数のログ コレクタ」のように、半分のファイアウォールでログ コレクタ 1 を最優先にし、もう半分のファイアウォールでログ コレクタ 2 を最優先にします。

5. **OK** をクリックして変更内容を保存します。
6. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択してから、Panorama および追加したコレクタ グループに、変更内容を **Commit and Push**（コミットしてプッシュ）します。

STEP 7 | セカンダリ Panorama がアクティブになるように、プライマリ Panorama でフェイルオーバーをトリガーします。

プライマリ Panorama 上で、以下を行います。

1. **[Panorama]** > **[高可用性]** の順に選択します。
2. Operational Commands（操作コマンド）セクションで **Suspend local Panorama**（ローカルの **Panorama** をサスペンド）をクリックします。

STEP 8 | セカンダリ Panorama からプライマリ Panorama のローカル ログ コレクタへの接続を設定します。

セカンダリ Panorama 上で、以下を行います。

1. Panorama Web インターフェイスで、**Panorama** > **Managed Collectors**（管理対象コレクタ）の順に選択し、プライマリ Panorama のローカル ログ コレクタを選択します。
2. プライマリおよびセカンダリ Panorama HA ピアの IP アドレスおよび FQDN を **Panorama Server IP**（**Panorama** サーバー**IP**）フィールドおよび **Panorama Server IP 2**（**Panorama Server IP 2**）フィールドにそれぞれ入力します。

   これらのフィールドは両方とも必須です。
3. **OK** をクリックして変更内容を保存します。
4. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択してから、Panorama およびコレクタ グループに、変更内容を **Commit and Push**（コミットしてプッシュ）します。

STEP 9 | プライマリ Panorama がアクティブになるように、セカンダリ Panorama でフェイルバックをトリガーします。

セカンダリ Panorama 上で、以下を行います。

1. **[Panorama]** > **[高可用性]** の順に選択します。
2. Operational Commands（操作コマンド）セクションで **Suspend local Panorama**（ローカルの **Panorama** をサスペンド）をクリックします。

STEP 10 | ファイアウォールから Panorama へのログ転送を設定します。

プライマリ Panorama 上で、以下を行います。

1. ファイアウォールからPanorama へのログ転送の設定を行います。
2. Panorama へのログ転送の確認

© 2019 Palo Alto Networks, Inc.

ローカル ログ収集を使用するレガシー モードの Panorama バーチャル アプライアンスのデプロイ

以下の図は、一元的なログ収集デプロイ環境の Panorama を示しています。この例では、Panorama 管理サーバーは、アクティブ/パッシブ高可用性（HA）設定でデプロイされた 2 つのレガシー モードの Panorama バーチャル アプライアンスで構成されています。この設定は、Panorama が最大で 10,000 ログ/秒を処理する VMware 仮想インフラストラクチャ内のファイアウォール管理に適しています。このファイアウォールは、Panorama 管理サーバーの NFS データストア（ESXi サーバーのみ）または仮想ディスクにログを送信します。デフォルト設定ではアクティブおよびパッシブ ピアの両方がログを受信しますが、ログ転送とバッファのデフォルトの変更を行い、アクティブ ピアのみが受信するようにすることもできます。5200 Series および 7000 Series のファイアウォールでは、アクティブ ピアのみがログを受信します。デフォルト設定では、レガシー モードの Panorama バーチャル アプライアンスは内部ディスクの約 11GB のパーティションを使用してログを保存しますが、必要な場合は Panorama バーチャル アプライアンスでのログ ストレージ容量の拡張を行うこともできます。

ロギング レートが増加して *10,000* ログ/秒を超えるようになった場合は、専用のログ コレクタを使用する Panorama のデプロイを行うことをお勧めします。

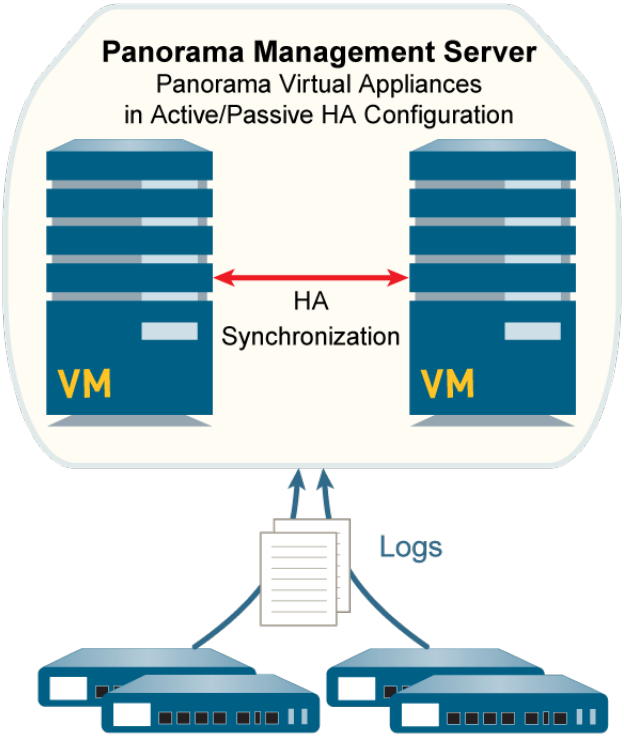


図 **23 :** ローカル ログ収集を使用するレガシー モードの **Panorama** バーチャル アプライアンス

ローカル ログ収集を使用する Panorama バーチャル アプライアンスをデプロイするには、以下のステップを実行します。すでに実行したステップ（初期セットアップなど）は省略してください。

STEP 1 | 各 Panorama バーチャル アプライアンスの初期セットアップを実行します。

1. Panorama バーチャル アプライアンスのインストールを行います。バーチャル アプライアンスが Panorama モードで起動するようにするには、インストール時に仮想ロギング ディスクを追加しないでください。

© 2019 Palo Alto Networks, Inc.

デフォルトでは、*Panorama* は、システム ディスク上の *11GB* のパーティションをログ ストレージ用に使用します。ストレージがさらに必要な場合は、インストール後に専用の仮想ロギング ディスクを *8TB* まで追加できます。

2. Panorama バーチャル アプライアンスの初期設定の実行を行います。
3. Panorama の登録とライセンスのインストールを行います。
4. Panorama のコンテンツ更新とソフトウェア更新のインストールを行います。

STEP 2 | Panorama バーチャル アプライアンスを HA 設定でセットアップします。

1. Panorama での HA のセットアップを行います。
2. Panorama HA フェイルオーバーのテストを行います。

STEP 3 | 次の作業を行って Panorama のログ収集を準備します。

1. Panorama にログを転送するものそれぞれに対して管理対象デバイスとしてのファイアウォールの追加を行います。
2. Panorama へのログ転送の設定

STEP 4 | 変更をコミットします。

Commit（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

© 2019 Palo Alto Networks, Inc.

WildFire アプライアンスの管理

Panorama M-Series アプライアンスまたはバーチャル アプライアンスを使用して、最大 200 台のスタンドアロン WildFire アプライアンスおよび WildFire アプライアンス クラスタ ノードを管理できます。ローカル CLI では、WildFire アプライアンスおよびアプライアンス クラスタを個別に管理できますが、Panorama では、複数のアプライアンスおよびアプライアンス クラスタを一元的に管理および監視できます。一元的な管理により、共通の設定、設定の更新、およびソフトウェア アップグレードを管理対象 WildFire アプライアンスの一部またはすべてにプッシュできるため、WildFire アプライアンスおよびアプライアンス クラスタの設定を簡単に一致させることができます。

Panorama を使用して WildFire アプライアンス クラスタを管理する場合、Panorama は管理対象の WildFire アプライアンスと同等以上のバージョンを実行する必要があります。

> Panorama で管理するスタンドアロン WildFire アプライアンスの追加
> Panorama での WildFire アプライアンスの基本設定
> WildFire アプライアンスとクラスタのカスタム証明書を使用する認証のセットアップ
> Panorama 管理からの WildFire アプライアンスの削除
> WildFire クラスタの管理

Panorama で管理するスタンドアロン WildFire アプライアンスの追加

Panorama M-Series またはバーチャル アプライアンスでは、最大 200 台の WildFire アプライアンスを管理できます。WildFire アプライアンス 200 台という制限は、スタンドアロン アプライアンスおよび WildFire アプライアンス クラスタ ノードの合計です（Panorama でクラスタを設定してノードを追加した場合）。

Panorama が最低でもバージョン 8.0.1 で動作していること、および Panorama に追加したすべての WildFire アプライアンスも最低でバージョン 8.0.1 で動作していることを確認してください。

STEP 1 | ローカル CLI を使用し、Panorama で管理する各 WildFire アプライアンスが PAN-OS 8.0.1 以降を実行していることを確認します。

```
admin@qa16> show system info | match version
sw-version: 8.0.1-c45
wf-content-version: 702-283
logdb-version: 8.0.15
```

STEP 2 | WildFire アプライアンスの管理に使用する各 Panorama アプライアンスで、Panorama がバージョン 8.0.1 以降で動作していることを確認します。

Dashboard（ダッシュボード）> **General Information**（一般情報）> **Software Version**（ソフトウェア バージョン）の順に選択すると、動作しているソフトウェアのバージョンが表示されます。

STEP 3 | WildFire アプライアンスが WildFire アプライアンス クラスタに属しているかスタンドアロン アプライアンスであるかが分からない場合は、WildFire アプライアンス CLI で **Node mode** が **stand_alone** になっていることを確認し、**Application status** で **global-db-service** と **global-queue-service** が **ReadyStandalone** になっていることを確認します。

```
admin@WF-500> show cluster membership
Service Summary:  wfpc signature
Cluster name:
Address:          10.10.10.100
Host name:        WF-500
Node name:        wfpc-012345678901-internal
Serial number:    012345678901
Node mode:     stand_alone
Server role:      True
HA priority:
Last changed:     Mon, 06 Mar 2017 16:34:25 -0800
Services:         wfcore signature wfpc infra
Monitor status:
                  Serf Health Status: passing
                      Agent alive and reachable
Application status:
                  global-db-service: ReadyStandalone
        wildfire-apps-service: Ready
        global-queue-service: ReadyStandalone
        wildfire-management-service: Done
        siggen-db: ReadyMaster
Diag report:
```


© 2019 Palo Alto Networks, Inc.

```
                    10.10.10.100: reported leader '10.10.10.100', age 0.
                    10.10.10.100: local node passed sanity check.
```

STEP 4 | Panorama で管理する WildFire アプライアンスが新しい場合は、『Get Started with WildFire (WildFire を使い始める) 』を確認し、WildFire ライセンスが有効であることを確認したり、ログを有効にしたり、ファイアウォールを WildFire アプライアンスに接続したり、基本的な WildFire 機能を設定したりすることなど、基本的な手順を完了していることを確認します。

STEP 5 | Panorama サーバーが管理する各 WildFire アプライアンスのローカル CLI で、Panorama サーバーの IP アドレスを設定します。

スタンドアロン WildFire アプライアンスを Panorama アプライアンスに登録する前に、まず Panorama の IP アドレスまたは FQDN を各 WildFire アプライアンスで設定する必要があります。この設定により、各 WildFire アプライアンスは、どの Panorama アプライアンスによって管理されるかを認識するようになります。

1. プライマリ Panorama アプライアンスの管理インターフェイスの IP アドレスまたは FQDN を設定します。

```
admin@WF-500# set deviceconfig system panorama-server <ip-address | FQDN>
```

2. バックアップ Panorama アプライアンスを高可用性のために使用する場合は (推奨) 、バックアップ Panorama アプライアンスの管理インターフェイスの IP アドレスまたは FQDN を設定します。

```
admin@WF-500# set deviceconfig system panorama-server-2 <ip-address |
 FQDN>
```

STEP 6 | プライマリ Panorama アプライアンスで WildFire アプライアンスを登録します。

1. Panorama Web インターフェイスから、**Panorama** > **Managed WildFire Appliances** (管理対象 **WildFire** アプライアンス) の順に選択し、**Add Appliance** (アプライアンスの追加) を選択します。
2. 各 WildFire アプライアンスのシリアル番号を別々の行に入力します。シリアル番号のリストがない場合は、各 WildFire アプライアンスで次のコマンドを実行します。

```
admin@WF-500> show system info | match serial
serial: 012345678901
```

show cluster membership など、WildFire アプライアンスのシリアル番号を表示するローカル CLI コマンドはいくつかあります。

3. **OK** をクリックします。

IP アドレスやソフトウェア バージョンなど、WildFire アプライアンスですでにコミットされている設定に関する情報が、利用可能な場合は表示されます。

STEP 7 | (任意) WildFire アプライアンスの設定を Panorama アプライアンスにインポートします。

1. インポートする設定があるアプライアンスを管理対象 WildFire アプライアンスのリストから選択します。
2. **Import Config** (設定のインポート) を選択します。
3. **Yes** (はい) を選択します。

設定をインポートすると、表示される情報が更新されて、インポートした設定が Panorama アプライアンスの候補設定の一部になります。

© 2019 Palo Alto Networks, Inc.

4. **Commit to Panorama**（**Panorama** へのコミット）を選択し、インポートした WildFire アプライアンスの設定を Panorama の実行中の設定にします。

STEP 8 | WildFire アプライアンス インターフェイスを設定するか、または設定を確認します。

各 WildFire アプライアンスには、次の4つのインターフェイスがあります。**Management**（管理）(Ethernet0)、**Analysis Network Environment**（分析ネットワーク環境）(Ethernet1)、**Ethernet2**、および **Ethernet3** です。

1. **Panorama** > **Managed WildFire Appliances**（管理対象 **WildFire** アプライアンス）の順に選択し、WildFire アプライアンスを選択します。
2. **Interfaces**（インターフェイス）を選択します。
3. インターフェイスを選択して、設定や編集を行います。インターフェイスを有効にして、インターフェイスごとに、速度とデュプレックス、IP アドレスとネットマスク、デフォルト ゲートウェイ、MTU、DNS サーバー、リンク状態、**Management Services**（管理サービス）を設定できます。アクセス許可 IP アドレスを **Add**（追加）し、インターフェイスが指定アドレスからのみトラフィックを受け入れるようにすることもできます。

   Analysis Network Environment（分析ネットワーク環境）、**Ethernet2**、**Ethernet3** の各インターフェイスでは、**Ping** のみが **Management Services**（管理サービス）オプションとしてサポートされます。

   Management（管理）インターフェイスでは、**Ping**、**SSH**、**SNMP** が **Management Services**（管理サービス）オプションとしてサポートされます。**Management**（管理）インターフェイスでは、インターネットに直接接続できない場合のために、プロキシ サーバー設定もサポートされます。
4. 設定や設定の確認の後で **OK** をクリックします。

STEP 9 | 設定を Panorama アプライアンスでコミットし、アプライアンス（単数か複数）にプッシュします。

1. **Commit and Push**（コミットしてプッシュ）を選択します。
2. プッシュしない設定が Panorama アプライアンスにある場合は、**Edit Selections**（選択内容の編集）によって、設定のプッシュ先のアプライアンスを選択します。プッシュした設定により、WildFire アプライアンスで動作中の設定は上書きされます。

STEP 10 | 設定を確認します。

1. **Panorama** > **Managed WildFire Appliances**（管理対象 **WildFire** アプライアンス）の順に選択します。
2. 次のフィールドを確認します。
   - **Connected**（接続済み） — 状態が **Connected**（接続済み）である。
   - **Role**（ロール） — 各 WildFire アプライアンスのロールが **Standalone**（スタンドアロン）である。
   - **Config Status**（設定状態） — 状態が `In Sync` である。
   - **Last Commit State**（最終コミット状態） — `Commit succeeded` である。

© 2019 Palo Alto Networks, Inc.

Panorama での WildFire アプライアンスの基本設定

コンテンツ更新、WildFire クラウド サーバー、WildFire クラウド サービス、ロギング、認証などの基本的な設定は、Panorama での全般的なクラスタ設定方法とほぼ同じです。クラスタを選択してクラスタで設定を行う代わりに、WildFire アプライアンスを選択してそのアプライアンスについて個別に設定を行います。Panorama に追加する各 WildFire アプライアンスを選択して設定します。

「WildFire アプライアンスの設定」では、WildFire アプライアンスをネットワークに統合して CLI を使用した基本的なセットアップの実行方法を説明していますが、コンセプトは Panorama を使用した基本的なセットアップを実行する場合と同じです。



多くの設定は、デフォルト、*WildFire* アプライアンスでの既存の設定からの情報、*WildFire* アプライアンスを *Panorama* に追加するときに行った設定のいずれかにより、値が入力済みです。

- WildFire アプライアンスの認証の設定

WildFire アプライアンスの認証の設定

きめ細かな認証パラメータが設定されたローカルの管理者ユーザーを設定する、ならびに承認および認証用の RADIUS、TACAS+、または LDAP を活用することにより、WildFire アプライアンス用に強化された認証を作成し、設定します。

Panorama から管理者を設定してプッシュする際は、WildFire アプライアンスの既存の管理者を、Panorama で設定した管理者で上書きします。

- WildFire アプライアンスの管理者アカウントの設定
- WildFire アプライアンスの RADIUS 認証の設定
- WildFire アプライアンスの TACACS+ 認証の設定
- WildFire アプライアンスの LDAP 認証の設定

WildFire アプライアンスの管理者アカウントの設定

Panorama™ 管理サーバーから管理する WildFire アプライアンスの詳細な認証パラメーターを使用して1人以上の管理者を作成します。さらに、WildFire アプライアンスの CLI で直接設定可能な Panorama からローカル管理者を設定できます。ただし、新しい構成の変更を専用の WildFire アプライアンスにプッシュすると、ローカル管理者が WildFire アプライアンス用に設定された管理者で上書きされます。

STEP 1 | Panorama Web インターフェイスへのログイン.

STEP 2 | Panorama で管理するスタンドアロン WildFire アプライアンスの追加.

STEP 3 | (任意) 認証プロファイルを設定して、WildFire アプライアンス CLI にアクセスする管理者のログイン資格情報を検証する認証サービスを定義します。

STEP 4 | 必要に応じて、1つ以上の管理者アカウントを設定します。

Panorama で作成された管理者アカウントは、後で WildFire アプライアンスにインポートされ、Panorama で管理されます。

STEP 5 | WildFire アプライアンスの認証の設定

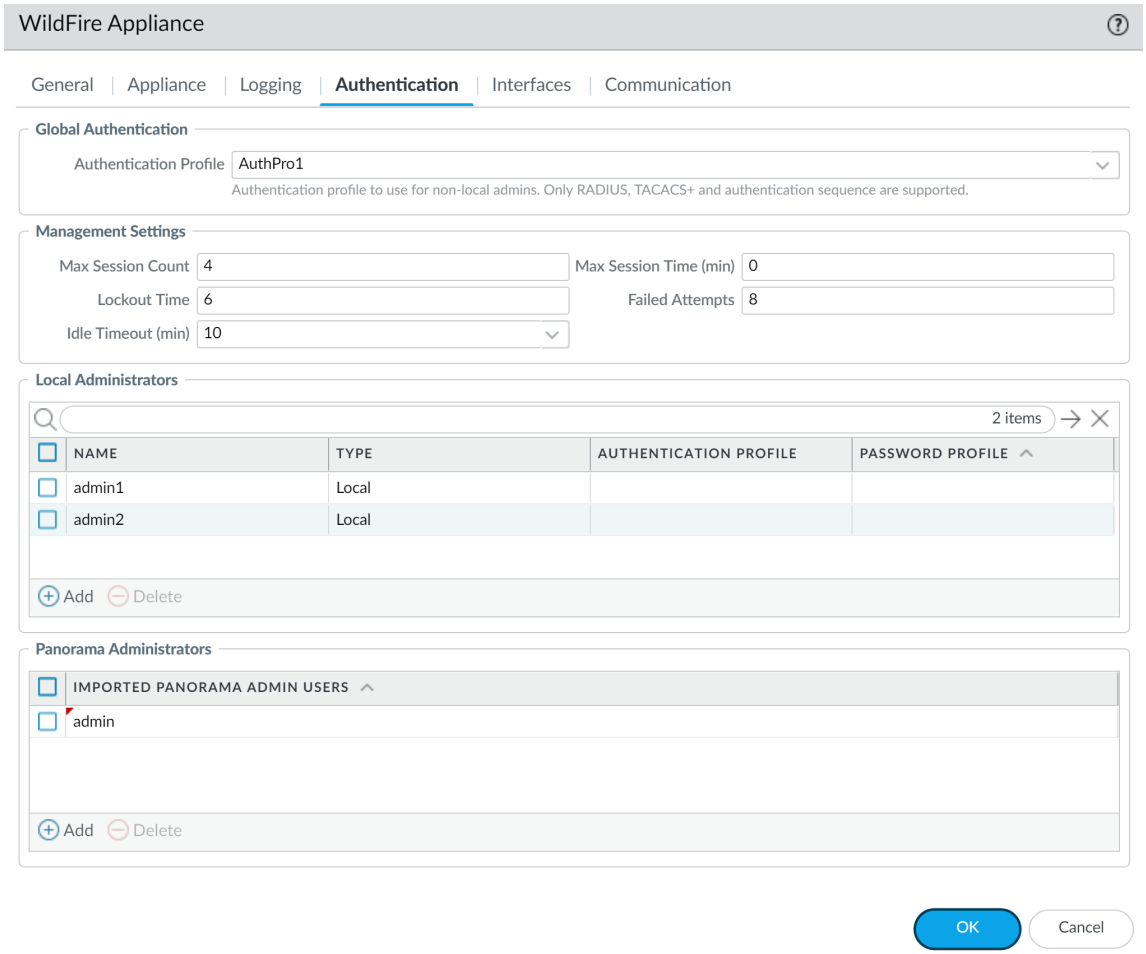
© 2019 Palo Alto Networks, Inc.

1. **Panorama** > **Managed WildFire Appliances**（管理対象 **WildFire** アプライアンス）の順に選択し、以前に追加した WildFire アプライアンスを選択します。
2. (任意) 前のステップで設定した **Authentication Profile** (認証プロファイル) を選択します。
3. WildFire アプライアンスの認証 **Timeout Configuration** (タイムアウト設定) を設定します。
   1. ユーザーが WildFire アプライアンス CLI からロックアウトされるまでの **Failed Attempt** (試行失敗回数) の数を入力します。
   2. **Lockout Time** (ロックアウト時間) を分単位で入力します。WildFire アプライアンス は、ユーザーが設定された数の試行失敗回数に達すると、ユーザー アカウントをロックアウトします。
   3. アクティブではないユーザー アカウントが自動的にログアウトされるまでの時間である、**Idle Timeout** (待機タイムアウト) を分単位で入力します。
   4. WildFire アプライアンス に同時にアクセスできるユーザー アカウントの数を設定するには、**Max Session Count** (最大セッション カウント) を入力します。
   5. 管理者が自動的にログアウトする前にログインできる**Max Session Time** (最大セッション時間) を入力します。
4. WildFire アプライアンス管理者を追加します。

   管理者は、ローカル管理者またはインポートされた Panorama 管理者のいずれかとして追加できますが、両方を追加することはできません。ローカル管理者とインポートされた Panorama 管理者の両方として同じ管理者を追加することはサポートされておらず、Panorama コミットが失敗します。例えば、**admin1** を ローカル管理者と Panorama 管理者の両方として追加する場合、Panorama へのコミットは失敗します。

   1. WildFire アプライアンスに固有の新しい管理者を**Add** (追加) して設定します。これらの管理者は、それらが作成された WildFire アプライアンスに固有であり、この表からこれらの管理者を管理します。
   2. Panorama で設定された管理者を **Add** (追加) します。これらの管理者は Panorama で作成され、WildFire アプライアンスにインポートされます。
5. **OK** をクリックすると、WildFire アプライアンス認証設定を保存します。

© 2019 Palo Alto Networks, Inc.



STEP 6 | 設定の変更を **Commit** (コミット) してから、**Commit and Push** (コミットしてプッシュ) します。

STEP 7 | WildFire アプライアンス CLI にアクセスして、ローカルの管理者ユーザーを使用して WildFire アプライアンスにアクセスできることを確認します。

WildFire アプライアンスの *RADIUS* 認証の設定

RADIUS サーバーを使用して、WildFireアプライアンス CLI への管理アクセスを認証します。RADIUS サーバーでベンダー固有属性 (VSA) を定義し、管理者認証を管理することもできます。VSA を使用すれば、ディレクトリ サービスを介してロール、アクセス ドメイン、管理者のユーザー グループをすばやく変更できます。この方法は多くの場合、Panorama™ 管理サーバーで設定し直すよりも簡単です。

Palo Alto Networks RADIUS ディクショナリーを *RADIUS* サーバーにインポートして、*Panorama* と *RADIUS* サーバー間の通信に必要な認証属性を定義することができます。

STEP 1 | Panorama Web インターフェイスへのログイン.

STEP 2 | Panorama で管理するスタンドアロン WildFire アプライアンスの追加.

STEP 3 | RADIUS 認証を設定します。

© 2019 Palo Alto Networks, Inc.

1. RADIUS サーバー プロファイルを追加します。

   このプロファイルは、WildFire アプライアンスが RADIUS サーバーに接続する方法を定義します。

   1. **Panorama** > **Server Profiles**（サーバー プロファイル）> **RADIUS** の順に追加し、プロファイルを **Add**（追加）します。
   2. サーバー プロファイルを識別する **Profile Name**（プロファイル名）を入力します。
   3. 認証要求がタイムアウトするまでの**Timeout (**タイムアウト**)** 時間を秒単位で入力します（デフォルトは 3、範囲は1 ~ 20）。
   4. WildFire アプライアンスが RADIUS サーバーに認証するために使用する **Authentication Protocol**（認証プロトコル）（デフォルトは **CHAP**）を選択します。

      RADIUS サーバーがサポートする場合は *CHAP* を選択します。このプロトコルは *PAP* よりも安全です。

   5. 各 RADIUS サーバーを **Add**（追加）して、以下を入力します。

      1. サーバーを識別するための**Name**（名前）。
      2. **RADIUS Server**（**RADIUS** サーバー）の IP アドレス あるいは FQDN。
      3. **Secret**（シークレット）/**Confirm Secret**（再入力 シークレット）（ユーザー名とパスワードを暗号化するための鍵）。
      4. 認証要求用のサーバー **Port**（ポート）（デフォルトは1812）。

   6. **OK** をクリックしてサーバー プロファイルを保存します。
2. RADIUS サーバー プロファイルを認証プロファイルに割り当てます。

   認証プロファイルにより、一連の管理者に共通の認証設定が定義されます。

   1. **Panorama** > **Authentication Profile**（認証プロファイル）の順に選択し、プロファイルを **Add**（追加）します。
   2. 認証プロファイルを識別する **Name**（名前）を入力します。
   3. **Type**（タイプ）を **RADIUS** に設定します。
   4. 設定した **Server Profile**（サーバー プロファイル）を選択します。
   5. **Retrieve user group from RADIUS**（**RADIUS** からユーザー グループを取得）を選択して、RADIUS サーバーで定義された VSA からユーザー グループ情報を収集します。

      Panorama は、グループ情報を認証プロファイルの Allow List（許可リスト）で指定したグループと照合します。

   6. **Advanced**（詳細）を選択し、Allow List（許可リスト）で、この認証プロファイルで認証することが許可された管理者を **Add**（追加）します。
   7. **OK** をクリックして認証プロファイルを保存します。

STEP 4 | WildFire アプライアンスの認証の設定

1. **Panorama** > **Managed WildFire Appliances**（管理対象 **WildFire** アプライアンス）の順に選択し、以前に追加した WildFire アプライアンスを選択します。
2. 前のステップで設定した **Authentication Profile (**認証プロファイル**)** を選択します。

   グローバル認証プロファイルが割り当てられていない場合は、リモート認証を活用するために、個々のローカル管理者に認証プロファイルを割り当てる必要があります。
3. WildFire アプライアンスの認証 **Timeout Configuration (**タイムアウト設定**)** を設定します。

   1. ユーザーが WildFire アプライアンス CLI からロックアウトされるまでの **Failed Attempt (**試行失敗回数**)** の数を入力します。
   2. **Lockout Time (**ロックアウト時間**)** を分単位で入力します。WildFire アプライアンス は、ユーザーが設定された数の試行失敗回数に達すると、ユーザー アカウントをロックアウトします。
   3. アクティブではないユーザー アカウントが自動的にログアウトされるまでの時間である、**Idle Timeout (**待機タイムアウト**)** を分単位で入力します。

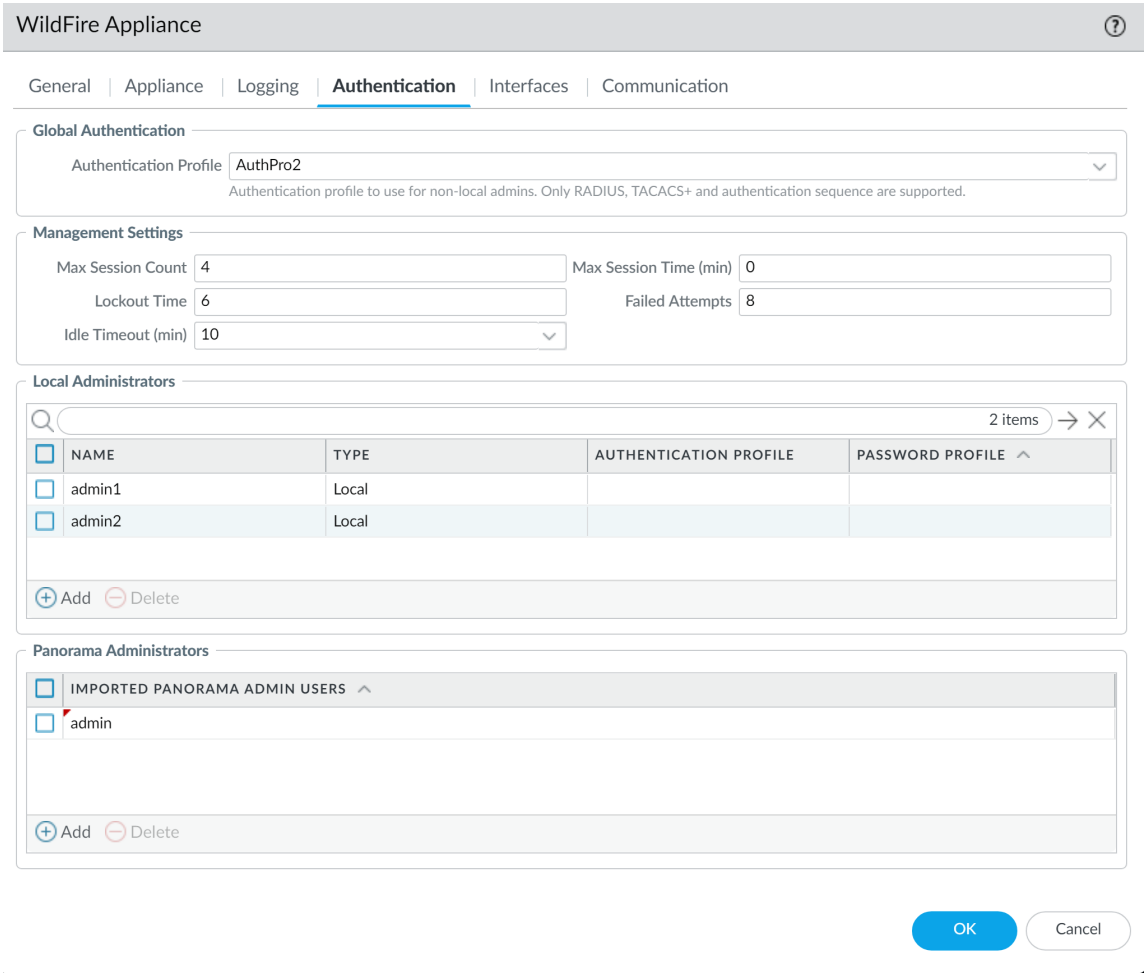
© 2019 Palo Alto Networks, Inc.

4. WildFire アプライアンス に同時にアクセスできるユーザー アカウントの数を設定するには、**Max Session Count** (最大セッション カウント) を入力します。
5. 管理者が自動的にログアウトする前にログインできる**Max Session Time** (最大セッション時間) を入力します。

4. WildFire アプライアンス管理者を追加します。

   管理者は、ローカル管理者またはインポートされた Panorama 管理者のいずれかとして追加できますが、両方を追加することはできません。ローカル管理者とインポートされた Panorama 管理者の両方として同じ管理者を追加することはサポートされておらず、Panorama コミットが失敗します。例えば、`admin1` をローカル管理者と Panorama 管理者の両方として追加する場合、Panorama へのコミットは失敗します。

   1. WildFire アプライアンスに固有の新しい管理者を**Add** (追加) して設定します。これらの管理者は、それらが作成された WildFire アプライアンスに固有であり、この表からこれらの管理者を管理します。
   2. Panorama で設定された管理者を **Add** (追加) します。これらの管理者は Panorama で作成され、WildFire アプライアンスにインポートされます。
5. **OK** をクリックすると、WildFire アプライアンス認証設定を保存します。



STEP 5 | 設定の変更を **Commit** (コミット) してから、**Commit and Push** (コミットしてプッシュ) します。

STEP 6 | WildFire アプライアンス CLI にアクセスして、ローカルの管理者ユーザーを使用して WildFire アプライアンスにアクセスできることを確認します。

© 2019 Palo Alto Networks, Inc.

WildFire アプライアンスの TACACS+ 認証の設定

TACACS+ サーバーを使用して、WildFire アプライアンス CLI への管理アクセスを認証できます。TACACS + サーバーでベンダー固有属性 (VSA) を定義し、管理者認証を管理することもできます。VSA を使用すれば、ディレクトリ サービスを介してロール、アクセス ドメイン、管理者のユーザー グループをすばやく変更できます。この方法は多くの場合、Panorama で設定し直すよりも簡単です。

STEP 1 | Panorama Web インターフェイスへのログイン.

STEP 2 | Panorama で管理するスタンドアロン WildFire アプライアンスの追加.

STEP 3 | TACACS+ 認証を設定します。

1. TACACS+サーバー プロファイルを追加します。

   このプロファイルは、WildFire アプライアンスが TACACS+ サーバーに接続する方法を定義します。

   1. **Panorama** > **Server Profiles** (サーバー プロファイル) > **TACACS+** の順に選択し、プロファイルを **Add** (追加) します。
   2. サーバー プロファイルを識別する **Profile Name** (プロファイル名) を入力します。
   3. 認証要求がタイムアウトするまでの**Timeout (タイムアウト)** 時間を秒単位で入力します (デフォルトは 3、範囲は1 ~ 20) 。
   4. Panorama が TACACS+ サーバーに認証するために使用する **Authentication Protocol** (認証プロトコル) (デフォルトは **CHAP**) を選択します。
   5. TACACS+ サーバーがサポートする場合は **CHAP** を選択します。このプロトコルは **PAP** よりも安全です。
   6. 各 TACACS+ サーバーを **Add** (追加) して、以下を入力します。
      1. サーバーを識別するための**Name** (名前) 。
      2. **TACACS+ Server** (**TACACS+** サーバー) の IP アドレス あるいは FQDN。
      3. **Secret** (シークレット) **/Confirm Secret** (再入力 シークレット) (ユーザー名とパスワードを暗号化するための鍵) 。
      4. 認証要求用のサーバー **Port** (ポート) (デフォルトは49) 。
   7. **OK** をクリックしてサーバー プロファイルを保存します。
2. TACACS+ サーバー プロファイルを認証プロファイルに割り当てます。

   認証プロファイルにより、一連の管理者に共通の認証設定が定義されます。

   1. **Panorama** > **Authentication Profile** (認証プロファイル) の順に選択し、プロファイルを **Add** (追加) します。
   2. プロファイルを識別する **Name** (名前) を入力します。
   3. **Type** (タイプ) を **TACACS+** に設定します。
   4. 設定した **Server Profile** (サーバー プロファイル) を選択します。
   5. **Retrieve user group from TACACS+** (**TACACS+** からユーザー グループを取得) を選択して、TACACS+ サーバーで定義された VSA からユーザー グループ情報を収集します。

      Panorama は、グループ情報を認証プロファイルの Allow List (許可リスト) で指定したグループと照合します。
   6. **Advanced** (詳細) を選択し、Allow List (許可リスト) で、この認証プロファイルで認証することが許可された管理者を **Add** (追加) します。
   7. **OK** をクリックして認証プロファイルを保存します。

STEP 4 | WildFire アプライアンスの認証の設定

1. **Panorama** > **Managed WildFire Appliances** (管理対象 **WildFire** アプライアンス) の順に選択し、以前に追加した WildFire アプライアンスを選択します。

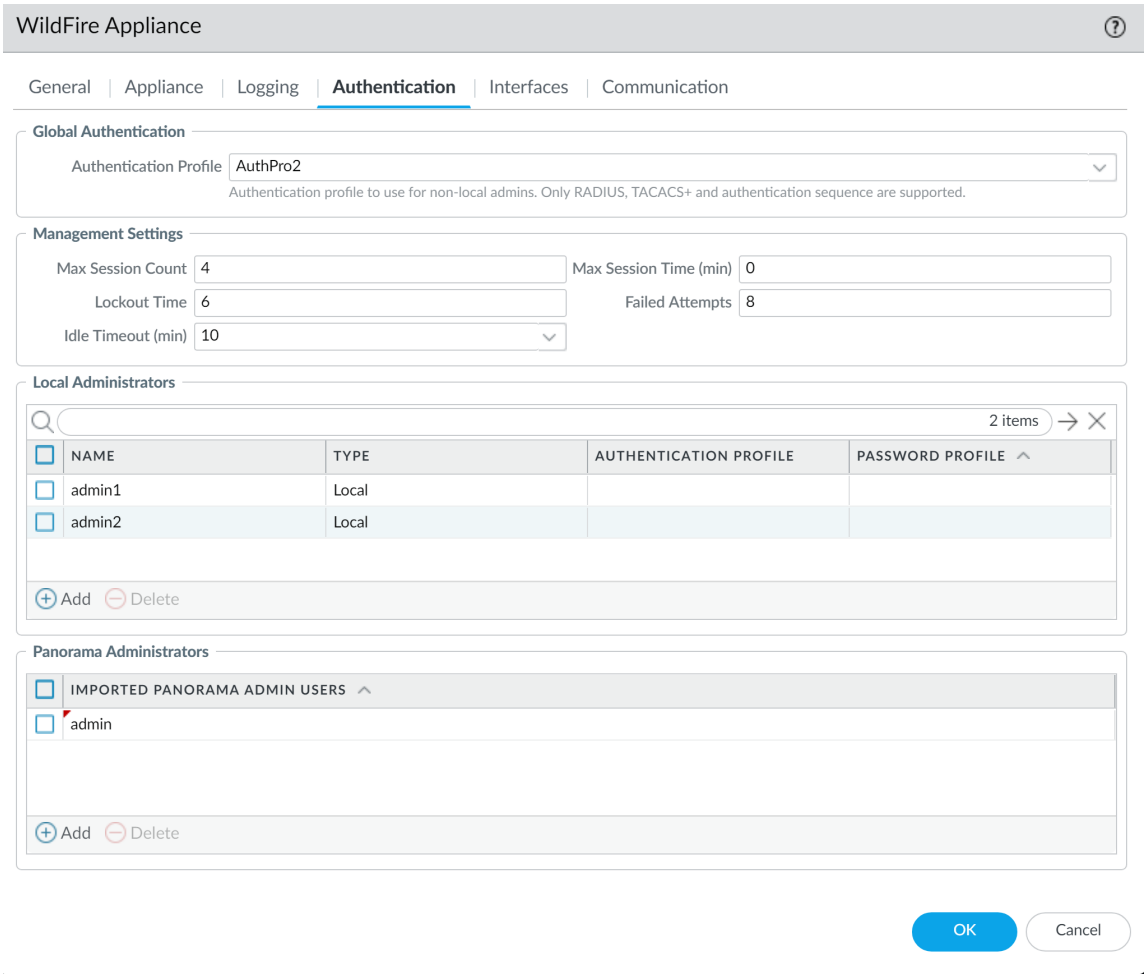
© 2019 Palo Alto Networks, Inc.

2. 前のステップで設定した **Authentication Profile** (認証プロファイル) を選択します。

   グローバル認証プロファイルが割り当てられていない場合は、リモート認証を活用するために、個々のローカル管理者に認証プロファイルを割り当てる必要があります。
3. WildFire アプライアンスの認証 **Timeout Configuration** (タイムアウト設定) を設定します。
   1. ユーザーが WildFire アプライアンス CLI からロックアウトされるまでの **Failed Attempt** (試行失敗回数) の数を入力します。
   2. **Lockout Time** (ロックアウト時間) を分単位で入力します。WildFire アプライアンス は、ユーザーが設定された数の試行失敗回数に達すると、ユーザー アカウントをロックアウトします。
   3. アクティブではないユーザー アカウントが自動的にログアウトされるまでの時間である、**Idle Timeout** (待機タイムアウト) を分単位で入力します。
   4. WildFire アプライアンス に同時にアクセスできるユーザー アカウントの数を設定するには、**Max Session Count** (最大セッション カウント) を入力します。
   5. 管理者が自動的にログアウトする前にログインできる**Max Session Time** (最大セッション時間) を入力します。
4. WildFire アプライアンス管理者を追加します。

   管理者は、ローカル管理者またはインポートされた Panorama 管理者のいずれかとして追加できますが、両方を追加することはできません。ローカル管理者とインポートされた Panorama 管理者の両方として同じ管理者を追加することはサポートされておらず、Panorama コミットが失敗します。例えば、**admin1** を ローカル管理者と Panorama 管理者の両方として追加する場合、Panorama へのコミットは失敗します。
   1. WildFire アプライアンスに固有の新しい管理者を**Add** (追加) して設定します。これらの管理者は、それらが作成された WildFire アプライアンスに固有であり、この表からこれらの管理者を管理します。
   2. Panorama で設定された管理者を **Add** (追加) します。これらの管理者は Panorama で作成され、WildFire アプライアンスにインポートされます。
5. **OK** をクリックすると、WildFire アプライアンス認証設定を保存します。

© 2019 Palo Alto Networks, Inc.



STEP 5 | 設定の変更を **Commit** (コミット) してから、**Commit and Push** (コミットしてプッシュ) します。

STEP 6 | WildFire アプライアンス CLI にアクセスして、ローカルの管理者ユーザーを使用して WildFire アプライアンスにアクセスできることを確認します。

WildFire アプライアンスの LDAP 認証の設定

LDAP を使用して WildFire アプライアンス CLI にアクセスするエンド ユーザーを認証することができます。

STEP 1 | Panorama Web インターフェイスへのログイン.

STEP 2 | Panorama で管理するスタンドアロン WildFire アプライアンスの追加.

STEP 3 | LDAP サーバー プロファイルを追加します。

このプロファイルは、WildFire アプライアンスが LDAP サーバーに接続する方法を定義します。

1. **Panorama** > **Server Profiles** (サーバー プロファイル) > **LDAP**を選択し、サーバー プロファイルを **Add** (追加) します。
2. サーバー プロファイルを識別する **Profile Name** (プロファイル名) を入力します。

© 2019 Palo Alto Networks, Inc.

3. LDAP サーバーを **Add** (追加) します (最大 4 件) 。各サーバーについて、**Name** (名前) (サーバーを識別するため) 、**LDAP Server** (サーバー) の IP アドレスあるいは FQDN、およびサーバーの **Port** (ポート) (デフォルトは 389) を入力します。

   FQDN アドレス オブジェクトを使用してサーバーを識別し、後でアドレスを変更する場合は、変更をコミットし、新しいサーバー アドレスを有効にする必要があります。
4. サーバーの **Type** (タイプ) を選択します。
5. **Base DN** (ベース **DN**) を選択します。

   ディレクトリのベース DN を識別するには、**Active Directory Domains and Trusts(Active Directory** ドメインと信頼関係)Microsoft 管理コンソールスナップインを開き、トップレベル ドメインの名前を使用します。
6. **Bind DN** と **Password** (パスワード) を入力して、ファイアウォールを認証するための認証サービスを有効にします。

   *Bind DN (*バインド *DN)* アカウントには、*LDAP* ディレクトリを参照する権限が必要です。
7. **Bind Timeout (**バインドのタイムアウト) および **Search Timeout** (検索タイムアウト) を秒単位で入力します (デフォルトはどちらも 30) 。
8. **Retry Interval** (再試行間隔) を秒単位で入力します (デフォルトは 60) 。
9. (LDAP のみ) ディレクトリサーバーとの保護された接続のためにエンドポイントで SSL または TLS を使いたい場合は、 **Require SSL/TLS secured connection** (**SSL/TLS** で保護された接続を要求) オプションを有効にしてください (デフォルトで有効) 。サーバー ポートによってエンドポイントが使用するプロトコル :
   - 389 (デフォルト) – TLS (具体的には、WildFire アプライアンスは StartTLS 操作を使用して、最初のプレーンテキスト接続を TLS にアップグレードします)
   - 636 – SSL
   - その他の任意のポート – WildFire アプライアンスはまず TLS を使用しようとします。ディレクトリ サーバーで TLS がサポートされていない場合は、WildFire アプライアンスは SSL にフォールバックします。
10. (LDAP のみ) 保護を強化するには、**Verify Server Certificate for SSL sessions** (**SSL** セッションのサーバー証明書を確認) オプションを有効化します。すると、エンドポイントは SSL/TLS 接続にディレクトリサーバーが提示する証明書を確認します。この検証を有効にする場合は、**Require SSL/TLS secured connection** (**SSL/TLS**で保護された接続を要求) オプションを有効化する必要があります。進めるための確認において、証明書は次のいずれかの条件に合う必要があります。
    - 次のものはPanorama 証明書のリストにあります : **Panorama** > **Certificate Management** (証明書の管理) > **Certificates** (証明書) > **Device Certificates** (デバイス証明書) 。必要に応じて、証明書を Panorama にインポートします。
    - 証明書の署名者は信頼できる証明機関のリストにあること : **Panorama** > **Certificate Management (Panorama** 証明書管理) > **Certificates (**証明書)。
11. **OK** をクリックしてサーバー プロファイルを保存します。

STEP 4 | WildFire アプライアンスの認証の設定

1. **Panorama** > **Managed WildFire Appliances** (管理対象 **WildFire** アプライアンス) の順に選択し、以前に追加した WildFire アプライアンスを選択します。
2. WildFire アプライアンスの認証 **Timeout Configuration** (タイムアウト設定) を設定します。
   1. ユーザーが WildFire アプライアンス CLI からロックアウトされるまでの **Failed Attempt** (試行失敗回数) の数を入力します。
   2. **Lockout Time** (ロックアウト時間) を分単位で入力します。WildFire アプライアンス は、ユーザーが設定された数の試行失敗回数に達すると、ユーザー アカウントをロックアウトします。

© 2019 Palo Alto Networks, Inc.

3. アクティブではないユーザー アカウントが自動的にログアウトされるまでの時間である、**Idle Timeout** (待機タイムアウト) を分単位で入力します。
4. WildFire アプライアンス に同時にアクセスできるユーザー アカウントの数を設定するには、**Max Session Count** (最大セッション カウント) を入力します。
5. 管理者が自動的にログアウトする前にログインできる**Max Session Time** (最大セッション時間) を入力します。

3. WildFire アプライアンス管理者を追加します。

   管理者は、ローカル管理者またはインポートされた Panorama 管理者のいずれかとして追加できますが、両方を追加することはできません。ローカル管理者とインポートされた Panorama 管理者の両方として同じ管理者を追加することはサポートされておらず、Panorama コミットが失敗します。例えば、`admin1` をローカル管理者と Panorama 管理者の両方として追加する場合、Panorama へのコミットは失敗します。

   - ローカルの管理者を設定します。

     WildFire アプライアンスに固有の新しい管理者を設定します。これらの管理者は、それらが作成された WildFire アプライアンスに固有であり、この表からこれらの管理者を管理します。

     1. 1名以上のローカル管理者を **Add** (追加) します。
     2. ローカル管理者の **Name** (名前) を入力します。
     3. 前に作成した **Authentication Profile** (認証プロファイル) を割り当てます。

        LDAP 認証プロファイルは、個々のローカル管理者に対してのみサポートされます。

     4. **Use Public Key Authentication (SSH)** (公開キーの認証 (SSH) の使用) を 有効化 (チェックを入れる) して、認証用の公開キー ファイルをインポートします。
     5. **Password Profile** (パスワードのプロファイル) を選択して、有効期限パラメータをセットします。

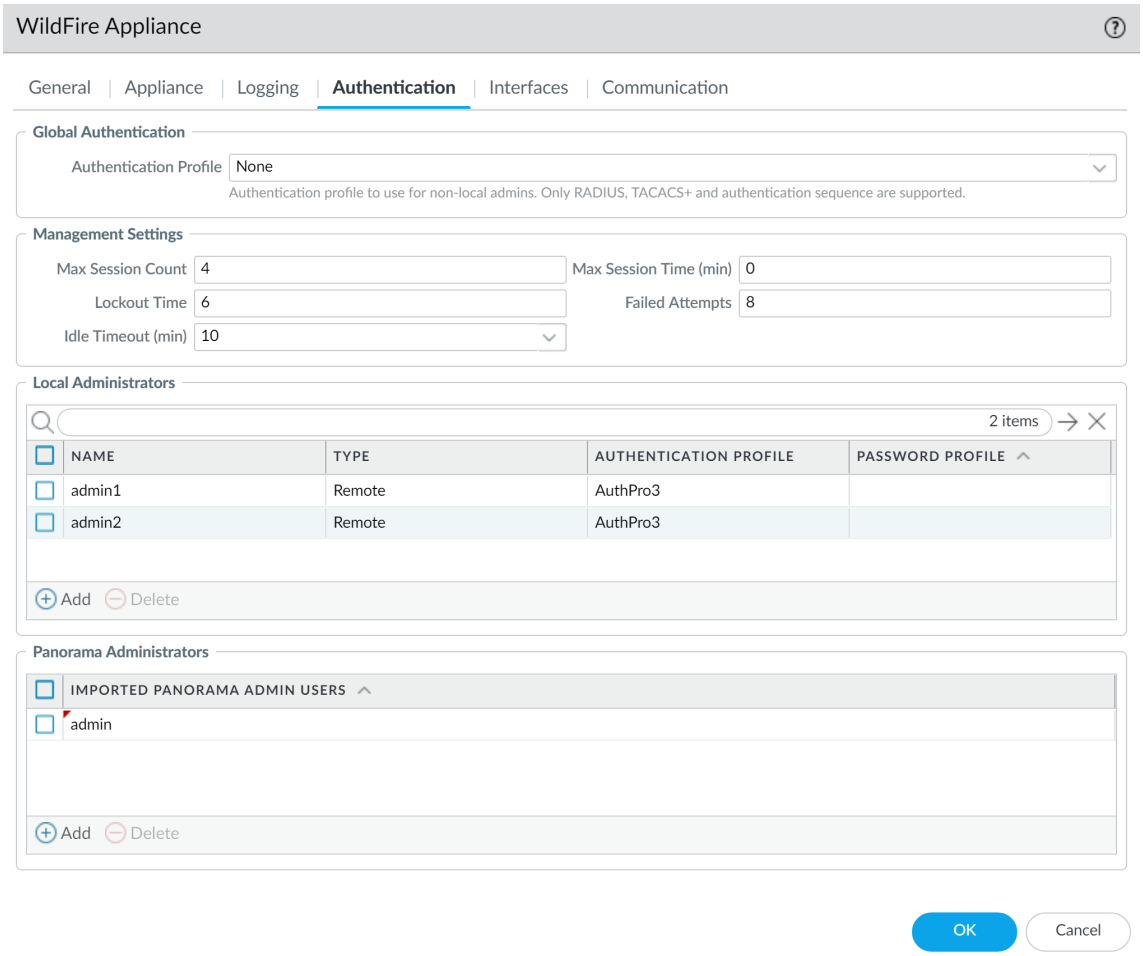
   - 既存の Panorama 管理者をインポートする

     Panorama で設定された既存の管理者を インポートします。これらの管理者は Panorama で設定、管理され、WildFire アプライアンスにインポートされます。

     1. 既存の Panorama 管理者を **Add** (追加) する

4. **OK** をクリックすると、WildFire アプライアンス認証設定を保存します。

© 2019 Palo Alto Networks, Inc.



STEP 5 | 設定の変更を **Commit** (コミット) してから、**Commit and Push** (コミットしてプッシュ) します。

STEP 6 | WildFire アプライアンス CLI にアクセスして、ローカルの管理者ユーザーを使用して WildFire アプライアンスにアクセスできることを確認します。

© 2019 Palo Alto Networks, Inc.

WildFire アプライアンスとクラスタのカスタム証明書を使用する認証のセットアップ

デフォルトでは、WildFire アプライアンスは、他の Palo Alto Networks® ファイアウォールとアプライアンスとの相互認証に事前定義された証明書を使用して、管理アクセスとデバイス間通信に使用される SSL 接続を確立します。ただし、代わりにカスタム証明書を使用して認証を設定することもできます。カスタム証明書を使用すると、Panorama™ で管理されている WildFire アプライアンスまたは WildFire クラスタとファイアウォールの相互認証を確実にするための信頼関係を確立することができます。こうした証明書は、Panorama またはファイアウォールでローカルに生成したり、信頼できるサードパーティ認証局（CA）から取得したり、エンタープライズ プライベートキー インフラストラクチャ（PKI）から証明書を取得することができます。

カスタム証明書の使用の詳細については、 SSL/TLS 接続を相互に認証する方法を参照してください。

- Panorama の管理対象の WildFire アプライアンスのカスタム証明書を設定する
- WildFire クラスタ用の単一のカスタム証明書で認証を設定する
- Panorama で設定された WildFire アプライアンスにカスタム証明書を適用する

Panorama の管理対象の WildFire アプライアンスのカスタム証明書を設定する

Panorama™を使用して WildFire® アプライアンスまたは WildFire クラスタを管理する場合は、WildFire アプライアンス CLI ではなく、Panorama Web インターフェイスを使用してカスタム証明書認証を設定できます。またファイアウォールまたは Panorama では、この接続を使用して分析のためにサンプルを WildFire に転送します。

この手順では、単一の WildFire アプライアンスに一意の証明書をインストールする方法について説明します。WildFire アプライアンスがクラスタの一部である場合、そのデバイスと各クラスタ メンバーには一意のクライアント証明書があります。クラスタ内のすべての WildFire アプライアンスに単一の証明書をデプロイする方法については、WildFire クラスタの単一のカスタム証明書による認証設定を参照してください。

STEP 1 | WildFire およびファイアウォール用のキーペアと認証局（CA）証明書を取得します。

STEP 2 | ファイアウォールの識別情報と Wildfire アプライアンスのキーペアを検証するために CA 証明書をインポートします。

1. **Panorama** > **Certificate Management**（ 証明書の管理 ） > **Certificates**（ 証明書 ） > **Import**を選択します。
2. Panorama で CA 証明書とキーペアをインポートします。

STEP 3 | ルート CA および中間 CA が含まれる証明書プロファイルを設定します。この証明書プロファイルは、WildFire アプライアンスとファイアウォールの相互認証方法を定義します。

1. **Panorama** > **Certificate Management**（証明書の管理） > **Certificate Profile**（証明書プロファイル）の順に選択します。
2. 証明書プロファイルの設定を行います。

   証明書プロファイルの一部として中間 CA を設定する場合、ルート CA も含める必要があります。

STEP 4 | WildFire アプライアンスの SSL/TLS プロファイルを設定します。

© 2019 Palo Alto Networks, Inc.

PAN-OS 8.0 以降のリリースでは *TLS 1.2* 以上しかサポートされないため、最大バージョンを*TLS 1.2* または*max*（最大）設定する必要があります。

1. **Panorama** > **Certificate Management**（証明書の管理） > **SSL/TLS Service Profile**（**SSL/TLS** サービス プロファイル）の順に選択します。
2. SSL/TLS サービス プロファイルを設定し、WildFire アプライアンスおよびそのファイアウォールが SSL/TLS サービスに使用する証明書およびプロトコルを定義します。

STEP 5 | WildFire で保護されたサーバー通信を設定します。

1. **Panorama** > **Managed WildFire Clusters (**管理された **WildFire** クラスター)または **Panorama** > **Managed WildFire Clusters (**管理された **WildFire** クラスター)を選択して、クラスタまたはアプライアンスを選択します。
2. **Communication**（通信）を選択します。
3. **Customize Secure Server Communication**（セキュリティで保護されたサーバー通信のカスタマイズ）機能を有効にします。
4. **SSL/TLS Service Profile**（**SSL/TLS** サービスプロファイル）を選択します。この SSL/TLS サービス プロファイルは、WildFire アプライアンスとファイアウォールまたは Panorama 間のすべての SSL 接続に適用されます。
5. WildFire アプライアンスとファイアウォールまたは Panorama 間の通信用に設定した**Certificate Profile**（証明書プロファイル）を選択します。
6. **Custom Certificate Only**（カスタム証明書のみ）が無効（チェックボックスがオフ）になっていることを確認します。これにより、WildFire アプライアンス はカスタム証明書に移行する際に事前定義された証明書でファイアウォールとの通信を継続できます。
7. （任意）認証リストを設定します。
   1. Authorization List（承認リスト）を **Add**（追加）します。
   2. 識別子タイプとして証明書プロファイルで設定した **Subject**（サブジェクト）または **Subject Alt Name**（サブジェクト代替名）を選択します。
   3. 識別子が Subject（サブジェクト）の場合は Common Name（共通名（CN））を入力するか、識別子が Subject Alt Name（サブジェクト代替名）の場合は IP アドレス、ホスト名、または電子メール アドレスを入力します。
   4. **OK** をクリックします。
   5. **Check Authorization List**（承認リストのチェック）を有効にしてリストを適用します。
8. **OK** をクリックします。
9. 変更を **Commit (**コミット)します。

STEP 6 | CA 証明書をインポートして WildFire アプライアンス の証明書を検証します。

1. ファイアウォール インターフェイスにログインします。
2. 証明書をインポートします。

STEP 7 | ファイアウォールのローカル証明書または SCEP 証明書を設定します。

- ローカル証明書を使用している場合は、ファイアウォールのキーペアをインポートします。
- ファイアウォールの証明書に SCEP を使用している場合は、SCEP プロファイルを設定します。

STEP 8 | ファイアウォールまたは Panorama の プロファイルを設定します。このプロファイルは、各クライアント ファイアウォールまたは Panorama アプライアンスで個別に設定することも、テンプレートを使用して Panorama から管理対象ファイアウォールに設定をプッシュすることもできます。

1. ファイアウォールの場合は **Device**（デバイス） > **Certificate Management**（証明書の管理） > **Certificate Profile**（証明書プロファイル）を選択し、また、Panorama の場合は **Panorama** >

© 2019 Palo Alto Networks, Inc.

Certificate Management（証明書の管理）> **Certificate Profile**（証明書プロファイル）を選択します。
2. 証明書プロファイルの設定を行います。

STEP 9 | 各ファイアウォールまたは Panorama アプライアンスにカスタム証明書をデプロイします。
1. ファイアウォール インターフェイスにログインします。
2. ファイアウォールの場合は **Device**（デバイス）> **Setup**（セットアップ）> **Management**（管理）を、Panorama の場合は **Panorama** > **Setup**（セットアップ）> **Management**（管理）を選択し、セキュア通信を **Edit**（編集）します
3. **Certificate Type**（証明書タイプ）、**Certificates**（証明書）、または**Certificate Profile**（証明書プロファイル）を選択します。
4. カスタマイズ通信設定で、**WildFire Communication**（**WildFire** 通信）を設定します。
5. **OK** をクリックします。
6. 変更を **Commit** (コミット)します。

STEP 10 | すべての管理対象のデバイスにカスタム証明書をデプロイした後で、カスタム証明書認証を適用します。
1. Panoramaにログインします。
2. **Panorama** > **Managed WildFire Clusters** (管理された **WildFire** クラスター)または **Panorama** > **Managed WildFire Clusters** (管理された **WildFire** クラスター)を選択して、クラスタまたはアプライアンスを選択します。
3. **Communication**（通信）を選択します。
4. **Custom Certificate Only**（カスタム証明書のみ）を選択します。
5. **OK** をクリックします。
6. 変更を **Commit** (コミット)します。

この変更をコミットすると、WildFire はカスタム証明書の適用を直ちに開始します。

WildFire クラスタ用の単一のカスタム証明書で認証を設定する

クラスタ内の各 WildFire アプライアンスに一意の証明書を割り当てる代わりに、単一の共有クライアント証明書を WildFire クラスタ全体に割り当てることができます。これにより、クラスタメンバーごとに個別の証明書を構成するのではなく、単一の証明書をクラスタ内のすべての WildFire アプライアンスにプッシュすることができます。個々の WildFire アプライアンスはクライアント証明書を共有するため、各 WildFire アプライアンスに固有のホスト名（DNS 名）を設定する必要があります。その後、すべてのホスト名を証明書属性として共有証明書に追加するか、クラスタ内のすべての WildFire アプライアンスのすべてのカスタムホスト名に一致する 1 ワイルドカード文字列を使用できます。

Panorama™と通信するときに使用する WildFire クラスタ用の単一のカスタム証明書を設定するには、次の手順を実行します。

STEP 1 | Panorama のサーバー キーペアと CA 証明書を取得します。

STEP 2 | ルート認証局（CA）および中間 CA が含まれる証明書プロファイルを設定します。この証明書プロファイルは、WildFire クラスタ（クライアント）と Panorama アプライアンス（サーバー）間の認証を定義します。
1. **Panorama** > **Certificate Management**（証明書の管理）> **Certificate Profile**（証明書プロファイル）の順に選択します。
2. 証明書プロファイルの設定を行います。

   証明書プロファイルの一部として中間 CA を設定する場合、ルート CA も含める必要があります。

STEP 3 | SSL/TLS サービス プロファイルの設定を行います。

© 2019 Palo Alto Networks, Inc.

1. **Panorama** > **Certificate Management**（証明書の管理）> **SSL/TLS Service Profile**（**SSL/TLS** サービス プロファイル）の順に選択します。
2. SSL/TLS サービス プロファイルを設定し、WildFire クラスタおよび Panorama アプライアンスが SSL/TLS サービスに使用する証明書およびプロトコルを定義します。

STEP 4 | クラスタ内の各ノードを Panorama に接続します 。

STEP 5 | クラスタ内の各ノードで一意のホスト名（DNS 名）を設定するか、クラスタ内の WildFire アプライアンスに設定されているすべてのカスタム DNS 名と一致するシングル ワイルドカードを含む文字列を使用します。

シングル ワイルドカード文字列を使用する場合は、ワイルドカード文字列値の要件と制限についてRFC-6125 のセクション 6.4.3 を参照してください。カスタム DNS 名を設定するときは、これらの要件と制限事項をご理解ください。

1. ノードの WildFire CLI にログインします。
2. 次のコマンドを使用して、ノードに固有のカスタム DNS 名を割り当てます。

```
admin@WF-500> configure
```

```
admin@WF-500# set deviceconfig setting wildfire custom-dns-name <dns-name>
```

3. 変更を **Commit**（コミット）します。
4. クラスタ内の各ノードの手順を繰り返します。

STEP 6 | Panorama で、クラスタ内のすべてのノードの クライアント証明書を作成します。証明書の属性で、クラスタ ノードに割り当てたカスタム DNS 名ごとにホスト名エントリを追加するか、「* .example.com」などのすべてのノード ホスト名に一致する 1 つのワイルドカード文字列を 1 つのホスト名エントリに追加します。各カスタム DNS 名が共通の文字列を共有する場合にのみこれを実行できます。

STEP 7 | Panorama で、クライアント証明書の証明書プロファイルを設定します。

1. Panorama に対して **Panorama** > **Certificate Management**（証明書の管理）> **Certificate Profile**（証明書プロファイル）の順に選択します。
2. 証明書プロファイルの設定を行います。

STEP 8 | 各ノードにカスタム証明書を展開します。この証明書プロファイルには、Panorama サーバー証明書に署名した CA 証明書が含まれている必要があります。

1. **Panorama** > **Managed WildFire Clusters**（管理対象 **WildFire** クラスタ）の順に選択し、クラスタ名を選択します。
2. **Communication**（通信）を選択します。
3. セキュア クライアント設定で、**Certificate Type**（証明書タイプ）、**Certificates**（証明書）、**Certificate Profile**（証明書プロファイル）を選択します。
4. **OK** をクリックします。
5. 変更を **Commit** (コミット) します。

STEP 9 | Panorama で保護されたサーバー通信を設定します。

1. **Panorama** > **Setup** > **Management**（管理）と **Edit**（編集）を選択して、**Customize Secure Server Communication**（セキュリティで保護されたサーバー通信のカスタマイズ）を選択します。
2. **Customize Secure Server Communication**（保護されたサーバー通信のカスタマイズ）を有効化します。

© 2019 Palo Alto Networks, Inc.

3. **SSL/TLS Service Profile**（**SSL/TLS** サービスプロファイル）を選択します。この SSL/TLS サービスプロファイルは、WildFire と Panorama 間のすべての SSL 接続に適用されます。
4. Panorama の **Certificate Profile**（証明書プロファイル）を選択します。
5. **Custom Certificate Only**（カスタム証明書のみ）を有効化します。
6. **OK** をクリックします。
7. 変更を **Commit (コミット)** します。

Panorama で設定された WildFire アプライアンスにカスタム証明書を適用する

デフォルトでは、Panorama™ は WildFire® アプライアンスと通信して設定をプッシュする際に事前定義済みの証明書を使用します。あるいは、カスタム証明書を、Panorama が管理対象の WildFire アプライアンスまたはクラスタに設定をプッシュするために使用する接続の相互認証を確立するように設定します。Panorama でサーバー証明書を、WildFire アプライアンスでクライアント証明書を設定するには、次の手順を実行します。

STEP 1 | Panorama およびWildFire アプライアンスのためのキーペアと認証局（CA）証明書を取得します。

STEP 2 | Wildfire アプライアンスの識別情報と Panorama のキーペアを検証するために CA 証明書をインポートします。

1. **Panorama** > **Certificate Management**（ 証明書の管理 ）> **Certificates**（ 証明書 ）> **Import**を選択します。
2. Panorama で CA 証明書とキーペアをインポートします。

STEP 3 | ルート CA および中間 CA が含まれる証明書プロファイルを設定します。この証明書プロファイルは、WildFire アプライアンス（クライアント）と Panorama バーチャル アプライアンスまたは M-Series アプライアンス（サーバー）間の認証を定義します。

1. **Panorama** > **Certificate Management**（証明書の管理）> **Certificate Profile**（証明書プロファイル）の順に選択します。
2. 証明書プロファイルの設定を行います。

   証明書プロファイルの一部として中間 CA を設定する場合、ルート CA も含める必要があります。

STEP 4 | SSL/TLS サービス プロファイルの設定を行います。

1. **Panorama** > **Certificate Management**（証明書の管理）> **SSL/TLS Service Profile**（**SSL/TLS** サービス プロファイル）の順に選択します。
2. SSL/TLS サービス プロファイルを設定し、WildFire および Panorama アプライアンスが SSL/TLS サービスに使用する証明書およびプロトコルを定義します。

STEP 5 | Panorama アプライアンスでセキュア サーバー通信を設定します。

1. **Panorama** > **Setup** > **Management**（管理）と **Edit**（編集）を選択して、**Customize Secure Server Communication**（セキュリティで保護されたサーバー通信のカスタマイズ）を選択します。
2. **Customize Secure Server Communication**（セキュリティで保護されたサーバー通信のカスタマイズ）機能を有効にします。
3. **SSL/TLS Service Profile**（**SSL/TLS** サービスプロファイル）を選択します。
4. **Certificate Profile**（証明書プロファイル）ドロップダウンから証明書プロファイルを選択します。
5. **Custom Certificate Only**（カスタム証明書のみ）が無効（チェックボックスがオフ）になっていることを確認します。これにより、Panorama はカスタム証明書に移行する際に事前定義された証明書で WildFire との通信を継続できます。
6. （任意）認証リストを設定します。

© 2019 Palo Alto Networks, Inc.

1. Authorization List（承認リスト）を **Add**（追加）します。
2. 識別子タイプとして証明書プロファイルで設定した **Subject**（サブジェクト）または **Subject Alt Name**（サブジェクト代替名）を選択します。
3. 識別子が `Subject`の場合は **Common Name**（共通名（**CN**））を入力し、識別子が `Subject Alt Name` の場合は **IP address**（**IP** アドレス）、**hostname**（ホスト名）、または**email**（電子メール アドレス）を入力します。
4. **OK** をクリックします。
5. **Check Authorization List**（承認リストのチェック）オプションを有効にして、Panorama が承認リストを適用するように設定します。

7. **OK** をクリックします。
8. 変更を **Commit** (コミット)します。

STEP 6 | CA 証明書をインポートして Panorama のキーペアを検証します。

1. Panorama ユーザー インターフェイスにログインします。
2. 証明書をインポートします。

STEP 7 | WildFire アプライアンスのローカル証明書または SCEP 証明書を設定します。

1. ローカル証明書を使用している場合は、WF-500 アプライアンスのキーペアをインポートします。
2. WildFire アプライアンスの証明書に SCEP を使用している場合は、SCEP プロファイルを設定します。

STEP 8 | WildFire アプライアンスの証明書プロファイルを設定します。

1. **Panorama** > **Certificate Management**（証明書の管理）> **Certificate Profile**（証明書プロファイル）の順に選択します。
2. 証明書プロファイルの設定を行います。

STEP 9 | 管理対象の各 WildFire アプライアンスにカスタム証明書をデプロイします。

1. Panoramaにログインします。
2. **Panorama** > **Managed WildFire Appliances**（管理対象 **WildFire** アプライアンス）の順に選択し、クラスタまたはアプライアンス名を選択します。
3. **Communication**（通信）を選択します。
4. セキュア クライアント設定で、それぞれのドロップダウン リストから **Certificate Type**（証明書タイプ）、**Certificates**（証明書）、**Certificate Profile**（証明書プロファイル）を選択します。
5. **OK** をクリックします。
6. 変更を **Commit** (コミット)します。

STEP 10 | すべての管理対象の WildFire アプライアンスにカスタム証明書をデプロイした後で、カスタム証明書認証を適用します。

1. **Panorama** > **Setup**（セットアップ）> **Management**（管理）の順に選択し、セキュア通信設定を **Edit**（編集）します。
2. **Allow Custom Certificate Only**（カスタム証明書のみを許可）します。
3. **OK** をクリックします。
4. 変更を **Commit** (コミット)します。

この変更をコミットすると、切断待機時間カウントダウンが開始されます。待機時間が終了すると、Panorama およびその管理対象の WildFire アプライアンスは、設定された証明書なしでは接続できません。

© 2019 Palo Alto Networks, Inc.

Panorama 管理からの WildFire アプライアンスの削除

Panorama 管理から WildFire スタンドアロン アプライアンスを削除できます。WildFire スタンドアロン アプライアンスを Panorama 管理から削除すると、一元管理の利益を得ることはできなくなり、ローカル CLI とスクリプトを使用して、そのアプライアンスを管理することになります。

STEP 1 | **Panorama** > **Managed WildFire Appliances**（管理対象 **WildFire** アプライアンス）の順に選択します。

STEP 2 | 各アプライアンスのチェックボックスをオンにするか、アプライアンスの行をクリックし、Panorama 管理から削除する WildFire アプライアンス（複数可）を選択します。

STEP 3 | 選択した WildFire アプライアンスを Panorama 管理から **Remove**（削除）します。

© 2019 Palo Alto Networks, Inc.

WildFire クラスタの管理

WildFireアプライアンスクラスタは、サンプル分析とストレージ容量を増やし、より大きなファイアウォールグループをサポートし、複数のWildFireアプライアンスの設定と管理を簡素化するためにリソースをプールする、WildFireアプライアンスの相互接続グループです。セキュリティを強化し、送信されるコンテンツの機密性を維持するために、クラスタ内の WildFire アプライアンス間の通信を暗号化することもできます。WildFire クラスタおよびデプロイメント プロセスの詳細については、 WildFireアプライアンス クラスタを参照してください。

Panorama を使用して WildFire クラスタを管理するために次のタスクを実行できます。

- Panoramaで集中的にクラスタを構成する
- PanoramaをWildFireクラスタのステータスの表示
- インターネット接続を使用してクラスタをセンターでアップグレードする
- インターネット接続を使用してクラスタをセンターでアップグレードする
- Panorama で集中的に定義済みの証明書を使用したアプライアンス間暗号化の設定
- Panorama で集中的にカスタム証明書を使用したアプライアンス間暗号化の設定

Panoramaで集中的にクラスタを構成する

Panorama Mシリーズまたは仮想アプライアンスにWildFireアプライアンスクラスタを設定する前に、高可用性コントローラノードのペアとして設定できる2つのWildFireアプライアンスと、クラスタの分析、ストレージ容量、および復元力を高めるワーカーノードとして機能するために必要な追加のWildFireアプライアンスを用意してください。

WildFireアプライアンスが新しい場合は、 WildFireで始動する をチェックして、WildFireライセンスの有効性の確認、ログの有効化、ファイアウォールのWildFireアプライアンスへの接続、基本的なWildFire機能の設定などの基本手順を完了させます。

*WildFire*アプライアンスクラスタを作成するには、クラスタに配置するすべてのWildFireアプライアンスをPAN-OS 8.0.1以降にアップグレードする必要があります。*Panorama*を使用して*WildFire*アプライアンスクラスタを管理する場合、*Panorama*は*PAN-OS 8.0.1*以降を実行する必要があります。クラスタに追加する各*WildFire*アプライアンスで、システム情報の表示 | バージョンの一致を実行します。 *WildFire*アプライアンスの*CLI*でバージョンと一致し、アプライアンスが*PAN-OS 8.0.1*以降を実行していることを確認します。クラスタ (またはスタンドアロンアプライアンス)の管理に使用する各*Panorama* アプライアンスでは、*Dashboard* (ダッシュボード) > *General Information* (一般情報) > *Software Version* (ソフトウェアバージョン) が実行中のソフトウェアバージョンを表示します。

WildFireアプライアンスが使用可能になったら、適切なタスクを実行します。

- Panoramaにクラスタを設定してノードを追加する
- Panoramaの一般的なクラスタ設定を構成する
- WildFire クラスタの認証の設定
- Panoramaの管理からクラスタを削除する

*Panorama*を使用したクラスタからのノードの削除には対応していません。代わりに、ローカルの*WildFire CLI*を使用してRemove a Node from a Cluster Locally (ローカルでクラスタからノードを削除) します 。

© 2019 Palo Alto Networks, Inc.

*Panorama*にクラスタを設定してノードを追加する

PanoramaからWildFireアプライアンスクラスタを設定する前に、upgrade Panorama to 8.0.1（Panoramaを8.0.1以降にアップグレード）し、クラスタに追加するupgrade all WildFire appliances（すべてのWildFireアプライアンスを8.0.1以降にアップグレードする）必要があります。すべてのWildFireアプライアンスは、同じバージョンのPAN-OSを実行する必要があります。

Panorama M-Series またはバーチャル アプライアンスでは、最大 200 台の WildFire アプライアンスを管理できます。200 WildFireアプライアンスの上限は、スタンドアロンアプライアンスとWildFireアプライアンスのクラスタノードを合計したものです(Add Standalone WildFire Appliances to Manage with Panorama（パノラマで管理するスタンドアロンWildFireアプライアンスを追加する）場合も同様です)。特に明記されている場合を除き、設定はPanoramaで行われます。

各*WildFire*アプライアンスのクラスタノードには、同じサブネット内に静的*IP*アドレスが設定され、低レイテンシ接続が設定されている必要があります。

STEP 1 | ローカルCLIを使用して、WildFireアプライアンスクラスタを管理するPanoramaサーバのIPアドレスを設定します。

クラスタまたはスタンドアロンのWildFireアプライアンスをPanoramaアプライアンスに登録する前に、まずWildFire CLIを使用して各WildFireアプライアンスにPanorama IPアドレスまたはFQDNを設定する必要があります。この設定により、各 WildFire アプライアンスは、どの Panorama アプライアンスによって管理されるかを認識するようになります。

1. 各WildFireアプライアンスで、主要なPanoramaアプライアンスの管理インターフェイスのIPアドレスまたはFQDNを設定します。

```
admin@WF-500# set deviceconfig system panorama-server <ip-address | FQDN>
```

2. 各WildFireアプライアンスで、高可用性のためにバックアップPanoramaアプライアンスを使用する場合（推奨）、バックアップPanoramaアプライアンスの管理インターフェイスのIPアドレスまたはFQDNを設定します。

```
admin@WF-500# set deviceconfig system panorama-server-2 <ip-address |
 FQDN>
```

3. 各WildFireアプライアンスで設定を確定します。

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

STEP 2 | プライマリパノラマアプライアンスで、WildFireアプライアンスを登録します。

新しく登録されたアプライアンスは、ローカルクラスタ設定のためにすでにクラスタに属していない限り、スタンドアロンモードです。

1. **Panorama** > **Managed WildFire Appliances**（管理された**WildFire** アプライアンス）および**Add Appliance**（アプライアンスを追加）を選択します。
2. 各 WildFire アプライアンスのシリアル番号を別々の行に入力します。ローカルCLIを使用してWildFireアプライアンスのシリアル番号のリストがない場合は、各WildFireアプライアンスで**show system info**（システム情報を表示）を実行してシリアル番号を入手してください。
3. **OK** をクリックします。

   IP アドレスやソフトウェア バージョンなど、WildFire アプライアンスですでにコミットされている設定に関する情報が、利用可能な場合は表示されます。すでにクラスタに属しているWildFireアプライアンス（たとえば、ローカルクラスタ設定のため）は、クラスタ情報と接続ステータスを表示します。

© 2019 Palo Alto Networks, Inc.

STEP 3 | （任意）WildFire アプライアンスの設定を Panorama アプライアンスにインポートします。

設定をインポートすると、Panoramaの設定を再利用または編集してから、1つ以上のWildFireアプライアンスクラスタまたはスタンドアロンのWildFireアプライアンスにプッシュすることができるため、時間が節約されます。インポートする設定がない場合は、この手順をスキップしてください。パノラマから設定をプッシュすると、プッシュされた設定はローカル設定を上書きします。

1. **Panorama** > **Managed WildFire Appliances**（管理された**WildFire** アプライアンス）を選択し、管理対象のWildFireアプライアンスのリストからインポートする設定のアプライアンスを選択します。
2. **Import Config**（設定のインポート）を選択します。
3. **Yes**（はい）を選択します。

   設定をインポートすると、表示される情報が更新されて、インポートした設定が Panorama アプライアンスの候補設定の一部になります。
4. **Commit to Panorama**（**Panorama** へのコミット）を選択し、インポートした WildFire アプライアンスの設定を Panorama の実行中の設定にします。

STEP 4 | 新しいWildFireアプライアンスクラスタを作成します。

1. **Managed WildFire Clusters**（管理された**WildFire**クラスター）を選択してください。

   Appliance (アプライアンス) > **No Cluster Assigned (割り当てられたクラスタなし)**はスタンドアロンのWildFireアプライアンス（ノード）を表示し、クラスタに割り当てられていないノード数を示します。
2. **Create Cluster**（クラスタの作成）。
3. 英数字のクラスタ**Name**（名）を入力します。最大63文字まで入力できます。**Name**（名前）には、小文字の文字と数字、ハイフンとピリオドが含まれています（最初の文字または最後の文字でない場合）。スペースやその他の文字は使用できません。
4. **OK** をクリックします。

   新しいクラスタ名が表示されますが、割り当てられたWildFireノードはありません。

STEP 5 | WildFireアプライアンスを新しいクラスタに追加します。

クラスタに追加された最初のWildFireアプライアンスは自動的にコントローラノードになり、クラスタに追加された2番目のWildFireアプライアンスは自動的にコントローラのバックアップノードになります。以降のクラスタに追加されたWildFireアプライアンスはすべてワーカーノードになります。ワーカーノードはコントローラノード設定を使用して、クラスタが一貫した構成を持つようにします。

1. 新しいクラスタを選択します。
2. **Clustering**（クラスタリング）を選択します。
3. クラスタに属していないWildFireアプライアンスのリストを**Browse**（閲覧）します。
4. クラスタに追加する各WildFireアプライアンス(⊕)を追加します。最大で 20 個の ノードをクラスタに追加できます。クラスタに追加する各WildFireアプライアンスは、自動的に割り当てられたロールとともに表示されます。
5. **OK** をクリックします。

STEP 6 | **Management**（管理）、**Analysis Environment Network**（分析環境のネットワーク）、HA、およびクラスタ管理インターフェイスを構成します。

Management（管理）、**Analysis Environment Network**（分析環境のネットワーク）、まだ構成されていない場合は、各クラスタメンバー（コントローラおよびワーカーノード）の管理、分析環境ネットワーク、およびクラスタ管理インターフェイスを構成します。クラスタ管理インターフェイスは、クラスタ内での管理と通信のための専用インターフェイスであり、管理インターフェイスとは異なります。

© 2019 Palo Alto Networks, Inc.

コントローラノードとコントローラバックアップノードの両方で、HAインターフェイスを個別に設定します。HAインターフェイスは、プライマリコントローラとバックアップコントローラのノードを接続し、フェールオーバーに応答する準備ができて同期可能にします。

クラスタノードには、*4*つの*WildFire*アプライアンスインターフェイスのそれぞれに*IP*アドレスが必要です。ワーカーノードで*HA*サービスを構成することはできません。

1. 新しいクラスタを選択します。
2. **Clustering**（クラスタリング）を選択します。
3. 管理インターフェイスがクラスタノード上に設定されていない場合は、**Interface Name** (インターフェース名) > **Management** (管理)を選択し、インターフェイスのIPアドレス、ネットマスク、サービス、およびその他の情報を入力します。
4. 分析環境ネットワークのインターフェイスがクラスタノード上に構成されていない場合は、**Interface Name** (インターフェース名) > **Analysis Environment Network** (環境ネットワーク分析)を選択し、インターフェイスのIPアドレス、ネットマスク、サービス、およびその他の情報を入力します。
5. コントローラノードとコントローラバックアップノードの両方で、HA制御リンクに使用するインタフェースを選択します。Haサービスの両方のコントローラノードで同じインターフェイスを設定する必要があります。たとえば、コントローラノードでコントローラバックアップノードで**Ethernet3**を選択します。
6. 各コントローラー・ノードに対して、**Clustering Services** (クラスタリングサービス) > **HA**を選択します。（**HA** オプションはワーカーノードでは使用できません）。 また、インターフェイスにpingを実行する機能が必要な場合は、**Management Services** (管理サービス) > **Ping**を選択します。
7. **OK** をクリックします。
8. （推奨）コントローラノードとコントローラバックアップノード間のバックアップHA制御リンクとして使用するインタフェースを選択します。HAバックアップサービスでは、両方のノードで同じインタフェースを使用する必要があります。たとえば、両方のノードで**Management**（管理）を選択します。

   両方のノードの**Clustering Services** (クラスタリングサービス) > **HA Backup** (バックアップ)を選択します。これらの**Management Services**（管理サービス）をインターフェイスに追加する場合は**Ping**、**SSH**、および**SNMP**を選択することもできます。

   Analysis Environment Network（分析環境ネットワーク）インターフェイスは、*HA*または*HA*バックアップインターフェイスまたはクラスタ管理インターフェイスにすることはできません。
9. クラスタ内の管理と通信に使用する専用インタフェースを選択します。両方のノードで同じインターフェイスを使用する必要があります（たとえば、**Ethernet2**）。
10. 両方のノードの**Clustering Services** (クラスタリングサービス) > **HA Cluster Management** (HAクラスター管理)を選択します。また、インターフェイスにpingを実行する機能が必要な場合は、**Management Services** (管理サービス) > **Ping**を選択します。

    クラスタ内のワーカーノードは、専用の管理および通信インタフェース用のコントローラノードの設定を自動的に継承します。

STEP 7 | Panoramaアプライアンスで設定をコミットし、クラスタにプッシュします。

1. **Commit and Push**（コミットしてプッシュ）を選択します。
2. プッシュしない設定が Panorama アプライアンスにある場合は、**Edit Selections**（選択内容の編集）によって、設定のプッシュ先のアプライアンスを選択します。プッシュされた構成は、クラスタノードの実行コンフィギュレーションを上書きし、すべてのクラスタノードが同じ構成で実行されるようにします。

STEP 8 | 設定を確認します。

© 2019 Palo Alto Networks, Inc.

1. **Panorama** > > **Managed WildFire Clusters**（管理WildFire クラスター）を選択。
2. 次のフィールドを確認します。
   - **Appliance**（アプライアンス）—スタンドアロンアプライアンスとして表示する代わりに、クラスタに追加されたWildFireノードはクラスタ名で表示されます。
   - **Cluster Name**（クラスター名）—各ノードのクラスタ名が表示されます。
   - **Role**（役割）—各ノードの適切なロール（、、または(**Controller**（コントローラ）、**Controller Backup**（コントローラバックアップ）、または**Worker**（ワーカー））が表示されます。
   - **Config Status**（設定状態）— 状態が `In Sync` である。
   - **Last Commit State**（最終コミット状態）— `Commit succeeded` である。

STEP 9 | （Panorama Webインターフェイスではなく）プライマリコントローラノードでローカルCLIを使用して、設定が同期していることを確認します。

それらが同期されていない場合は、コントローラーノードの高可用性構成を手動で同期させ、構成をコミットします。

Panoramaで他のほとんどの設定を行うことはできますが、コントローラノードの高可用性設定を同期させるには、プライマリコントローラノードのCLIで行う必要があります。

1. プライマリコントローラノードで、設定が同期されていることを確認します。

```
admin@WF-500(active-controller)> show high-availability all
```

出力の最後に、`Configuration Synchronization`（設定の同期）出力を探します）:

```
Configuration Synchronization:
    Enabled: yes
    Running Configuration: synchronized
```

実行中の設定が同期されている場合、手動でコンフィギュレーションを同期する必要はありません。ただし、設定が同期されていない場合は、手動で設定を同期する必要があります。

2. 設定が同期されていない場合は、プライマリコントローラノードで、高可用性設定をリモートピアコントローラノードに同期させます。

```
admin@WF-500(active-controller)> request high-availability sync-to-remote
 running-config
```

プライマリコントローラノードの設定とコントローラバックアップノードの設定が一致しない場合は、プライマリコントローラノードの設定がコントローラバックアップノードの設定を上書きします。

3. 設定をコミットします：

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

Panoramaの一般的なクラスタ設定を構成する

一部の一般的な設定はオプションで、一部の一般的な設定はデフォルト値であらかじめ設定されています。少なくとも、これらの設定をチェックして、クラスタ構成がニーズに合っていることを確認することが最善です。一般的な設定は次のとおりです。

- WildFireパブリッククラウドに接続し、サンプルをパブリッククラウドに送信する。
- データ保持ポリシーの設定。

© 2019 Palo Alto Networks, Inc.

- ログの設定。
- ファイアウォールがWildFireに送信するサンプルのタイプに最も適した解析環境をカスタマイズし、解析環境を設定する（環境に最も適したVMイメージ）
- DNSサーバ、NTPサーバなどのIPアドレスを設定する。

STEP 1 | WildFireアプライアンスクラスタノードの設定を設定します。

多くの設定には、デフォルト値、コントローラノードの以前の設定値、または設定したばかりの設定のいずれかがあらかじめ設定されています。

1. クラスタを選択します。
2. **Appliance**（アプライアンス）を選択します。
3. 新しい情報を入力するか、事前入力された情報をクラスタコントローラノードから保持するか、事前入力された情報を編集します。
   - **Domain**（ドメイン）名。
   - **Primary DNS Server**（プライマリ **DNS** サーバー）および **Secondary DNS Server**（セカンダリ **DNS** サーバー）の IP アドレス。
   - **NTP Server Address**（サーバーアドレス）および **Primary DNS Server**（プライマリ **DNS** サーバー）および **Secondary DNS Server**（セカンダリ **DNS** サーバー）の**Authentication Type**（認証タイプ）。**Authentication Type**（認証タイプ）オプションは、**None**（なし）、**Symmetric Key**（対称キー）、および**AutoKey**（**AutoKey**）です。

STEP 2 | 一般クラスター設定をする。

多くの設定には、デフォルト値、コントローラノードの以前の設定値、または設定したばかりの設定のいずれかがあらかじめ設定されています。

1. 新しいクラスタ> **General**（一般）を選択します。
2. （オプション）コントローラノードがDNSプロトコルを使用してサービスステータスをアドバタイズするように **Enable DNS**（**DNS**を有効化）します。クラスタコントローラは、管理（MGT）インターフェイスポートでDNSサービスを提供します。
3. **Register Firewall To**（ファイアウォールの登録）し、クラスタコントローラによって通知されたサービスを使用します。Palo Alto Networksは、高可用性の利点を提供するため、両方のコントローラを権限サーバーとして追加することを推奨しています。フォームを使用します。

   ```
   wfpc.service.<cluster-name>.<domain>
   ```

   たとえば、*paloaltonetworks.com*ドメイン内の*mycluster*という名前のクラスタのドメイン名：

   ```
   wfpc.service.mycluster.paloaltonetworks.com
   ```

4. クラスタ用の**Content Update Server**（コンテンツアップデートサーバー）を入力します。最も近いサーバーに接続するには、デフォルトの `updates.paloaltonetworks.com`FQDNを使用します。証明書の共通名（CN）をサーバーの IP アドレスまたは FQDN と照合し、更新サーバーのアイデンティティを確認するには、**Check Server Identity**（サーバー アイデンティティのチェック）を行います。
5. （オプション）公開されている**WildFire Cloud Server**（**WildFire**クラウドサーバ）の場所を入力するか、デフォルトの`wildfire.paloaltonetworks.com`Panorama を使用して、クラスタ（または Panorama によって管理されるスタンドアロンアプライアンス）が最も近い WildFire クラウドサーバに情報を送信できるようにします。このフィールドを空白のままにして、WildFireクラウドサーバに接続しないと、クラスタはWildFireパブリッククラウドから直接シグネチャアップデートを受信することができず、分析のためのサンプルを送信したりパブリッククラウドにデータを提供することができません。

© 2019 Palo Alto Networks, Inc.

6. クラスタをパブリックWildFireクラウドに接続する場合は、有効にするクラウドサービスを選択します。
   - **Send Analysis Data**（分析データの送信）—ローカルマルウェア分析に関するXMLレポートを送信します。実際のサンプルを送信すると、クラスタはレポートを送信しません。
   - **Send Malicious Samples**（悪意のあるサンプルを送信）—マルウェアサンプルを送信します。
   - **Send Diagnostics**（診断送信）—診断データを送信します。
   - **Verdict Lookup**（評決検索）—ローカルの分析を実行してローカルのWildFireアプライアンスクラスタの負荷を軽減する前に、自動的にWildFireパブリッククラウドに判定を問い合わせます。
7. クラスタが分析するサンプルのタイプに基づいて、使用する**Sample Analysis Image**（サンプル分析イメージ）を選択します。
8. クラスタが**Benign/Grayware**（良性/グレーウェア)サンプルデータ（1～90日の範囲、デフォルトは14日）と**Malicious**（悪意のある）サンプルデータ（最小1日、最大（不確定）、デフォルトは不定）を保持する時間を設定します。悪質のあるサンプルデータには、フィッシング判定が含まれます。
9. （オプション）**Preferred Analysis Environment**（優先分析環境）を選択して、環境に応じて**Executables**（実行可能）または**Documents**（ドキュメント）にさらに多くのリソースを割り当てます。**Default**（デフォルト）割り当てでは、**Executables**（実行可能ファイル）と **Documents**（ドキュメント）が均等になります。使用可能なリソース量は、クラスタ内のWildFireノードの数によって異なります。

STEP 3 | プライマリとバックアップのPanoramaサーバが設定されていることを確認してください。

バックアップPanoramaサーバを設定していない場合、バックアップPanoramaサーバを追加することができます。

1. クラスタを選択します。
2. **Appliance**（アプライアンス）を選択します。
3. 集中型クラスタ管理用の高可用性構成を使用している場合、プライマリ**Panorama Server**（**Panorama**サーバー）とバックアップ**Panorama Server 2**（**Panorama**サーバ - **2**）のIPアドレスまたはFQDNを確認（または入力）します。

STEP 4 | （オプション）ログ転送を含む、クラスタのシステムおよび構成ログの設定を構成します。

1. クラスタを選択します。
2. **Logging**（ロギング）を選択します。
3. **System**（システム）または**Configuration**（設定）を選択して、それぞれシステムまたは構成ログを構成します。それらを構成するプロセスも同様です。
4. ログ転送インスタンスを**Add**（追加）（⊕）および 名前 を付け、**Filter**（フィルタ）を選択し、**Forward Method**（転送方法）（**SNMP**、**Email**（Eメール）、**Syslog**、または**HTTP**）を設定します。

STEP 5 | 管理者認証を構成します。

1. クラスタを選択します。
2. **Authentication**（認証）を選択します。
3. **None**（なし）または**radius**（半径）のいずれかの**Authentication Profile**（認証プロファイル）を選択します。サポートされている外部認証方法はRADIUSのみです。
4. 管理ユーザーの**Local Authentication**（ローカル認証）モードを**Password**（パスワード）または**Password Hash**（パスワードハッシュ）に設定し、**Password**（パスワード）を入力します。

STEP 6 | Panoramaアプライアンスで設定をコミットし、クラスタにプッシュします。

1. **Commit and Push**（コミットしてプッシュ）を選択します。
2. プッシュしない設定が Panorama アプライアンスにある場合は、**Edit Selections**（選択内容の編集）によって、設定のプッシュ先のアプライアンスを選択します。プッシュされた構成は、クラス

© 2019 Palo Alto Networks, Inc.

タノードの実行コンフィギュレーションを上書きし、すべてのクラスタノードが同じ構成で実行されるようにします。

WildFire クラスタの認証の設定

きめ細かな認証パラメータが設定されたローカルの管理者ユーザーを設定する、ならびに承認および認証用の RADIUS、TACAS+、または LDAP を活用することにより、WildFire クラスタ内のすべての WildFire アプライアンス用に強化された認証を作成し、設定します。

Panorama から管理者を設定してプッシュする際は、WildFire クラスタ内のすべての WildFire アプライアンスの既存の管理者を、Panorama で設定した管理者で上書きします。

- WildFire クラスタの管理者アカウントの設定
- WildFire クラスタの RASIUS 認証の設定
- WildFire クラスタの TACACS+ 認証の設定
- WildFire クラスタの LDAP 認証の設定

WildFire クラスタの管理者アカウントの設定

Panorama™ 管理サーバーから WildFire クラスタ内で管理するすべての WildFire アプライアンスの詳細な認証パラメーターを使用して1人以上の管理者を作成します。さらに、WildFire アプライアンスの CLI で直接設定可能な Panorama からローカル管理者を設定できます。ただし、新しい構成の変更を専用の WildFire アプライアンスにプッシュすると、ローカル管理者が WildFire アプライアンス用に設定された管理者で上書きされます。

STEP 1 | Panorama Web インターフェイスへのログイン.

STEP 2 | Panoramaで集中的にクラスタを構成する.

STEP 3 | (任意) 認証プロファイルを設定して、WildFire アプライアンス CLI にアクセスする管理者のログイン資格情報を検証する認証サービスを定義します。

STEP 4 | 必要に応じて、1つ以上の管理者アカウントを設定します。

Panorama で作成された管理者アカウントは、後でWildFire クラスタ内の WildFire アプライアンスにインポートされ、Panorama で管理されます。

STEP 5 | WildFire クラスタ内の WildFire アプライアンスの認証の設定

1. **Panorama** > **Managed WildFire Clusters**（管理対象 **WildFire** クラスタ）の順に選択し、以前に選択した WildFire クラスタを選択します。
2. (任意) 前のステップで設定した **Authentication Profile** (認証プロファイル) を選択します。
3. WildFire アプライアンスに対して認証の **Timeout Configuration** (タイムアウト設定) を構成します。
    1. ユーザーが WildFire アプライアンス CLI からロックアウトされるまでの **Failed Attempt** (試行失敗回数) の数を入力します。
    2. **Lockout Time** (ロックアウト時間) を分単位で入力します。WildFire アプライアンス は、ユーザーが設定された数の試行失敗回数に達すると、ユーザー アカウントをロックアウトします。
    3. アクティブではないユーザー アカウントが自動的にログアウトされるまでの時間である、**Idle Timeout** (待機タイムアウト) を分単位で入力します。
    4. WildFire アプライアンス に同時にアクセスできるユーザー アカウントの数を設定するには、**Max Session Count** (最大セッション カウント) を入力します。
    5. 管理者が自動的にログアウトする前にログインできる**Max Session Time** (最大セッション時間) を入力します。
4. WildFire アプライアンス管理者を追加します。

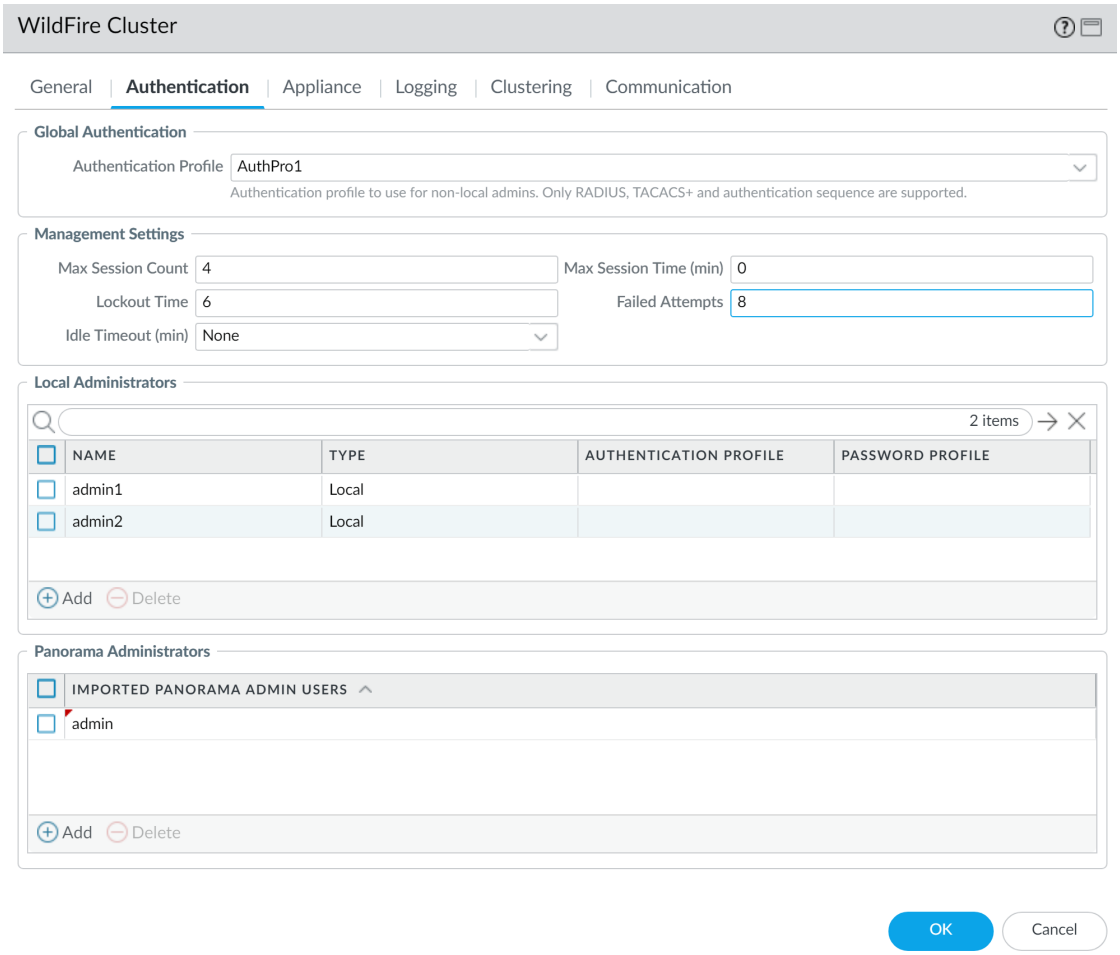
    管理者は、ローカル管理者またはインポートされた Panorama 管理者のいずれかとして追加できますが、両方を追加することはできません。ローカル管理者とインポートされた Panorama 管理者

© 2019 Palo Alto Networks, Inc.

の両方として同じ管理者を追加することはサポートされておらず、Panorama コミットが失敗します。例えば、**admin1** をローカル管理者と Panorama 管理者の両方として追加する場合、Panorama へのコミットは失敗します。

1. WildFire クラスタ内の WildFire アプライアンスに固有の新しい管理者を**Add** (追加) して設定します。これらの管理者は、それらが作成された WildFire クラスタ内の WildFire アプライアンスに固有であり、この表からこれらの管理者を管理します。
2. Panorama で設定された管理者を **Add** (追加) します。これらの管理者は Panorama で作成され、WildFire クラスタ内のアプライアンスにインポートされます。

5. **OK** をクリックすると、WildFire クラスタ認証設定を保存します。



STEP 6 | 設定の変更を **Commit** (コミット) してから、**Commit and Push** (コミットしてプッシュ) します。

STEP 7 | WildFire アプライアンス CLI にアクセスして、ローカルの管理者ユーザーを使用して WildFire アプライアンスにアクセスできることを確認します。

WildFire クラスタの RASIUS 認証の設定

RADIUS サーバーを使用して、WildFire クラスタ内の WildFireアプライアンス の CLI への管理アクセスを認証します。RADIUS サーバーでベンダー固有属性 (VSA) を定義し、管理者認証を管理することもできます。VSA を使用すれば、ディレクトリ サービスを介してロール、アクセス ドメイン、管理者のユーザー グループをすばやく変更できます。この方法は多くの場合、Panorama™ 管理サーバーで設定し直すよりも簡単です。

© 2019 Palo Alto Networks, Inc.

Palo Alto Networks RADIUS ディクショナリーを *RADIUS* サーバーにインポートして、*Panorama* と *RADIUS* サーバー間の通信に必要な認証属性を定義することができます。

STEP 1 | Panorama Web インターフェイスへのログイン.

STEP 2 | Panoramaで集中的にクラスタを構成する.

STEP 3 | RADIUS 認証を設定します。

1. RADIUS サーバー プロファイルを追加します。

   このプロファイルは、WildFire クラスタ内の WildFire アプライアンスが RADIUS サーバーに接続する方法を定義します。

   1. **Panorama** > **Server Profiles**（サーバー プロファイル）> **RADIUS** の順に追加し、プロファイルを **Add**（追加）します。
   2. サーバー プロファイルを識別する **Profile Name**（プロファイル名）を入力します。
   3. 認証要求がタイムアウトするまでの**Timeout (**タイムアウト**)** 時間を秒単位で入力します（デフォルトは 3、範囲は1 ~ 20）。
   4. Panorama が RADIUS サーバーに認証するために使用する **Authentication Protocol**（認証プロトコル）（デフォルトは **CHAP**）を選択します。

      RADIUS サーバーがサポートする場合は *CHAP* を選択します。このプロトコルは *PAP* よりも安全です。

   5. 各 RADIUS サーバーを **Add**（追加）して、以下を入力します。
      1. サーバーを識別するための**Name**（名前）。
      2. **RADIUS Server**（**RADIUS** サーバー）の IP アドレス あるいは FQDN。
      3. **Secret**（シークレット）/**Confirm Secret**（再入力 シークレット）（ユーザー名とパスワードを暗号化するための鍵）。
      4. 認証要求用のサーバー **Port**（ポート）（デフォルトは1812）。
   6. **OK** をクリックしてサーバー プロファイルを保存します。
2. RADIUS サーバー プロファイルを認証プロファイルに割り当てます。

   認証プロファイルにより、一連の管理者に共通の認証設定が定義されます。

   1. **Panorama** > **Authentication Profile**（認証プロファイル）の順に選択し、プロファイルを **Add**（追加）します。
   2. 認証プロファイルを識別する **Name**（名前）を入力します。
   3. **Type**（タイプ）を **RADIUS** に設定します。
   4. 設定した **Server Profile**（サーバー プロファイル）を選択します。
   5. **Retrieve user group from RADIUS**（**RADIUS** からユーザー グループを取得）を選択して、RADIUS サーバーで定義された VSA からユーザー グループ情報を収集します。

      Panorama は、グループ情報を認証プロファイルの Allow List（許可リスト）で指定したグループと照合します。
   6. **Advanced**（詳細）を選択し、Allow List（許可リスト）で、この認証プロファイルで認証することが許可された管理者を **Add**（追加）します。
   7. **OK** をクリックして認証プロファイルを保存します。

STEP 4 | WildFire クラスタの認証を設定します。

1. **Panorama** > **Managed WildFire Clusters**（管理対象 **WildFire** クラスタ）の順に選択し、以前に設定した WildFire クラスタを選択します。
2. 前のステップで設定した **Authentication Profile (**認証プロファイル**)** を選択します。

© 2019 Palo Alto Networks, Inc.

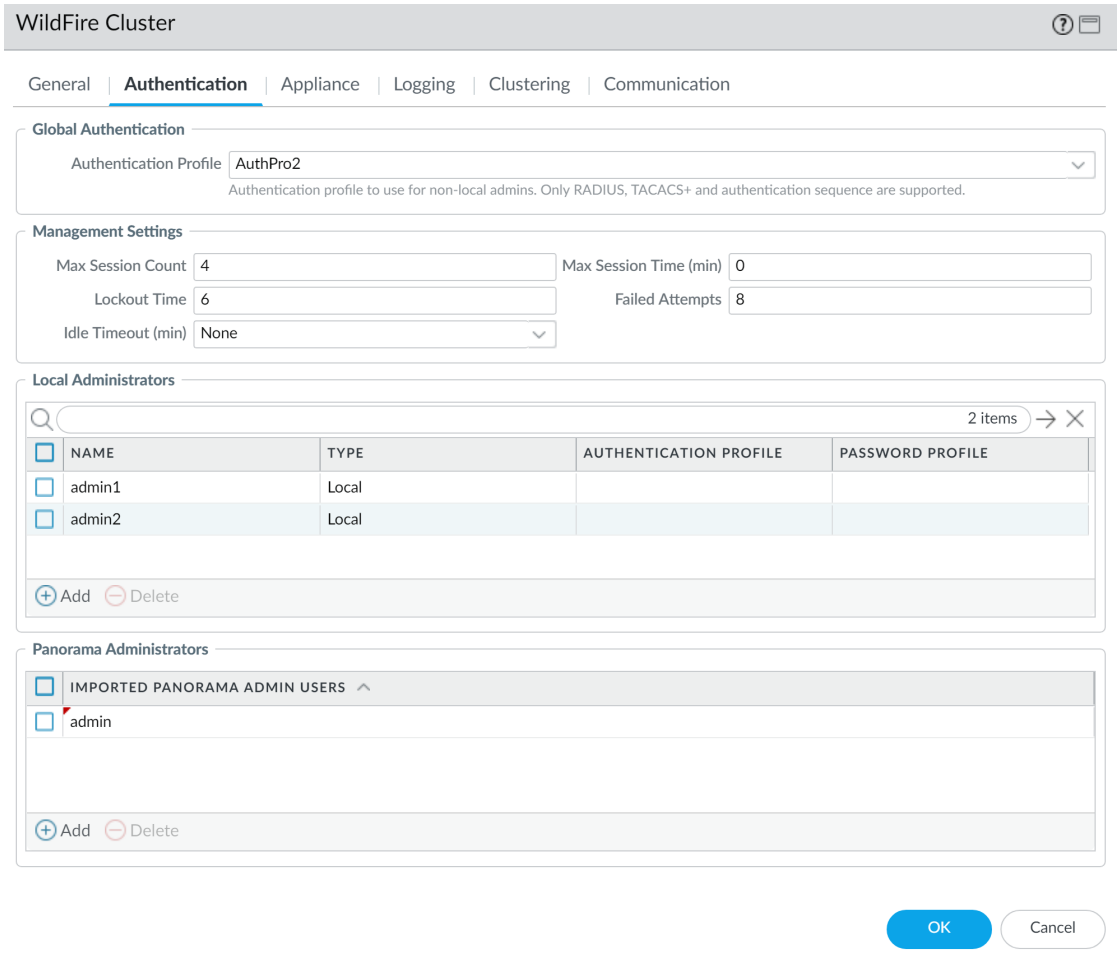
グローバル認証プロファイルが割り当てられていない場合は、リモート認証を活用するために、個々のローカル管理者に認証プロファイルを割り当てる必要があります。

3. WildFire アプライアンスの認証 **Timeout Configuration** (タイムアウト設定) を設定します。
   1. ユーザーが WildFire アプライアンス CLI からロックアウトされるまでの **Failed Attempt** (試行失敗回数) の数を入力します。
   2. **Lockout Time** (ロックアウト時間) を分単位で入力します。WildFire アプライアンス は、ユーザーが設定された数の試行失敗回数に達すると、ユーザー アカウントをロックアウトします。
   3. アクティブではないユーザー アカウントが自動的にログアウトされるまでの時間である、**Idle Timeout** (待機タイムアウト) を分単位で入力します。
   4. WildFire アプライアンス に同時にアクセスできるユーザー アカウントの数を設定するには、**Max Session Count** (最大セッション カウント) を入力します。
   5. 管理者が自動的にログアウトする前にログインできる**Max Session Time** (最大セッション時間) を入力します。
4. WildFire アプライアンス管理者を追加します。

   管理者は、ローカル管理者またはインポートされた Panorama 管理者のいずれかとして追加できますが、両方を追加することはできません。ローカル管理者とインポートされた Panorama 管理者の両方として同じ管理者を追加することはサポートされておらず、Panorama コミットが失敗します。例えば、`admin1` をローカル管理者と Panorama 管理者の両方として追加する場合、Panorama へのコミットは失敗します。

   1. WildFire クラスタ内の WildFire アプライアンスに固有の新しい管理者を**Add** (追加) して設定します。これらの管理者は、それらが作成された WildFire クラスタ内の WildFire アプライアンスに固有であり、この表からこれらの管理者を管理します。
   2. Panorama で設定された管理者を **Add** (追加) します。これらの管理者は Panorama で作成され、WildFire クラスタ内のアプライアンスにインポートされます。
5. **OK** をクリックすると、WildFire クラスタ認証設定を保存します。

© 2019 Palo Alto Networks, Inc.



STEP 5 | 設定の変更を **Commit** (コミット) してから、**Commit and Push** (コミットしてプッシュ) します。

STEP 6 | WildFire アプライアンス CLI にアクセスして、ローカルの管理者ユーザーを使用して WildFire アプライアンスにアクセスできることを確認します。

WildFire クラスタの TACACS+ 認証の設定

TACACS+ サーバーを使用して、WildFire クラスタ内の WildFireアプライアンス の CLI への管理アクセスを認証できます。TACACS+ サーバーでベンダー固有属性（VSA）を定義し、管理者認証を管理することもできます。VSA を使用すれば、ディレクトリ サービスを介してロール、アクセス ドメイン、管理者のユーザー グループをすばやく変更できます。この方法は多くの場合、Panorama で設定し直すよりも簡単です。

STEP 1 | Panorama Web インターフェイスへのログイン.

STEP 2 | Panoramaで集中的にクラスタを構成する.

STEP 3 | TACACS+ 認証を設定します。

1. TACACS+サーバー プロファイルを追加します。

   このプロファイルは、WildFire アプライアンスが TACACS+ サーバーに接続する方法を定義します。

© 2019 Palo Alto Networks, Inc.

1. **Panorama** > **Server Profiles**（サーバー プロファイル）> **TACACS+** の順に選択し、プロファイルを **Add**（追加）します。
2. サーバー プロファイルを識別する **Profile Name**（プロファイル名）を入力します。
3. 認証要求がタイムアウトするまでの**Timeout** (タイムアウト) 時間を秒単位で入力します（デフォルトは 3、範囲は1 ~ 20）。
4. Panorama が TACACS+ サーバーに認証するために使用する **Authentication Protocol**（認証プロトコル）（デフォルトは **CHAP**）を選択します。
5. TACACS+ サーバーがサポートする場合は **CHAP** を選択します。このプロトコルは **PAP** よりも安全です。
6. 各 TACACS+ サーバーを **Add**（追加）して、以下を入力します。
   1. サーバーを識別するための**Name**（名前）。
   2. **TACACS+ Server**（**TACACS+** サーバー）の IP アドレス あるいは FQDN。
   3. **Secret**（シークレット）/**Confirm Secret**（再入力 シークレット）（ユーザー名とパスワードを暗号化するための鍵）。
   4. 認証要求用のサーバー **Port**（ポート）（デフォルトは49）。
7. **OK** をクリックしてサーバー プロファイルを保存します。

2. TACACS+ サーバー プロファイルを認証プロファイルに割り当てます。

   認証プロファイルにより、一連の管理者に共通の認証設定が定義されます。

   1. **Panorama** > **Authentication Profile**（認証プロファイル）の順に選択し、プロファイルを **Add**（追加）します。
   2. プロファイルを識別する **Name**（名前）を入力します。
   3. **Type**（タイプ）を **TACACS+** に設定します。
   4. 設定した **Server Profile**（サーバー プロファイル）を選択します。
   5. **Retrieve user group from TACACS+**（**TACACS+** からユーザー グループを取得）を選択して、TACACS+ サーバーで定義された VSA からユーザー グループ情報を収集します。

      Panorama は、グループ情報を認証プロファイルの Allow List（許可リスト）で指定したグループと照合します。
   6. **Advanced**（詳細）を選択し、Allow List（許可リスト）で、この認証プロファイルで認証することが許可された管理者を **Add**（追加）します。
   7. **OK** をクリックして認証プロファイルを保存します。

STEP 4 | WildFire クラスタの認証を設定します。

1. **Panorama** > **Managed WildFire Clusters**（管理対象 **WildFire** クラスタ）の順に選択し、以前に設定した WildFire クラスタを選択します。
2. 前のステップで設定した **Authentication Profile** (認証プロファイル) を選択します。

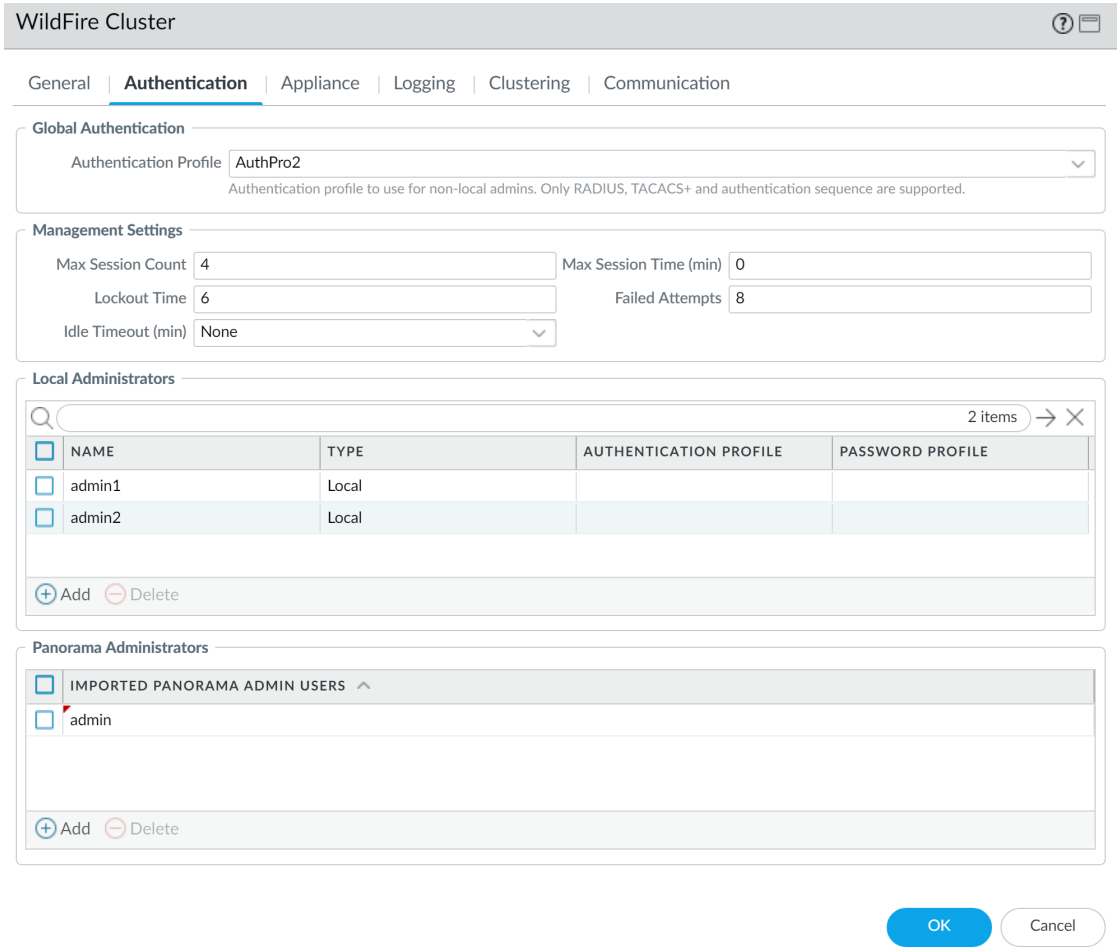
   グローバル認証プロファイルが割り当てられていない場合は、リモート認証を活用するために、個々のローカル管理者に認証プロファイルを割り当てる必要があります。
3. WildFire アプライアンスの認証 **Timeout Configuration** (タイムアウト設定) を設定します。
   1. ユーザーが WildFire アプライアンス CLI からロックアウトされるまでの **Failed Attempt** (試行失敗回数) の数を入力します。
   2. **Lockout Time** (ロックアウト時間) を分単位で入力します。WildFire アプライアンス は、ユーザーが設定された数の試行失敗回数に達すると、ユーザー アカウントをロックアウトします。
   3. アクティブではないユーザー アカウントが自動的にログアウトされるまでの時間である、**Idle Timeout** (待機タイムアウト) を分単位で入力します。
   4. WildFire アプライアンス に同時にアクセスできるユーザー アカウントの数を設定するには、**Max Session Count** (最大セッション カウント) を入力します。
   5. 管理者が自動的にログアウトする前にログインできる**Max Session Time** (最大セッション時間) を入力します。

© 2019 Palo Alto Networks, Inc.

4. WildFire アプライアンス管理者を追加します。

   管理者は、ローカル管理者またはインポートされた Panorama 管理者のいずれかとして追加できますが、両方を追加することはできません。ローカル管理者とインポートされた Panorama 管理者の両方として同じ管理者を追加することはサポートされておらず、Panorama コミットが失敗します。例えば、**admin1** をローカル管理者と Panorama 管理者の両方として追加する場合、Panorama へのコミットは失敗します。

   1. WildFire クラスタ内の WildFire アプライアンスに固有の新しい管理者を**Add** (追加) して設定します。これらの管理者は、それらが作成された WildFire クラスタ内の WildFire アプライアンスに固有であり、この表からこれらの管理者を管理します。
   2. Panorama で設定された管理者を **Add** (追加) します。これらの管理者は Panorama で作成され、WildFire クラスタ内のアプライアンスにインポートされます。
5. **OK** をクリックすると、WildFire クラスタ認証設定を保存します。



STEP 5 | 設定の変更を **Commit** (コミット) してから、**Commit and Push** (コミットしてプッシュ) します。

STEP 6 | WildFire アプライアンス CLI にアクセスして、ローカルの管理者ユーザーを使用して WildFire アプライアンスにアクセスできることを確認します。

WildFire クラスタの LDAP 認証の設定

LDAP を使用して、エンドユーザーによる WildFire クラスタ内の WildFire アプライアンスの CLI へのアクセスを認証することができます。

© 2019 Palo Alto Networks, Inc.

STEP 1 | Panorama Web インターフェイスへのログイン.

STEP 2 | Panoramaで集中的にクラスタを構成する.

STEP 3 | LDAP サーバー プロファイルを追加します。

このプロファイルは、WildFire アプライアンスが LDAP サーバーに接続する方法を定義します。

1. **Panorama** > **Server Profiles**（サーバー プロファイル）> **LDAP**を選択し、サーバー プロファイルを **Add**（追加）します。
2. サーバー プロファイルを識別する **Profile Name**（プロファイル名）を入力します。
3. LDAP サーバーを **Add** (追加) します（最大 4 件）。各サーバーについて、**Name** (名前) (サーバーを識別するため）、**LDAP Server** (サーバー) の IP アドレスあるいは FQDN、およびサーバーの **Port** (ポート) (デフォルトは 389）を入力します。

   FQDN アドレス オブジェクトを使用してサーバーを識別し、後でアドレスを変更する場合は、変更をコミットし、新しいサーバー アドレスを有効にする必要があります。
4. サーバーの **Type** (タイプ) を選択します。
5. **Base DN**（ベース **DN**）を選択します。

   ディレクトリのベース DN を識別するには、**Active Directory Domains and Trusts(Active Directory** ドメインと信頼関係)Microsoft 管理コンソールスナップインを開き、トップレベル ドメインの名前を使用します。
6. **Bind DN** と **Password**（パスワード）を入力して、ファイアウォールを認証するための認証サービスを有効にします。

   *Bind DN (*バインド *DN)* アカウントには、*LDAP* ディレクトリを参照する権限が必要です。
7. **Bind Timeout (**バインドのタイムアウト) および **Search Timeout (**検索タイムアウト) を秒単位で入力します（デフォルトはどちらも 30）。
8. **Retry Interval**（再試行間隔）を秒単位で入力します（デフォルトは 60）。
9. （LDAP のみ）ディレクトリサーバーとの保護された接続のためにエンドポイントで SSL または TLS を使いたい場合は、 **Require SSL/TLS secured connection**（**SSL/TLS** で保護された接続を要求）オプションを有効にしてください（デフォルトで有効）。サーバー ポートによってエンドポイントが使用するプロトコル：
   - 389（デフォルト）– TLS（具体的には、WildFire アプライアンスは StartTLS 操作を使用して、最初のプレーンテキスト接続を TLS にアップグレードします）
   - 636 – SSL
   - その他の任意のポート – WildFire アプライアンスはまず TLS を使用しようとします。ディレクトリ サーバーで TLS がサポートされていない場合は、WildFire アプライアンスは SSL にフォールバックします。
10. （LDAP のみ）保護を強化するには、**Verify Server Certificate for SSL sessions**（**SSL** セッションのサーバー証明書を確認）オプションを有効化します。すると、エンドポイントは SSL/TLS 接続にディレクトリサーバーが提示する証明書を確認します。この検証を有効にする場合は、**Require SSL/TLS secured connection**（**SSL/TLS**で保護された接続を要求）オプションを有効化する必要があります。進めるための確認において、証明書は次のいずれかの条件に合う必要があります。
    - 次のものはPanorama 証明書のリストにあります：**Panorama** > **Certificate Management**（証明書の管理）> **Certificates**（証明書）> **Device Certificates**（デバイス証明書）。必要に応じて、証明書を Panorama にインポートします。
    - 証明書の署名者は信頼できる証明機関のリストにあること：**Panorama** > **Certificate Management (Panorama** 証明書管理) > **Certificates (**証明書)。
11. **OK** をクリックしてサーバー プロファイルを保存します。

© 2019 Palo Alto Networks, Inc.

STEP 4 | WildFire クラスタの認証を設定します。

1. **Panorama** > **Managed WildFire Clusters**（管理対象 **WildFire** クラスタ）の順に選択し、以前に設定した WildFire クラスタを選択します。
2. WildFire アプライアンスの認証 **Timeout Configuration** (タイムアウト設定) を設定します。
   1. ユーザーが WildFire アプライアンス CLI からロックアウトされるまでの **Failed Attempt** (試行失敗回数) の数を入力します。
   2. **Lockout Time** (ロックアウト時間) を分単位で入力します。WildFire アプライアンス は、ユーザーが設定された数の試行失敗回数に達すると、ユーザー アカウントをロックアウトします。
   3. アクティブではないユーザー アカウントが自動的にログアウトされるまでの時間である、**Idle Timeout** (待機タイムアウト) を分単位で入力します。
   4. WildFire アプライアンス に同時にアクセスできるユーザー アカウントの数を設定するには、**Max Session Count** (最大セッション カウント) を入力します。
   5. 管理者が自動的にログアウトする前にログインできる**Max Session Time** (最大セッション時間) を入力します。
3. WildFire アプライアンス管理者を追加します。

   管理者は、ローカル管理者またはインポートされた Panorama 管理者のいずれかとして追加できますが、両方を追加することはできません。ローカル管理者とインポートされた Panorama 管理者の両方として同じ管理者を追加することはサポートされておらず、Panorama コミットが失敗します。例えば、`admin1` をローカル管理者と Panorama 管理者の両方として追加する場合、Panorama へのコミットは失敗します。

   - ローカルの管理者を設定します。

     WildFire クラスタ内の WildFire アプライアンスに固有の新しい管理者を設定します。これらの管理者は、それらが作成された WildFire クラスタ内の WildFire アプライアンスに固有であり、この表からこれらの管理者を管理します。

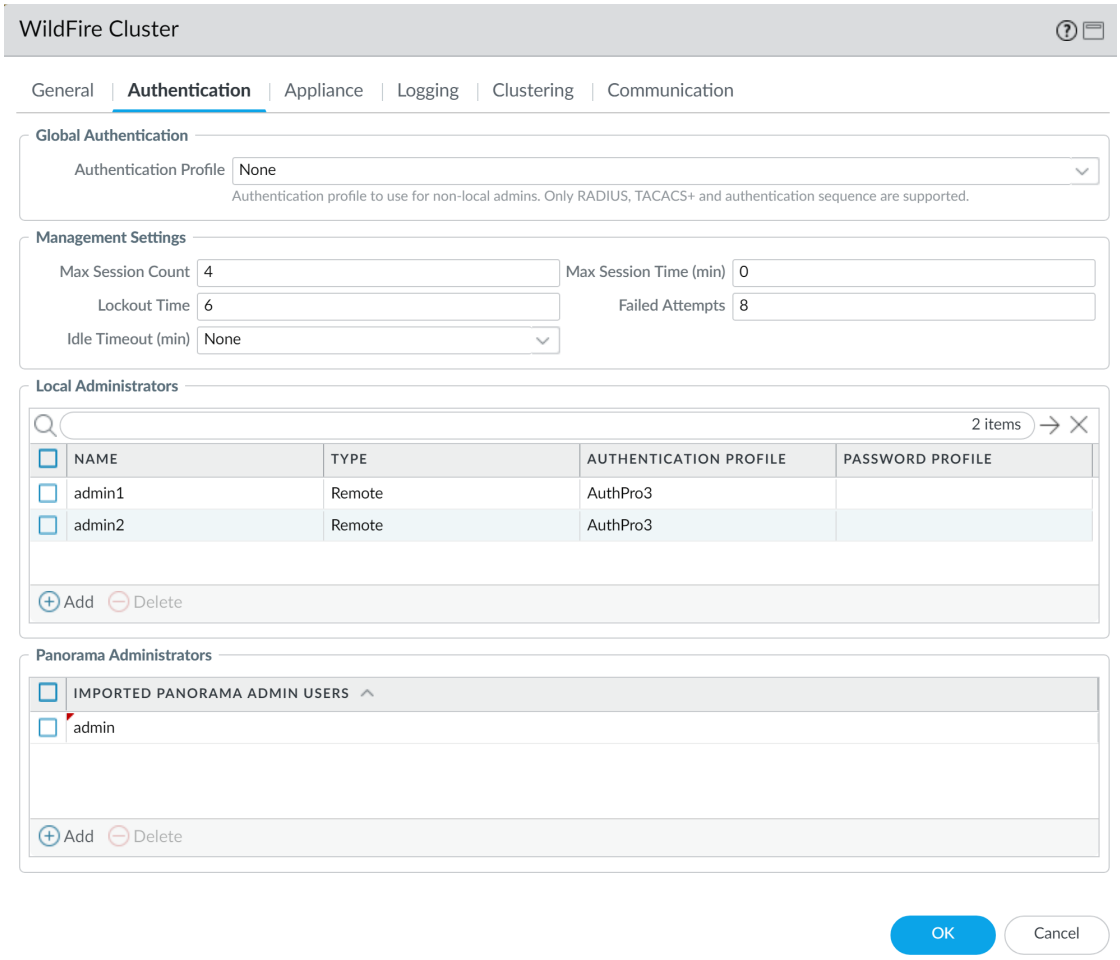
     1. 1名以上のローカル管理者を **Add** (追加) します。
     2. ローカル管理者の **Name**（名前）を入力します。
     3. 前に作成した **Authentication Profile** (認証プロファイル) を割り当てます。

        LDAP 認証プロファイルは、個々のローカル管理者に対してのみサポートされます。
     4. **Use Public Key Authentication (SSH)** (公開キーの認証 (SSH) の使用) を 有効化 (チェックを入れる) して、認証用の公開キー ファイルをインポートします。
     5. **Password Profile** (パスワードのプロファイル) を選択して、有効期限パラメータをセットします。
   - 既存の Panorama 管理者をインポートする

     Panorama で設定された既存の管理者を インポートします。これらの管理者は Panorama で設定、管理され、WildFire クラスタ内のすべての WildFire アプライアンスにインポートされます。

     1. 既存の Panorama 管理者を **Add** (追加) する
4. **OK** をクリックすると、WildFire クラスタ認証設定を保存します。

© 2019 Palo Alto Networks, Inc.



STEP 5 | 設定の変更を **Commit** (コミット) してから、**Commit and Push** (コミットしてプッシュ) します。

STEP 6 | WildFire アプライアンス CLI にアクセスして、ローカルの管理者ユーザーを使用して WildFire アプライアンスにアクセスできることを確認します。

Panoramaの管理からクラスタを削除する

Panorama 管理からクラスタを削除するには、**Panorama** > **Managed WildFire Clusters** (管理された**WildFire** クラスタ)をクリックし、削除するクラスタの行を選択し（クラスタ名をクリックしない）、**Remove From Panorama.**（パノラマから削除）を選択します。

Panorama管理からWildFireアプライアンスクラスタを削除すると、Panorama Webインターフェイスはそのクラスタ内のWildFireアプライアンスを読み取り専用モードにします。削除されたクラスタのWildFireアプライアンスはPanorama Webインターフェイスに表示されますが、読み取り専用モードではWildFireアプライアンスに設定をプッシュしたり、Panoramaで管理することはできません。Panorama管理から削除された後、WildFireアプライアンスのクラスタメンバーはローカルクラスタ設定を使用し、ローカルCLIを使用してクラスタを管理できます。

Panorama管理からクラスタを削除した後、Panoramaでクラスタ内のWildFireアプライアンスを管理するには、そのクラスタをPanorama（**Panorama** > **Managed WildFire Clusters** (管理された**WildFire** クラスタ) > **Import Cluster Config** (クラスタ設定のインポート)）に再度インポートします。

© 2019 Palo Alto Networks, Inc.

STEP 1 | クラスタのコントローラノードを選択します。クラスタ名は自動的にCluster（クラスタ）に入力されます。

STEP 2 | **OK** をクリックします。クラスタバックアップコントローラーノードおよびワーカーノードは自動的に移入されます

STEP 3 | **OK**をクリックしてクラスタをインポートします。

STEP 4 | 変更を **Commit**（コミット）します。

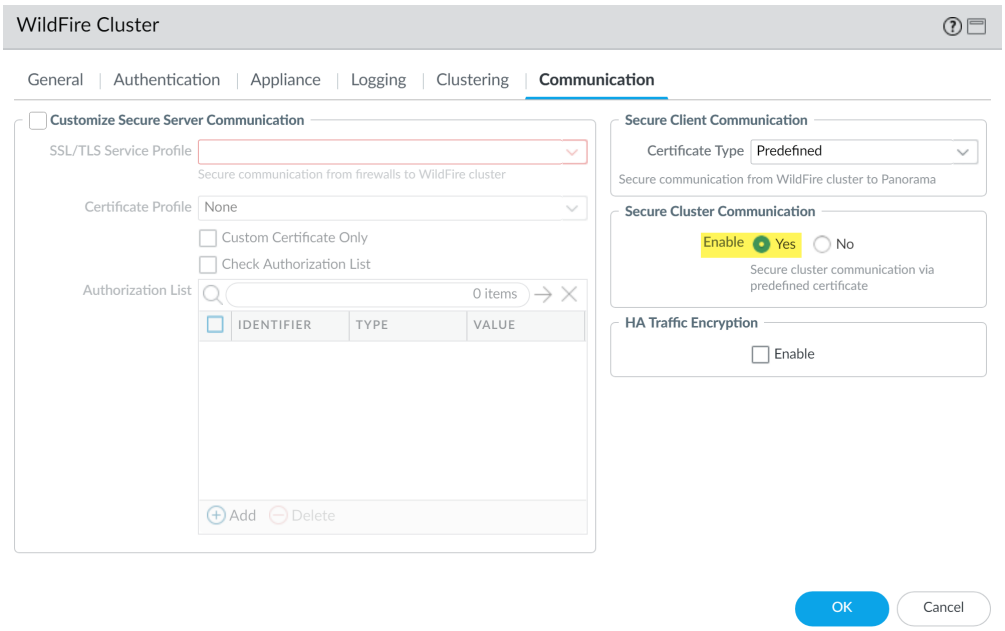
Panorama で集中的に定義済みの証明書を使用したアプライアンス間暗号化の設定

STEP 1 | 管理対象の各 WildFire アプライアンスを PAN-OS 8.1.x にアップグレードします。すべての管理対象アプライアンスは、アプライアンス間暗号化を有効にするために PAN-OS 8.1 以降を実行している必要があります。

STEP 2 | WildFire アプライアンス クラスタが正しく設定され、正常な状態で動作していることを確認します。

STEP 3 | Panorama 上で、**Panorama**（**Panorama**）> **Managed WildFire Clusters**（管理された **WildFire** クラスタ）> *WF_cluster_name*（*WF* クラスタ名）> **Communication**（通信）の順に選択します。

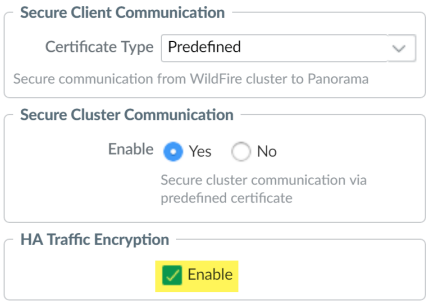
STEP 4 | セキュア クラスタ 通信を **Enable**（有効）にします。



STEP 5 | （推奨）HA トラフィックの暗号化を **Enable**（有効）にします。このオプションの設定は、HA ペア間の HA トラフィックを暗号化し、Palo Alto Networks が推奨するベストプラクティスです。

HA トラフィック暗号化は、*FIPS/CC* モードで動作しているときは無効にできません。

© 2019 Palo Alto Networks, Inc.



STEP 6 | **OK**をクリックして、**WildFire Cluster**（**WildFire** クラスタ）を保存します。

STEP 7 | 変更を **Commit (**コミット**)**します。

Panorama で集中的にカスタム証明書を使用したアプライアンス間暗号化の設定

STEP 1 | 管理対象の各 WildFire アプライアンスを PAN-OS 8.1.x にアップグレードします。すべての管理対象アプライアンスは、アプライアンス間暗号化を有効にするために PAN-OS 8.1 以降を実行している必要があります。

STEP 2 | WildFire アプライアンス クラスタが正しく設定され、正常な状態で動作していることを確認します。

STEP 3 | 既存の WildFire セキュア通信設定を確認します。以前にカスタム証明書を使用して WildFire アプライアンスとファイアウォールを安全な通信用に設定していた場合、そのカスタム証明書を WildFire アプライアンス間のセキュア通信に使用することもできます。

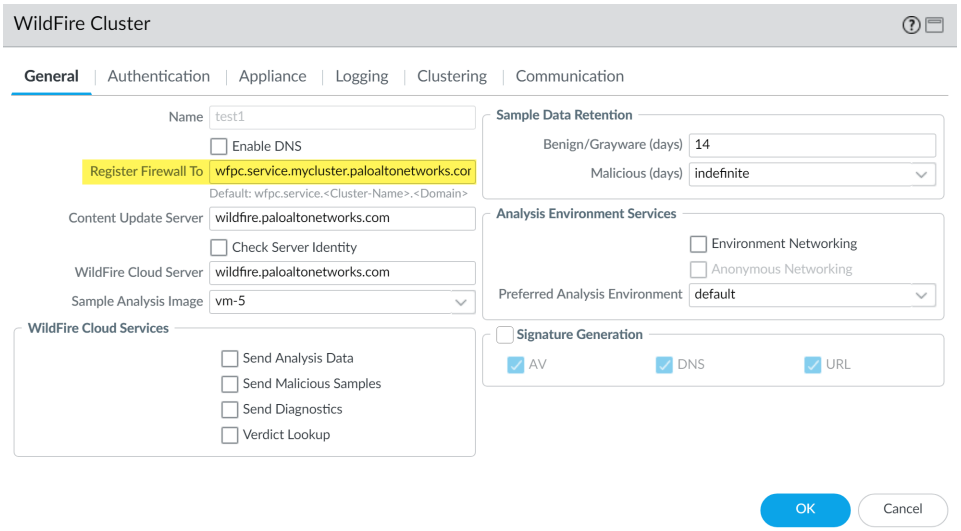
1. **PanoramaManaged WildFire Clusters (**管理された**WildFire** クラスター**)**> *WF_cluster_name*> **Communication**（通信）を選択します。
2. **Customize Secure Server Communication**（セキュリティで保護されたサーバー通信のカスタマイズ）が有効になっていて、その証明書を使用する場合は、使用されているカスタム証明書の詳細を特定します。それ以外の場合は、ステップ 5 に進み、新しいカスタム証明書のインストール プロセスを開始します。
3. ステップ 4 でファイアウォール登録アドレスを定義するために使用されるカスタム証明書 FQDN（DNS名）を決定します。

> カスタム証明書名と関連付けられた *FQDN* に注意してください。これらは、設定プロセス中に複数回参照されます。

STEP 4 | Panorama にファイアウォール登録アドレスを設定します。

1. Panorama 上で、**Panorama >Managed WildFire Clusters (**管理された **WildFire** クラスター**) >>** *WF_cluster_name*> **General**（全般）を選択します。
2. ファイアウォールの登録先フィールドに、カスタム証明書に含まれる認証に使用される DNS 名（通常は SubjectName または SubjectAltName）を指定します。たとえば、デフォルトのドメイン名は **`wfpc.service.mycluster.paloaltonetworks.com`** です。

© 2019 Palo Alto Networks, Inc.

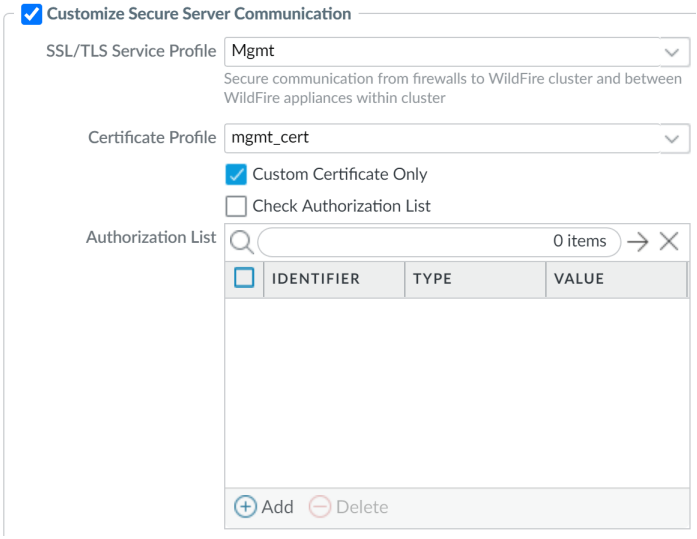


STEP 5 | Panorama の WildFire セキュア サーバー通信 を設定します。ファイアウォールと WildFire クラスタ間のセキュア通信をすでに設定していて、既存のカスタム証明書を使用している場合は、以下のステップ 4 に進みます。

1. Panorama 上で、**Panorama >Managed WildFire Clusters (管理されたWildFire クラスター) >>** *WF_cluster_name*> **Communication**（通信）を選択します。
2. **Customize Secure Server Communication**（保護されたサーバー通信のカスタマイズ）をクリックします。
3. WildFire アプライアンスおよび関連するファイアウォールで使用されるカスタム証明書を設定、展開します。SSL/TLS サービスプロファイルは、WildFire アプライアンス ピアおよびファイアウォールと通信するために WildFire アプライアンスが使用するカスタム証明書を定義します。また、WildFire アプライアンス クラスタに関連付けられたファイアウォールでカスタム証明書の設定を行う必要があります。これは、ステップ 9 の後半で設定します。
   1. SSL/TLSサービスプロファイル ドロップダウン リストを開き、SSL/TLS サービスプロファイルをクリックします。使用するカスタム証明書を使用して SSL/TLS サービス プロファイルを設定します。SSL/TLS サービス プロファイルを設定したら、OK をクリックして、新しく作成した SSL/TLS サービス プロファイルを選択します。
   2. 証明書プロファイル ドロップダウン リストを開き、証明書プロファイル をクリックします。ファイアウォールと WildFire アプライアンス間、およびピアの WildFire アプライアンス間のセキュアな接続を確立するために使用されるカスタム証明書を識別する、証明書プロファイルを設定します。証明書プロファイルを設定したら、OK をクリックして、新しく作成したプロファイルを選択します。
4. **Custom Certificate Only**（カスタム証明書のみ）チェックボックスをオンにします。これにより、デフォルトの事前構成済み証明書の代わりに構成したカスタム証明書を使用できます。
5. （任意）認証リストを設定します。認証リストは、カスタム証明書のサブジェクトまたはサブジェクト名を確認します。カスタム証明書で提示された **Subject**（サブジェクト）または **Subject Alt Name**（サブジェクト代替名）が許可リストの ID と一致しない場合、認証は拒否されます。
   1. Authorization List（承認リスト）を **Add**（追加）します。
   2. 識別子タイプとしてカスタム証明書プロファイルで設定した **Subject**（サブジェクト）または **Subject Alt Name**（サブジェクト代替名）を選択します。
   3. 識別子が Subject（サブジェクト）の場合は Common Name（共通名（CN））を入力し、識別子が Subject Alt Name（サブジェクト代替名）の場合は IP アドレス、ホスト名、または電子メール アドレスを入力します。
   4. **OK** をクリックします。

© 2019 Palo Alto Networks, Inc.

5. **Check Authorization List**（承認リストのチェック）を選択して認証リストを適用します。
6. **OK** をクリックします。



STEP 6 | セキュア クラスタ 通信を **Enable**（有効）にします。

STEP 7 | （推奨）HA トラフィックの暗号化を **Enable**（有効）にします。このオプションの設定は、HA ペア間の HA トラフィックを暗号化し、Palo Alto Networks が推奨するベストプラクティスです。

HA トラフィック暗号化は、*FIPS/CC* モードで動作しているときは無効にできません。

STEP 8 | **OK**をクリックして、**WildFire Cluster**（**WildFire** クラスタ）を保存します。

STEP 9 | WildFire アプライアンス クラスタをファイアウォール カスタム証明書に関連付けるには、Panorama のファイアウォールのセキュア通信設定を構成します。これにより、ファイアウォールと WildFire アプライアンス クラスタ間の安全な通信チャネルが提供されます。ファイアウォールと WildFire アプライアンス クラスタ間のセキュア通信をすでに設定していて、既存のカスタム証明書を使用している場合は、次のステップに進みます。

1. **Device**（デバイス）> **Setup**（セットアップ）> **Management**（管理）> **Secure Communication Settings**（セキュア通信設定）を選択して、**Secure Communication Settings**（セキュア通信設定）の **Edit**（編集）アイコンをクリックすることで、 ファイアウォールのカスタム証明書設定を設定します。
2. それぞれのドロップダウン リストから**Certificate Type**（証明書タイプ）、 **Certificates**（証明書）、および**Certificate Profile**（証明書プロファイル）を選択し、カスタム証明書を使用するように設定します。
3. カスタマイズ通信で、**WildFire Communication**（**WildFire** 通信）を設定します。
4. **OK** をクリックします。

STEP 10 | 変更を **Commit** (コミット)します。

Panoramaを使用したWildFireクラスタのステータスの表示

設定済みのWildFireアプライアンスクラスタが正常に動作していることを確認するには、Panoramaアプライアンスを使用して現在のステータスを表示します。

© 2019 Palo Alto Networks, Inc.

*Palo Alto Networks*では、*WildFire*アプライアンス*CLI*を使用して*WildFire*クラスタのステータスを確認することを推奨しています。*Panorama* から表示されない追加のステータスの詳細がコマンド出力に表示されます。

STEP 1 | プライマリパノラマアプライアンスで、**Panorama > Managed WildFire Clusters**（パノラマ> 管理された**WildFire** クラスタ）を選択します。

STEP 2 | **Cluster Status**（クラスタステータス）列で、次のことを確認します。

1. wfpcと署名サービスが実行されている。
2. その他の操作はなし。異常な操作とその状態には次のものが含まれる：
   - 廃止[要求/継続/拒否/成功/失敗]
   - 中断[要求/継続中/拒否/成功/失敗]
   - 再起動[要求/継続/拒否/成功/失敗]
   - クラスタ[オフライン/ スプリットブレイン/ 準備未完了]
   - サービス[中断/なし]
   - HA [peer-offline / cfg-not-sync / cfg-sync-off]

STEP 3 | **Config Status**（設定ステータス）列で、次のことを確認します。

1. アプライアンスの設定は、Panoramaアプライアンスに保存されている設定と**In Sync**（同期）していない。
2. その他のステータスはない。異常状態には以下が含まれます：
   - Out of Sync [アプライアンスの設定がPanoramaの保存された設定と**Out of Sync**（非同期）である。虫眼鏡の上にマウスを置くと、同期不良の原因が表示されます]。

STEP 4 | **Connected**（接続済み）列で、設定済みのWildFireアプライアンスが**Connected**（接続済み）のステータスを表示していることを確認します。

インターネット接続を使用してクラスタをセンターでアップグレードする

クラスタ内のWildFireアプライアンスは、Panoramaによって管理されている場合に並行してアップグレードできます。Panorama がインターネットに直接接続している場合、Panorama から直接新しいリリースを確認してダウンロードすることができます。

*Panorama*は、同じソフトウェアバージョンまたはそれ以降のソフトウェアバージョンで動作する*WildFire*アプライアンスとアプライアンスクラスタのみを管理できます。

STEP 1 | Panoramaを、WildFireクラスタにインストールする対象のソフトウェアリリースと同等以上のリリースにアップグレードします。

Panorama のアップグレード方法の詳細については、Panorama のコンテンツ更新とソフトウェア更新のインストールを参照してください。

STEP 2 | 一時的にサンプル分析を停止する。

1. ファイアウォールが新しいサンプルをWildFireアプライアンスに転送するのを停止します。
   1. ファイアウォール インターフェイスにログインします。
   2. **Device (デバイス) > Setup**（セットアップ）**> WildFire** の順に選択し、**General Settings**（一般設定）を編集します。
   3. **WildFire Private Cloud**（**WildFire**プライベートクラウド）フィールドをクリアにする
   4. **OK**、**Commit (コミット)** の順にクリックします。

© 2019 Palo Alto Networks, Inc.

2. ファイアウォールがすでにアプライアンスに送信されているサンプルの分析が完了したことを確認します。
    1. Panorama Web インターフェイスにログインします。
    2. **Panorama > Managed WildFire Clusters**（パノラマ>管理された**WildFire** クラスタ）を選択し、クラスタ分析環境の**Utilization**（利用）を**View**（表示）します。
    3. 進行中のサンプル分析が**Virtual Machine Usage**（バーチャルマシン利用）に表示されないことを確認します。

    *WildFire*アプライアンスが最近提出されたサンプルの分析を終了するのを待たない場合は、次のステップに進むことができます。ただし、*WildFire*アプライアンスは分析キューから保留中のサンプルを削除します。

STEP 3 | 最新のWildFireアプライアンスコンテンツアップデートをインストールします。

これらのアップデートでは、最新の脅威情報をアプライアンスに装備し、マルウェアを正確に検出します。

最初に、コンテンツ更新をインストールしてからソフトウェア更新をインストールします。*Panorama* でインストールしていなければならない最低バージョンについては『リリースノート』をご覧ください。

1. WildFireコンテンツアップデートをダウンロードする：
    1. **Panorama > Device Deployment**（デバイスのデプロイ）**> Dynamic Updates**（動的更新）の順に選択します。
    2. WildFireコンテンツアップデートリリースパッケージを選択し、**Download**（ダウンロード）をクリックします。
2. **Install (**インストール**)**をクリックします。
3. アップグレードするWildFireクラスタまたは個々のアプライアンスを選択します。
4. **OK** をクリックしてインストールを開始します。

STEP 4 | WildfireアプライアンスにPAN-OSソフトウェアバージョンをダウンロードします。

WildFireアプライアンスをアップグレードするときにメジャーリリースのバージョンをスキップすることはできません。たとえば、PAN-OS 6.1からPAN-OS 7.1にアップグレードする場合は、まずPAN-OS 7.0をダウンロードしてインストールする必要があります。

1. WildFireソフトウェアのアップグレードをダウンロードする：
    1. **Panorama > Device Deployment**（デバイスのデプロイ）**> Software**（ソフトウェア）の順に選択します。
    2. **Check Now**（今すぐ確認）をクリックして、更新されたリリースのリストを取得します。
    3. インストールするWildFireリリースを選択し、**Download**（ダウンロード）をクリックします。
    4. **Close**（閉じる）をクリックして**Download Software**（ソフトウェアのダウンロード）ウィンドウを閉じます。
2. **Install (**インストール**)**をクリックします。
3. アップグレードするWildFireクラスタを選択します。
4. インストールモードを選択します：
    - （8.0.2以降）**Select Reboot device after install**（インストール後にリブートデバイスを選択）します。
    - （8.0.1以降）**Upload only**（アップロードのみ）を選択します。
5. **OK** をクリックしてインストールを開始します。
6. （オプション）パノラマのインストール状況を監視します。

© 2019 Palo Alto Networks, Inc.

7. （8.0.1のみ）アップグレードパッケージのアップロードが完了したら、各ノードにアップグレードをインストールします。
   1.
```
admin@WF-500 (passive-controller)> request system software install
 version 8.0.2
```
   2. 更新が完了したことを確認してください。以下のコマンドを実行して、ジョブのtype（タイプ）が **Install**（インストール）、status（状態）が **FIN**（終了）になっているエントリを探します。

```
admin@WF-500(passive-controller)> show jobs all

Enqueued Dequeued ID Type Status Result Completed
------------------------------------------------------
14:53:15 14:53:15 5 Install FIN    OK   14:53:19
```
   3. アプライアンスを正常に再起動します。

```
admin@WF-500(passive-controller)> request cluster reboot-local-node
```

   *WildFire*アプライアンスに保存されているサンプル数に応じて、アップグレードプロセスには*10*分か*1*時間以上かかります。
   4. クラスタ内の各WildFireワーカーノードに対してこの手順を繰り返します。

STEP 5 | （オプション）WildFireコントローラノードの再起動タスクのステータスを表示します。

WildFireクラスタコントローラで、次のコマンドを実行し、ジョブタイプ**Install**（インストール）およびstatus（状態）が **FIN** （終了）になっているエントリを探します。

```
admin@WF-500(active-controller)> show cluster task pending
```

STEP 6 | WildFireアプライアンスがサンプル分析を再開する準備が整っていることを確認します。

1. sw-versionフィールドに8.0.1が表示されていることを確認します。

```
admin@WF-500(passive-controller)> show system info | match sw-version
```

2. すべてのプロセスが実行されていることを確認します。

```
admin@WF-500(passive-controller)> show system software status
```

3. 自動コミット（**AutoCom**）ジョブが完了したことを確認します。

```
admin@WF-500(passive-controller)> show jobs all
```

インターネット接続を使用してクラスタをセンターでアップグレードする

クラスタ内のWildFireアプライアンスは、Panoramaによって管理されている場合に並行してアップグレードできます。Panoramaがインターネットに直接接続していない場合、Palo Alto Networksのサポートサイトからソフトウェアのコンテンツとアップデートをダウンロードし、パノラマで配信する前に内蔵サーバーにホストする必要があります。

© 2019 Palo Alto Networks, Inc.

*Panorama*は、同じソフトウェアバージョンまたはそれ以降のソフトウェアバージョンで動作する*WildFire*アプライアンスとアプライアンスクラスタのみを管理できます。

STEP 1 | Panoramaを、WildFireクラスタにインストールする対象のソフトウェアリリースと同等以上のリリースにアップグレードします。

Panorama のアップグレード方法の詳細については、Panorama のコンテンツ更新とソフトウェア更新のインストールを参照してください。

STEP 2 | 一時的にサンプル分析を停止する。

1. ファイアウォールが新しいサンプルをWildFireアプライアンスに転送するのを停止します。
   1. ファイアウォール インターフェイスにログインします。
   2. **Device (**デバイス) > **Setup** (セットアップ) > **WildFire** の順に選択し、**General Settings** (一般設定) を編集します。
   3. **WildFire Private Cloud** (**WildFire**プライベートクラウド) フィールドをクリアにする
   4. **OK**、**Commit (**コミット**)** の順にクリックします。
2. ファイアウォールがすでにアプライアンスに送信されているサンプルの分析が完了したことを確認します。
   1. Panorama Web インターフェイスにログインします。
   2. **Panorama** > **Managed WildFire Clusters** (パノラマ>管理された**WildFire** クラスタ) を選択し、クラスタ分析環境の**Utilization** (利用) を**View** (表示) します。
   3. 進行中のサンプル分析が**Virtual Machine Usage** (バーチャルマシン利用) に表示されないことを確認します。

   *WildFire*アプライアンスが最近提出されたサンプルの分析を終了するのを待たない場合は、次のステップに進むことができます。ただし、*WildFire*アプライアンスは分析キューから保留中のサンプルを削除します。

STEP 3 | インターネットにアクセスできるホストに、WildFireコンテンツ更新とソフトウェア更新にダウンロードします。Panorama がそのホストにアクセスできる必要があります。

1. インターネットにアクセスできるホストを使用して、Palo Alto Networks のカスタマー サポート Web サイトにログインします。
2. コンテンツ更新のダウンロード：
   1. Tools (ツール)セクションで **Dynamic Updates (**動的更新**)** をクリックします。
   2. 目的のコンテンツ更新を**Download (**ダウンロード**)** し、ファイルをホストに保存します。アップデートするコンテンツ タイプごとにこのステップを繰り返します。
3. ソフトウェア更新のダウンロード：
   1. Palo Alto Networksカスタマーサポート ウェブサイトのメイン ページに戻り、Tools (ツール) セクションの**Software Updates (**ソフトウェア更新**)** をクリックします。
   2. Download (ダウンロード) 列の表示を確認し、インストールするバージョンを決定します。アップデートパッケージのファイル名は、アップグレードのモデルとリリースを示します。WildFire_<release>.
   3. ファイル名をクリックして、そのファイルをホストに保存します。

STEP 4 | 最新のWildFireアプライアンスコンテンツアップデートをインストールします。

これらのアップデートでは、最新の脅威情報をアプライアンスに装備し、マルウェアを正確に検出します。

© 2019 Palo Alto Networks, Inc.

最初に、コンテンツ更新をインストールしてからソフトウェア更新をインストールします。*Panorama* でインストールしていなければならない最低バージョンについては『リリースノート』をご覧ください。

1. WildFireコンテンツアップデートをダウンロードする：
   1. **Panorama > Device Deployment**（デバイスのデプロイ）**> Dynamic Updates**（動的更新）の順に選択します。
   2. **Upload (アップロード)**をクリックし、コンテンツの**Type (タイプ)**を選択し、WildFireコンテンツ更新ファイルを**Browse (閲覧)**して**OK**をクリックします。
   3. **Install From File**（ファイルからインストール）をクリックし、アップグレードするクラスタ内のパッケージ**Type (タイプ)**、**File Name**（ファイル名）、およびWildFireアプライアンスを選択し、**OK**をクリックします。
2. **OK** をクリックしてインストールを開始します。

STEP 5 | WildfireアプライアンスにPAN-OSソフトウェアバージョンをダウンロードします。

WildFireアプライアンスをアップグレードするときにメジャーリリースのバージョンをスキップすることはできません。たとえば、PAN-OS 6.1からPAN-OS 7.1にアップグレードする場合は、まずPAN-OS 7.0をダウンロードしてインストールする必要があります。

1. WildFireソフトウェアのアップグレードをダウンロードする：
   1. **Panorama > Device Deployment**（デバイスのデプロイ）**> Software**（ソフトウェア）の順に選択します。
   2. **Check Now**（今すぐ確認）をクリックして、更新されたリリースのリストを取得します。
   3. インストールするWildFireリリースを選択し、**Download**（ダウンロード）をクリックします。
   4. **Close**（閉じる）をクリックして**Download Software**（ソフトウェアのダウンロード）ウィンドウを閉じます。
2. **Install (インストール)**をクリックします。
3. アップグレードするWildFireクラスタを選択します。
4. インストールモードを選択します：
   - （8.0.2以降）**Select Reboot device after install**（インストール後にリブートデバイスを選択）します。
   - （8.0.1以降）**Upload only**（アップロードのみ）を選択します。
5. **OK** をクリックしてインストールを開始します。
6. （オプション）パノラマのインストール状況を監視します。
7. （8.0.1のみ）アップグレードパッケージのアップロードが完了したら、各ノードにアップグレードをインストールします。
   1. ```
      admin@WF-500 (passive-controller)> request system software install
       version 8.0.2
      ```
   2. 更新が完了したことを確認してください。以下のコマンドを実行して、ジョブのtype（タイプ）が **Install**（インストール）、status（状態）が **FIN**（終了）になっているエントリを探します。

      ```
      admin@WF-500(passive-controller)> show jobs all

      Enqueued Dequeued ID Type Status Result Completed
      ------------------------------------------------------
      14:53:15 14:53:15 5 Install FIN    OK   14:53:19
      ```
   3. アプライアンスを正常に再起動します。

© 2019 Palo Alto Networks, Inc.
      ```

```
admin@WF-500(passive-controller)> request cluster reboot-local-node
```

*WildFire*アプライアンスに保存されているサンプル数に応じて、アップグレードプロセスには*10*分か*1*時間以上かかります。

4. クラスタ内の各WildFireワーカーノードにおいて手順7を繰り返します。

STEP 6 | （オプション）WildFireコントローラノードの再起動タスクのステータスを表示します。

WildFireクラスタコントローラで、次のコマンドを実行し、ジョブタイプ**Install**（インストール）およびstatus（状態）が **FIN** （終了）になっているエントリを探します。

```
admin@WF-500(active-controller)> show cluster task pending
```

STEP 7 | WildFireアプライアンスがサンプル分析を再開する準備が整っていることを確認します。

1. sw-versionフィールドに8.0.1が表示されていることを確認します。

```
admin@WF-500(passive-controller)> show system info | match sw-version
```

2. すべてのプロセスが実行されていることを確認します。

admin@WF-500(passive-controller)> **show system software status**

3. 自動コミット（**AutoCom**）ジョブが完了したことを確認します。

```
admin@WF-500(passive-controller)> show jobs all
```


© 2019 Palo Alto Networks, Inc.

ライセンスの管理と更新

Panorama™ 管理サーバーを使用すると、ファイアウォールおよび専用のログ コレクタ上でライセンス、ソフトウェア更新、およびコンテンツ更新を一元的に管理できます。ライセンスや更新のデプロイ時に、Panorama は Palo Alto Networks® ライセンス サーバーまたは更新サーバーに接続し、要求の正当性を確認してから、ライセンスあるいは更新の取得およびインストールを許可します。この機能によって、ファイアウォールや専用ログコレクタごとに繰り返し同じタスクを実行する必要がなくなるため、デプロイが容易になります。特に、インターネットに直接アクセスできない管理対象ファイアウォールや、（Web インターフェイスがない）専用ログコレクタを管理する場合に便利です。

更新をデプロイする前に、「Panorama、ログ コレクタ、ファイアウォール、および WildFire のバージョン互換性」を読み、更新バージョンの互換性に関する重要な詳細情報をご確認ください。

サポート サブスクリプションは各ファイアウォールで直接アクティベーションする必要があります。Panorama を使用してサポート サブスクリプションをデプロイすることはできません。

Panorama管理サーバーでライセンスをアクティベートする、あるいは更新をインストールする方法については、Panorama の登録とライセンスのインストールとコンテンツ更新およびPanoramaソフトウェア更新のインストールを参照してください。

> Panorama を使用したファイアウォールのライセンス管理
> Panorama を使用したファイアウォール、ログ コレクタ、および WildFire アプライアンスへの更新のデプロイ

Panorama を使用したファイアウォールのライセンス管理

以下の手順では、認証（*auth*）コードを使用して新しいライセンスを取得し、ライセンス キーを管理対象ファイアウォールにプッシュする方法を説明します。また、インターネットに直接アクセスできないファイアウォールのライセンス ステータスを手動で更新（リフレッシュ）する方法についても説明します。ファイアウォールがインターネットに直接接続されている場合、Panorama™ はライセンス サーバーに毎日自動的にチェックインを行い、ライセンスの延長や更新を取得し、それらをファイアウォールにプッシュします。チェックインは午前 1 時から午前 2 時の間に行われるようハードコードされており、この時間を変更することはできません。



Panorama を使用して、ファイアウォールのサポート ライセンスをアクティベートすることはできません。これらのサポート ライセンスをアクティベーションするには、個々のファイアウォールにアクセスする必要があります。

Panorama のライセンスをアクティベートする方法については、「Panorama の登録とライセンスのインストール」を参照してください。

- 新規に購入したライセンスをアクティベートします。
  1. **Panorama** > **Device Deployment**（デバイスのデプロイ） > **Licenses**（ライセンス）の順に選択して、**Activate**（アクティベーション）をクリックします。
  2. 新しいライセンスを持つ各ファイアウォールに対して Palo Alto Networks® が発行した **Auth Code**（認証コード）を入力します。
  3. ライセンスの **Activate**（アクティベーション） を行います。
  4. （WildFire® サブスクリプションのみ）新しい WildFire サブスクリプションを持つ各ファイアウォール上でコミットを実行し、アクティベーションを完了させます。
     - 保留中の変更をすべて **Commit**（コミット）します。そのためには、各ファイアウォールのWebインターフェイスにアクセスする必要があります。
     - 保留中の設定変更がない場合は、軽微な変更を行って **Commit**（コミット）します。たとえば、ルールの説明を更新して変更をコミットします。ファイアウォールが同じデバイスグループに属している場合、各ファイアウォールに個別にアクセスすることなく、Panoramaからルール変更をプッシュし、それらすべてのファイアウォールに対してコミットを実行できます。



WildFire サブスクリプションがサポートしている高度なファイル タイプがWildFire 分析プロファイル ルールに含まれていることを確認します。

- ファイアウォールのライセンス状態を更新します。
  1. **[Panorama]** > [デバイスのデプロイ] > [ライセンス] の順に選択します。

     ページの各エントリは、ライセンスがアクティブか非アクティブかを示します。また、アクティブなライセンスの有効期限も表示されます。
  2. 以前にファイアウォール上で直接、サポート サブスクリプションの認証コードをアクティベートしている場合は、**Refresh**（更新）をクリックして、リストからファイアウォールを選択します。Panorama がライセンスを取得し、ファイアウォールにデプロイして、Panorama Web インターフェイスのライセンス状態を更新します。
  3. (エンタープライズ データ損失防止 (DLP) ライセンスのみ) 更新されたライセンスを、エンタープライズ DLP を利用してマネージドファイアウォールにプッシュします。
     1. **Commit (コミット)** および **Commit to Panorama (Panorama へのコミット)** を選択します。

© 2019 Palo Alto Networks, Inc.

2. **Commit**（コミット）> **Push to Devices**（デバイスへのプッシュ）の順に選択し、**Edit Selections**（選択内容の編集）を行います。
3. **Template (テンプレート)** を選択し、エンタープライズ DLP を活用するマネージドファイアウォールと関連するテンプレート スタックを選択します。

   [OK] クリックして続行します。
4. テンプレート設定をプッシュして、エンタープライズ DLP ライセンスを正常に更新します。

© 2019 Palo Alto Networks, Inc.

Panorama を使用したファイアウォール、ログ コレクタ、および WildFire アプライアンスへの更新のデプロイ

Panorama™ を使用すると、ソフトウェアおよびコンテンツ更新を一部のファイアウォール、専用のログ コレクタ、または WildFire® アプライアンスおよびアプライアンス クラスタに限定してデプロイしてから、残りの管理対象アプライアンスに更新をインストールできます。Panorama で、コンテンツの定期的な更新をスケジュール設定する場合は、インターネットに直接接続する必要があります。ソフトウェアまたはコンテンツの更新をオンデマンドで (スケジュール設定なしで) デプロイする場合の手順は、Panorama がインターネットに接続しているかどうかによって異なります。スケジュール設定されている更新プロセスが開始した、あるいは 5 分以内に開始する場合に手動でコンテンツ更新をデプロイすると、警告が表示されます。

更新をデプロイすると、Panorama は、管理対象アプライアンス (ファイアウォール、ログ コレクタ、および WildFire アプライアンス) に対して、更新が提供されたことを通知します。これを受けて、各アプライアンスは、Panorama から更新パッケージを取得します。デフォルトでは、管理対象アプライアンスは、Panorama の管理 (MGT) インターフェイス経由で更新を取得します。ただし、MGT インターフェイスのトラフィック負荷を軽減するために、アプライアンスの別のインターフェイスを使用して更新を取得する場合は、複数のインターフェイスを使用するように Panorama を設定してください。

Panorama を使用して、1 つまたは複数のファイアウォールのコンテンツ バージョンを以前にインストールしたコンテンツ バージョンにすばやく戻すことができます。新しいコンテンツ バージョンがファイアウォールにインストールされた後、新しくインストールされたコンテンツ バージョンがネットワーク操作を不安定にしたり、中断したりすると、以前にインストールされたバージョンに戻すことができます。

デフォルトでは、各タイプにつき最大 *2* つのソフトウェア更新またはコンテンツ更新を *Panorama* にダウンロードできます。この上限値を超えてダウンロードを実行すると、選択したタイプの最も古い更新が削除されます。上限を変更する方法については、「ソフトウェア更新とコンテンツ更新が格納される Panorama ストレージの管理」を参照してください。

- サポートされている更新
- Panorama を使用してコンテンツ更新のスケジュールを設定
- Panorama がインターネットに接続されている状態でログ コレクタをアップグレード
- Panorama がインターネットに接続されていない状態でログ コレクタをアップグレード
- Panorama がインターネットに接続されている状態でファイアウォールをアップグレード
- Panorama がインターネットに接続されていない状態でファイアウォールをアップグレード
- ZTP ファイアウォールのアップグレード
- Panorama でコンテンツのアップデートを元に戻す

サポートされている更新

インストール可能なソフトウェアとコンテンツ更新は、各ファイアウォール、ログ コレクタ、WildFire® アプライアンスおよびアプライアンス クラスタでアクティブになっているサブスクリプションによって異なります。

© 2019 Palo Alto Networks, Inc.

アプライアンス タイプ	ソフトウェア更新	コンテンツアップデート
ログ コレクタ	Panorama™	アプリケーション（ログ コレクタは脅威シグネチャを必要としません） Antivirus（アンチウイルス） BrightCloud URL フィルタリング WildFire®
ファイアウォール	PAN-OS® GlobalProtect™ エージェント/アプリ	アプリケーション [applications] アプリケーションおよび脅威 Antivirus（アンチウイルス） BrightCloud URL フィルタリング WildFire
WildFire	PAN-OS VM イメージ	WildFire

Panorama を使用してコンテンツ更新のスケジュールを設定

Panorama™ は、ファイアウォール、ログ コレクタ、WildFire® アプライアンスおよびアプライアンス クラスタ上でサポートされている更新のスケジュールを設定する際、インターネットに直接接続する必要があります。インターネットに直接接続できない場合は、オンデマンドの更新のみを行うことができます。（ログ コレクタ用にアンチウイルス、WildFire、または BrightCloud URL の更新のスケジュールを設定するには、ログ コレクタで Panorama 7.0.3 以降のバージョンを実行していなければなりません）。更新を受信する各ファイアウォール、ログ コレクタ、WildFire アプライアンスまたはアプライアンス クラスタは、インストールに成功した（設定ログ）か失敗した（システムログ）かを示すログを生成します。Panorama 管理サーバーの更新のスケジュールを設定するには、「Panorama からインターネットに接続できる場合の更新のインストール」を参照してください。

更新をデプロイする前に、「Panorama、ログ コレクタ、ファイアウォール、および WildFire のバージョン互換性」を読み、コンテンツ リリース バージョンの互換性に関する重要な詳細情報をご確認ください。*Panorama* でインストールしていなければならない最低バージョンについては『リリースノート』をご覧ください。

同じタイプの更新の場合、*Panorama* は一度に *1* つの更新しかダウンロードできません。そのため、同じ期間に同じタイプの更新を複数ダウンロードするスケジュールを設定した場合、最初のダウンロードしか成功しません。同じタイプの複数の更新を成功させるには、更新をスタッガーします。

お使いのファイアウォールが *Palo Alto Networks®* の更新サーバーに直接接続する場合は、*Panorama* テンプレート（*Device*（デバイス）> *Dynamic Updates*（動的更新）を使用してコンテンツ更新スケジュールをファイアウォールにプッシュ送信することもできます。更新ファイルがリリースされてから一定時間インストールを遅らせたい場合は、テンプレートを使用してスケジュールをデプロイする必要があります。非常に希なケースですが、コンテンツ更新にエラーが含まれている場合があるため、この遅延を指定しておくことで、ファイアウォールが更新ファイルをインストールする前に *Palo Alto Networks* によってそのような更新ファイルが特定・削除される可能性が高まります。

スケジュール設定する更新タイプごとに、以下の手順を実行します。

© 2019 Palo Alto Networks, Inc.

STEP 1 | **Panorama** > **Device Deployment**（デバイスのデプロイ）> **Dynamic Updates**（動的更新）の順に選択し、**Schedules**（スケジュール）をクリックして、スケジュールを **Add**（追加）します。

STEP 2 | スケジュール設定を識別する **Name**（名前）、更新の **Type**（タイプ）、および更新頻度（**Recurrence**（繰り返し））を指定します。頻度のオプションは、更新の **Type**（タイプ）によって異なります。

PAN-OS® は、スケジュールの更新に *Panorama* の時間帯を使用します。

Type（タイプ）を **App and Threat**（アプリケーションと脅威）に設定した場合はアプリケーション コンテンツ（脅威コンテンツではなく）だけが必要となるため、ログコレクタはそのコンテンツだけをインストールします。ファイアウォールはアプリケーションおよび脅威コンテンツをどちらも使用します。詳細は、「Panorama、ログ コレクタ、ファイアウォール、および WildFire のバージョン互換性」を参照してください。

STEP 3 | 次のいずれかのスケジュール アクションを選択し、次にファイアウォールあるいはログコレクタを選択します。

- **Download And Install**（ダウンロードおよびインストール）（推奨設定）— **Devices**（デバイス）（ファイアウォール）、**Log Collectors**（ログ コレクタ）、または **WildFire Appliances and Clusters**（**WildFire** アプライアンスおよびクラスタ）を選択します。
- **Download Only**（ダウンロードのみ）— 更新をダウンロードしますが、インストールは行いません。

STEP 4 | **OK** をクリックします。

STEP 5 | **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択して、変更内容を **Commit**（コミット）します。

Panorama がインターネットに接続されている状態でログ コレクタをアップグレード

ログ コレクタにインストールできるソフトウェア更新およびコンテンツ更新のリストについては、サポートされている更新を参照してください。

ログデータの損失を防ぐため、コレクタグループ内のすべてのログ コレクタを同時にアップグレードする必要があります。コレクタ グループ内のログ コレクタがすべて同じ PAN-OS バージョンを実行していない場合、ログ転送またはログ収集が発生することはありません。また、コレクタ グループのログ コレクタのログデータは、すべてのログ コレクタが同じ PAN-OS バージョンを実行するまで **ACC** または **Monitor (監視)**タブには表示されません。たとえば、コレクタグループ内にある 3 つのログ コレクタの内 2 つをアップグレードすると、コレクタグループのログ コレクタにログは転送されません。

PAN-OS® 9.0 では、ローカルおよび専用ログ コレクタに新しいログデータ形式が導入されています。PAN-OS 10.0 へのアップグレードパスでは、PAN-OS 9.0 にアップグレードする際に、既存のログデータが新しい形式に自動的に移行されます。再フォーマット中、ログデータは **ACC** または **Monitor (監視)** タブには表示されません。さらに、再フォーマットが完了するまで、新しいログデータがログ コレクタに転送されることはありません。再フォーマット中、新しいログはファイアウォールシステムディスクに書き込まれ、処理が正常に完了すると新しいログが適切なログ コレクタに転送されます。

Palo Alto Networks ではメンテナンス ウィンドウが開いている間にログ コレクタのアップグレードを行うことをお勧めしています。アップグレードではログ形式の移行を行うため、ローカルおよび専用ログ コレクタのログデータ量に応じて、さらに数時間かかる場合があります。

© 2019 Palo Alto Networks, Inc.

STEP 1 | ログ コレクタをアップグレードする前に、Panorama 管理サーバー上で適切な Panorama™ ソフトウェア リリースが実行されていることを確認します。



Palo Alto Networks® では、*Panorama* とログ コレクタで同じ *Panorama* ソフトウェア リリースを実行すること、および *Panorama*、ログ コレクタ、すべての管理対象ファイアウォールで同じバージョンのコンテンツ リリースを実行することを強くお勧めしています。ソフトウェアおよびコンテンツの互換性に関する重要な詳細情報については、「Panorama、ログ コレクタ、ファイアウォール、および WildFire のバージョン互換性」を参照してください。

Panorama では、ログ コレクタと同じ (またはそれ以降の) ソフトウェア リリースを実行する必要がありますが、コンテンツ リリースのバージョンは、ログ コレクタと同じか、それ以前である必要があります。

- ソフトウェア リリースのバージョン – Panorama 管理サーバーで実行しているソフトウェアのリリースが、ログ コレクタを更新するリリースと同じかそれ以降にまだなっていない場合は、それと同じか以降の Panorama リリースを Panorama にインストールしてから (「Panorama のコンテンツ更新とソフトウェア更新のインストール」を参照)、ログ コレクタを更新する必要があります。
- コンテンツ リリースのバージョン – コンテンツ リリースのバージョンについては、すべてのログ コレクタで実行されているコンテンツ リリースのバージョンが、最新であるか、または最低でも Panorama で実行されているバージョンより新しいことを確認する必要があります。そうでない場合は、最初に、管理対象ファイアウォールを更新 (Panorama を使用) してから、ログ コレクタを更新し、Panorama 管理サーバーでコンテンツ リリースのバージョンを更新します。

ソフトウェアとコンテンツのバージョンを確認するには、以下のようにします。

- **Panorama** 管理サーバー—Panorama 管理サーバーで実行中のソフトウェアとコンテンツのバージョンを確認するために、Panorama Web インターフェイスにログインし、General Information (一般情報) 設定 (**Dashboard** (ダッシュボード)) に移動します。
- ログ コレクタ—ログ コレクタで実行中のソフトウェアとコンテンツのバージョンを確認するために、各ログ コレクタの CLI にログインし、**`show system info`** コマンドを実行します。

STEP 2 | 最新のコンテンツ更新をインストールします。



Panorama ソフトウェア リリースに必要なコンテンツ リリースの最低バージョンについては、『Release Notes (リリース ノート)』を参照してください。

1. **Check Now** (今すぐチェック) (**Panorama** > **Device Deployment** (デバイスのデプロイ) > **Dynamic Updates** (動的更新)) をクリックして、最新の更新がないかを確認します。更新が入手可能な場合は、Action (アクション) 列に **Download** (ダウンロード) リンクが表示されます。
2. まだインストールしていない場合は、該当するコンテンツ更新を **Download** (ダウンロード) します。ダウンロードが正常に完了すると、Action (アクション) 列のリンクが **Download** (ダウンロード) から **Install** (インストール) に変わります。
3. 他のすべてより先にコンテンツ更新 (アプリケーションまたはアプリケーションと脅威の更新)を **Install** (インストール) します。

   Install (インストール) をクリックし、ログ コレクタを選択して **OK** をクリックします。

   アプリケーションおよび脅威コンテンツの両方がサブスクリプションに含まれているかどうかに関わらず、*Panorama* にはアプリケーション コンテンツのみが必要であり、それだけをインストールします。詳細は、「Panorama、ログ コレクタ、ファイアウォール、および WildFire のバージョン互換性」を参照してください。
4. 必要に応じて、他のすべての更新 (アンチウイルス、WildFire、あるいは URL フィルタリング) に対して、任意の順序で一度に 1 つずつ、サブステップ 2 および 3 を繰り返します。

© 2019 Palo Alto Networks, Inc.

STEP 3 | アップグレード パスを PAN-OS 10.0 に決定します。

現在実行されている PAN-OS バージョンから PAN-OS 10.0 へのパスでは、任意の機能リリース バージョンのインストールをスキップすることはできません。アップグレード パスの一部として通過する各リリースについて、『Release Notes (リリース ノート) 』で既知の問題とデフォルト動作の変更を確認し、『New Features Guide (新機能ガイド) 』でアップグレード/ダウングレードに関する考慮事項を確認してください。

(7.1 以前のリリースからアップグレードした場合は必須) PAN-OS 8.0 では新しいログ保存形式が導入されました。PAN-OS 8.0 にアップグレードした後、アップグレードパスを続行する前に、Panorama ログを新しいログ形式に移行する必要があります。ログの移行は 1 回限りのタスクです。すでにログ コレクタのログをアップグレードして PAN-OS 8.0 にアップグレードした場合は、再度それらを移行する必要はありません。



複数のログ コレクタをアップグレードする場合は、アップグレードするすべてのログ コレクタのアップグレード パスを確認し、プロセスを合理化してから、イメージのダウンロードを開始してください。

STEP 4 | PAN-OS 10.0 に更新する予定のすべてのログ コレクタに対してステップ 3 で特定したアップグレードパスを引き続き使用して、ログ コレクタを対象の Panorama リリースにアップグレードします。

1. Panorama で **Check Now** (今すぐチェック) (**Panorama** > **Device Deployment** (デバイスのデプロイ) > **Software** (ソフトウェア)) をクリックして、最新の更新がないかを確認します。更新が入手可能な場合は、Action (アクション) 列に **Download** (ダウンロード) リンクが表示されます。
2. アップグレード パスの各リリースで、アップグレードするリリース バージョンのモデル固有のファイルを **Download** (ダウンロード) します。たとえば、M-Series アプライアンスを Panorama 10.0 にアップグレードするには、 `Panorama_m-10.0.0` イメージをダウンロードします。

   ダウンロードが正常に完了すると、そのイメージの Action (アクション) 列が **Download** (ダウンロード) から **Install** (インストール) に変わります。
3. アップグレード パスの最初 (または次) のバージョンで **Install** (インストール) をクリックし、該当するログ コレクタを選択します。
4. アップグレード パス中にある、インストールしようとしているバージョンに応じて、次のいずれかを選択します (ステップ 3) 。
   - **Upload only to device (do not install)** (デバイスへのアップロードのみ (インストールしない)) 。
   - **Reboot device after Install** (インストール後にデバイスを再起動) 。
5. **OK** をクリックしてアップロードまたはインストールを開始します。
6. ログ コレクタが目的のリリースを実行するまで、サブステップ 3 から 5 を繰り返します。

STEP 5 | PAN-OS 10.0 に正常にアップグレードした後、ログ形式の移行ステータスを確認します。

1. Panorama CLI へのログインログ コレクタの Panorama CLI にログインします。
2. 次のコマンドを実行して、ログ形式の移行ステータスを確認します。

```
admin> debug logdb show-es-upgrade-time
```

ログ形式の移行が進行中の場合の応答例 :

```
Response from logger 23456212: 50.98% of indices upgraded complete.
 Approximately less than a minute remaining until migration is complete.
 Once the log migration is complete, please run the 'show log-collector-
es-cluster health' command to check the ElasticSearch cluster status to
 verify logging and reporting functionality is restored.
```


© 2019 Palo Alto Networks, Inc.

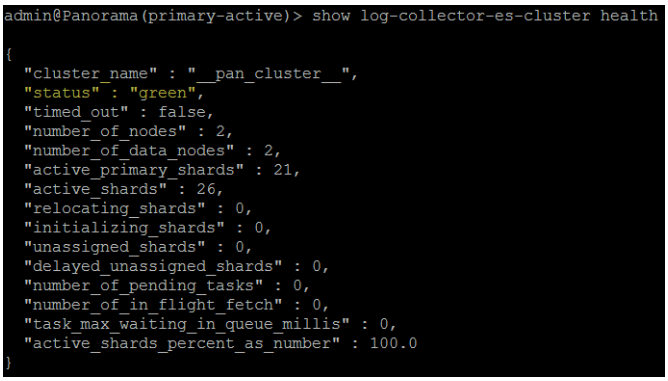
ログ形式の移行が完了したときの応答：

```
Response from logger 23456212: 100% of indices complete, please run the
 'show log-collector-es-culster health' command to check the ElasticSearch
 cluster status to verify logging and reporting functionality is restored.
```

3. ログ形式の移行が完了したら、次のコマンドを実行して ElasticSearch クラスタのステータスを確認し、次の手順に進みます。

```
admin> show log-collector-es-cluster health
```

ElasticSearch クラスタの「status」が「green」に表示されたら、次の手順に進みます。



STEP 6 | ログ コレクタにインストールされているソフトウェアおよびコンテンツ更新のバージョンを確認します。

show system info 操作コマンドを入力します。出力は以下のようになります。

```
sw-version: 10.0.0
app-version: 8270-6076
app-release-date: 2020/05/08 18:21:51
```

Panorama がインターネットに接続されていない状態でログ コレクタをアップグレード

ログ コレクタにインストールできるソフトウェア更新およびコンテンツ更新のリストについては、サポートされている更新を参照してください。

PAN-OS® 9.0 では、ローカルおよび専用ログ コレクタに新しいログデータ形式が導入されています。PAN-OS 10.0 へのアップグレードパスでは、PAN-OS 9.0 にアップグレードする際に、既存のログデータが新しい形式に自動的に移行されます。再フォーマット中、ログデータは **ACC** または **Monitor (監視)** タブには表示されません。さらに、再フォーマットが完了するまで、新しいログデータがログ コレクタに転送されることはありません。再フォーマット中、新しいログはファイアウォールシステムディスクに書き込まれ、処理が正常に完了すると新しいログが適切なログ コレクタに転送されます。

ログデータの損失を防ぐため、コレクタグループ内のすべてのログ コレクタを同時にアップグレードする必要があります。コレクタ グループ内のログ コレクタがすべて同じ PAN-OS バージョンを実行していない場合、ログ転送またはログ収集が発生することはありません。また、コレクタ グループのログ コレクタのログデータは、すべてのログ コレクタが同じ PAN-OS バージョンを実行するまで **ACC** または **Monitor (監視)**タブには表示されません。たとえば、コレクタグループ内にある 3 つのログ コレクタの内 2 つをアップグレードすると、コレクタグループのログ コレクタにログは転送されません。

© 2019 Palo Alto Networks, Inc.

Palo Alto Networks ではメンテナンス ウィンドウが開いている間にログ コレクタのアップグレードを行うことをお勧めしています。アップグレードではログ形式の移行を行うため、ローカルおよび専用ログ コレクタのログデータ量に応じて、さらに数時間かかる場合があります。

STEP 1 | ログ コレクタをアップグレードする前に、Panorama 管理サーバー上で適切な Panorama™ ソフトウェア リリースが実行されていることを確認します。



Palo Alto Networks® では、*Panorama* とログ コレクタで同じ *Panorama* ソフトウェア リリースを実行すること、および *Panorama*、ログ コレクタ、すべての管理対象ファイアウォールで同じバージョンのコンテンツ リリースを実行することを強くお勧めしています。ソフトウェアおよびコンテンツの互換性に関する重要な詳細情報については、「Panorama、ログ コレクタ、ファイアウォール、および WildFire のバージョン互換性」を参照してください。

Panorama では、ログ コレクタと同じ (またはそれ以降の) ソフトウェア リリースを実行する必要がありますが、コンテンツ リリースのバージョンは、ログ コレクタと同じか、それ以前である必要があります。

- ソフトウェア リリースのバージョン – Panorama 管理サーバーで実行しているソフトウェアのリリースが、ログ コレクタを更新するリリースと同じかそれ以降にまだなっていない場合は、それと同じか以降の Panorama リリースを Panorama にインストールしてから (「Panorama のコンテンツ更新とソフトウェア更新のインストール」を参照)、ログ コレクタを更新する必要があります。
- コンテンツ リリースのバージョン – コンテンツ リリースのバージョンについては、すべてのログ コレクタで実行されているコンテンツ リリースのバージョンが、最新であるか、または最低でも Panorama にインストールするバージョンもしくは Panorama で実行されているバージョンより新しいことを確認する必要があります。そうでない場合は、最初に、管理対象ファイアウォールを更新 (Panorama を使用) してから、ログ コレクタを更新し、Panorama 管理サーバーでコンテンツ リリースのバージョンを更新します (「Panorama のコンテンツ更新とソフトウェア更新のインストール」を参照)。

ソフトウェアとコンテンツのバージョンを確認するには、以下のようにします。

- **Panorama** 管理サーバー—Panorama 管理サーバーで実行中のソフトウェアとコンテンツのバージョンを確認するために、Panorama Web インターフェイスにログインし、General Information (一般情報) 設定 (**Dashboard** (ダッシュボード)) に移動します。
- ログ コレクタ—ログ コレクタで実行中のソフトウェアとコンテンツのバージョンを確認するために、各ログ コレクタの CLI にログインし、**`show system info`** コマンドを実行します。

STEP 2 | ログ コレクタにインストールする必要のあるコンテンツ更新を決定します。Panorama でインストールしていなければならない最低バージョンについては『リリースノート』をご覧ください。



最初に、コンテンツ更新をインストールしてからソフトウェア更新をインストールします。

1. **`show system info`** CLI コマンドを実行し、更新の最新バージョンを表示します。
2. コンテンツ更新ごとに、更新が必要であるかどうかを確認し、ステップ 4 でダウンロードする必要があるコンテンツ更新を確認しておきます。

   Panorama で実行しているコンテンツ リリースのバージョンが、管理対象ファイアウォールとログ コレクタで実行しているバージョンと同じか、それ以前であることを確認します。
3. (必要に応じて) ログ コレクタでコンテンツのバージョンを更新するには、最初に管理対象ファイアウォールを同じバージョンまたはより新しいバージョンのコンテンツ リリースにアップグレードします。

© 2019 Palo Alto Networks, Inc.

STEP 3 | アップグレード パスを PAN-OS 10.0 に決定します。

現在実行されている PAN-OS バージョンから PAN-OS 10.0 へのパスでは、任意の機能リリース バージョンのインストールをスキップすることはできません。アップグレード パスの一部として通過する各リリースについて、『Release Notes (リリース ノート) 』で既知の問題とデフォルト動作の変更を確認し、『New Features Guide (新機能ガイド) 』でアップグレード/ダウングレードに関する考慮事項を確認してください。

(7.1 以前のリリースからアップグレードした場合は必須) PAN-OS 8.0 では新しいログ保存形式が導入されました。PAN-OS 8.0 にアップグレードした後、アップグレードパスを続行する前に、Panorama ログを新しいログ形式に移行する必要があります。ログの移行は 1 回限りのタスクです。すでにログ コレクタのログをアップグレードして PAN-OS 8.0 にアップグレードした場合は、再度それらを移行する必要はありません。



複数のログ コレクタをアップグレードする場合は、アップグレードするすべてのログ コレクタのアップグレード パスを確認し、プロセスを合理化してから、イメージのダウンロードを開始してください。

STEP 4 | Panorama に接続してファイルをアップロードできるホストに、SCP または HTTPS でコンテンツとソフトウェア更新をダウンロードします。

1. インターネットにアクセスできるホストを使用して、Palo Alto Networks のカスタマー サポート Web サイトにログインします。
2. コンテンツ更新のダウンロード :
   1. Resources (リソース) セクションで **Dynamic Updates** (動的更新) をクリックします。
   2. 目的のコンテンツ更新を **Download** (ダウンロード) し、ファイルをホストに保存します。アップデートするコンテンツ タイプごとにこのステップを繰り返します。
3. ソフトウェア更新のダウンロード :
   1. Palo Alto Networks® のカスタマー サポート Web サイトのメイン ページに戻り、Resources (リソース) セクションの **Software Updates** (ソフトウェア更新) をクリックします。
   2. Download (ダウンロード) 列の表示を確認し、インストールするバージョンを決定します。M-Series アプライアンスの更新パッケージのファイル名は、「Panorama_m」で始まり、その後にリリース番号が続いています。たとえば、M-Series アプライアンスを Panorama 10.0.0 にアップグレードするには、 `Panorama_m-10.0.0` イメージをダウンロードします。

      Filter By (フィルタ基準) ドロップダウンで *Panorama M Images* (*Panorama M* イメージ) (*M-Series* アプライアンスの場合) を選択すると、*Panorama* イメージをすばやく見つけることができます。
4. 該当するファイル名をクリックし、ファイルをホストに保存します。

STEP 5 | ログ コレクタにコンテンツ更新をインストールします。



コンテンツ更新をインストールする必要がある場合は、ソフトウェア更新をインストールする前に、その作業を行ってください。また、コンテンツ更新のインストールは、ファイアウォール、ログ コレクタの順に行い、その後、*Panorama* 上でコンテンツ リリースのバージョンを更新してください。

アプリケーション更新あるいはアプリケーションおよび脅威更新をまずインストールした後、必要に応じて、任意の順序で一度に 1 つずつ、他の更新 (アンチウイルス、WildFire®、あるいは URL フィルタリング) をすべてインストールします。



アプリケーションおよび脅威コンテンツの両方がサブスクリプションに含まれているかどうかに関わらず、*Panorama* にはアプリケーション コンテンツのみが必要であり、そ

© 2019 Palo Alto Networks, Inc.

れだけをインストールします。詳細は、「Panorama、ログ コレクタ、ファイアウォール、および WildFire のバージョン互換性」を参照してください。

1. PanoramaでPanorama > Device Deployment > Dynamic Updates(Panorama > デバイスのデプロイ > ダイナミック更新) の順に選択します。
2. Upload (アップロード) をクリックして、更新の Type (タイプ) を選択します。次に、ホスト上の該当するコンテンツ更新ファイルを Browse (参照) して OK をクリックします。
3. Install From File (ファイルからインストール) をクリックし、更新の Type (タイプ) を選択してから、アップロードした更新の File Name (ファイル名) を選択します。
4. ログ コレクタを選択します。
5. OK をクリックしてインストールを開始します。
6. コンテンツ更新ごとに、これらのステップを繰り返します。

STEP 6 | ソフトウェア更新をインストールします。

1. Panorama > Device Deployment (デバイスのデプロイ) > Software (ソフトウェア) を選択します。
2. ホスト上で Upload (アップロード) をクリックし、該当するソフトウェア更新ファイルを Browse (参照) して OK をクリックします。
3. アップロードしたリリースの Action (アクション) 列にある Install (インストール) をクリックします。
4. 更新をインストールするログ コレクタを選択します。
5. アップグレード パス中にある、インストールしようとしているソフトウェアのバージョンに応じて、次のいずれかを選択します (ステップ 3)。
   - Upload only to device (do not install) (デバイスへのアップロードのみ (インストールしない))。
   - Reboot device after Install (インストール後にデバイスを再起動)。
6. OK をクリックしてインストールを開始します。

STEP 7 | PAN-OS 10.0 へのアップグレードが正常に完了したら、ログ形式の移行ステータスを確認します。

1. Panorama CLI へのログインログ コレクタの Panorama CLI にログインします。
2. 次のコマンドを実行して、ログ形式の移行ステータスを確認します。

```
admin> debug logdb show-es-upgrade-time
```

ログ形式の移行が進行中の場合の応答例：

```
Response from logger 23456212: 50.98% of indices upgraded complete.
 Approximately less than a minute remaining until migration is complete.
 Once the log migration is complete, please run the 'show log-collector-
es-cluster health' command to check the ElasticSearch cluster status to
 verify logging and reporting functionality is restored.
```

ログ形式の移行が完了したときの応答：

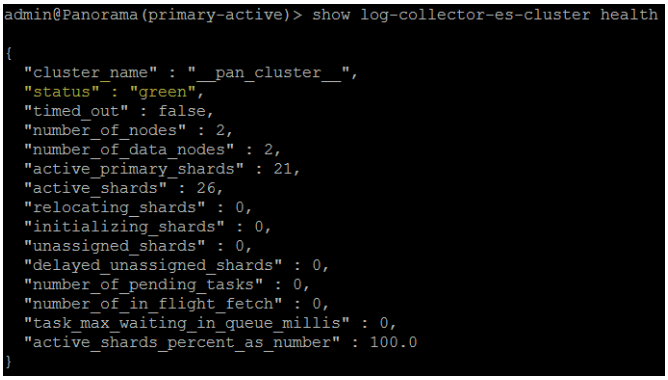
```
Response from logger 23456212: 100% of indices complete, please run the
 'show log-collector-es-culster health' command to check the ElasticSearch
 cluster status to verify logging and reporting functionality is restored.
```

3. ログ形式の移行が完了したら、次のコマンドを実行して ElasticSearch クラスタのステータスを確認し、次の手順に進みます。

© 2019 Palo Alto Networks, Inc.

```
admin> show log-collector-es-cluster health
```

ElasticSearch クラスタの「status」が「green」に表示されたら、次の手順に進みます。



STEP 8 | 各ログ コレクタにインストールされているソフトウェアおよびコンテンツのバージョンを確認します。

ログコレクタのCLIにログインし、操作コマンド**show system info**を入力します。出力は以下のようになります。

```
sw-version: 10.0.0
app-version: 8270-6076
app-release-date: 2020/05/08 18:21:51
```

Panorama がインターネットに接続されている状態でファイアウォールをアップグレード

PAN-OS 10.0 リリース ノートを確認してから、次の手順に従い Panorama で管理するファイアウォールをアップグレードします。この手順は、高可用性 (HA) 設定でデプロイされたスタンド アロン ファイアウォールとファイアウォールに適用されます。

Panorama が直接更新サーバーに接続できない場合は、*Panorama* にイメージを手動でダウンロードしてファイアウォールに配信できるように、Panorama がインターネットに接続されていないときにファイアウォールをアップグレードする手順に従います。

Panorama からファイアウォールをアップグレードする前に、次のことを行う必要があります :

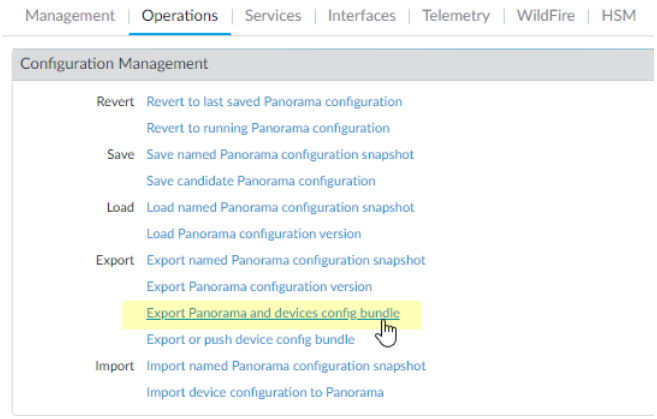
- Panorama がアップグレードしているものと同じかそれ以降の PAN-OS バージョンを実行していることを確認してください。管理対象ファイアウォールを PAN-OS 10.0 にアップグレードする前に、Panorama のコンテンツおよびソフトウェア アップグレードのインストールと、Panorama を使用したファイアウォール、ログ コレクタ、および WildFire アプライアンスへの更新のデプロイを行い、Panorama とログ コレクタ PAN-OS 10.0 にアップグレードします。
- ファイアウォールが信頼できる電源に接続されていることを確認してください。アップグレード中に電力が失われると、ファイアウォールを使用できなくなる可能性があります。

STEP 1 | アップグレードする各管理対象ファイアウォールで、現在の設定ファイルのバックアップを保存します。

© 2019 Palo Alto Networks, Inc.

ファイアウォールは自動的に設定のバックアップを作成しますが、アップグレード前にバックアップを作成して外部に保存しておくことをお勧めします。

1. Panorama Web インターフェイスで、**Panorama** > **Setup**（セットアップ）> **Operations**（操作）を選択し、**Export Panorama and devices config bundle**（**Panorama** および**Device**（デバイス）の設定バンドルのエクスポート）をクリックして、最新の Panorama と各管理アプライアンスの最新の設定バックアップを生成してエクスポートします。

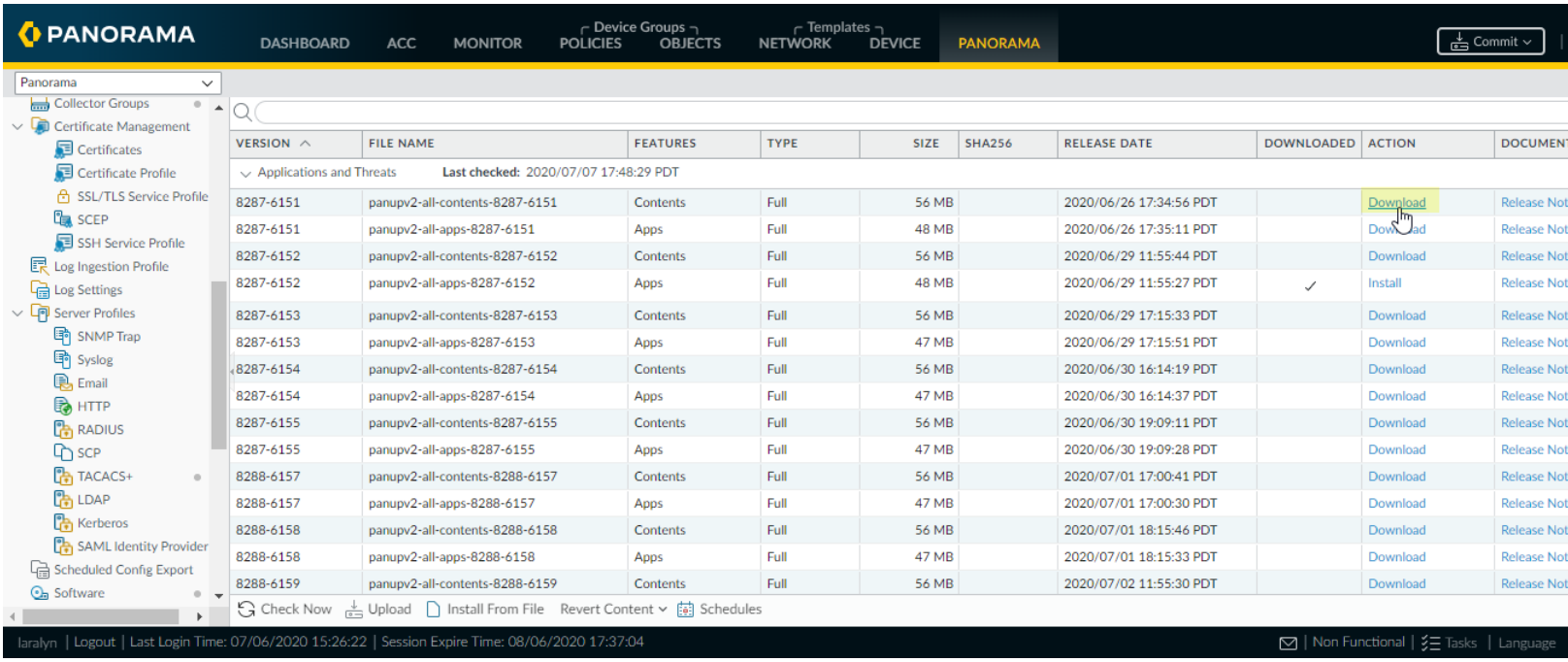


2. エクスポート ファイルをファイアウォールの外部に保存します。アップグレードで問題が発生した場合は、このバックアップを使用して設定を復元することができます。

STEP 2 | アップグレードするファイアウォールのコンテンツ リリース バージョンを更新します。

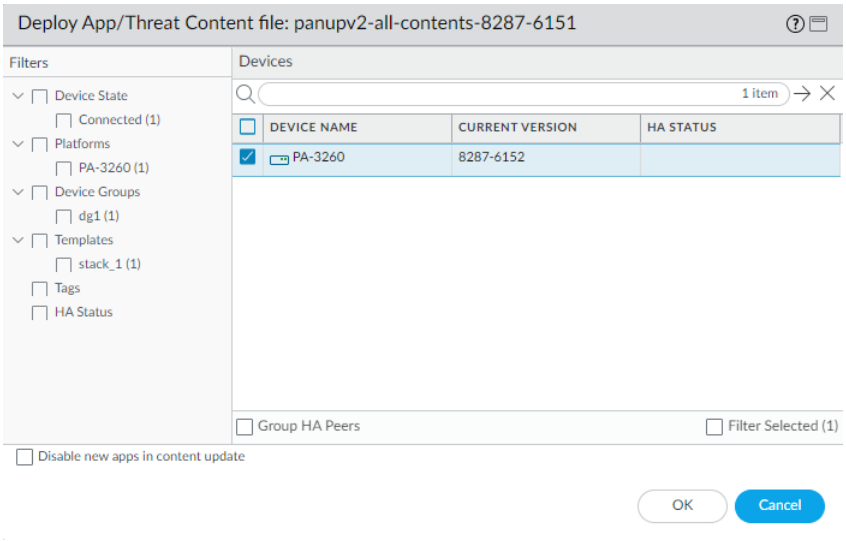
PAN-OS 10.0 のリリースに必要な最低コンテンツ リリース バージョンについては、リリース ノートをご覧ください。Panorama と管理対象のファイアウォールのコンテンツ更新をデプロイする際は、必ずアプリケーションと脅威更新に関するベストプラクティスに従ってください。

1. **Panorama** > **Device Deployment**（デバイスのデプロイメント）> **Dynamic Updates**（動的更新）を選択して、最新の更新を **Check Now**（今すぐチェック）します。更新が入手可能な場合は、Action（アクション）列に **Download**（ダウンロード）リンクが表示されます。



© 2019 Palo Alto Networks, Inc.

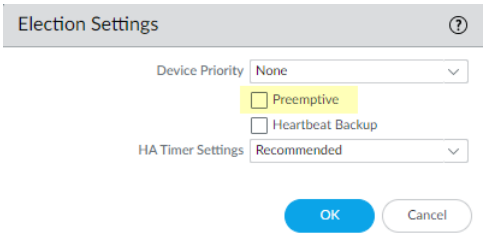
2. まだインストールしていない場合は、最新のコンテンツ リリース バージョンを **Download**（ダウンロード）します。
3. **Install**（インストール）をクリックし、更新をインストールするファイアウォールを選択してから、**OK** をクリックします。HA ファイアウォールをアップグレードする場合は、両方のピアのコンテンツを更新する必要があります。



デフォルトでは、各タイプのソフトウェア更新またはコンテンツ更新を最大 *2* つ *Panorama* アプライアンスにアップロードできます。同じタイプの更新をもう *1* つダウンロードすると、*Panorama* は、そのタイプの最も古いバージョンの更新を削除します。単一タイプで *3* 個以上のソフトウェア更新またはコンテンツ更新をアップロードする必要がある場合は、*CLI* コマンド ***setmax-num-images count <number>*** を使用して最大数を拡大してください。

STEP 3 | （HA ファイアウォールのアップグレードのみ）HA ペアの一部であるファイアウォールをアップグレードする場合は、プリエンプションを無効にします。各 HA ペアの 1 つのファイアウォールでのみ、この設定を無効にする必要があります。

1. **Device**（デバイス）> **High Availability**（高可用性）を選択して **Election Settings**（選択設定）を編集します。
2. 有効になっている場合は、**Preemptive**（プリエンプティブ）設定を無効（クリア）して、**OK** をクリックします。



3. 変更を **Commit**（コミット）します。アップグレードを続行する前に、コミットが成功していることを確認してください。

STEP 4 | アップグレード パスを PAN-OS 10.0 に決定します。

現在実行されている PAN-OS バージョンから PAN-OS 10.0.0 へのアップグレードパスに機能リリース バージョンのインストールをスキップすることはできません。アップグレード パスの一部として通過する各リリースについて、『Release Notes（リリース ノート）』で既知の問題とデフォルト動作の変

© 2019 Palo Alto Networks, Inc.

更を確認し、『New Features Guide（新機能ガイド）』でアップグレード/ダウングレードに関する考慮事項を確認してください。



複数のファイアウォールをアップグレードする場合は、すべてのファイアウォールのアップグレード パスを確認し、プロセスを合理化してから、イメージのダウンロードを開始してください。

STEP 5 | 対象の PAN-OS 10.0 リリース イメージをダウンロードします。

1. **Panorama** > **Device Deployment**（デバイスのデプロイメント）> **Software**（ソフトウェア）を選択して、最新のリリース バージョンを **Check Now**（今すぐチェック）します。
2. アップグレードするリリース バージョンのファイアウォール固有のファイルを **Download**（ダウンロード）します。アップグレードするファイアウォールのモデル（またはファイアウォール シリーズ）ごとに個別のインストール ファイルをダウンロードする必要があります。

   たとえば、PA-220、および PA-5250 の各ファイアウォールを PAN-OS 10.0.0 にアップグレードするには、`PanOS_220-10.0.0`、`PanOS_3000-10.0.0`、および `PanOS_5200-10.0.0` の各イメージをダウンロードします。イメージを正常にダウンロードすると、アクション列がそのイメージの **Install**（インストール）に変わります。

STEP 6 | PAN-OS 10.0 のソフトウェアのアップデートをインストールします。



ブランチ ファイアウォールをアップグレードする前にハブ ファイアウォールを *PAN-OS 10.0.0* から *PAN-OS 10.0.1* 以降のリリースにアップグレードする必要があります。ハブ ファイアウォールの前にブランチ ファイアウォールをアップグレードすると、モニタリングのデータ *(Panorama* > *SD-WAN* > *Monitoring (*モニタリング*))* が不正確になり、また、*SD-WAN* リンクが間違って `down` と表示される可能性があります。

1. アップグレードするファイアウォールモデルに対応するアクション列の **Install**（インストール）をクリックします。例えば、PA-220 ファイアウォールをアップグレードする場合は、PanOS_220-10.0.0 に対応する行の**Install**（インストール）をクリックします。
2. ソフトウェア ファイルのデプロイ ダイアログで、アップグレードするすべてのファイアウォールを選択します。ダウンタイムを短縮するには、各 HA ペアで 1 つのピアだけを選択します。アクティブ/パッシブ ペアの場合、パッシブ ピアを選択します。アクティブ/アクティブ ペアの場合は、アクティブ-セカンダリ ピアを選択します。
3. （HA ファイアウォールのアップグレードのみ）**Group HA Peers**（グループ **HA** ピア）が選択されないことを確認してください。
4. **Reboot device after Install**（インストール後にデバイスを再起動）を選択します。
5. アップグレードを開始するには、**OK** をクリックします。
6. インストールが正常に完了したら、次のいずれかの方法によって再起動します。
   - 再起動を促されたら、**Yes**（はい）をクリックします。
   - 再起動を促されなかったら、**Device**（デバイス）> **Setup**（セットアップ）> **Operations**（操作）を選択し、**Reboot Device**（デバイスの再起動）を選択します。
7. ファイアウォールの再起動が完了したら、**Panorama** > **Managed Devices**（管理対象デバイス）を選択し、アップグレードしたファイアウォールのソフトウェア バージョンが 10.0.0 であることを確認します。また、アップグレードしたパッシブ ファイアウォールの HA ステータスがまだパッシブであることを確認します。

STEP 7 | （HA ファイアウォールのアップグレードのみ）各 HA ペアの 2 番目の HA ピアをアップグレードします。

1. （アクティブ/パッシブ アップグレードのみ）アップグレードする各アクティブ/パッシブペアでアクティブデバイスをサスペンドします。

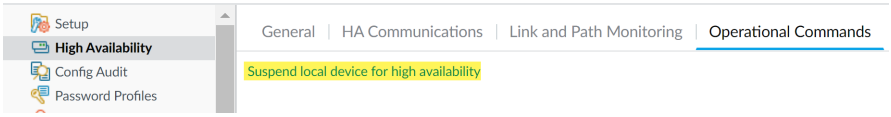
   1. コンテキストをアクティブなファイアウォールに切り替えます。

© 2019 Palo Alto Networks, Inc.

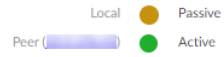
2. **Dashboard**（ダッシュボード）の高可用性ウィジット内で、, verify that **Local**（ローカル）ファイアウォールの状態が **Active**（アクティブ）であり、**Peer**（ピア）が **Passive**（パッシブ）であることを確認します。



3. **Device**（デバイス）> **High Availability**（高可用性）> **Operational Commands**（操作コマンド）> **Suspend local device**（ローカル **Device**（デバイスのサスペンド）。



4. **Dashboard**（ダッシュボード）の高可用性ウィジットに戻り、**Local**（ローカル）が **Passive**（パッシブ）に、**Peer**（ピア）が **Active**（アクティブ）に変更したことを確認します。



2. Panorama コンテキストに戻り、**Panorama** > **Device Deployment**（デバイスのデプロイ）> **Software**（ソフトウェア）を選択します。
3. アップグレードする HA ペアのファイアウォール モデルに対応するアクション列の **Install**（インストール）をクリックします。
4. ソフトウェア ファイルのデプロイ ダイアログで、アップグレードするすべてのファイアウォールを選択します。今回は、アップグレードしたばかりの HA ファイアウォールのピアだけを選択します。
5. **Group HA Peers**（グループ **HA** ピア）が選択されないことを確認してください。
6. **Reboot device after Install**（インストール後にデバイスを再起動）を選択します。
7. アップグレードを開始するには、**OK** をクリックします。
8. インストールが正常に完了したら、次のいずれかの方法によって再起動します。
   - 再起動を促されたら、**Yes**（はい）をクリックします。
   - 再起動を促されなかったら、**Device**（デバイス）> **Setup**（セットアップ）> **Operations**（操作）を選択し、**Reboot Device**（デバイスの再起動）を選択します。
9. （アクティブ/パッシブ アップグレードのみ）アップグレードしたばかりのピアの CLI から、次のコマンドを実行してファイアウォールを再び機能させます。

   ```
   request high-availability state functional
   ```

STEP 8 | 各管理対象ファイアウォールで実行されているソフトウェアおよびコンテンツ リリース バージョンを確認します。

1. Panorama で、**Panorama** > **Managed Devices**（管理対象デバイス）を選択します。
2. ファイアウォールを見つけ、表のコンテンツおよびソフトウェアのバージョンを確認します。

   HA ファイアウォールの場合、各ピアの HA ステータスが想定どおりであることを確認することもできます。

© 2019 Palo Alto Networks, Inc.

	DEVICE NAME	MODEL	IP Address IPV4	TEMPLATE	Status DEVICE STATE	HA STATUS	CERTIFICATE	L... M... D...	SOFTWARE VERSION	APPS AND THREAT	ANTIVIRUS
DG-VM (5/5 Devices Connected): Shared > DG-VM											
	PA-VM-6	PA-VM		Stack-VM	Connected		pre-defined		8.1.0	8320-6307	3881-4345
	PA-VM-73	PA-VM		Stack-Test73	Connected		pre-defined		9.1.3	8320-6307	3873-4337
	PA-VM-95	PA-VM		Stack-VM	Connected		pre-defined		10.0.0	8320-6307	3881-4345
	PA-VM-96	PA-VM		Stack-VM	Connected	Passive	pre-defined		10.0.0	8299-6216	3881-4345
	PA-VM			Stack-Test92	Connected	Active	pre-defined		10.0.0	8299-6216	3881-4345

STEP 9 | （HA ファイアウォールのアップデートのみ）アップグレード前に HA ファイアウォールの一方でプリエンプションを無効にした場合は、**Election Settings**（選択設定）（**Device**（デバイス）> **High Availability**（高可用性））を編集し、そのファイアウォールの **Preemptive**（プリエンプティブ）設定を再び有効にして、変更を **Commit**（コミット）します。

Panorama がインターネットに接続されていない状態でファイアウォールをアップグレード

ファイアウォールにインストールできるソフトウェア更新およびコンテンツ更新のリストが「サポートされている更新」に記載されています。

STEP 1 | 管理対象ファイアウォールをアップグレードする前に、Panorama 管理サーバーおよびログ コレクタ上で適切な Panorama™ ソフトウェア リリースが実行されていることを確認します。

Palo Alto Networks® では、*Panorama* とログ コレクタで同じ *Panorama* ソフトウェア リリースを実行すること、および *Panorama*、ログ コレクタ、すべての管理対象ファイアウォールで同じバージョンのコンテンツ リリースを実行することを強くお勧めしています。

ソフトウェアおよびコンテンツの互換性に関する重要な詳細情報については、「Panorama、ログ コレクタ、ファイアウォール、および WildFire のバージョン互換性」を参照してください。

Panorama では、ファイアウォールと同じ（またはそれ以降の）ソフトウェア リリースを実行する必要がありますが、コンテンツ リリースのバージョンは、ファイアウォールと同じか、それ以前である必要があります。

- ソフトウェア リリースのバージョン – Panorama 管理サーバーまたはログ コレクタで実行しているソフトウェアのリリースが、ファイアウォールを更新するリリースと同じかそれ以降にまだなっていない場合は、それと同じか以降の Panorama リリースを Panorama とログ コレクタにインストールしてから（「Panorama のコンテンツ更新とソフトウェア更新のインストール」を参照）、ファイアウォールを更新する必要があります。
- コンテンツ リリースのバージョン – コンテンツ リリースのバージョンについては、すべてのファイアウォールで実行されているコンテンツ リリースのバージョンが、最新であるか、または最低でも Panorama とログ コレクタで実行されているバージョンより新しいことを確認する必要があります。そうでない場合は、管理対象ファイアウォールを更新してから、Panorama がインターネットに接続されていない状態でログ コレクタをアップグレードし、Panorama 管理サーバーでコンテンツ リリースのバージョンを更新してください（「Panorama のコンテンツ更新とソフトウェア更新のインストール」を参照）。

© 2019 Palo Alto Networks, Inc.

ソフトウェアとコンテンツのバージョンを確認するには、以下のようにします。

- **Panorama** 管理サーバー – Panorama Web インターフェイスにログインし、General Information（一般情報）設定（**Dashboard**（ダッシュボード））に移動します。
- ログ コレクタ – 各ログ コレクタの CLI にログインし、**`show system info`** コマンドを実行します。

STEP 2 | アップグレードする各管理対象ファイアウォールで、現在の設定ファイルのバックアップを保存します。

ファイアウォールは自動的に設定のバックアップを作成しますが、アップグレード前にバックアップを作成して外部に保存しておくことをお勧めします。

1. **Export Panorama and devices config bundle**（**Panorama** およびデバイスの設定バンドルのエクスポート）（**Panorama** > **Setup**（セットアップ）> **Operations**（操作））を選択し、Panorama と各管理対象アプライアンスの最新の設定のバックアップを生成してエクスポートします。
2. エクスポート ファイルをファイアウォールの外部に保存します。アップグレードで問題が発生した場合は、このバックアップを使用して設定を復元することができます。

STEP 3 | インストールする必要のあるコンテンツ更新を確認します。PAN-OS® リリース用にインストールする必要のあるコンテンツ リリースの最低バージョンについては、『Release Notes（リリース ノート）』を参照してください。

Palo Alto Networks では、*Panorama*、ログ コレクタ、およびすべての管理対象ファイアウォールで実行するコンテンツ リリースのバージョンを同じにすることを強くお勧めしています。

コンテンツ更新ごとに、更新が必要であるかどうかを確認し、ステップ 5 でダウンロードする必要があるコンテンツ更新を確認しておきます。

Panorama で実行しているコンテンツ リリースのバージョンが、管理対象ファイアウォールとログ コレクタで実行しているバージョンと同じか、それ以前であることを確認します。

STEP 4 | Panorama 10.0 に更新するファイアウォールのソフトウェア アップグレード パスを決定します。PAN-OS 10.0 へのアップグレード パスについては、『New Features Guide（新機能ガイド）』を参照してください。

Panorama にログインし、**Panorama** > **Managed Devices**（管理対象デバイス）の順に選択して、アップグレードするファイアウォールの現在のソフトウェア バージョンを確認しておきます。

アップグレード パスの一環として対応するリリース毎について、既知の問題およびデフォルトの動作に関する変更については、Release Notes（リリースノート）で確認し、アップグレードまたはダウングレードに関する考慮事項については、New Features Guide（新機能ガイド）で確認することを強く推奨します。

STEP 5 | Panorama に接続してファイルをアップロードできるホストに、SCP または HTTPS でコンテンツとソフトウェア更新をダウンロードします。

デフォルトでは、各タイプのソフトウェア更新またはコンテンツ更新を最大 2 つ Panorama アプライアンスにアップロードできます。同じタイプの更新をもう 1 つダウンロードすると、Panorama は、そのタイプの最も古いバージョンの更新を削除します。1 つのタイプのソフトウェア更新またはコンテンツ更新を 3 つ以上アップロードする必要がある場合は、**`set max-num-images count <number>`**CLI コマンドを使用して、Panorama が保存できるイメージの最大数を増やします。

© 2019 Palo Alto Networks, Inc.

1. インターネットにアクセスできるホストを使用して、Palo Alto Networks のカスタマー サポート Web サイトにログインします。
2. コンテンツ更新のダウンロード：
   1. Resources（リソース）セクションで **Dynamic Updates**（動的更新）をクリックします。
   2. コンテンツ リリースの最新バージョン（または、最低でも、Panorama 管理サーバーに対してインストールまたは実行するのと同じか、それ以降のバージョン）を **Download**（ダウンロード）して、ホストにファイルを保存します。更新する必要のあるコンテンツ タイプごとに、この作業を繰り返します。
3. ソフトウェア更新のダウンロード：
   1. Palo Alto Networks カスタマーサポート Web サイトのメイン ページに戻り、Resources（リソース）セクションの **Software Updates**（ソフトウェア更新）をクリックします。
   2. ダウンロード列を参照し、インストールする必要のあるバージョンを確認します。更新パッケージのファイル名は、モデルを示しています。たとえば、PA-220、および PA-5260 の各ファイアウォールを PAN-OS 8.0.8 にアップグレードするには、`PanOS_220-8.0.8`、`PanOS_3000-8.0.8`、および `PanOS_5200-8.0.8` の各イメージをダウンロードします。

      Filter By（フィルタ基準）ドロップダウンで *PAN-OS for the PA*（*PA* の *PAN-OS*）*-<series/model>* を選択すると、特定の *PAN-OS* イメージをすばやく見つけることができます。
4. 該当するファイル名をクリックし、ファイルをホストに保存します。

STEP 6 | 管理対象ファイアウォールにコンテンツ更新をインストールします。

最初に、コンテンツ更新をインストールしてからソフトウェア更新をインストールします。

アプリケーション更新あるいはアプリケーションおよび脅威更新をまずインストールした後、必要に応じて、任意の順序で一度に 1 つずつ、他の更新（アンチウイルス、WildFire®、あるいは URL フィルタリング）をすべてインストールします。

1. **Panorama** > **Device Deployment**（デバイスのデプロイ）> **Dynamic Updates**（ダイナミック更新）を選択します。
2. **Upload**（アップロード）をクリックして、更新の **Type**（タイプ）を選択します。次に、該当するコンテンツ更新ファイルを **Browse**（参照）して、**OK** をクリックします。
3. **Install From File**（ファイルからインストール）をクリックし、更新の **Type**（タイプ）を選択してから、アップロードしたコンテンツ更新の **File Name**（ファイル名）を選択します。
4. 更新をインストールするファイアウォールを選択します。
5. **OK** をクリックしてインストールを開始します。
6. コンテンツ更新ごとに、これらのステップを繰り返します。

STEP 7 | （GlobalProtect™ ポータルとして機能しているファイアウォールのみ）GlobalProtect エージェント/アプリ ソフトウェア更新をファイアウォールにアップロードしてアクティベートします。

ファイアウォール上の更新をアクティベートして、ユーザーがエンドポイント（クライアント システム）にダウンロードできるようにします。

1. インターネットにアクセスできるホストを使用して、Palo Alto Networks のカスタマー サポート Web サイトにログインします。
2. 該当する GlobalProtect エージェント/アプリ ソフトウェア更新をダウンロードします。
3. Panorama で **Panorama** > **Device Deployment**（デバイスのデプロイ）> **GlobalProtect Client**（**GlobalProtect** クライアント）を選択します。

© 2019 Palo Alto Networks, Inc.

4. ファイルをダウンロードしたホスト上で、**Upload**（アップロード）をクリックします。次に、該当する GlobalProtect エージェント/アプリ ソフトウェア更新を **Browse**（参照）し、**OK** をクリックします。
5. **Activate From File**（ファイルからアクティベーション）をクリックし、アップロードした GlobalProtect エージェント/アプリ更新の **File Name**（ファイル名）を選択します。

   アクティベートできるエージェント/アプリ ソフトウェアのバージョンは、一度に *1* つのみです。新しいバージョンをアクティベートしたが、以前のバージョンを必要としているエージェントがある場合は、以前のバージョンを再びアクティベートして、それらのエージェントが以前の更新をダウンロードできるようにする必要があります。
6. 更新をアクティベートするファイアウォールを選択します。
7. **OK** をクリックして、アクティベーションを実行します。

STEP 8 | PAN-OS ソフトウェア更新をアップロードします。

1. **Panorama** > **Device Deployment**（デバイスのデプロイ） > **Software**（ソフトウェア）を選択します。
2. ホスト上で **Upload**（アップロード）をクリックし、該当するソフトウェア更新ファイルを **Browse**（参照）して **OK** をクリックします。

STEP 9 | PAN-OS ソフトウェア更新をインストールします。

高可用性（*HA*）のファイアウォールのソフトウェア更新時にダウンタイムが発生しないようにするために、一度に *1* つだけ *HA* ピアをアップデートします。

アクティブ/アクティブ ファイアウォールの場合、どちらのピアからアップデートしても構いません。

アクティブ/パッシブ ファイアウォールの場合、最初にパッシブ ピアをアップデートし、アクティブ ピアはサスペンド（フェイルオーバー）し、アクティブ ピアをアップデートし、次にアクティブ ピアを稼動状態に戻す（フェイルバック）必要があります。

ブランチ ファイアウォールをアップグレードする前にハブ ファイアウォールを *PAN-OS 10.0.0* から *PAN-OS 10.0.1* 以降のリリースにアップグレードする必要があります。ハブ ファイアウォールの前にブランチ ファイアウォールをアップグレードすると、モニタリングのデータ *(Panorama > SD-WAN > Monitoring (*モニタリング*))* が不正確になり、また、*SD-WAN* リンクが間違って `down` と表示されます。

1. ご自分のファイアウォール構成に該当するステップを実行し、アップロードした PAN-OS ソフトウェア更新をインストールします。
   - 非 **HA** ファイアウォール –Action（アクション）列の **Install**（インストール）をクリックし、アップグレードするファイアウォールをすべて選択し、**Reboot device after install**（インストール後にデバイスを再起動）を選択して **OK** をクリックします。
   - アクティブ/アクティブ **HA** ファイアウォール：
     1. アップグレードする最初のピア上で、プリエンプション設定が無効になっていることを確認します（**Device**（デバイス） > **High Availability**（高可用性） > Election Settings（選択設定））。有効になっている場合は、**Election Settings**（選択設定）を編集し、**Preemptive**（プリエンプティブ）設定を無効に（クリア）して、変更内容を **Commit**（コミット）します。この設定は、各 HA ペアの一方のファイアウォールでのみ無効にする必要がありますが、続行する前にコミットが成功していることを確認してください。
     2. **Install**（インストール）をクリックして、**Group HA Peers**（グループ **HA** ピア）を無効に（クリア）します。次に、**Reboot device after install**（インストール後にデバイスを再起

© 2019 Palo Alto Networks, Inc.

動）を選択して、**OK** をクリックします。ファイアウォールの再起動が完了するのを待ってから、続行してください。

3. **Install**（インストール）をクリックして、**Group HA Peers**（グループ **HA** ピア）を無効に（クリア）します。次に、前のステップで更新しなかった HA ピアを選択し、**Reboot device after install**（インストール後にデバイスを再起動）を選択して **OK** をクリックします。

- アクティブ/パッシブ **HA** ファイアウォール –この例では、アクティブ ファイアウォールの名前が fw1、パッシブ ファイアウォールの名前が fw2 です。

1. アップグレードする最初のピア上で、プリエンプション設定が無効になっていることを確認します（**Device**（デバイス）> **High Availability**（高可用性）> Election Settings（選択設定））。有効になっている場合は、**Election Settings**（選択設定）を編集し、**Preemptive**（プリエンプティブ）設定を無効に（クリア）して、変更内容を **Commit**（コミット）します。この設定は、各 HA ペアの一方のファイアウォールでのみ無効にする必要がありますが、続行する前にコミットが成功していることを確認してください。
2. 該当する更新の Action（アクション）列で **Install**（インストール）をクリックして、**Group HA Peers**（グループ **HA** ピア）を無効に（クリア）します。次に、fw2 で **Reboot device after install**（インストール後にデバイスを再起動）を選択して **OK** をクリックします。fw2 の再起動が完了するまで待ってから、続行します。
3. fw2 の再起動が完了したら、fw1（**Dashboard**（ダッシュボード）> High Availability（高可用性））で fw2 が依然としてパッシブ ピアであることを確認します（ローカル ファイアウォールの状態は、`active`、ピア（fw2）は `passive`）。
4. fw1 にアクセスし、**Suspend local device**（ローカル デバイスをサスペンド）（**Device**（デバイス）> **High Availability**（高可用性）> **Operational Commands**（操作コマンド））を選択します。
5. fw2（**Dashboard**（ダッシュボード）> High Availability（高可用性）にアクセスし、ローカル ファイアウォールの状態が `active`、ピアが `suspended` であることを確認します。
6. Panorama にアクセスし、**Panorama** > **Device Deployment**（デバイスのデプロイ）> **Software**（ソフトウェア）の順に選択して、該当するリリースの Action（アクション）列にある **Install**（インストール）をクリックします。次に、**Group HA Peers**（グループ **HA** ピア）を無効に（クリア）し、fw1 で **Reboot device after install**（インストール後にデバイスを再起動）を選択して OK をクリックします。fw1 の再起動が完了するまで待ってから、続行します。
7. fw1 にアクセスして（**Device**（デバイス）> **High Availability**（高可用性）> **Operational Commands**（操作コマンド））、**Make local device functional**（ローカル デバイスの機能を有効化）をクリックしてから、続行する前に 2 分間待機します。
8. fw1（**Dashboard**（ダッシュボード）> High Availability（高可用性）で、ローカル ファイアウォールの状態が `passive`、ピア（fw2）が `active` であることを確認します。

2. 上記のステップを完了して PAN-OS リリースを更新したら、ターゲットの PAN-OS 10.0 リリースがすべてのファイアウォールで実行されるまで、ステップ 8 とステップ 9 を繰り返し、必要に応じて次の PAN-OS リリースをアップグレード パスにアップロードします。

STEP 10 | 管理対象の各ファイアウォールにインストールされているソフトウェアおよびコンテンツのバージョンを確認します。

1. **Panorama** > **Managed Devices**（管理対象デバイス）を選択します。
2. ファイアウォールを探し、Software Version（ソフトウェア バージョン）、Apps and Threat（アプリケーションおよび脅威）、Antivirus（アンチウイルス）、URL Filtering（URL フィルタリング）、および GlobalProtect Client（GlobalProtect クライアント）の各列の値を確認します。

STEP 11 | アップグレード前に HA ファイアウォールの一方でプリエンプションを無効にした場合は、**Election Settings**（選択設定）（**Device**（デバイス）> **High Availability**（高可用性））を編集し、そのファイアウォールの **Preemptive**（プリエンプティブ）設定を再び有効にします。

© 2019 Palo Alto Networks, Inc.

ZTP ファイアウォールのアップグレード

Panorama™ 管理サーバに ZTP ファイアウォールを正常に追加した後、ZTP ファイアウォールのターゲット PAN-OS バージョンを設定します。Panorama は、ZTP ファイアウォールにインストールされた PAN-OS バージョンが、Panorama に初めて正常に接続した後に、設定されたターゲット PAN-OS バージョンあるいはそれ以降のバージョンであるかどうかを確認します。ZTP ファイアウォールにインストールされている PAN-OS バージョンがターゲットの PAN-OS バージョンより古い場合、ZTP ファイアウォールはターゲットの PAN-OS バージョンがインストールされるまでアップグレード サイクルに入ります。

STEP 1 | Panorama への ZTP ファイアウォールの追加.

STEP 2 | 管理ユーザーとしてPanorama Web インターフェイスへのログイン。

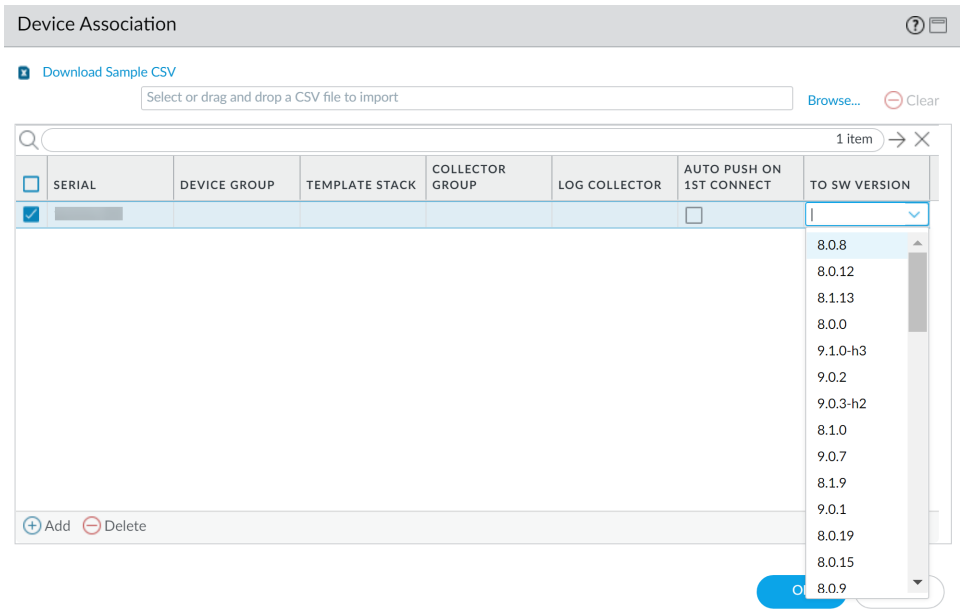
STEP 3 | **Panorama**（**Panorama**）> **Device Deployment**（デバイス デプロイメント）> **Updates**（アップデート）そして **Check Now**（今すぐチェック）の順に選択して、最新の PAN-OS リリースを確認します。

STEP 4 | **Panorama**（**Panorama**）> **Managed Devices**（管理対象デバイス）> **Summary**（概要）の順に選択して、次に 1 つ以上の ZTP ファイアウォールを選択します。

STEP 5 | 選択した ZTP ファイアウォールを再関連付けします。

STEP 6 | **To SW Version**（**SW** バージョン指定）列で、ZTP ファイアウォールのターゲット PAN-OS バージョンを選択します。

STEP 7 | **OK** をクリックして、設定の変更を保存します。



STEP 8 | **Commit**（コミット）を選択して、設定の変更を **Commit and Push**（コミットしてプッシュ）します。

STEP 9 | ZTP ファイアウォール ソフトウェアのアップグレードを確認します。

1. **Panorama**（**Panorama**）> **Managed Devices**（管理対象デバイス）> **Summary**（概要）の順に選択して、ZTP ファイアウォールに移動します。

© 2019 Palo Alto Networks, Inc.

2. **Software Version**（ソフトウェア バージョン）列に正しいターゲット PAN-OS リリースが表示されていることを確認します。

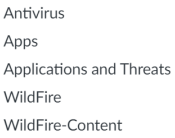
Panorama でコンテンツのアップデートを元に戻す

Panorama™ を使用すると、Panorama から 1 つ以上のファイアウォール、ログ コレクタ、または WildFire アプライアンス上のアプリケーション、アプリケーションと脅威、アンチウイルス、WildFire®、WildFire コンテンツのバージョンをすばやく元に戻すことができます。Panorama を使用すると、管理対象デバイスにインストールされているコンテンツバージョンを元に戻すことができ、コンテンツ更新のアプリケーションや新しい脅威シグネチャの導入や変更に伴うリスクを軽減する集中ワークフローを活用できます。Panorama は、コンテンツを元に戻すときに各デバイスのシステムログを生成します。管理対象デバイスにアップデートするコンテンツをデプロイする時は、必ずアプリケーションと脅威更新に関するベストプラクティスをご利用ください。

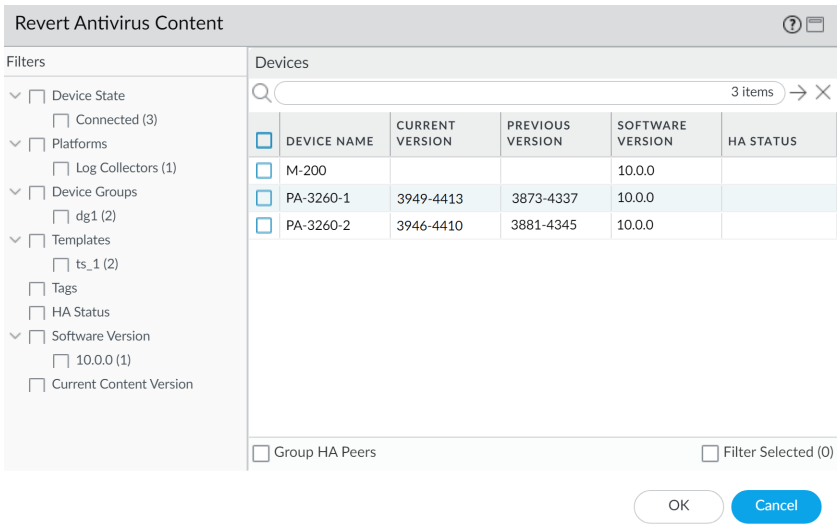
STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | **Panorama** > **Device Deployment**（デバイスのデプロイ）> **Dynamic Updates**（動的更新）、および**Revert Content**（コンテンツを元に戻す）を選択します。

STEP 3 | 元に戻す必要があるコンテンツ タイプを選択します。



STEP 4 | コンテンツを元に戻すファイアウォールを 1 つ以上選択し、**OK** をクリックします。元に戻すコンテンツ バージョンは、現在デバイスにインストールされているバージョンより古いバージョンである必要があります。



ネットワーク アクティビティのモニター

Panorama™ 管理サーバーでは、ネットワーク トラフィックを包括的にグラフィックで表示できます。Panorama の可視化ツール（アプリケーション コマンド センター（ACC）、ログ、レポート生成機能）を使用すると、すべてのネットワーク アクティビティを一元的に分析、調査およびレポートして、潜在的なセキュリティへの影響がある エリアを識別し、安全なアプリケーション有効化ポリシーに変換できます。

このセクションでは、以下のトピックについて説明します。

> Panorama を使用した可視化
> Panorama への Traps ESM ログの取り込み
> 「ユース ケース：Panorama を使用したアプリケーションのモニタリング
> 「ユース ケース：Panoramaを使用してインシデントに対処

Panorama を使用した可視化

一元的なデプロイおよびファイアウォール設定機能に加えて、Panorama では、ネットワークを通過するすべてのトラフィックをモニターしてレポートできます。レポート機能は、Panorama とファイアウォールでほとんど変わりませんが、Panorama には、すべての管理対象ファイアウォールの集約情報を一括管理画面で表示できるという利点があります。この集約ビューにより、ネットワーク全体のユーザー アクティビティ、トラフィック パターン、および潜在的な脅威の傾向に関する実用的な情報を得られます。

Panorama のアプリケーション コマンド センター (ACC) 、アプリケーション スコープ、ログ ビューアー、標準およびカスタマイズ可能なレポート オプションを使用して、ネットワークを通過するトラフィックの詳細をすばやく把握できます。この情報を表示できることで、現在のポリシーで十分な箇所と不十分な箇所を評価できます。次に、このデータを使用して、ネットワーク セキュリティ戦略を強化できます。たとえば、セキュリティ ルールを改善して、ネットワークのすべてのユーザーのコンプライアンスとアカウンタビリティを向上させることができます。また、ネットワーク容量を管理して資産のリスクを最小限に抑えながら、ネットワーク内のユーザーから求められるリッチ アプリケーションのニーズを満たすこともできます。

以下のトピックでは、Panorama のレポート機能の概要について説明します。また、いくつかのユースケースを使用して、各自のネットワーク インフラストラクチャ内でこれらの機能をどのように使用するのかについても説明します。使用可能なレポートおよびチャートの一覧と、それぞれの説明は、オンライン ヘルプを参照してください。

- ACC およびアプリケーション スコープを使用したネットワークのモニタリング
- ログ データの分析
- レポートの生成、スケジュール設定、および電子メール送信
- スケジュールされたレポートの鍵制限の設定

ACC およびアプリケーション スコープを使用したネットワークのモニタリング

ACC とアプリケーション スコープのどちらも、ネットワークを通過するトラフィックから記録されたデータをモニターおよびレポートできます。

Panorama の ACC には、ネットワーク トラフィックのサマリーが表示されます。Panorama では、ネットワーク上のすべての管理対象ファイアウォールから動的にデータをクエリして、ACC にそのデータを表示できます。これにより、Palo Alto Networks 次世代ファイアウォールのネットワーク全体で、アプリケーション、ユーザー、およびコンテンツ アクティビティ (URL カテゴリ、脅威、およびデータやファイルを効率よくブロックするセキュリティ ポリシー) ごとにトラフィックをモニターできます。

アプリケーション スコープでは、ネットワーク上の予期しない動作または異常な動作を一目で識別できます。これには、多数のチャートおよびレポート (サマリー レポート、変化モニター、脅威モニター、脅威マップ、ネットワーク モニター、トラフィック マップ) が含まれており、脅威やアプリケーション、またはフローの送信元や宛先によってトラフィック フローを分析できます。また、セッション数、またはバイト数でソートすることもできます。



デバイス グループとテンプレートの管理者は、アクセス ドメイン内のデバイス グループのネットワークと *ACC* データのみを比較できます。

ACC およびアプリケーション スコープを使用することで、以下のような内容を把握できます。

© 2019 Palo Alto Networks, Inc.

ACC	Monitor（監視）> AppScope（アプリケーション スコープ）
• ネットワーク上で使用されている上位のアプリケーションは? 高リスク アプリケーションの数は?ネットワーク上の高リスク アプリケーションの上位のユーザーは? • 過去 1 時間で閲覧された上位の URL カテゴリは?	• アプリケーション使用率の傾向は? 使用量が増加した上位 5 つのアプリケーションは? 使用量が減少した上位 5 つのアプリケーションは? • 先週または先月と比較して、今週はどのようにユーザー アクティビティが変化したのか?
• 帯域幅を消費している上位のアプリケーションは?最も帯域幅を使用しているユーザー/ホストは? • どのようなコンテンツまたはファイルがブロックされているのか? このファイル ブロッキング/データ フィルタリング ルールをトリガーしている特定のユーザーはいるのか? • 2 つの固有の IP アドレス間で交換されたトラフィック量は? 特定のユーザーによって生成されたトラフィック量は?宛先サーバーまたはクライアントの地理的な場所は?	• ネットワーク帯域幅の大部分を占有しているユーザーやアプリケーションは?過去 30 日でこの消費量がどのように変化したのか? • ネットワーク上の脅威は? これらの受信トラフィックおよび送信トラフィックの脅威は地理的にどのように分布しているのか?

次に、この情報を使用して、ネットワーク上のトラフィック パターンを維持したり、変更を適用したりできます。Panorama の可視化ツールがネットワークの利用規定の形成方法に与える影響についての概要は、「ユース ケース：Panorama を使用したアプリケーションのモニタリング」を参照してください。

以下に、ACC 内の移動に役立つヒントをいくつか示します。

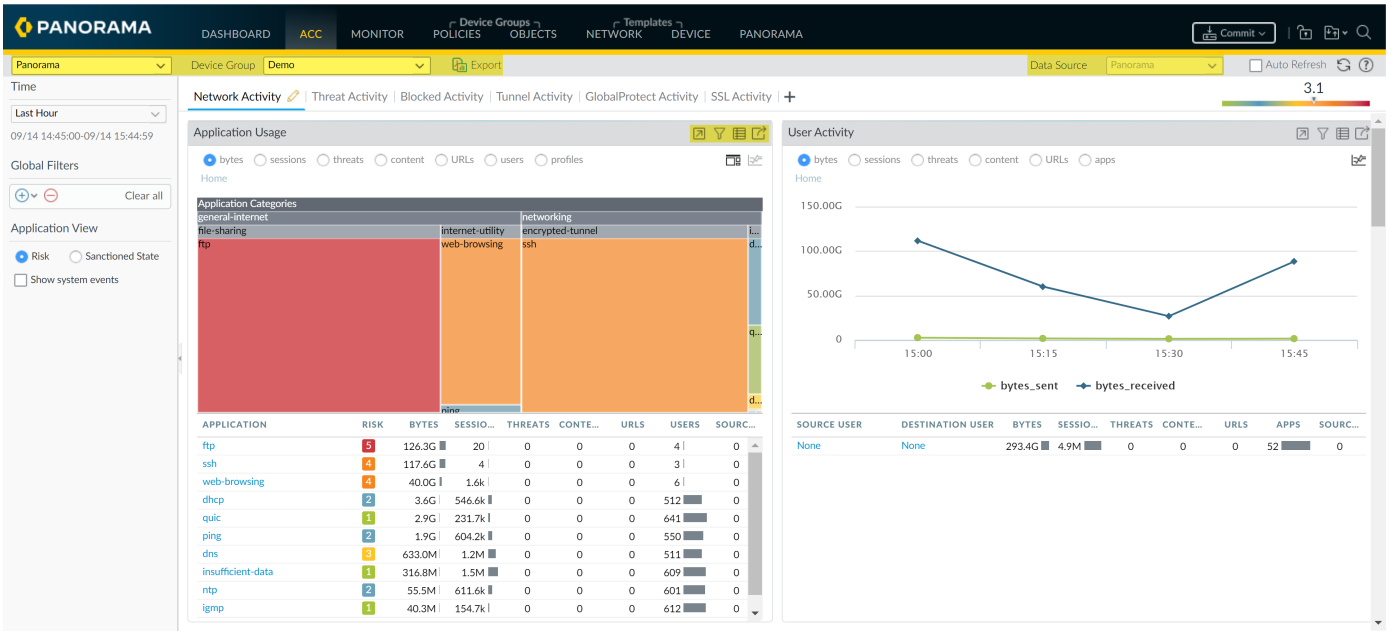


図 24：ACC 内移動のヒント

- **Switch from a Panorama view to a Device view**（Panorama ビューからデバイス ビューに切り替え）—**Context**（コンテキスト）ドロップダウンメニューを使用し、任意の管理対象ファイアウォールのWebインターフェイスにアクセスします。詳細は、「ファイアウォールと Panorama 間のコンテキスト切り替え」を参照してください。

© 2019 Palo Alto Networks, Inc.

- **Change Device Group and Data Source**（デバイスグループおよびデータソースを変更）—ACCのチャートに統計情報を表示するのに使用するデフォルトの **Data Source**（データソース）は **Panorama** ローカルデータであり、**Device Group**（デバイスグループ）設定はデフォルトで **All**（すべて）になっています。Panorama のローカル データを使用することで、チャートのロード時間を短縮できます。しかし、管理対象のファイアウォールがすべてPAN-OS 7.0以降のリリースで動いていればデータソースを**Remote Device Data**（リモート デバイスデータ）に変えることができます。管理対象のファイアウォールにPAN-OS 7.0とそれ以前のバージョンが混在している場合、Panoramaデータのみを表示できます。リモート デバイス データを使用するように設定すると、Panorama はすべての管理対象ファイアウォールをポーリングし、データの集約ビューを表示します。画面には、ポーリング対象のファイアウォールの合計数や、クエリに応答したファイアウォール数が表示されます。
- **Select the Tabs and Widgets to View**（表示するタブおよびウィジェットを選択）—ACCには3つのタブと各種のウィジェットが含まれており、必要な情報を探しやすくなっています。アプリケーションウィジェットとホスト情報ウィジェットを除き、その他のすべてのウィジェットは、対応する機能のライセンスがファイアウォールに供与されており、ログが有効になっている場合にのみデータを表示します。
- **Tweak Time Frame and Refine Data**（期間およびデータの微調整）— ACC のレポート期間は、過去 15 分、過去の時間、日、週、月、またはカスタム定義された時間になります。デフォルト設定では、各ウィジェットには上位10項目が表示され、その他の項目はすべて**others**（その他）にまとめられます。様々な属性（例：セッション、バイト数、脅威、コンテンツ、URL）を使用して各ウィジェットのデータをソートできます。また、ローカル フィルターを設定し、ウィジェット内のタブやグラフの表示をフィルタリングし、さらにそのウィジェット フィルターをグローバルフィルターにしてACC内のすべてのウィジェットに適用することもできます。

ログ データの分析

Panorama の **Monitor**（監視）タブでは、ログ データにアクセスできます。これらのログは、管理対象ファイアウォールによって処理されて Panorama に転送されたセッションのアーカイブ済みリストです。

ログ データは、大まかに 2 つのタイプに分類できます。1 つはネットワーク上のトラフィック フローに関する詳細情報（アプリケーション、脅威、ホスト情報プロファイル、URL カテゴリ、コンテンツ/ファイル タイプなど）を含むログ データで、もう 1 つはシステム イベント、設定の変更および User-ID™ マッピング情報を記録するログ データです。

管理対象ファイアウォールのログ転送設定に基づいて、**Monitor**（監視）> **Logs**（ログ）タブに、トラフィック フロー、脅威、URL フィルタリング、データ フィルタリング、ホスト情報プロファイル（HIP）マッチ、および WildFire™ 送信のログを含めることができます。ログを見直すことによって、特定のセッションまたはトランザクションの豊富な情報を確認できます。この情報には、たとえば、セッションを開始したユーザー、ファイアウォールがセッションで実行したアクション（許可または拒否）、送信元および宛先のポート、ゾーン、アドレスなどの情報が含まれています。システム ログおよび設定ログを見れば、設定の変更や、設定済みのしきい値を超えたときにファイアウォールによってトリガーされたアラームが分かります。

Panorama が PAN-OS 7.0 以前のソフトウェア バージョンで動作するファイアウォールを管理する場合、ファイアウォールが送信する WildFire サンプルに対する分析情報を Panorama が収集するのに使用する WildFire サーバーを指定します。Panorama はこの情報を利用し、PAN-OS 7.0 で導入されたフィールドの値が欠けている WildFire 送信ログを完成させます。それより古いバージョンのファイアウォールはこのフィールドを自動で埋めることはありません。サーバーを指定するには、Panorama > Setup（セットアップ）> WildFire を選択し、General Settings（一般設定）を編集して WildFire Private Cloud（WildFire プライベート クラウド）の名前を入力します。デフォルトの値は、米国でホストされている WildFire クラウドである wildfire-public-cloud です。

© 2019 Palo Alto Networks, Inc.

レポートの生成、スケジュール設定、および電子メール送信

レポートは、すぐに実行したり、スケジュールして特定の間隔で実行したりすることができます。保存したりエクスポートしたり、特定の受信者に電子メールで送信したりすることができます。電子メールは、Panorama へのアクセス権のない管理者とレポートを共有する場合に特に便利です。Panorama では、Palo Alto Networks のファイアウォールと同じレポート タイプがサポートされます。

Panorama 10.0.2 と Cloud Services プラグイン バージョン 1.8.0 より、Cortex Data Lake データに関するスケジュールされたレポートを生成することができます。

PAN-OS 10.0.3 以降のバージョンでは、この機能はデフォルトで有効になっています。

これを実行するには、最初に以下を入力することで Panorama CLI から該当の機能を有効化する必要があります

```
admin@Panorama> request plugins cloud_services logging-service sched-report-enable
```

通常のコミットでは、この変更は有効になりません。代わりに、設定モードに切り替える必要があります。

```
admin@Panorama> configure
```

そして、以下を入力します

```
admin@Panorama# commit force
```

次に、スケジュールされたレポートを生成するために、以下の手順に従ってください。

Panorama とレポート生成対象のファイアウォールには、同じリリースのソフトウェアをインストールしておくことをお勧めします。例として、*Panorama* 管理サーバが *Panorama 10.0* で稼働している場合は、その管理対象ファイアウォールに *PAN-OS 10.0* をインストールしてからレポートを生成します。このようにすることで、*Panorama* ソフトウェアのリリースではサポートされているが、ファイアウォールのそれより古いリリースの *PAN-OS* ではサポートされていないフィールドを含むレポートを作成したときに発生する可能性のある問題を回避できます。

STEP 1 | Panorama 事前定義済みレポートを設定します。

1. **Panorama** > **Setup** (セットアップ) > **Management** (管理) を選択し、**Logging and Reporting** (ロギングとレポート作成) を編集します。
2. (任意) **Log Export and Reporting** (ログのエクスポートとレポート作成) を選択し、**Use Data for Pre-Defined Reports** (事前定義済みレポート用にデータを使用) を有効化 (チェック) して、時間ごとのレポート集約をログ コレクタにオフロードします。

   この設定は、*VM-50*、*VM-50 Lite* および *PA-200* ファイアウォールで有効化することが推奨されます。
3. **Pre-Defined Reports** (事前定義済みレポート) を選択し 、Panorama からプッシュする事前定義済みレポートを有効化 (チェック) します。
4. **Commit** (コミット) > **Commit to Panorama** (**Panorama** へのコミット) の順に選択し、設定変更を **Commit** (コミット) します。

© 2019 Palo Alto Networks, Inc.

5. (VM-50、VM-50 Lite、PA-200 ファイアウォールのみ) ファイアウォール CLI にアクセス して、事前定義済みレポートの生成を有効化します。

   このコマンドは、各VM-50、VM-50 Lite、および PA-200 ファイアウォール上で実行する必要があります。

```
admin> debug run-panorama-predefined-report yes
```

STEP 2 | ファイアウォールから送信される、ユーザーとユーザー グループの情報を受信して保存するように Panorama を設定します。

IP アドレスだけではなく、ユーザー名とグループに基づいてレポートを生成するには、この設定が必要です。

1. Panorama でユーザー グループの情報をレポートに組み込む場合は、管理対象ファイアウォールを PAN-OS 8.1 以降にアップグレードします。Panorama では、以前のリリースを実行しているファイアウォールからグループ情報を同期できません。
2. **Panorama** > **Setup**（セットアップ）> **Management**（管理）を選択して Panorama 設定を編集し、グループでのレポートとフィルタリングの有効化を行う必要もあります。
3. デバイス グループを追加していない場合は追加します。デバイス グループごとに、次のように操作します。
   - **Master Device**（マスター デバイス）を選択します。これは、ユーザーとユーザー グループの情報を Panorama に提供するファイアウォールです。
   - Panorama が **Store users and groups from Master Device**（マスター デバイスからのユーザーおよびグループを保存）できるようにします。

STEP 3 | レポートを生成します。

タイプに基づいてレポートを生成する手順は以下のとおりです。

- カスタム レポート:
  1. **Monitor**（監視）> **Manage Custom Reports**（カスタム レポートの管理）を選択し、レポートを **Add**（追加）します。
  2. レポートを識別する **Name**（名前）を入力します。
  3. レポート用の **Database**（データベース）を選択します。

     Summary Databases（サマリー データベース）または**Detailed Logs**（詳細ログ）データベースに基づいてレポートを生成できます。

     Panorama 管理サーバーとログ コレクタに保存されているログに基づいてレポートを生成するには、**Panorama Data**（**Panorama** データ）を選択します（パフォーマンスを高めるために推奨）。

     管理対象ファイアウォールに保存されているログに基づいてレポートを生成するには、**Remote Device Data**（リモート デバイス データ）を選択します。このオプションは、Panorama にまだ転送していないログがファイアウォールにある場合のためのものです。ただし、Panorama がファイアウォールに直接問い合わせる必要があるため、このオプションは低速になります。
  4. **Scheduled**（スケジュール済み）を選択します。
  5. **Time Frame**（期間）、**Sort By**（ソート基準）、**Group By**（グループ化基準）設定、およびレポートに表示する列（ログ属性）を選択し、ログ フィルタリング基準を定義します。

     正確なレポートを生成するには *Sort By (*ソート基準*)* による並び替えを選択する必要があります。*Sort By (*ソート基準*)* による並び替えを選択しない場合、生成されたカスタムレポートには、選択したデータベースに一致する最新のログが入力されます。

© 2019 Palo Alto Networks, Inc.

6. （任意）ログ属性に基づいてログ フィルタリング条件をさらに微調整するには、**Query Builder**（クエリ ビルダー）を使用します。
7. レポート設定をテストするには、**Run Now**（今すぐ実行）を選択します。必要に応じて設定を変え、レポートに表示される情報を変更します。
8. **OK** をクリックしてカスタム レポートを保存します。

- **PDF Summary Report**（**PDF** サマリー レポート）:

1. **Monitor**（監視）> **PDF Reports**（**PDF** レポート）> **Manage PDF Summary**（**PDF** サマリーの管理）の順に選択し、レポートを追加します。
2. レポートを識別する **Name**（名前）を入力します。
3. 各レポート グループのドロップダウンを使用し、1 つ以上の要素を選択して、PDF サマリー レポートを設計します。最大 18 のエレメントを含められます。
4. **OK** をクリックして設定を保存します。

STEP 4 | **Report Group**（レポート グループ）を設定します。

レポート グループには、事前定義済みレポート、PDF サマリー レポート、およびカスタム レポートを含めることができます。Panorama は、含まれているすべてのレポートを 1 つの PDF に結合します。

1. **Monitor**（監視）> **PDF Reports**（**PDF** レポート）> **Report Groups**（レポート グループ）の順に選択し、レポート グループを **Add**（追加）します。
2. レポート グループを識別するための **Name**（名前）を入力します。
3. （任意）**Title Page**（タイトル ページ）を選択して、PDF 出力の **Title**（タイトル）を追加します。
4. 事前定義済みレポート、カスタム レポート、PDF サマリー レポートのリストでレポートを選択します。
5. 選択したレポートをレポート グループに **Add**（追加）します。
6. **OK** をクリックして設定を保存します。

STEP 5 | 電子メールサーバーのプロファイルを設定します。

プロファイルにより、ファイアウォールがサーバーに接続してメールを送信する方法を定義します。

1. **Panorama** > **Server Profiles**（サーバー プロファイル）> **Email**（メール）を選択し、サーバー プロファイルを **Add**（追加）します。
2. プロファイルを識別する **Name**（名前）を入力します。
3. 最大 4 個の SMTP サーバーを **Add**（追加）し、SMTP サーバーごとに次の情報を **Add**（追加）します。
   - **Name**（名前）– SMTP サーバーを識別する名前（1 ~ 31 文字）。このフィールドは単なるラベルであり、既存のサーバーのホスト名である必要はありません。
   - 電子メール表示名 - 電子メールの From（送信者）フィールドに表示される名前。
   - **From**（送信者）- 電子メール通知の送信元の電子メール アドレス。
   - **To**（宛先）- 電子メール通知の送信先の電子メール アドレス。
   - **Additional Recipient**（その他の受信者）- 通知を 2 番目のアカウントに送信するには、ここに追加のアドレスを入力します。
   - **Email Gateway**（電子メール ゲートウェイ）- 電子メールの送信に使用する SMTP ゲートウェイの IP アドレスまたはホスト名。
4. **OK** をクリックしてプロファイルを保存します。

STEP 6 | レポートの電子メール配信をスケジュール設定します。

1. **Monitor**（監視）> **PDF Reports**（**PDF** レポート）> **Email Scheduler**（電子メール スケジューラ）の順に選択し、メール スケジューラ プロファイルを **Add**（追加）します。
2. プロファイルを識別する **Name**（名前）を入力します。

© 2019 Palo Alto Networks, Inc.

3. **Report Group**（レポート グループ）、先ほど作成したメール サーバー プロファイル（**Email Profile**（電子メール プロファイル））、およびレポートの **Recurrence**（繰り返し）（デフォルトは **Disable**（無効化））を選択します。
4. メール設定が正しいことを確認するには、**Send test email**（テスト電子メールの送信）によってテスト メールを送信します。
5. **OK** をクリックして変更内容を保存します。
6. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

スケジュールされたレポートの鍵制限の設定

Panorama™ 管理サーバーと PA-7000 シリーズ ファイアウォールのレポートは、1つ以上のログ コレクタからの鍵 (集約可能な一意の値) を利用して、レポートを作成および生成します。スケジュールされたレポートの精度を向上させるために、キーの最大制限と最小制限ができるようになりました。サポートされる鍵の数を増やすことにより、スケジュールされたレポートに、集計、並べ替え、およびグループ化できるデータをさらに含めることができるようになりました。

デフォルトの最小鍵制限は、以下の計算を使用するスケジュールされたレポート用に、**Sort By** (ソート基準) と **Group By** (グループ基準) の値を基準にしています。

```
<Sort By value> x 100 x <Group By value>
```

例えば、**Sort By** (ソート基準) が **Top 25** と設定されており、**Group By** (グループ基準) が **5 Groups** と設定されている場合、デフォルトの最小鍵制限は 12,500 個です。**Group By** (グループ基準) の値は、**None** (なし) に設定されている場合は計算に考慮されません。デフォルトの最小鍵制限は、最大鍵制限を超えることができないように制限されています。

M-Series アプライアンスと *Panorama* バーチャル アプライアンスの鍵のみ設定可能です。*PA-7000* シリーズの鍵制限は設定できません。

サポートされている最大鍵数と最小鍵数は、次の Panorama モデルで増加します。

Panorama モデル	最小鍵制限	最大鍵制限
PA-7000シリーズ	1,000 - デフォルト、設定不可	25,000 - デフォルト、設定不可
M-200	15,000	50,000
M-500	15,000	50,000
M-600	15,000	50,000
レガシー モードの Panorama バーチャル アプライアンス	5,000	25,000
Panorama バーチャル アプライアンス (すべての対応モデル)	15,000	50,000

STEP 1 | Panorama CLI への**ログイン**を行います。

STEP 2 | 次のコマンドを使用して、最大鍵制限を設定します。

鍵の最大制限は 0 から 50 の間に設定できます。ここで、50 は 50,000 個に相当します。この例では、Panorama バーチャル アプライアンスの最大鍵数を 30,000 個に設定しています。

© 2019 Palo Alto Networks, Inc.

```
admin@Panorama> request max-report-keys set limit <Key Limit>
```

```
admin@Panorama> request max-report-keys set limit 30

cfg.report.max-keys-limit: 30
```

STEP 3 | 次のコマンドを使用して、最小鍵制限を設定します。

鍵の最小制限は 0 から 15 の間に設定できます。ここで、15 は 15,000 個に相当します。この例では、Panorama バーチャル アプライアンスの最小鍵数を 15,000 個に設定しています。

```
admin@Panorama> request min-report-keys set limit <Key Limit>
```

```
admin@Panorama> request min-report-keys set limit 15

cfg.report.min-keys-limit: 15
```

STEP 4 | (任意) 最小鍵制限をデフォルト設定にセットします。

```
admin@Panorama> request min-report-keys set limit 0
```

STEP 5 | 次のコマンドを使用して、新しい最大および最小鍵制限を Panorama にコミットします:

```
admin@Panorama> commit-all
```


© 2019 Palo Alto Networks, Inc.

Panorama への Traps ESM ログの取り込み

可視化は、攻撃を防止してその影響を小さくするための最初の重要なステップです。この課題に対応できるようにするため、Panorama ではファイアウォール ログ（ネットワークのイベント）および Traps™ ESM サーバー ログ（エンドポイントのセキュリティ イベント）を統合して確認できるようにして、疑わしいアクティビティや悪意のあるアクティビティを追跡できるようにしています。

ネットワークとエンドポイントで発生するイベントに気付き、その状況に対処できるようにするため、Traps エージェントが ESM サーバーにレポートするセキュリティ イベントは Panorama に転送されます。Panorama は Syslog レシーバとして動作し、TCP、UDP、SSL のいずれかで Syslog を使用して、Traps ESM コンポーネントからのログを取り入れることができます。さらに Panorama は、エンドポイントで発生する個別のセキュリティ イベントをネットワークで発生していることと関連付けて、一致の根拠を生成できます。この根拠により、イベントの時系列の順序と流れで状況を把握し、問題を調査して、ネットワークのセキュリティ ギャップを修正できるようになります。

STEP 1 | Panorama でログ インジェスト プロファイルを定義し、コレクタ グループを所属させます。



レガシー モードの *Panorama* バーチャル アプライアンスは *Traps* ログを取り入れることができません。

1. **Panorama** > **Log Ingestion Profile**（ログインジェストプロファイル）を選択し、**Add**（追加）をクリックします。
2. プロファイルの**Name**（名前）を入力します。
3. **Add**（追加）をクリックし、ESM サーバーの詳細を入力します。プロファイルには最大 4 台の ESM サーバーを追加できます。
   1. **Source Name**（ソース名）を入力します。
   2. Panorama で syslog メッセージを受信する **Port**（ポート）を指定します。範囲は 23000 ~ 23999 です。
   3. **Transport**（トランスポート）層プロトコル（TCP、UDP、SSL）を選択します。
   4. **External Log type**（外部ログ タイプ）と、ご利用の Traps_ESM の **Version**（バージョン）を選択します。たとえば、Trap ESM 4.0 または 4.1 の場合、 **3.4.1+**を選択します。

      Traps ログ形式が更新されると、Panorama では、更新されたログ定義がコンテンツ更新で使用できるようになります。
4. **Panorama** > **Collector Groups**（コレクタグループ） > **Log Ingestion**（ログインジェスト）を選択し、ログインジェストプロファイルを**Add**（追加）して、コレクタグループが、プロファイルにリストされている ESM サーバーからログを受信できるようにします。

   Panorama と ESM サーバーの間の安全な Syslog 通信のために SSL を有効にしている場合は、コレクタ グループに属する管理対象コレクタに証明書を適用する必要があります（**Panorama** > **Managed Collectors**（管理対象コレクタ） > **General**（全般）の順に選択し、**Inbound Certificate for Secure Syslog**（保護された **Syslog** の着信証明書）に使用する証明書を選択）。
5. Panorama とコレクタグループに変更を **Commit**（コミット）します。

STEP 2 | ESM サーバーで Panorama を Syslog レシーバとして設定します。

Traps ESM 4.0 以降は、外部 syslog レシーバおよび Panorama をサポートします。以前のTrap ESM リリースでは、複数の syslog レシーバへのログ転送がサポートされていないため、 **Syslog**設定では、Panorama を Syslog レシーバとして設定する必要があります（Traps ESM 3.4 の場合は、 外部ロギングプラットフォームへのログ転送の有効化を参照してください）。

Traps ESM 4.0 以降のリリースの場合：

© 2019 Palo Alto Networks, Inc.

1. ESM コンソールで、**Settings**（設定）> **ESM** > **Panorama** を選択し、さらに**Enable log forwarding to Panorama**（**Panorama**への口グ転送の有効化）を選択します。
2. **Panorama Server**（**Panorama** サーバー）として Panorama のホスト名または IP アドレスを入力し、Panorama がリッスンする **Panorama Server Port**（**Panorama** サーバー ポート）を入力します。オプションの **Panorama Failover Server**（**Panorama** フェイルオーバー サーバー）でこの手順を繰り返します。
3. 転送レイヤー **Communication Protocol**（通信プロトコル）を選択します：（TCP、TCP with SSL、またはUDP）。TCP with SSL を選択すると、ESM サーバーでは、クライアント認証を有効にするためにサーバー証明書が必要となります。

   保護された Syslog の着信証明書のルート CA 証明書を Panorama からエクスポートし、ESM サーバーをインストールしたホストの信頼されたルート証明書ストアにその証明書をインポートする必要があります。

STEP 3 | ESM 口グおよび相関されたイベントを表示します。

1. **Monitor**（監視）> **External Logs**（外部口グ）> **Traps ESM** を選択すると、Panorama に取り込まれた口グが表示されます。
2. **Monitor**（監視）> **Automated Correlation Engine**（自動相関エンジン）> **Correlated Events**（相関されたイベント）を選択し、**Wildfire and Traps ESM Correlated C2**（**Wildfire** および **Traps ESM** の相関 **C2**）という相関オブジェクト名で絞り込んで相関イベントを検索します。ネットワークのホストが C&C アクティビティを示し、それが WildFire 仮想環境の悪意のあるファイルで見られる動作と一致すると、Panorama は相関されたイベントを生成します。この相関されたイベントにより、Traps エージェントとファイアウォールがネットワークで感染した 1 つ以上のホストから観察した、疑わしいアクティビティについて警告されます。

© 2019 Palo Alto Networks, Inc.

「ユース ケース：Panorama を使用したアプリケーションのモニタリング

この例のプロセスでは、現在のポリシーの効率性を評価し、ネットワークの利用規定を強化するためにポリシーを調整する必要のある箇所を決定します。

Panorama にログインすれば、**Dashboard**（ダッシュボード）の **Top Applications**（上位アプリケーション）ウィジットで、過去 1 時間で最も使用されたアプリケーションのプレビューを表示できます。ウィジェットを表示するには、ツールバーで **Widgets** > **Application** > **Top Applications** (ウィジェット > アプリケーション > 上位アプリケーション)を選択します。上位アプリケーションのリストにざっと目を通し、各アプリケーション ブロックの上にマウスを置いて詳細を確認できます。または、**ACC** タブを選択して、順番に並んでいるリストで同じ情報を確認することもできます。以下の画像は、**Dashboard**（ダッシュボード）の **Top Applications**（上位アプリケーション）ウィジットのビューです。

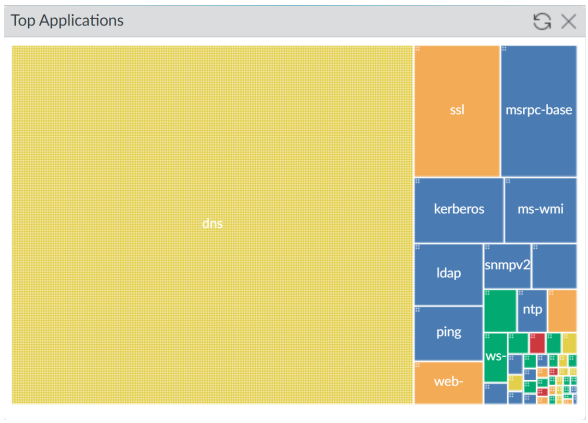


図 **26 :** 上位アプリケーション ウィジット

このビューのデータ ソースは、アプリケーション統計データベースです。これには、トラフィック ログは使用されず、セキュリティ ルールでログを有効にしているかどうかに関係なく生成されます。このビューには、ネットワークで許可され、定義したポリシー ルールでブロックされずに通過するすべてのトラフィックが表示されます。

ACC タブでは、**Data Source**（データ ソース）を選択して **Panorama** のローカル データベースに切り替えたり、管理対象ファイアウォールに問い合わせて（**Remote Device Data**（リモート デバイス データ））データを取得したりできます。この情報は、Panorama によって自動的に集約されて表示されます。管理対象のファイアウォールからデータをロードする時間は、表示するデータの期間やネットワーク上で生成されるトラフィック量によって異なるため、フローを迅速化できるようにデータ ソースとして Panorama を使用する（Panorama へのログ転送を有効にする）ことを検討してください。管理対象のファイアウォールに PAN-OS 7.0 とそれ以前のバージョンが混在している場合、**Remote Device Data**（リモート デバイス データ）は利用できません。

「図 26 : 上位アプリケーション ウィジット」の **Dashboard**（ダッシュボード）の例では、一般的なアプリケーションとして DNS を示しています。ここでDNS アプリケーション ブロックをクリックすると、DNS がグローバルフィルターとして適用された状態で Panorama が **ACC** > **Network Activity** (ACC > ネットワーク アクティビティ)タブを開き、アプリケーション情報、アプリケーションにアクセスしたユーザー、リスク　レベルについての詳細情報、アプリケーションの特性を表示します。

© 2019 Palo Alto Networks, Inc.

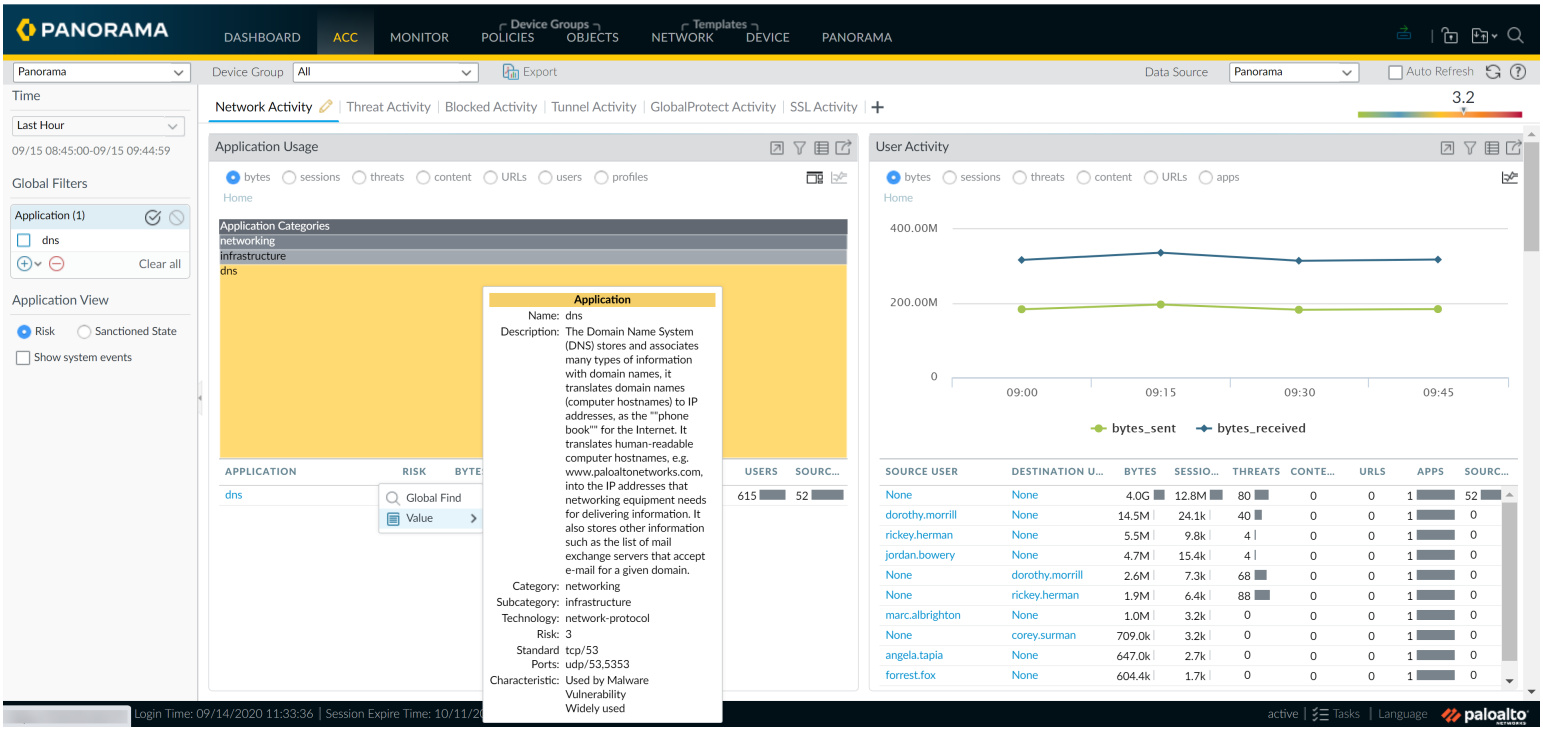


図 **27 : Network Activity**（ネットワーク アクティビティ）タブ

User Activity（ユーザー アクティビティ）ウィジェットには、DNS を使用しているユーザー数や生成されるトラフィック量が表示されます。User-ID を有効にしている場合、このトラフィックを生成しているユーザーの名前を表示でき、すべてのセッション、コンテンツ、あるいは各ユーザーに関連する脅威を詳しく確認することができます。

Threat Activity（脅威アクティビティ）タブで **Compromised Hosts**（侵入されたホスト）ウィジットを閲覧すれば、どの相関オブジェクトがマッチするか、また、ユーザーおよびアプリケーションに関連する一致の根拠を確認できます。また、**Threat Activity**（脅威アクティビティ）ウィジットでは脅威名、カテゴリー、および ID を表示することもできます。

DNS セットをグローバルフィルターとして **Destination IP Activity**（宛先 **IP** のアクティビティ）および **Destination Regions**（宛先リージョン）ウィジェットとともに使用し、トラフィックの宛先を確認します。また、この接続を完了させるセキュリティ ルールおよび進入・退出ゾーンを確認することもできます。

詳細は、フィルタリングしたビューのトラフィック ログ を表示し、使用されたポート、送信済みパケット、送信済みバイト、受信済みバイトを各ログ エントリで確認してください。必要に応じて詳細または概要が表示されるように列を調整します。

Monitor（監視）> **App-Scope**（アプリケーション スコープ）> **Traffic Map**（トラフィック マップ）タブにはトラフィック フローの地理マップが表示され、受信トラフィックと送信トラフィックを対比したビューが得られます。また、**[Monitor]** > [アプリケーション スコープ] > [変化モニター] タブを使用して、トラフィック パターンの変化を表示することもできます。たとえば、この時間に使用された上位のアプリケーションを先週または先月と比較して、パターンや傾向があるかどうかを判断できます。

明らかになったすべての情報を使用して、ポリシー設定に行う変更を評価できます。以下に、考慮すべき推奨事項を示します。

- Panorama で制限的なプレ ルールを作成してすべての DNS トラフィックをブロックするか許可します。次に、Panorama デバイス グループを使用し、このポリシー ルールを作成して 1 つ以上のファイアウォールにプッシュします。

© 2019 Palo Alto Networks, Inc.

- 帯域幅使用制限を適用して、非ビジネス トラフィックの優先順位を下げる QoS プロファイルおよびポリシー ルールを作成します。Panorama デバイス グループおよびテンプレートを使用して QoSを設定し、ルールをファイアウォール（複数可）にプッシュします。
- 特定のユーザーのアクティビティやネットワーク上で使用された上位のアプリケーションのアクティビティをまとめるカスタム レポート グループをスケジュール設定し、アクションを実行する前にもう 1 週間またはもう 2 週間そのパターンを観察します。

特定のアプリケーションをチェックする以外に、上位アプリケーションのリストに不明なアプリケーションが入っていないかどうかもチェックします。これらは、定義された App-ID™ シグネチャに一致しなかったアプリケーションで、unknown-udp および unknown-tcp として表示されます。これらの不明なアプリケーションを詳しく調べるには、名前をクリックして未分類トラフィックの詳細にドリルダウンします。

同じプロセスを使用して、不明なトラフィックを開始したホストの送信元 IP アドレスの上位リストと、セッションの確立先だった宛先ホストの IP アドレスを調査します。デフォルトでは、不明なアプリケーションが検出されると、トラフィック ログが記録され、デフォルトでパケット キャプチャ（pcap）が行われます。左側の列の緑の矢印は、アプリケーション データのパケット キャプチャの目印です。緑の矢印をクリックすると、ブラウザに pcap が表示されます。

サーバーの IP アドレス（宛先 IP）、宛先ポート、およびパケット キャプチャが分かっていると、アプリケーションの識別や、ネットワーク上のアクションの実行方法の決定がしやすくなります。たとえば、カスタム アプリケーションを作成して、不明な TCP または UDP トラフィックとしてラベルを付ける代わりにこのトラフィックを識別することができます。不明なアプリケーションの識別の詳細は、「不明なアプリケーションの特定」の記事を参照してください。また、アプリケーションを識別するカスタム シグネチャの作成の詳細は、「カスタム アプリケーション シグネチャ」の記事を参照してください。

© 2019 Palo Alto Networks, Inc.

「ユース ケース：Panoramaを使用してインシデントに対処

ネットワークの脅威は、ドライブ バイ ダウンロードによるマルウェアやスパイウェアの感染、フィッシング攻撃、パッチを当てていないサーバー、ランダムまたは標的を定めたサービス拒否（DoS）攻撃など、さまざまな経路から生じます。ネットワークの攻撃や感染に対応するには、攻撃について管理者にアラートを通知し、必要な調査の証拠を提供するプロセスやシステムが求められます。この証拠を活用して、攻撃を開始するために使用された送信元やメソッドを追跡できます。

Panorama の利点は、ネットワーク全体の管理対象ファイアウォールから収集されたパターンやログを一元的な統合ビューに表示できることにあります。自動相関エンジンからの情報は、単独で使用することも、セキュリティ情報イベント管理（SIEM）から生成されたレポートやログと併用することもできます。これにより、攻撃のトリガー方法や、今後の攻撃およびネットワークの損傷による損失を防ぐ方法を調査できます。

このユース ケースにより、以下のことを確認できます。

- インシデントの通知方法は?
- インシデントが誤検知でないことを裏付ける方法は?
- 即座に実行するアクションは?
- トリガー イベントの前または後のイベント シーケンスを再構築するために利用可能な情報をどのように使用するのか?
- ネットワークを保護するために考慮する必要のある変更は?

このユース ケースでは、特定のインシデントを追跡し、Panorama の可視化ツールを使用してレポートに答える方法を示します。

- インシデントの通知
- ACC でウィジットを確認
- 脅威ログの確認
- WildFire ログの確認
- データ フィルタリング ログの確認
- セキュリティ ルールの更新

インシデントの通知

インシデントについてアラートを受け取る方法はいくつかありますが、Palo Alto Networks ファイアウォールの設定方法や、詳細な分析のために使用できるサードパーティ ツールによって異なります。Panorama または Syslog サーバーに記録されるログ エントリによってトリガーされた電子メール通知を受信したり、SIEM ソリューションで生成される特殊なレポートで通知を受けたり、サードパーティの有料サービスまたはエージェントで通知を付けたりできます。この例では、Panorama から電子メール通知を受信します。この電子メールにより、Zero Access gent.Gen Command And Control Traffic（Zero Access gent.Gen コマンド アンド コントロール トラフィック）がスパイウェア シグネチャとマッチしたことを示すアラートによってトリガーされたイベントが通知されます。また、この電子メールには、セッションの送信元および宛先 IP アドレス、脅威 ID、イベントがログに記録されたときのタイムスタンプも含まれます。

ACC でウィジットを確認

ACC > **Threat Activity**（脅威アクティビティ）タブの**Compromised Hosts**（侵入されたホスト）ウィジェットおよび**Threat Activity**（脅威アクティビティ）をチェックし、重大度が致命的あるいは高の脅威

© 2019 Palo Alto Networks, Inc.

があるかどうか確認します。**Compromised Hosts**（侵入されたホスト）ウィジェットにてマッチ オブジェクトを調べ、マッチ数のリンクをクリックしてそのインシデントの一致の根拠を確認します。

脅威ログの確認

アラートの調査を開始するには、脅威 ID を使用して、Panorama で脅威ログを検索します（**[Monitor]** > [ログ] > [脅威]）。Threat (脅威)ログから被害者の IP アドレスを検索し、ログ エントリ内のダウンロード アイコンをクリックしてパケット キャプチャ（PCAP）をエクスポートし、さらにWireShark などのネットワーク アナライザ ツールを使用することで、パケットの詳細を確認できます。HTTP の場合、インシデントを検証するために、プロトコル、疑わしいホスト、URL 文字列、ユーザー エージェント、IP アドレスおよびポートの異常な形式または偽の HTTP リファラを検索します。これらの pcap のデータは、類似するデータ パターンの検索、カスタム シグネチャの作成、またはセキュリティ ポリシーの変更を行って、今後の脅威への対応を改善する場合にも役立ちます。

この手動レビューの結果、シグネチャが信頼できるという確信がある場合、シグネチャをアラート アクションからブロック アクションに移行して、より積極的なアプローチを行うことを検討してください。攻撃者の IP を IP ブロック リストに追加して、その IP アドレスからのトラフィックが今後内部ネットワークに到達しないようにすることを選択する場合もあります。

DNS ベースのスパイウェア シグネチャがある場合、ローカル *DNS* サーバーの *IP* アドレスが *Victim IP*（被害者 *IP*）アドレスとして表示される可能性があります。一般的にこの原因は、ファイアウォールがローカル *DNS* サーバーの外部にあり、*DNS* クエリで、要求元のクライアントの *IP* アドレスが表示される代わりに、ローカル *DNS* サーバーが送信元 *IP* として表示されるためです。

この問題が発生した場合、ネットワーク上の感染したホストを識別するために、セキュリティ ルールのアンチスパイウェア プロファイルの *DNS* シンクホール アクションを有効にします。*DNS* シンクホールでは、有害ドメインへのアウトバウンド接続を制御し、*DNS* クエリを未使用の内部 *IP* アドレス（応答を外に出さないシンクホール）にリダイレクトできます。侵入されたホストが有害ドメインへの接続を開始すると、接続要求は、ファイアウォールによって、ユーザーが定義した *IP* アドレスにリダイレクトされ、インターネットに送出されるのではなく、シンクホールに封じ込められます。これで、シンクホールに接続されたすべてのホストのトラフィック ログを確認して、侵入されたすべてのホストを特定し、是正措置を講じて拡散を防止できます。

インシデントの調査を続行するには、攻撃者と被害者の IP アドレスに関する情報を使用して、以下のような詳細情報を確認します。

- 攻撃者の地理的な場所は?IP アドレスは個別の IP アドレスと NAT された IP アドレスのどちらか?
- イベントの発生原因（Web サイトに誘導されたユーザー、ダウンロード、電子メールで送信された添付ファイル）は?
- マルウェアは伝搬されるのか?ネットワーク上に他に侵入されたホスト/エンドポイントは存在するのか?
- ゼロデイの脆弱性か?

各ログ エントリのログ詳細には、そのイベントに関連するログが表示されます。この情報には、Traffic（トラフィック）、Threat（脅威）、URL Filtering（URL フィルタリング）またはその他のログが示されます。この情報を確認して、インシデントの原因となったイベントと相関させることができます。たとえば、送信元 IP および宛先 IP として IP アドレスを使用して、トラフィック ログ（**[Monitor]** > [ログ] > [トラフィック]）をフィルタリングし、この被害者の IP アドレスで接続を確立するのに使用したすべての外部および内部ホスト/クライアントの全体像を把握できます。

© 2019 Palo Alto Networks, Inc.

WildFire ログの確認

脅威ログの他に被害者の IP アドレスを使用して、WildFire Submissions（WildFire の送信）ログをフィルタリングします。WildFire Submissions（WildFire の送信）のログには、分析のために Wildfire サービスにアップロードされたファイルに関する情報が含まれています。通常、スパイウェアは密かに組み込まれるため、被害者が疑わしいファイルを最近ダウンロードしたかどうかを WildFire 送信ログで確認します。WildFire の調査レポートには、ファイルまたは .exe の取得元 URL やコンテンツの動作に関する情報が表示されます。これにより、ファイルが有害かどうか、レジストリ キーを変更したかどうか、ファイルの読み取り/書き込みを行ったかどうか、新しいファイルを作成したかどうか、ネットワーク接続チャネルを開いたのかどうか、アプリケーションのクラッシュを引き起こしたかどうか、プロセスを生成したかどうか、ファイルをダウンロードしたかどうか、他の有害な動作が示されているかどうかがわかります。この情報を使用して、感染を引き起こしたアプリケーション（web-browsing、SMTP、FTP）をブロックするかどうかを判断し、より厳格な URL フィルタリング ポリシーを作成して、一部のアプリケーション/アクション（ファイルのダウンロードなど）を特定のユーザー グループに限定します。

Panorama から *WildFire* ログにアクセスするには、*WildFire* サブスクリプション、セキュリティ ポリシーに添付されたファイル ブロッキング プロファイル、および *Panorama* に転送される脅威ログが必要です。

Panorama が *PAN-OS 7.0* 以前のソフトウェア バージョンで動作するファイアウォールを管理する場合、ファイアウォールが送信する *WildFire* サンプルに対する分析情報を *Panorama* が収集するのに使用する *WildFire* サーバーを指定します。*Panorama* はこの情報を利用し、*PAN-OS 7.0* で導入されたフィールドの値が欠けている *WildFire* 送信ログを完成させます。それより古いバージョンのファイアウォールはこのフィールドを自動で埋めることはありません。サーバーを指定するには、*Panorama* > *Setup*（セットアップ）> *WildFire* を選択し、*General Settings*（一般設定）を編集して*WildFire Private Cloud*（*WildFire* プライベート クラウド）の名前を入力します。デフォルトの値は、米国でホストされている *WildFire* クラウドである *wildfire-public-cloud* です。

WildFire でファイルが有害であると判断された場合、新しいアンチウイルス シグネチャが 24 ~ 48 時間以内に作成され、使用できるようになります。WildFire サブスクリプションがある場合、次の WildFire シグネチャの更新の一部としてシグネチャが 30 ~ 60 分以内に使用できるようになります。マルウェアをブロックするように設定されていれば、Palo Alto Networks 次世代ファイアウォールでシグネチャを受信するとすぐに、ファイルがブロックされて、ブロックされたファイルに関する情報が脅威ログに表示されます。この脅威から保護して、ネットワーク上にマルウェアが拡散することを防止するために、このプロセスは緊密に統合されています。

データ フィルタリング ログの確認

データ フィルタリング ログ（**Monitor Logs**[監視] > [ログ] > **Data Filtering** [データ フィルタリング]）も有害なネットワーク アクティビティを調査するための重要なソースです。アラートが通知されるすべてのファイルのログを定期的に確認できますが、ログを使用して、被害者の IP アドレスまたはユーザーからの（への）ファイルやデータの転送を追跡したり、トラフィックの方向やフロー（サーバーからクライアントまたはクライアントからサーバー）を確認したりすることもできます。イベントの前または後のイベントを再作成するには、宛先となる被害者の IP アドレスのログをフィルタリングし、ネットワーク アクティビティのログを確認します。

Panorama では、すべての管理対象ファイアウォールから情報が集約されるため、ネットワーク内のすべてのアクティビティの有益な概要を得られます。ネットワーク上のトラフィックを調査するために使用できるその他の可視化ツールには、**Threat Map**（脅威マップ）、**Traffic Map**（トラフィック マップ）、および **Threat Monitor**（脅威モニター）などがあります。脅威マップやトラフィック マップ（**[Monitor]** > [アプリケーション スコープ] > [脅威マップ] または[トラフィック マップ]）では、受信トラフィックおよび送信トラフィックの地理的な地域を可視化できます。これは、外部からの潜在的な攻撃（DDoS 攻撃など）を示す可能性のある異常なアクティビティを表示する場合に特に役立ちます。たとえば、東ヨーロッパのビジネス トランザクションは多くないのに、マップでその地域へのトラフィックが異常なレベルを示

© 2019 Palo Alto Networks, Inc.

している場合、マップの対応するエリアをクリックして、上位アプリケーション、セッション数に関するトラフィックの詳細、送受信バイト数、上位の送信元および宛先、ユーザーまたは IP アドレス、検出された脅威（存在する場合）の重大度に関する ACC 情報を起動して表示します。脅威モニター（**[Monitor]** > [アプリケーション スコープ] > [脅威モニター]）には、ネットワーク上の上位 10 個の脅威やネットワーク上の上位の攻撃者または上位の被害者のリストが表示されます。

セキュリティ ルールの更新

明らかになったすべての情報を使用して、ネットワークに対する脅威の影響（攻撃の規模、送信元、侵入されたホスト、リスク ファクタ）を把握し、実施する変更（存在する場合）を評価できます。以下に、考慮すべき推奨事項を示します。

- DoS 保護プロファイルを強化して、ランダム早期ドロップを設定したり、TCP フラッドの SYN Cookie を破棄したりして、DDoS 攻撃を未然に防ぎます。ICMP および UDP トラフィックを制限することを検討してください。ログで発見した傾向およびパターンに基づいて、使用できるオプションを評価し、Panorama テンプレートを使用して変更を実装します。

  ダイナミック ブロック リスト（**[Objects]** > [ダイナミック ブロック リスト]）を作成して、複数の情報源（独自の脅威ログの分析、特定の IP アドレスからの DDOS 攻撃、またはサードパーティの IP ブロック リスト）で明らかになった特定の IP アドレスをブロックします。

  リストは、テキスト ファイルで、Web サーバー上に置かれている必要があります。Panorama のデバイス グループを使用して、オブジェクトを管理対象ファイアウォールにプッシュし、ファイアウォールが Web サーバーにアクセスして、定義した頻度でリストをインポートできるようにします。ダイナミック ブロック リストを作成したら、送信元および宛先フィールドのアドレス オブジェクトを使用して、定義した IP アドレス、範囲、またはサブネットからの（への）トラフィックをブロックするセキュリティ ルールを定義します。このアプローチでは、問題を解決してポリシーのより大きな変更を行ってネットワークを保護するまで侵入者をブロックできます。
- 共有ポリシー ルールまたはデバイス グループ ルールを作成して、感染を引き起こした特定のアプリケーション（web-browsing、SMTP、FTP）をブロックするかどうかを判断し、より厳格な URL フィルタリング ポリシーを作成して、一部のアプリケーション/アクション（ファイルのダウンロードなど）を特定のユーザー グループに限定します。
- Panorama では、ファイアウォール コンテキストに切り替えて、ネットワーク上でボットネットに感染している可能性のあるホストを特定する Botnet レポートを得られるよう、ファイアウォールを設定する事ができます。

Panorama の高可用性

システムやネットワークの障害が発生した場合に備えて冗長性を提供するため、2 つの Panorama™ 管理サーバーを高可用性 (HA) 構成でデプロイできます。Panorama では、片方のピアがアクティブでプライマリ、もう片方がパッシブでセカンダリの HA 構成がサポートされます。プライマリ ピアで障害が発生した場合は、自動的にフェイルオーバーされてセカンダリ ピアがアクティブになります。

> Panorama HA の前提条件
> HA 設定の Panorama での優先度とフェイルオーバー
> フェイルオーバーのトリガー
> Panorama HA での口ギングに関する考慮事項
> Panorama HA ピア間の同期
> Panorama HA ペアの管理

Panorama HA の前提条件

HA の Panorama を設定するには、以下の要件を満たす同一の Panorama サーバーのペアが必要です。

- 同じフォーム ファクタ - ピアは、同じモデルと同じモードでなければなりません。両方ともM-600 アプライアンス、M-500 アプライアンス、M-200 アプライアンス、および Panorama モード、管理専用モードまたはレガシー モードの AWS、 Azure、GCP ならびに ESXi の Panorama バーチャル アプライアンス (ESXi と vCloud Air のみ) 。ログ コレクタ モードの Panorama アプライアンスでは、HA がサポートされません。
- **The same Panorama OS version** (同じ **Panorama OS** バージョン) – 設定情報を同期し、等価性を保持してシームレスなフェイルオーバーを行うには、同じバージョンの Panorama を実行する必要があります。
- **The same set of licenses** (同じライセンス セット) – 同じファイアウォール管理容量のライセンスを持っている必要があります。
- (Panorama バーチャル アプライアンスのみ) **Unique serial number** (一意のシリアル番号) – 一意のシリアル番号が必要です。両方の Panorama インスタンスのシリアル番号が同じの場合、問題が解決されるまでインスタンスがサスペンド モードになります。

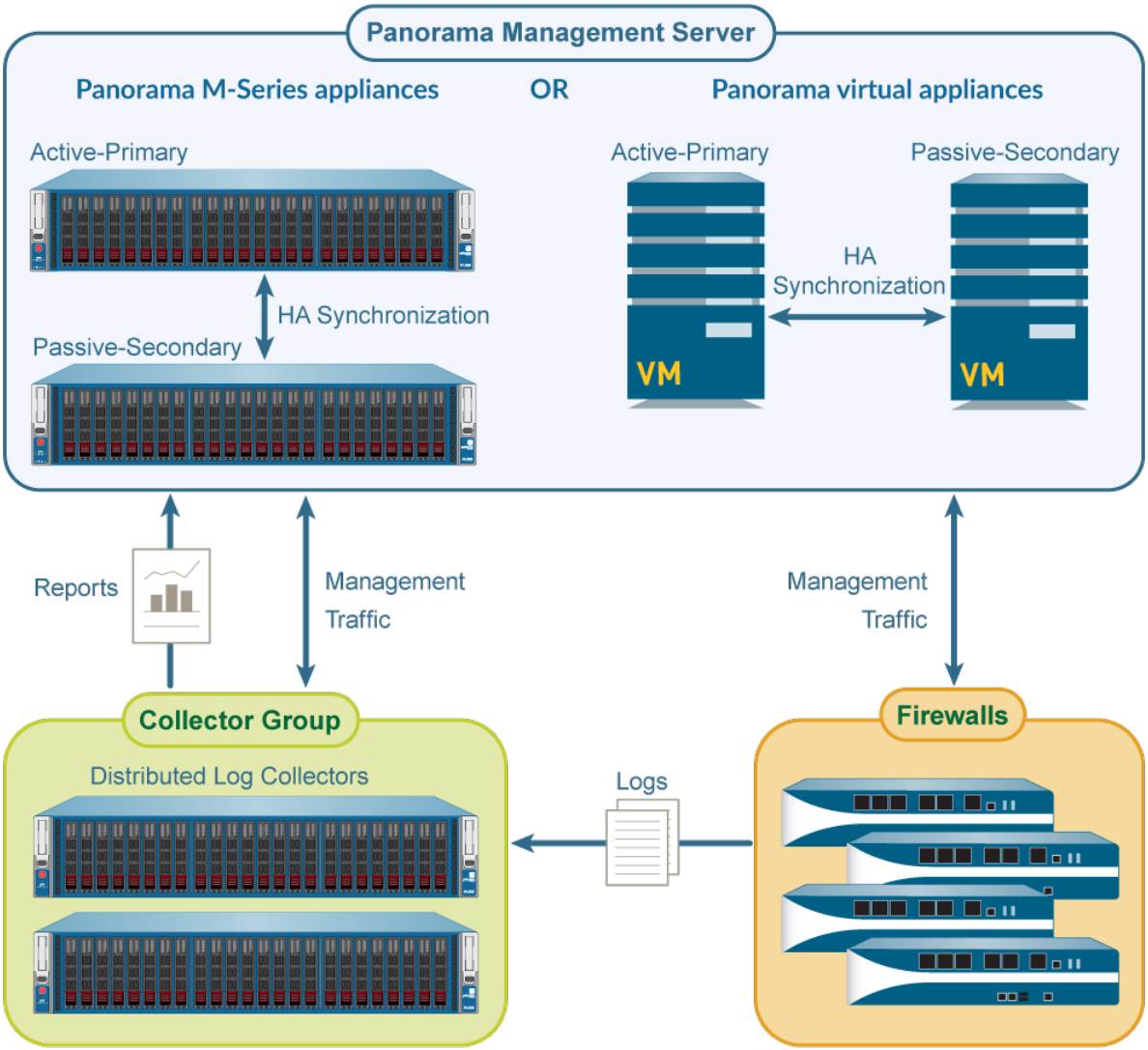


図 28 : Panorama HA 編成

© 2019 Palo Alto Networks, Inc.

HA 設定の Panorama サーバーはピアであり、一部の例外を除き、ファイアウォール、ログ コレクタ、WildFire アプライアンス、アプライアンス クラスタの中央管理にどちらのピア（アクティブまたはパッシブ）も使用できます（Panorama HA ピア間の同期を参照）。HA ピアでは、管理対象のファイアウォール、ログ コレクタ、WildFire アプライアンス、アプライアンス クラスタにプッシュされる設定要素を同期し、状態に関する情報を管理するために、管理（MGT）インターフェイスが使用されます。通常、Panorama HA ピアは、地理的に異なるサイトに配置されているため、各ピアに割り当てられる MGT インターフェイスの IP アドレスがネットワークを経由できることを確認する必要があります。HA 接続では、暗号化が有効になっている状態で TCP ポート 28 が使用されます。暗号化が有効になっていない場合、HA 接続および HA ピア間の設定の同期にポート 28769 および 28260 が使用されます。ピア間の遅延を500ms未満にすることが推奨されます。遅延を確認するには、通常トラフィックの期間中に Ping を使用します。

© 2019 Palo Alto Networks, Inc.

HA 設定の Panorama での優先度とフェイルオーバー

HA ペアの各 Panorama ピアには、優先度の値が割り当てられます。優先度の値がプライマリまたはセカンダリのどちらであるかによって、管理および口グ管理のメイン ポイントとなる Panorama ピアが決まります。プライマリとして設定されたピアはアクティブ状態となり、セカンダリ ピアはパッシブになります。アクティブ ピアは、設定のすべての変更を処理して管理対象ファイアウォールにプッシュします。パッシブ ピアは、設定を変更できず、管理対象ファイアウォールに設定をプッシュすることもできません。ただし、レポートまたはログ クエリの実行には、どちらのピアも使用できます。

アクティブPanoramaのパス、リンク、システム、またはネットワークで障害が発生した場合は、パッシブ ピアが同期され、いつでもアクティブ状態に移行できるよう維持されます。

フェイルオーバーが発生すると、Panoramaピアの状態 (アクティブまたはパッシブ) のみが変更し、優先度 (プライマリまたはセカンダリ) は変更しません。たとえば、プライマリ ピアで障害が発生すると、状態が active-primary から passive- primary に変わります。

以下の 2 つの例外を除き、すべての機能は active-secondary 状態のピアで実行できます。

- ライセンスの更新やソフトウェアのアップグレードといった、ファイアウォールあるいはログコレクタのデプロイ機能は管理できません。
- 優先度を手動でプライマリに変更するまでは、NFS に口ギングできません。NFS をサポートしているのは、レガシー モードの Panorama バーチャル アプライアンスだけです。

以下の表に、状態と優先度設定に基づく Panorama の機能の一覧を示します。

Capability	active-primary	passive-primary passive-secondary	active-secondary
Switch device context	■	■	■
Perform distributed reporting	■	■	■
Manage shared policy	■	■	■
Log to local disk	■	■ (Optional on the Panorama virtual appliance only)	■ (Optional on the Panorama virtual appliance only)
Log to an NFS partition (Panorama virtual appliance only)	■	■	■
Deploy software and licenses	■	■	■
Export Panorama configuration	■	■	■

図 29 : Panorama HA の機能

詳細は、Panorama HA の前提条件および Panorama での HA のセットアップを参照してください。

© 2019 Palo Alto Networks, Inc.

フェイルオーバーのトリガー

アクティブ Panorama で障害が発生すると、パッシブ Panorama がファイアウォールの管理タスクを引き継ぎますが、このイベントをフェイルオーバーと呼びます。アクティブ Panorama のモニター対象メトリックに障害が発生すると、フェイルオーバーがトリガーされます。この障害により、プライマリ Panorama の状態が active-primary から passive-primary に変わり、セカンダリ Panorama が active-secondary になります。

フェイルオーバーが引き起こされる条件は、以下のとおりです。

- Panorama ピア間で通信できず、アクティブ ピアがヘルス ポーリングおよび状態ポーリングに応答しない。使用されるメトリックはHA ハートビート ポーリングおよび Hello メッセージ。

  Panorama ピア間で通信できない場合は、フェイルオーバーがトリガーされる前に、ピアがまだ接続されているかどうかをアクティブな方がモニターします。このチェックは、フェイルオーバーを回避して両方の Panorama ピアがアクティブ状態になるスプリット ブレイン現象を防止するのに役立ちます。
- アクティブ ピアで指定された 1 つ以上の宛先 (IP アドレス) に到達できない。使用されるメトリックはHA パス モニタリング。

上記のフェイルオーバーのトリガー条件に加えて、管理者が Panorama ピアをサスペンド状態にした場合、またはプリエンプションが発生した際も、フェイルオーバーが引き起こされます。プリエンプションは、障害 (またはユーザーが開始したサスペンド) から回復した後でアクティブな動作を再開するための、プライマリ Panorama の設定です。デフォルトではプリエンプションが有効になっており、プライマリ Panorama が障害から回復して使用可能になると、セカンダリ Panorama は制御を放棄し、パッシブ状態に戻ります。プリエンプションが発生すると、そのイベントがシステム ログに記録されます。

NFS データストアにロギングしている場合は、(NFS にマウントされた) プライマリ ピアでアクティブ ロールが再開し、NFS データストアへの書き込みが許可されるため、プリエンプションを無効にしないでください。他のすべての導入では、特定の Panorama を確実に優先アクティブ ピアにする場合のみ、プリエンプションが必要です。

HA ハートビート ポーリングおよび Hello メッセージ

HA ピアでは、Hello メッセージおよびハートビートを使用して、ピアの応答状態と動作状態を確認します。設定した「Hello 間隔」で Hello メッセージがピアの一方から他方へ送信され、他方の状態を確認します。ハートビートは HA ピアに対する ICMP ping で、ピアがこの ping に応答することによって、ピアの接続および応答状態が確立します。デフォルトのハートビート間隔は 1,000 ミリ秒、Hello メッセージ間隔は 8,000 ミリ秒です。

HA パス モニタリング

パス モニタリングは、ある IP アドレスまたは IP アドレスのグループ (パス グループ) のネットワーク接続およびリンクの状態をチェックします。アクティブ ピアでは、ICMP ping を使用して、1 つ以上の宛先 IP アドレスに到達できることが確認されます。たとえば、ルーターまたはスイッチなどの相互接続されたネットワーク デバイスの可用性、サーバーへの接続状態、またはトラフィック フロー中に存在する他のいくつかの主要デバイスへの接続状態をモニタリングできます。モニタリング中のノード/デバイスが応答していない可能性がある場合、特に負荷がある場合は、パス モニタリング障害の原因となり、フェイルオーバーがトリガーされるため、このような状態でないことを確認します。

デフォルトの ping 間隔は 5,000 ミリ秒です。3 回 (デフォルト値) 連続して ping に失敗すると、その IP アドレスに到達不可能とみなされ、モニターする IP アドレスの一部またはすべてに到達不可能となった場合は、ピア障害がトリガーされます。デフォルトでは、いずれかの IP アドレスが到達不可能になると、HA 状態が non-functional に変わります。

© 2019 Palo Alto Networks, Inc.

Panorama HA でのロギングに関する考慮事項

HA 設定での Panorama のセットアップでは、ログ収集の冗長性が提供されます。管理対象のファイアウォールは SSL 経由で両方の Panorama ピアに接続されるため、状態が変化すると、各 Panorama から管理対象のファイアウォールにメッセージが送信されます。Panorama HA 状態がファイアウォールに通知され、ログを適宜転送できます。



デフォルトでは、管理対象のファイアウォールが *Panorama* に接続できない場合にログがバッファされ、接続が復元されると、最後に残された場所から送信が再開されます。

ロギング オプションは、ハードウェアベースの Panorama と Panorama バーチャル アプライアンスとで異なります。

- レガシー モードの Panorama バーチャル アプライアンスでのロギングのフェイルオーバー
- Panorama モードの M-Series アプライアンスまたは Panorama バーチャル アプライアンスでのロギングのフェイルオーバー

レガシー モードの Panorama バーチャル アプライアンスでのロギングのフェイルオーバー

レガシー モードの Panorama バーチャル アプライアンスには、以下のログ フェイルオーバー オプションがあります。

ログ保存エリア タイプ	説明
仮想ディスク	デフォルトでは、管理対象のファイアウォールから各 Panorama HA ピアに独立したログ ストリームとしてログが送信されます。デフォルト設定では、ピアが使用不可能になると、管理対象のファイアウォールでログがバッファされ、ピアが再接続された時点で、中断した時点からログ送信が再開されます (再開時点はディスク ストレージ容量および切断期間に左右されます)。 最大ログ ストレージ容量は、仮想プラットフォーム (VMware ESXi または vCloud Air) によって異なります。詳細は、「Panorama モデル」を参照してください。  ログの転送先をアクティブ ピアのみにするかどうかを選択できます (「ログ転送とバッファのデフォルトの変更」を参照)。ただし、*Panorama* では *HA* ペアにまたがったログの集約はサポートされていません。したがって、モニタリングまたはレポート作成用に仮想ディスクにロギングしている場合は、管理対象のファイアウォールからログを収集している *Panorama* ピアに対してクエリを実行する必要があります。
ネットワーク ファイル システム (NFS)	NFS ストレージは、VMware ESXi サーバー上で稼働している Panorama バーチャル アプライアンスにのみマウントできます。アクティブ-プライマリ Panorama のみが NFS ベースのログ パーティションにマウントされ、ログを受信できます。フェイルオーバー時には、プライマリ デバイスが passive-primary 状態になります。この場合、プリエンプションが行われるまで、アクティブ-セカンダリ Panorama でファイアウォールが管理されますが、ログは受信せず、NFS に書き込むこともできません。active-secondary ピアから NFS へのログを許可するには、そのピアを手動でプライマリに切り替え、NFS パーティションにマウントで

© 2019 Palo Alto Networks, Inc.

ログ保存エリア タイプ	説明
	きるようにする必要があります。手順は、「Panorama のフェイルオーバーにより NFS ロギングが再開された後の優先度の切り替え」を参照してください。

Panorama モードの M-Series アプライアンスまたは Panorama バーチャル アプライアンスでのロギングのフェイルオーバー

Panorama モードの M-600 アプライアンス、M-500 アプライアンス、M-200 アプライアンス、または Panorama バーチャル アプライアンスの HA ペア上のローカル ログ コレクタにファイアウォール ログを転送する場合は、コレクタ グループの設定を行うときに、どのファイアウォールがどのログ コレクタにログを送信するかを指定します。各 Panorama ピアのログ コレクタに対して別々のコレクタ グループを設定することも、両方のピアのログ コレクタを含む 1 つのコレクタ グループを設定することもできます。両方のローカル ログ コレクタを含むコレクタ グループでは、ログ転送設定リストにより、ファイアウォールからログを受信するログ コレクタが決定されます。PA-7000 シリーズと PA-5200 シリーズのファイアウォールでは、コレクタ グループ内のすべてのログ コレクタにログを送信するオプションがあります。この場合、Panorama は、常にラウンドロビンによる負荷分散を使用して、ログを受信するログ コレクタを選択します。

両方のログ コレクタを含むコレクタ グループでは、冗長性を有効にすることで、ログごとに 2 つのコピーを作成し、各コピーを別々のログ コレクタに配置することもできます。この冗長性により、いずれかのログ コレクタが利用不可になってもログは失われません。すべてのログがコレクタ グループに転送されていることを確認し、すべてのログ情報に関するレポートを実行できます。コレクタ グループ内の各ログ コレクタのディスク数が同じ場合にのみ、ログの冗長化が可能になります。

特定のコレクタ グループのすべてのログ コレクタが、同じモデルである必要があります（すべての *M-200* アプライアンス、すべての *M-500* アプライアンス、すべての *M-600* アプライアンス、または *Panorama* モードのすべての*Panorama* バーチャル アプライアンス）。

冗長性を有効にすると、作成されるログが多くなるため、この設定には、より大きなストレージ容量が必要です。冗長性を有効にすると、コレクタ グループ内のログ処理トラフィックが *2* 倍になり、最大ロギング率が半分になります。各ログ コレクタが、受信する各ログのコピーを配信する必要があるためです。（コレクタ グループの容量が不足すると、古いログが削除されます。）

© 2019 Palo Alto Networks, Inc.

Panorama HA ピア間の同期

Panorama HA ピアでは、アクティブな Panorama ピアの変更をコミットするたびに、実行中の設定が同期されます。候補設定は、アクティブ ピアで設定を保存するたび、またはフェイルオーバーが発生する直前にピア間で同期されます。

共有オブジェクトおよびポリシー ルール、デバイス グループのオブジェクトおよびルール、テンプレート設定、証明書、SSL/TLS サービスプロファイル、管理アクセス設定など、ペア全体に共通する設定は、Panorama HA ピア間で同期されます。

自動コミットリカバリを有効化すると、HA 同期はPanorama からのプッシュ後に、ファイアウォールがそれ自体と Panorama 間の接続テストを正常に完了した後にのみ実行されます。

以下のような各ピアに固有の設定は、同期されません。

- Panorama HA 設定 — 優先度の設定、ピア IP アドレス、パス モニタリングのグループおよび IP アドレス
- Panorama 設定 — 管理インターフェイスの IP アドレス、FQDN 設定、ログイン バナー、NTP サーバー、タイム ゾーン、地理的な位置、DNS サーバー、Panorama にアクセスするためのアクセス許可 IP アドレス、SNMP システム設定、動的コンテンツ更新スケジュール
- スケジュール設定された設定のエクスポート
- ロギング用の NFS パーティション設定およびすべてのディスク割り当てこれは、VMware ESXi サーバー上でレガシー モードで実行している Panorama バーチャル アプライアンスにのみ適用されます。
- Panorama ローカル ストレージ（SSD）でのタイプが異なるログおよびデータベースのディスク割り当て

> *Panorama* で秘密鍵と証明書の暗号化にマスター キーを使用する場合は、両方の *HA* ピアで、同じマスター キーを使用する必要があります。マスター キーが異なると、*HA* ピア間の同期が行われません。

詳細は、Panorama HA の前提条件および Panorama での HA のセットアップを参照してください。

© 2019 Palo Alto Networks, Inc.

Panorama HA ペアの管理

- Panorama での HA のセットアップ
- HA ピア間のカスタム証明書を使用する認証のセットアップ
- Panorama HA フェイルオーバーのテスト
- Panorama のフェイルオーバーにより NFS ロギングが再開された後の優先度の切り替え
- プライマリ Panorama のアクティブ状態への復元

ソフトウェアまたはコンテンツアップデートをインストールする方法についてはHA 設定の Panorama に更新をインストールをご覧ください。

Panorama での HA のセットアップ

「Panorama HA の前提条件」を確認してから、以下の手順を実行します。

STEP 1 | HA ピアで MGT ポート間の接続をセットアップします。

Panorama ピア間の通信には、MGT ポートが使用されます。HA ペアの Panorama サーバーの MGT ポートに割り当てる IP アドレスがルーティング可能であり、Panorama ピア間の通信をネットワーク経由で行えることを確認します。MGT ポートをセットアップするには、「Panorama バーチャル アプライアンスの初期設定の実行」または「M-Series アプライアンスの初期設定」を参照してください。

ペアのうちどちらかの **Panorama** ピアを選択して、残りの作業を完了させます。

STEP 2 | HA を有効化し、必要に応じて HA 接続の暗号化を有効にします。

1. **[Panorama]** > [高可用性] を選択し、[セットアップ] セクションを編集します。
2. **Enable HA**（**HA** の有効化）を選択します。
3. **Peer HA IP Address**（ピア **HA IP** アドレス）フィールドに、ピア Panorama に割り当てられた IP アドレスを入力します。
4. **Peer HA Serial (ピア HA シリアル)** フィールドに、ピア Panorama のシリアル番号を入力します。

   Panorama HA ピアのシリアル番号を入力して、Panorama IP に対するブルート フォース アタックに対する攻撃対象領域を減らします。
5. **Monitor Hold Time**（ホールド タイムのモニター）フィールドに、制御リンク障害に反応するまでにシステムが待機する時間（ミリ秒）を入力します（有効範囲は 1000 ~ 60000、デフォルトは 3000）。
6. 暗号化を行わない場合は、**Encryption Enabled**（暗号化を有効）チェック ボックスをオフにして、**OK** をクリックします。それ以上の操作は不要です。暗号化を行う場合は、**Encryption Enabled**（暗号化を有効）チェック ボックスをオンにして、**OK** をクリックし、以下のタスクを実行します。
   1. **Panorama** > **Certificate Management**（ 証明書の管理 ） > **Certificates**（ 証明書 ）を選択します。
   2. **Export HA key**（**HA** 鍵のエクスポート）を選択します。ピア Panorama がアクセスできるネットワーク上の場所に、HA 鍵を保存します。
   3. ピアPanoramaで**Panorama** > **Certificate Management** > **Certificates**(Panorama > 証明書の管理 > 証明書) に移動し、**Import HA key**(HA キーのインポート) を選択してキーを保存した場所を検索し、そのキーをインポートします。

STEP 3 | HA 優先度を設定します。

1. **[Panorama]** > [高可用性] で、[選択設定] セクションを編集します。

© 2019 Palo Alto Networks, Inc.

2. **Device Priority**（デバイス優先度）を **Primary**（プライマリ）または **Secondary**（セカンダリ）として定義します。1 つのピアをプライマリとして設定し、もう 1 つをセカンダリとして設定してください。

   両方のピアを同じ優先度に設定すると、シリアル番号が高いピアがサスペンド状態になります。

3. **Preemptive**（プリエンプティブ）動作を定義します。デフォルトでは、プリエンプションが有効になっています。プリエンプションの選択（有効または無効）は、両方のピアで同じにする必要があります。

   ロギングに *NFS* を使用しており、プリエンプションを無効にした場合に、*NFS* へのロギングを再開するには、「Panorama のフェイルオーバーにより NFS ロギングが再開された後の優先度の切り替え」を参照してください。

STEP 4 | パス モニタリングを設定するには、1 つ以上のパス グループを定義します。

パス グループには、ネットワーク接続を確認するために Panorama で ping する必要のある宛先 IP アドレス（ノード）が表示されます。

モニターするノードを含む各パス グループについて、以下の手順を実行します。

1. **[Panorama] > [高可用性]** を選択し、**[パス グループ] > セクション**で、**[追加]** をクリックします。
2. **Name**（名前）に、パス グループの名前を入力します。
3. このグループの **Failure Condition**（失敗条件）を選択します。
   - **any**（いずれか）を指定すると、いずれかの IP アドレスに到達できなくなった場合に、パス モニタリング障害がトリガーされます。
   - **all**（すべて）を指定すると、どの IP アドレスにも到達できない場合にのみ、パス モニタリング障害がトリガーされます。
4. 監視する各宛先 IP アドレスを **Add**（追加）します。
5. **OK** をクリックします。Path Group（パス グループ）セクションに新しいグループが表示されます。

STEP 5 | （任意）Panorama でパス モニタリングの失敗条件を選択します。

1. **Panorama** > **High Availability** (Panorama > 高可用性) を選択し、Path Monitoring (パス モニタリング)セクションを編集します。
2. **Failure Condition**（エラー条件）を選択します。
   - **all**（すべて）を指定すると、すべてのモニター対象パス グループが失敗した場合にのみ、フェイルオーバーがトリガーされます。
   - **any**（いずれか）を指定すると、いずれかのモニター対象パス グループが失敗した場合に、フェイルオーバーがトリガーされます。
3. **OK** をクリックします。

STEP 6 | 設定の変更をコミットします。

Commit（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

STEP 7 | 他の Panorama ピアを設定します。

HA ピアのもう一方のピアでステップ「2」～「6」を実行します。

STEP 8 | Panorama ピアを同期します。

© 2019 Palo Alto Networks, Inc.

1. アクティブ Panorama で **Dashboard**（ダッシュボード）にアクセスし、**Widgets**（ウィジット）> **System**（システム）> **High Availability**（高可用性）の順に選択して HA ウィジットを表示します。
2. **Sync to peer**（ピアと同期）を行い、**Yes**（はい）をクリックして、**Running Config**（実行中の設定）で **Synchronized**（同期済み）が表示されるまで待ちます。
3. パッシブ Panorama で **Dashboard**（ダッシュボード）にアクセスし、**Widgets**（ウィジット）> **System**（システム）> **High Availability**（高可用性）の順に選択して HA ウィジットを表示します。
4. **Running Config**（実行中の設定）で **Synchronized**（同期済み）が表示されることを確認します。

HA ピア間のカスタム証明書を使用する認証のセットアップ

Panorama HA 間の HA 接続を保護するためにカスタム証明書を使用する認証のセットアップ が可能です。

STEP 1 | Panorama の認証局（CA）証明書を生成します。

1. **Panorama** > **Certificate Management**（ 証明書の管理 ）> **Certificates**（ 証明書 ）を選択します。
2. 自己署名ルート CA 証明書を作成するかエンタープライズ CA から証明書をインポートします。

STEP 2 | ルート CA および中間 CA が含まれる証明書プロファイルを設定します。

1. **Panorama** > **Certificate Management**（証明書の管理）> **Certificate Profile**（証明書プロファイル）の順に選択します。
2. 証明書プロファイルの設定を行います。

STEP 3 | SSL/TLS サービス プロファイルの設定を行います。

1. **Panorama** > **Certificate Management**（証明書の管理）> **SSL/TLS Service Profile**（**SSL/TLS** サービス プロファイル）の順に選択します。
2. SSL/TLS プロファイルを設定し、Panorama およびその管理対象デバイスを SSL/TLS サービス用に使用する証明書とプロトコルを定義します。

STEP 4 | Panorama で保護されたサーバー通信を設定します。

1. **[Panorama]** > [セットアップ] > [管理] の順に選択し、[Panorama 設定] を 編集します。
2. **Custom Certificate Only**（カスタム証明書のみ）チェック ボックスがオフになっていることを確認します。これにより、カスタム証明書への移行中もすべてのデバイスの管理を続行できます。

   Custom Certificate Only（カスタム証明書のみ）チェック ボックスをオンにしていると、*Panorama* は事前定義済みの証明書を使用したデバイスを認証せず、管理することができません。
3. **SSL/TLS Service Profile**（**SSL/TLS** サービス プロファイル）ドロップダウンから SSL/TLS サービス プロファイルを選択します。この SSL/TLS サービス プロファイルは、Panorama、ファイアウォール、ログ コレクタ、Panorama の HA ピア間のすべての SSL 接続に適用されます。
4. **Certificate Profile**（証明書プロファイル）ドロップダウンから証明書プロファイルを選択します。
5. （任意）認証リストを設定します。
   1. Authorization List（承認リスト）で **Add**（追加）をクリックします。
   2. 識別子タイプとして **Subject**（サブジェクト）または **Subject Alt Name**（サブジェクト代替名）を選択します。
   3. Common Name（共通名）を入力します。
6. **Disconnect Wait Time (min)**（切断待機時間（分））に、Panorama が管理対象デバイスとの接続を切断して再開するまで待機する分数を入力します。このフィールドはデフォルトで空白であり、範囲は 0 ~ 44,640 分です。

© 2019 Palo Alto Networks, Inc.

切断待機時間は、新しい設定をコミットするまでカウント ダウンを開始しません。

1. **OK** をクリックします。
2. 変更を**Commit (コミット)** します。

STEP 5 | クライアント側の Panorama を 8.1 にアップグレードします。

Panorama のアップグレードを行います。

STEP 6 | 保護されたクライアント通信を設定します。

1. **Panorama** > **High Availability**（高可用性）の順に選択し、HA 設定を **Edit**（編集）します。
2. **Certificate**（証明書）および **Certificate Profile**（証明書プロファイル）を選択します。
3. **OK** をクリックします。
4. 変更を**Commit (コミット)** します。

Panorama HA フェイルオーバーのテスト

HA 設定が正しく動作することをテストするには、手動でフェイルオーバーをトリガーして、ピアの状態が正しく移行することを確認します。

STEP 1 | アクティブな Panorama ピアにログインします。

Panorama サーバーの状態は、Web インターフェイスの右下隅で確認できます。

STEP 2 | アクティブな Panorama ピアをサスペンド状態にします。

Panorama > **High Availability**（高可用性）の順に選択し、Operational Commands（操作コマンド）セクションの **Suspend local Panorama**（ローカル **Panorama** をサスペンド）リンクをクリックします。

STEP 3 | パッシブな Panorama ピアがアクティブとして引き継がれていることを確認します。

Panorama の **Dashboard**（**Dashboard**）の **High Availability**（高可用性）ウィジットで、**Local**（ローカル）パッシブ サーバーの状態が **active**（アクティブ）に、**Peer**（ピア）の状態が **suspended**（サスペンド）になっていることを確認します。

STEP 4 | サスペンドされたピアを稼働状態に戻します。プリエンプティブを有効にしている場合は、しばらく待ってからプリエンプションが発生していることを確認します。

Panorama で、以下のように以前にサスペンドしています。

1. **Panorama** > **High Availability**(Panorama > 高可用性)を選択し、Operational Commands (操作コマンド) セクションで、**Make local Panorama functional**(ローカル Panorama を稼働状態にする) をクリックします。
2. **Dashboard**（ダッシュボード）の **High Availability**（高可用性）ウィジットで、この（ローカルの）Panorama がアクティブ ピアとして引き継がれ、他のピアがパッシブ状態に変わっていることを確認します。

Panorama のフェイルオーバーにより NFS ロギングが再開された後の優先度の切り替え

ESXi サーバー上でレガシー モードで実行している Panorama バーチャル アプライアンスは、ロギングに NFS データストアを使用できます。HA 設定の場合、プライマリ Panorama ピアのみが NFS ベースのログ パーティションにマウントされ、NFS に書き込みを行えます。フェイルオーバーが発生すると、パッシブ Panorama がアクティブになり、active-secondary 状態になります。セカンダリ Panorama ピアでは、

© 2019 Palo Alto Networks, Inc.

ファイアウォールをアクティブに管理することはできますが、NFS パーティションを所有していないため、ログの受信や NFS への書き込みはできません。ファイアウォールがプライマリ Panorama ピアにログを転送できない場合、各ファイアウォールが自身のローカル ディスクにログを書き込みます。ファイアウォールは、passive-primary Panorama が再び使用可能になったときログの転送を再開できるように、自身が Panorama に転送した最後のログ エントリ セットを指すポインタを保持しています。

NFS パーティションへのロギングを開始できるように active-secondary Panorama ピアで優先度を手動で切り替えるには、このセクションの手順を使用します。通常、以下の場合に、この変更をトリガーする必要があります。

- プリエンプションが無効になっている。デフォルトでは、Panorama でプリエンプションが有効になっており、再び使用可能になるとプライマリ ピアがアクティブに戻ります。プリエンプションが無効になっている場合は、セカンダリ ピアで優先度をプライマリに切り替えて、NFS パーティションのマウント、管理対象のファイアウォールからのログの受信、NFS パーティションへの書き込みを行えるようにする必要があります。
- アクティブ Panorama が失敗し、短期間で障害から回復できない。優先度を切り替えないと、ファイアウォールでログ ストレージの最大容量に達した場合に、ローカル ディスクへのロギングを続行するために最も古いログが上書きされます。このため、ログが失われる可能性があります。

STEP 1 | 現在の passive-primary Panorama にログインして、**[Panorama]** > [セットアップ] > [操作] の順に選択し、[デバイスの操作] セクションで **[Panorama のシャットダウン]** をクリックします。

STEP 2 | active-secondary Panorama にログインして、**Panorama** > **High Availability**（高可用性）の順に選択して、Election Settings（選択設定）の編集で **Priority**（優先順位）を **Primary**（プライマリ）に設定します。

STEP 3 | **OK** をクリックして変更内容を保存します。

STEP 4 | **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

プロンプトが表示されても再起動しないでください。

STEP 5 | を行い、以下のコマンドを入力して、NFS パーティションの所有者をこのピアに変更します。`request high-availability convert-to-primary`

STEP 6 | **[Panorama]** > [セットアップ] > [操作] の順に選択し、[デバイスの操作] セクションで **[Panorama の再起動]** をクリックします。

STEP 7 | ステップ 1 でパワーオフした Panorama ピアをパワーオンします。これで、このピアが passive-secondary 状態になります。

プライマリ Panorama のアクティブ状態への復元

デフォルトでは、Panorama のプリエンプティブ機能により、プライマリ Panorama が使用可能になった時点で、アクティブ ピアとして機能を再開できます。ただし、プリエンプションが無効な場合に、障害、非稼働、またはサスペンド状態から回復した後でプライマリ Panorama を強制的にアクティブにするには、セカンダリ Panorama ピアをサスペンドする必要があります。

active-secondary Panorama は、自身がサスペンド状態になる前に、候補設定をパッシブPanoramaに転送して、コミットされていないすべての設定変更を保存し、他のピアからアクセスできるようにします。

STEP 1 | Panorama をサスペンドします。

1. サスペンド状態にする Panorama ピアにログインします。

© 2019 Palo Alto Networks, Inc.

2. **[Panorama]** > [高可用性] の順に選択し、[操作コマンド] セクションの [ローカル **Panorama** をサスペンド] リンクをクリックします。

STEP 2 | ユーザーの要求によりPanoramaがサスペンドの状態になっていることを確認します。

Dashboard（ダッシュボード）の **High Availability**（高可用性）ウィジットで、**Local**（ローカル）状態が **suspended**（サスペンド）になっていることを確認します。

ピアをサスペンドするとフェイルオーバーがトリガーされ、他の Panorama がアクティブ ピアとして引き継がれます。

STEP 3 | サスペンドされた Panorama を稼働状態に戻します。

1. **[Panorama]** > [高可用性] タブの [操作コマンド] セクションで、[ローカル **Panorama** を稼働状態にする] リンクをクリックします。
2. **Dashboard**（ダッシュボード）の **High Availability**（高可用性）ウィジットで、Panoramaがアクティブ状態またはパッシブ状態に変わったことを確認します。

Panorama の管理

このセクションでは、Panorama™ 管理サーバーを管理および維持する方法について説明します。このセクションは、以下のトピックで構成されています。

- 設定変更のプレビュー、検証、コミット
- 自動コミットリカバリを有効化
- Panorama およびファイアウォールの設定のバックアップを管理
- Panorama の設定変更の比較
- 設定変更を制限するためのロックの管理
- Panorama にカスタム ロゴを追加
- Panorama タスク マネージャの使用
- ログおよびレポートのストレージ割り当ておよび有効期間を管理
- Panorama のモニタリング
- Panorama の再起動またはシャットダウン
- Panorama のパスワード プロファイルおよび複雑性の設定

初期セットアップ (ネットワーク アクセス設定の定義、ライセンス、Panorama ソフトウェア バージョンのアップグレード、Panorama への管理アクセスのセットアップなど) を実行する手順の詳細は、「Panorama のセットアップ」を参照してください。

設定変更のプレビュー、検証、コミット

Panorama 設定への保留中の変更にPanorama のコミット、検証、およびプレビュー操作を実行し、ファイアウォール、ログ コレクタ、WildFire アプライアンス、アプライアンス クラスタなど、Panorama が管理するデバイスに変更をプッシュできます。保留中の変更を管理者または場所でフィルタリングし、それらの変更のみをコミット、プッシュ、検証、またはプレビューできます。場所は、特定のデバイス グループ、テンプレート、コレクタ グループ、ログ コレクタ、共有設定、Panorama 管理サーバーになります。

Panorama は実行中の設定をプッシュするため、変更は Panorama にコミットするまでデバイスにプッシュできません。変更をデバイスで有効にする準備が整っていない場合は、**Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）を選択し、変更をデバイスにプッシュせずに Panorama 設定にコミットできます。後で変更をデバイスで有効にする準備が整ったら、**Commit**（コミット）> **Push to Devices**（デバイスにプッシュ）を選択できます。Panorama とデバイスの両方で変更を有効にする準備が整っている場合は、次の手順で説明するように、**Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）を選択します。

STEP 1 | コミット、検証、プレビューを行う設定変更の範囲を設定します。

1. Webインターフェイスの上部にある **Commit**（コミット）をクリックします。
2. 以下のいずれかのオプションを選択します。
   - **Commit All Changes**（すべての変更をコミット）（デフォルト）– 管理権限があるすべての変更をコミットします。このオプションを選択すると、コミット スコープを手動で絞り込むことはできなくなります。代わりに、ログインに使用しているアカウントに割り当てられた管理者ロールによって、コミット スコープが指定されます。
   - **Commit Changes Made By**（指定対象による変更のコミット）– 管理者または場所によってコミット スコープを絞り込むことができます。ログインに使用しているアカウントに割り当てられた管理ロールによって、どの変更を絞り込めるかが決まります。

   他の管理者の変更をコミットするには、ログインに使用したアカウントにスーパーユーザー ロールが割り当てられているか、*Commit For Other Admins*（他の管理者に代わってコミット）権限が有効な管理者ロール プロファイルが割り当てられている必要があります。
3. （任意）管理者でコミット スコープを絞り込むには、**Commit Changes Made By**（指定対象による変更のコミット）を選択して、その横のリンクをクリックし、管理者を選択して **OK** をクリックします。
4. （任意）場所で絞り込むには、**Commit Changes Made By**（指定対象による変更のコミット）を選択し、コミット スコープから除外する変更をオフにします。

   含めた設定変更、除外した設定変更の依存関係により検証エラーが発生する場合、すべての変更を含めてコミットを行います。例えば、デバイス グループへの変更をコミットする場合、そのデバイス グループの同じルールベースのルールの追加、削除、または順序変更を行ったすべての管理者の変更を含める必要があります。

STEP 2 | コミットにより反映される変更をプレビューします。



同じデバイスを削除してからポリシー ルールに再び追加した後に変更をプレビューすると、*Panorama* はこの同じデバイスを実行中の構成で削除されたもの、および候補構成に追加されたものとして表示します。さらに、実行設定のデバイスターゲットリスト内でのデバイスの順序は、候補構成とは異なる場合があり、設定が変更されていない場合でも変更をプレビューすると変更として表示されます。

例えば変更内容をすべて覚えておらず、変更をすべて反映させて良いのか分からないと時はこのオプションが役立ちます。

© 2019 Palo Alto Networks, Inc.

Panorama は、Commit Scope（コミット スコープ）で選択した設定を、実行中の設定と比較します。プレビュー ウィンドウには設定が横に並べて表示され、色分けによって、どの変更が追加であるか（緑）、変更であるか（黄）、削除であるか（赤）が示されます。

Preview Changes（変更のプレビュー）を行い、**Lines of Context**（コンテクストの行数）を選択します。これは、ハイライト表示された差異の前後を示す、比較対象の設定ファイル中の行数です。この行により、プレビュー結果をWebインターフェイスの設定内容に反映させやすくなります。変更のプレビューが完了したら、プレビューウィンドウを閉じます。



プレビュー結果は新しいウィンドウで表示されるので、ブラウザでポップアップを許可しておく必要があります。プレビューウィンドウが開かない場合はブラウザ設定を参照し、ポップアップブロックの解除を行ってください。

STEP 3 | 変更をコミットする個別の設定をプレビューします。

設定のタイプや変更者など、変更の詳細について把握する場合は、これが役立つことがあります。

1. **Change Summary**（変更サマリー）をクリックします。
2. （任意）**Group By**（グループ化基準）により、列名（設定の **Type**（タイプ）など）によってグループ化します。
3. 変更のプレビューが完了したら、**Close**（閉じる）によって Change Summary（変更サマリー）ダイアログを閉じます。

STEP 4 | 確実にコミットが完了するよう、コミット前に変更内容を検証します。

1. **Validate Changes**（変更の検証）を行います。

   実際にコミットを行う際と同じエラーや警告がすべて結果に表示されます。
2. 検証結果で明らかになったエラーをすべて解決します。

STEP 5 | （任意）プッシュ スコープを変更します。

デフォルトでは、プッシュ スコープには、Panorama コミットを必要とする変更のあるすべての場所が含まれます。



Commit（コミット）> *Push to Devices*（デバイスにプッシュ）を選択すると、プッシュ スコープには、*Panorama* の動作中設定と同期していないデバイスに関連する、すべての場所が含まれます。

1. **Remove Selections (選択を削除)** して、プッシュ スコープにリストされているファイアウォールを削除します。
2. **Edit Selections**（選択内容の編集）を行い、次のように選択します。
   - **Device Groups**（デバイス グループ）– デバイス グループ、個別のファイアウォール、仮想システムのいずれかを選択します。
   - **Templates**（テンプレート）– テンプレート、テンプレート スタック、個別のファイアウォールのいずれかを選択します。
   - **Collector Groups**（コレクタ グループ）– コレクタ グループを選択します。
3. **OK** をクリックして、プッシュ スコープに対する変更を保存します。

STEP 6 | デバイス グループやテンプレートにプッシュする変更を検証します。

1. **Validate Device Group Push**（デバイス グループのプッシュの検証）または **Validate Template Push**（テンプレートのプッシュの検証）を行います。

   実際にプッシュ操作を行う際と同じエラーや警告がすべて結果に表示されます。
2. 検証結果で明らかになったエラーをすべて解決します。

© 2019 Palo Alto Networks, Inc.

STEP 7 | Panorama に変更をコミットし、その変更をデバイスにプッシュします。

設定変更を **Commit and Push**（コミットしてプッシュ）します。



Panorama タスク マネージャの使用保留中（任意でキャンセル可能）、進行中、完了済み、あるいは失敗したコミットの詳細情報を確認するためのものです。

© 2019 Palo Alto Networks, Inc.

自動コミットリカバリを有効化

Panorama™ 管理サーバから管理対象ファイアウォールにプッシュされたり、ファイアウォールでローカルにコミットされた設定変更による設定の破損を保証するには、**Automated Commit Recovery**（自動コミットリカバリ）を有効にして、管理対象ファイアウォールが各コミットの設定変更をテストできるようにし、変更によって、Panorama と管理対象ファイアウォール間の接続が切断されていないことを確認します。管理対象ファイアウォールが実行するテストの数と、管理対象ファイアウォールがその設定を以前に実行していた設定に自動的に戻す前に各テストが実行される間隔は、設定可能です。自動コミットリカバリを有効にすると、管理対象ファイアウォールの設定は元に戻りますが、Panorama 設定は戻りません。さらに、管理対象ファイアウォールは、Panorama への接続を 60 分ごとにテストして、無関係なネットワーク設定がファイアウォールと Panorama の接続を切断させた場合、もしくは過去にコミットした設定が接続状態に影響を与えた場合も、接続状態の継続を保証します。高可用性（HA）設定の場合、Panorama からのプッシュ後の HA ピア間の HA 同期は、接続テスト後にのみ実行されます。

自動コミット リカバリはデフォルトで有効に設定されています。ただし、自動コミット リカバリを無効にしてから、既存の実稼働環境でこの機能を再度有効にする場合は、最初に、Panorama と管理対象ファイアウォール間の接続を切断するポリシー ルールがないことを確認してください。たとえば、管理トラフィックがデータプレーンを通過する場合、ファイアウォールから Panorama へのトラフィックを制限するポリシー ルールが存在する可能性があります。

ファイアウォールの設定が最後に実行していた設定に、正常に戻った後、ファイアウォールは設定ログを生成します。さらに、ファイアウォールは、管理者がこの機能を無効にした場合、設定のプッシュ後に失敗した接続テストが原因で、設定の復帰イベントが開始した場合、および 60 分ごとに実行される Panorama 接続テストが失敗して、ファイアウォール設定が戻った場合に、システムログを生成します。

自動コミット トリカバリを有効にすることは、他の設定変更とは無関係です。他の設定変更と同時に有効にして、*Panorama* ファイアウォールと管理対象ファイアウォール間の接続が切断された場合、ファイアウォール設定は自動的に元に戻りません。

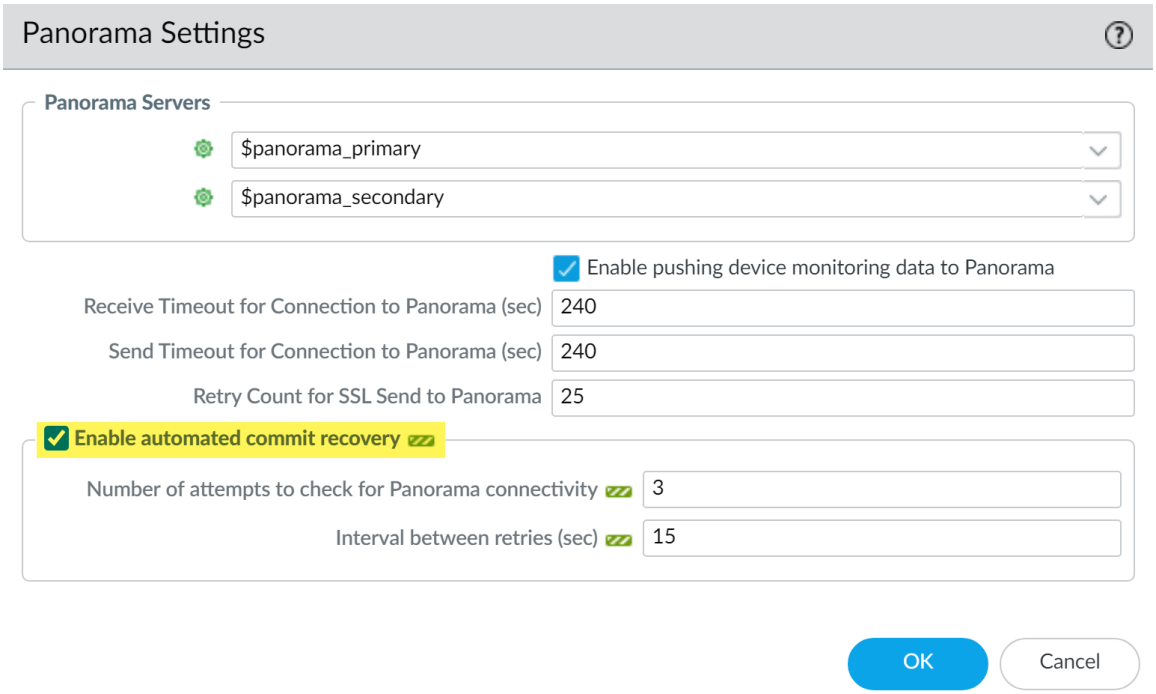
STEP 1 | Panorama Web インターフェイスへのログイン.

STEP 2 | **Device**（デバイス）> **Setup**（設定）> **Management**（管理）の順に選択して、**Template**（テンプレート）のコンテキスト ドロップダウンから目的のテンプレートまたはテンプレート スタックを選択します。

STEP 3 | 自動コミットリカバリを有効にします。

1. Panorama 設定を **Edit**（編集）（ ）します。
2. **Enable automated commit recovery**（自動コミット リカバリを有効）にします。
3. **Number of attempts to check for Panorama connectivity**（自動コミット リカバリ時に Panorama 接続をチェックする試行回数）を設定します（デフォルトは 1 回）。
4. **Interval between retries**（再試行の間隔）を設定します（デフォルトは 10 秒）。
5. **OK** をクリックして変更内容を保存します。

© 2019 Palo Alto Networks, Inc.



STEP 4 | **Commit**（コミット）> **Commit and Push**（コミットおよびプッシュ）の順に選択して、変更内容を **Commit and Push**（コミットおよびプッシュ）します。

STEP 5 | 管理対象ファイアウォールで自動コミット リカバリ機能が有効になっていることを確認します。

1. ファイアウォール Web インターフェースを起動します。
2. **Device**（デバイス）> **Setup**（設定）> **Management**（管理）の順に選択して、Panorama 設定で、**Enable automated commit recovery**（自動コミットリカバリを有効にする）が有効（チェック済み）になっていることを確認します。

© 2019 Palo Alto Networks, Inc.

Panorama およびファイアウォールの設定のバックアップを管理

Panoramaで現在実行している設定はすべてコミット済みの設定であり、そのためアクティブな状態になっています。候補設定は、現在アクティブな設定のコピー、および前回のコミット後に加えたアクティブでない変更から成ります。現在アクティブな設定あるいは候補設定の各バージョンのバックアップを保存することで、後で各バージョンを復元することが可能になります。たとえば、コミット検証の結果、修復したくなくなるほど多くのエラーが現在の候補設定に含まれていることが分かった場合、以前の候補設定を復元することができます。最初にバックアップを保存せずに、現在アクティブな設定に戻ることもできます。

設定変更を *Panorama* にコミットし、その変更内容を管理対象デバイスにプッシュする方法の詳細は、「Panorama のコミット、検証、およびプレビュー操作」を参照してください。

PAN-OS 5.0 以降を実行しているローカル ファイアウォールでコミットを行うと、現在アクティブな設定のバックアップが Panorama に送信されます。ローカル ファイアウォールでコミットを実行すると、バックアップが必ずトリガーされます。このコミットには、管理者がファイアウォールでローカルに実行するコミットや、PAN-OS が開始する自動コミット（FQDN 更新など）が含まれます。デフォルトではファイアウォールごとに最大 100 個のバックアップが Panorama に保存されるようになっていますが、設定を変えることもできます。Panoramaおよびファイアウォールの設定のバックアップを既存のホスト上に保存するために、Panoramaからエクスポートのスケジュール設定を行ったり、必要に応じてエクスポートを実行したりできます。また、ファイアウォールから Panorama デバイス グループおよびテンプレートに設定をインポートして、「ファイアウォールを Panorama 管理に移行」を行うこともできます。

(VMware ESXi と vCloud Air のみ) VMware スナップショット機能は、VMware ESXi と vCloud Air 上にデプロイされた Panorama バーチャル アプライアンスではサポートされていません。Panorama バーチャル アプライアンスのスナップショットを作成するとパフォーマンスに影響が及ぶ可能性があり、その結果、断続的で一貫性のないパケット損失が発生し、Panorama が応答しなくなる可能性があります。さらに、Panorama CLI と Web インターフェースへのアクセスができなくなる可能性があり、Panorama モード への切り替えはサポートされていません。代わりに、名前の付いた設定スナップショットを任意のネットワークの場所に保存してエクスポートします。

- 設定ファイルのエクスポートのスケジュール設定
- Panorama およびファイアウォールの設定の保存およびエクスポート
- Panorama の設定変更を元に戻す
- Panorama に保存される設定バックアップ ファイルの上限数の設定
- 管理対象ファイアウォールでの設定バックアップ ファイルのロード

設定ファイルのエクスポートのスケジュール設定

Panoramaは管理対象のすべてのファイアウォールのアクティブな設定と併せて、自身の現在アクティブな設定のバックアップも保存します。このバックアップは、（Panoramaあるいはファイアウォール）のシリアル番号に基づいて決定されたファイル名が付いたXMLフォーマットで保存されます。バックアップをリモートホストに定期的にエクスポートする方法は次の通りです。Panoramaはバックアップを単一のgzipファイルとしてエクスポートします。エクスポートのスケジューリングを行うにはスーパーユーザー権限が必要です。

Panorama で高可用性（*HA*）が設定されている場合は、各ピアで以下の手順を実行して、フェイルオーバー後もスケジュール設定されたエクスポートが継続して実行されるようにす

© 2019 Palo Alto Networks, Inc.

る必要があります。*Panorama* は、スケジュール設定されたエクスポートを *HA* ピア間で同期しません。

バックアップをオンデマンドでエクスポートするには、「Panorama およびファイアウォールの設定の保存およびエクスポート」を参照してください。

STEP 1 | **Panorama** > **Scheduled Config Export** (Panorama > スケジューリングされた設定のエクスポート)の順に選択し、**Add** (追加)をクリックします。

STEP 2 | スケジュール設定するエクスポートファイルの **Name**（名前）および **Description**（説明）を入力し、**Enable**（有効化）します。

STEP 3 | 日時の **Scheduled Export Start Time**（エクスポートの予定開始時間）を24時間形式で入力するか、ドロップダウンリストから選択を行います。

2 つ以上のサーバーにスケジュールされたエクスポートを設定する場合は、スケジュールされたエクスポートの開始時刻をずらします。同じ開始時刻に複数のエクスポートをスケジュールすると、エクスポートされた設定間で不一致が生じます。

STEP 4 | エクスポート **Protocol**（プロトコル）を Secure Copy（**SCP**）あるいはファイル転送プロトコル（**FTP**）に設定します。

STEP 5 | サーバーにアクセスするための詳細情報を入力します。ファイルのアップロードに使用する**Hostname** (ホスト名)あるいはIPアドレス、**Port** (ポート)、**Path** (パス)、および**Username** (ユーザー名)と**Password** (パスワード)などです。

Path（パス）は次の文字をサポートしています：．(ピリオド)、 + 、 { および } 、 / 、-、_ 、0～9、a～z、および A～Z。ファイル **Path**（パス）では、スペースはサポートされていません。

Hostname（ホストネーム）として、*IPv6* アドレスを使用して *FTP* サーバーにエクスポートする場合は、角括弧（*[]*）で囲まれたアドレスを入力する必要があります。例えば、***[2001:0db8:0000:0000:0000:8a2e:0370:7334]*** です。

エクスポート先を *BSD* サーバーにする場合は、*SSHD* パスワード プロンプトを ***<username>@<hostname> <password>:*** に変更する必要があります。

STEP 6 | （SCP のみ）**Test SCP server connection**（**SCP** サーバー接続のテスト）をクリックします。データの安全な転送を有効にするには、SCP サーバーのホスト キーを確認して受け入れる必要があります。ホスト キーを承認するまでの間、Panoramaは接続を確立しません。Panorama で HA が設定されている場合は、各ピアで以下の手順を実行し、それぞれが SCP サーバーのホスト キーを承認するようにします。Panorama から SCP サーバーに正常に接続できた場合、ssh-export-test.txt という名前のテスト ファイルが作成されてアップロードされます。

STEP 7 | **OK** をクリックして変更内容を保存します。

STEP 8 | **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

Panorama およびファイアウォールの設定の保存およびエクスポート

候補構成のバックアップを Panorama 上の永続的なストレージに保存すると、そのバックアップを後で復元することができます (Panorama の設定変更を元に戻すを参照)。さらに、Panorama を使用すると、指定

© 2019 Palo Alto Networks, Inc.

したデバイス グループ、テンプレート、およびテンプレート スタックの構成を保存して エクスポートすることができます。これは、システム イベントまたは管理者のアクションによって Panorama が再起動した場合に失われるはずの変更内容を保持するために役立ちます。再起動後、Panorama は、`running-config.xml` という名前のファイルに保存されている、現在アクティブな設定の最新バージョンに自動的に戻ります。バックアップを保存することは、現在アクティブな設定より古い Panorama 設定に戻る場合にも役立ちます。Panorama が自動的に候補設定を永続的なストレージに保存することはありません。デフォルト スナップショット ファイル (`.snapshot.xml`) として、あるいは任意の名前のスナップショット ファイルとして、手動で候補構成を保存する必要があります。Panorama は、スナップショット ファイルをローカルに保存します。ただし、このファイルは、外部のホストにエクスポートすることもできます。



設定のバックアップを保存しなくても、最後のコミットまたは再起動以降に行われた変更を元に戻すことができます。これを行うには、*Config (設定) > Revert Changes (変更を元に戻す)*を選択します (Panorama の設定変更を元に戻すを参照)。

Palo Alto Networks は、重要なすべての設定を外部のホストにバックアップすることをお勧めしています。

STEP 1 | 候補設定の変更を保存します。

- デフォルトのスナップショット ファイル (`.snapshot.xml`) を、すべての管理者が行ったすべての変更で上書きするには、以下のいずれかのステップを実行します。
  - **Panorama** > **Setup** (セットアップ) > **Operations** (操作) の順に選択し、**Save candidate Panorama configuration** (**Panorama** の候補設定の保存) を選択します。
  - スーパーユーザー ロールが割り当てられた管理者アカウント、または **Save For Other Admins** (他の管理者用に保存) 権限が有効な管理者ロール プロファイルを使用して、Panorama にログインします。次に、Web インターフェイスの上部で **Config** (設定) > **Save Changes** (変更の保存) の順に選択し、**Save All Changes** (すべての変更を保存) および **Save** (保存) を選択します。
- 管理者が特定のデバイス グループ、テンプレート、またはテンプレート スタック構成に加えた変更で、デフォルトのスナップショット (`.snapshot.xml`) を上書きするには、以下のステップを実行します。
  1. **Panorama** > **Setup (セットアップ)** > **Operations (運用)** を選択し、**Save candidate Panorama configuration (Panorama** の候補構成の保存) し、**Select Device Groups & Templates (**デバイスグループおよびテンプレートを選択) します。
  2. 元に戻す特定のデバイス グループ、テンプレート、またはテンプレート スタックを選択します。
  3. **OK** をクリックして操作を確定します。
  4. (任意) **Commit (**コミット**)** > **Commit to Panorama (Panorama** へのコミット**)** の順に選択し、実行中の設定に対して、変更内容を **Commit (**コミット**)** し、スナップショットでオーバーライドします。
- デフォルトのスナップショット ファイルを上書きせずに、すべての管理者が行ったすべての変更を含むスナップショットを作成するには、以下のステップを実行します。
  1. **Panorama** > **Setup** > **Operations** (Panorama > セットアップ > 操作)を選択し、**Save named Panorama configuration snapshot**(Panorama 設定スナップショットを名前を付けて保存) します。
  2. 新規または既存の設定ファイルの **Name** (名前) を指定します。
  3. **OK**、**Close** (閉じる) の順にクリックします。
- デフォルトのスナップショット ファイルのどの部分も上書きせずに、候補設定に対する特定の変更のみを保存するには、以下のステップを実行します。
  1. 任意の変更を保存するために必要なロール権限を持つ管理者アカウントを使用して Panorama にログインします。

© 2019 Palo Alto Networks, Inc.

2. Web インターフェイスの上部で **Config**（設定）> **Save Changes**（変更の保存）の順に選択します。
3. **Save Changes Made By**（指定対象による変更の保存）を選択します。
4. 管理者に基づいて Save Scope (保存範囲) をフィルタリングするには、<*administrator-name*> をクリックし、管理者を選択して **OK** をクリックします。
5. Save Scope（保存範囲）を場所でフィルタリングするには、除外する場所をクリアします。場所は、特定のデバイス グループ、テンプレート、コレクタ グループ、ログ コレクタ、共有設定、Panorama 管理サーバーになります。
6. **Save**（保存）をクリックし、新規または既存の設定ファイルの **Name**（名前）を指定して **OK** をクリックします。

- 特定のデバイス グループ、テンプレート、またはテンプレート スタック構成を保存するには、以下のステップを実行します。

  1. **Panorama** > **Setup** > **Operations** を選択して **Save named Panorama configuration snapshot** (名前を付けて **Panorama** 設定スナップショットを保存) し、**Select Device Groups & Templates** (デバイスグループおよびテンプレートを選択) します。
  2. 保存する特定のデバイス グループ、テンプレート、またはテンプレート スタックを選択します。
  3. **OK** をクリックして操作を確定します。

STEP 2 | Panoramaあるいはファイアウォールの外部にあるホストに候補設定あるいは現在実行中の設定をエクスポートします。

SCP または FTP サーバーに対して、日次エクスポートをスケジュールすることも (設定ファイルのエクスポートのスケジュール設定を参照)、オンデマンドで設定をエクスポートすることもできます。オンデマンドで エクスポートするには、**Panorama** > **Setup**（セットアップ）> **Operations**（操作）の順に選択し、以下のいずれかのオプションを選択します。

- **Export named Panorama configuration snapshot**（名前を付けて保存したPanorama候補設定のスナップショットをエクスポート）—現在アクティブな設定、名前を付けて保存した候補設定のスナップショット、または前回インポートした設定（候補または実行中の設定）をエクスポートします。Panoramaは、指定した**Name**（名前）のXMLファイルとして設定をエクスポートします。**Select Device Groups & Templates** (デバイス グループおよびテンプレートを選択) して、エクスポートするデバイス グループ、テンプレート、あるいはテンプレート スタック設定を指定します。
- **Export Panorama configuration version**（Panorama設定のバージョンをエクスポート）—現在アクティブな設定の**Version**（バージョン）を選択し、XMLファイルとしてエクスポートします。**Select Device Groups & Templates** (デバイス グループおよびテンプレートを選択) して、XML ファイルとしてエクスポートするデバイス グループ、テンプレート、あるいはテンプレート スタック設定を指定します。
- **Export Panorama and devices config bundle**（Panorama およびデバイスの設定バンドルのエクスポート）— Panorama および各管理対象ファイアウォールが実行している設定のバックアップの最新バージョンを生成およびエクスポートします。設定バンドルを毎日作成して Secure Copy (SCP) または FTP サーバーにエクスポートするプロセスを自動化する方法は、設定ファイルのエクスポートのスケジュール設定を参照してください。
- **Export or push device config bundle** (デバイス設定バンドルをエクスポート/プッシュ)—ファイアウォールの設定をPanoramaにインポートした後、Panoramaは、すべてのローカルポリシーおよびオブジェクトが削除されたファイアウォール設定バンドルを<firewall_name>_import.tgzという名前で作成します。そうすると、**Export or push device config bundle**（デバイス設定バンドルをエクスポート/プッシュ）して次のいずれかを行えるようになります。

  - 設定バンドルをファイアウォールに**Push & Commit**(プッシュおよびコミット)することで、ファイアウォールからローカル設定がすべて削除され、Panoramaでファイアーウォールを管理できるようになります。

© 2019 Palo Alto Networks, Inc.

- 設定をロードせずにファイアウォールに **Export**（エクスポート）する。設定を読み込む準備ができたら、ファイアウォールのCLI にログインし、設定モード コマンド **`load device-state`** を実行する必要があります。このコマンドを使用すると、**Push & Commit**（プッシュ & コミット）オプションと同じようにファイアウォールがクリーンアップされます。



ファイアウォールを Panorama 管理に移行を完全な手順で行うには、追加のステップが必要です。

Panorama の設定変更を元に戻す

変更内容を復元すると、現在の候補構成が別の設定に置き換えられます。変更を元に戻す操作が便利なのは、複数の設定に対する変更を手動で個々に取り消すのではなく、1 回の操作で取り消したいときです。

最後のコミット以降に Panorama 設定に対して行われた保留中の変更を元に戻すことができます。Panorama で保留中の変更をすべて元に戻すか、特定のデバイス グループ、テンプレート、またはテンプレート スタックを選択することができます。Panorama には、保留中の変更を管理者または場所でフィルタリングするオプションが用意されています。場所は、特定のデバイス グループ、テンプレート、コレクタ グループ、ログ コレクタ、共有設定、Panorama 管理サーバーになります。現在実行している設定よりも古い候補構成のスナップショット ファイルが保存されている場合は (Panorama およびファイアウォールの設定の保存およびエクスポートを参照)、その候補構成のスナップショットに復元することもできます。スナップショットを復元すると、最後のコミットより前に存在していた候補設定を復元できます。変更をコミットする際、Panorama は現在アクティブな設定の新しいバージョンを自動的に保存するため、後でこれらのバージョンを復元することができます。

Panorama 管理サーバの設定を元に戻すには、完全なコミットが必要であり、スーパーユーザーが実行しなければなりません。完全なコミットは、Panorama 設定の復元やロードなどの特定の Panorama 操作を実行するときに必要であり、カスタム管理者ロールプロファイルではサポートされていません。

- Panorama の現在アクティブな設定 (ファイル名 **`running-config.xml`**) を復元します。

  この操作では、前回のコミット以降に候補設定に対して加えた変更が取り消されます。

  - すべての管理者が行ったすべての変更を元に戻すには、以下のステップを実行します。
    - **Panorama** > **Setup**（セットアップ）> **Operations**（操作）, **Revert to running Panorama configuration**（実行中の **Panorama** 設定を復元）の順に選択し、**Yes**（はい）をクリックして操作を確定します。
    - スーパーユーザー ロールが割り当てられた管理者アカウント、または **Commit For Other Admins**（他の管理者用にコミット）権限が有効な管理者ロール プロファイルを使用して、Panorama にログインします。次に、**Config (設定)** > **Revert Changes (変更を元に戻す)** を選択し、**Revert All Changes (すべての変更を元に戻す)** および **Revert (元に戻す)** を選択します。
  - 特定の変更のみを候補設定に戻すには、以下のステップを実行します。
    1. 任意の変更を元に戻すために必要なロール権限を持つ管理者アカウントを使用して Panorama にログインします。

       コミット操作を制御する権限は、元に戻す操作も制御します。
    2. **Config (設定)** > **Revert Changes (変更を元に戻す)** を選択します。
    3. **Revert Changes Made By**（指定対象に基づいて変更を元に戻す）を選択します。
    4. 管理者に基づいて Revert Scope (元に戻す範囲) をフィルタリングするには、*<administrator-name>* をクリックし、管理者を選択して **OK** をクリックします。
    5. Revert Scope（元に戻す範囲）を場所でフィルタリングするには、除外する場所をクリアします。
    6. 変更に対して **Revert**（元に戻す）を実行します。

© 2019 Palo Alto Networks, Inc.

- 特定のデバイス グループ、テンプレート、またはテンプレート スタックの変更を実行コンフィギュレーションに戻すには、以下以下のステップを実行します。
  1. **Panorama** > **Setup** (セットアップ) > **Operations** (運用) を選択し、**Revert to running Panorama configuration** (実行中の Panorama 設定を復元) してから、**Select Device Groups & Templates** (デバイス グループおよびテンプレートを選択) します。
  2. 元に戻す特定のデバイス グループ、テンプレート、またはテンプレート スタックを選択します。
  3. **OK** をクリックして操作を確定します。
  4. (任意) **Commit** (コミット) > **Commit to Panorama** (Panorama へのコミット) の順に選択し、実行している設定に対して、変更内容を **Commit** (コミット) します。

- Panorama の候補構成のデフォルト スナップショット (`.snapshot.xml`) を復元します。
  - すべての管理者が行った、すべての変更を元に戻すには、以下のステップを実行します。
    1. **Panorama** > **Setup** (セットアップ) > **Operations** (操作) を選択し、**Revert to last saved Panorama configuration** (最後に保存した Panorama 設定を復元) を選択します。
    2. **Yes** (はい) をクリックして操作を確定します。
    3. (任意) **Commit** (コミット) > **Commit to Panorama** (Panorama へのコミット) の順に選択し、実行中の設定に対して、変更内容を **Commit** (コミット) し、スナップショットでオーバーライドします。
  - 特定のデバイス グループ、テンプレート、またはテンプレート スタックの変更を実行コンフィギュレーションに戻すには、以下以下のステップを実行します。
    1. **Panorama** > **Setup** (セットアップ) > **Operations** (運用) を選択し、**Revert to last saved Panorama configuration** (最後に保存した Panorama 設定を復元) してから、**Select Device Groups & Templates** (デバイス グループおよびテンプレートを選択) します。
    2. 元に戻す特定のデバイス グループ、テンプレート、またはテンプレート スタックを選択します。
    3. **OK** をクリックして操作を確定します。
    4. (任意) 実行している設定を上書きするには、**Commit** (コミット) > **Commit to Panorama** (Panorama へのコミット) を選択して、スナップショットでの変更内容を **Commit** (コミット) します。

- Panorama に保存されている、現在アクティブな設定の古いバージョンを復元します。
  - 管理者が行ったすべての変更を元に戻すには、以下のステップを実行します。
    1. **Panorama** > **Setup** (セットアップ) > **Operations** (運用) を選択し、**Load Panorama configuration version** (Panorama 設定バージョンの読み込み) を行って、**Select Device Groups & Templates** (デバイス グループおよびテンプレートを選択) します。
    2. 設定の **Version** (バージョン) を選択して **OK** をクリックします。
    3. (任意) 復元したバージョンで現在アクティブな設定を上書きするには、**Commit** (コミット) > **Commit to Panorama** (Panorama へのコミット) を選択して、変更内容を **Commit** (コミット) します。
  - 特定のデバイス グループ、テンプレート、またはテンプレートの変更を実行設定に戻すには、以下のステップを実行します。
    1. **Panorama** > **Setup** (セットアップ) > **Operations** (運用) を選択し、**Load Panorama configuration version** (Panorama 設定バージョンの読み込み) を行って、設定バージョンの **Name** (名前) を選択します。
    2. **Select Device Groups & Templates** (デバイス グループおよびテンプレートを選択) して、特定のデバイス グループ、テンプレート、あるいはテンプレート スタック設定を選択して、復元します。

© 2019 Palo Alto Networks, Inc.

3. **OK** をクリックして操作を確定します。
4. （任意）現在アクティブな設定をスナップショットで上書きするには、**Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）を選択して、変更内容を **Commit**（コミット）します。

- 以下のいずれかを復元します。
  - 名前を付けて保存した、Panorama が現在実行している設定 (以前にインポートしたもの)。
  - 名前を付けて保存した、Panorama 候補構成のスナップショット (デフォルトのスナップショットではない)。

1. **Panorama** > **Setup** (セットアップ) > **Operations** (運用) を選択し、**Load named Panorama configuration snapshot** (名前を付けて保存した **Panorama** 設定スナップショットを読み込み) を実行してインポートした構成ファイルの **Name** (名前) を選択します。
2. (任意)**Load Shared Objects** (共有オブジェクトの読み込み) または **Load Shared Policies** (共有ポリシーの読み込み) を行って、すべての共有オブジェクトまたはポリシーを読み込みます。すべての共有オブジェクトとポリシーをロードできるだけなく、次のステップで指定するデバイス グループとテンプレートで設定したすべてのオブジェクトとポリシーを読み込むことができます。
3. (任意) **Select Device Groups & Templates** (デバイス グループおよびテンプレートを選択) して、指定のデバイス グループ、テンプレート、あるいはテンプレート スタック設定を選択して読み込みます。Panorama 設定全体を元に戻す場合は、この手順をスキップしてください。
4. **OK** をクリックして操作を確定します。
5. （任意）現在アクティブな設定をスナップショットで上書きするには、**Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）を選択して、変更内容を **Commit**（コミット）します。

- 以前に外部ホストにエクスポートした、Panoramaが実行中の設定あるいは候補設定を復元します。

1. **Panorama** > **Setup**（セットアップ）> **Operations**（操作）を選択し、**Import named Panorama configuration snapshot**（名前を付けて保存した **Panorama** 設定スナップショットをインポート）をクリックし、さらに外部ホストにある設定ファイルを **Browse**（参照）して **OK** をクリックします。
2. **Load named Panorama configuration snapshot** (名前を付けて保存した **Panorama** 設定スナップショットの読み込み) を実行し、先ほどインポートした設定ファイルの **Name** (名前) を選択します。
3. (任意)**Load Shared Objects** (共有オブジェクトの読み込み) または **Load Shared Policies** (共有ポリシーの読み込み) を行って、すべての共有オブジェクトまたはポリシーを読み込みます。すべての共有オブジェクトとポリシーをロードできるだけでなく、次のステップで指定するデバイス グループとテンプレートで設定したすべてのオブジェクトとポリシーを読み込むことができます。
4. (任意) **Select Device Groups & Templates** (デバイス グループおよびテンプレートを選択) して、指定のデバイス グループ、テンプレート、あるいはテンプレート スタック設定を選択して読み込みます。Panorama 設定全体を元に戻す場合は、この手順をスキップしてください。
5. **OK** をクリックして操作を確定します。
6. （任意）インポートしたスナップショットで現在アクティブな設定を上書きするには、**Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）を選択して、変更内容を **Commit**（コミット）します。

Panorama に保存される設定バックアップ ファイルの上限数の設定

STEP 1 | **[Panorama]** > [セットアップ] > [管理] の順に選択し、[ロギングおよびレポート設定] を編集します

© 2019 Palo Alto Networks, Inc.

STEP 2 | **Log Export and Reporting**（ログのエクスポートとレポート）を選択して **Number of Versions for Config Backups**（設定バックアップのバージョン数）を入力します（デフォルトは 100、範囲は 1 ~ 1,048,576）。

STEP 3 | **OK** をクリックして変更内容を保存します。

STEP 4 | **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

管理対象ファイアウォールでの設定バックアップ ファイルのロード

Panorama を使用して、管理対象ファイアウォールに設定バックアップ ファイルをロードします。ファイアウォールで以前に保存またはコミットした設定に戻すことができます。Panorama により、選択したバージョンが管理対象ファイアウォールにプッシュされるため、ファイアウォールの現在の候補設定が上書きされます。

STEP 1 | **Panorama** > **Managed Devices**（管理対象デバイス）> **Summary**を選択します。

STEP 2 | Backups（バックアップ）列の **Manage**（管理）を選択します。

STEP 3 | Saved Configurations（保存された設定）または Committed Configurations（コミットされた設定）から選択します。

- バージョン番号をクリックし、そのバージョンの内容を確認します。
- 設定バージョンを **Load**（読み込み）ます。

STEP 4 | **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

© 2019 Palo Alto Networks, Inc.

Panorama の設定変更の比較

Panorama の設定の変更を比較するには、設定ファイル（候補設定、実行中の設定、Panorama に以前に保存されたまたはコミットされた他の設定バージョン）の 2 つのセットを選択します。並列比較により、以下が可能になります。

- Panorama にコミットする前に設定の変更をプレビューする。たとえば、候補設定と実行中の設定の変更をプレビューできます。変更の比較と識別が容易になるように、左ペインに古いバージョン、右ペインに新しいバージョンを選択することをお勧めします。
- 設定監査を実行し、設定ファイルの 2 つのセットの変更を確認および比較する。

デバイス グループとテンプレートの管理者は、アクセス ドメイン内のデバイス グループとテンプレートの設定のみを比較できます。

- Panorama の設定変更を比較する。
  1. **[Panorama]** > **[設定監査]** の順に選択します。
  2. 各ドロップダウンで、比較する設定を選択します。
  3. **Context**（コンテキスト）に含める行数を選択して、**Go**（実行）をクリックします。

     Panorama は、追加（緑）、変更（黄色）、削除（赤）した項目を色で区別します。



- 設定監査のために Panorama が保存するバージョンの数を設定する。
  1. **[Panorama]** > **[セットアップ]** > **[管理]** の順に選択し、**[ロギングおよびレポート設定]** を編集します
  2. **Number of Versions for Config Audit**（設定監査のバージョン数）を入力します（範囲は 1 ~ 1,048,576、デフォルト値は 100）。
  3. **OK** をクリックして変更内容を保存します。
  4. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

- コミット前の Panorama 設定ファイルを表示して比較する。
  1. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、**Preview Changes**（変更のプレビュー）を行います。
  2. 表示する **Lines of Context**（コンテクストの行数）の数を選択し、**OK** をクリックします。

© 2019 Palo Alto Networks, Inc.

設定変更を制限するためのロックの管理

候補設定あるいは現在アクティブな設定をロックすることで、設定を行った本人が手動でロックを解除する、あるいはファイアウォールが自動的にそれを削除する（コミット後）までの間、他の管理者がその設定を変更できなくなります。このロックにより、同時ログインセッションにおいて相互に依存する設定や同一の設定に対して、管理者が衝突する変更内容を設定できなくなります。



他の管理者が同時セッション中に変更している設定とは無関係の設定を変更している場合、設定のロックを行ってコミットの衝突を回避する必要はありません。*Panorama*はコミット操作をキューに並べ、管理者がコミットを開始した順番でコミットを実行していきます。詳細は、「Panorama のコミット、検証、およびプレビュー操作」を参照してください。

テンプレートあるいはデバイス グループに割り当てられているファイアウォールのローカルで管理者がコミットあるいは設定ロックをセットしている場合、そのテンプレートあるいはデバイス グループの設定のプッシュは失敗します。

- 現在のロックの詳細情報を表示します。

  例えば、他の管理者がロックを設定したかどうかや、ロックの説明として入力されたコメントを確認することができます。

  Web インターフェイスの上部にある、ロックされた南京錠（）をクリックします。隣りにある数値は、現在のロック数を示します。

- 設定をロックします。

  ファイアウォールあるいはPanorama設定を変更できない読み取り専用の管理者は、ロックをセットできません。

  1. Web インターフェイスの上隅にある南京錠のアイコンをクリックします。

     既存のロックが存在する（）あるいは存在しない（）かに基づき、異なったロック アイコンが表示されます。
  2. **Take a Lock**（ロックを選択）し、さらにロック**Type**（タイプ）を選択します。
     - **Config**（設定）– 他の管理者が候補設定を変更できないようにブロックします。

       変更をコミットできないカスタムロール管理者は、*Config*（設定）ロックをセットして候補設定に変更を保存できます。しかし、この管理者は変更をコミットできないため、*Panorama*がコミット後に自動的にロックを解除することはありません。管理者は、必要な変更を行ったら手動で*Config*（設定）ロックを解除する必要があります。

     - **Commit**（コミットロック）– 他の管理者が現在アクティブな設定を変更できないようにブロックします。
  3. **Location**（場所）を選択し、ロックのスコープを決定します。
     - **Shared**（共有）–変更の範囲を、すべてのデバイスグループおよびテンプレートを含む、Panorama設定全体に制限します。
     - テンプレート – 選択したテンプレートに含まれるファイアウォールに対する変更を制限します。（テンプレート スタックの個々のテンプレートはロックできますが、スタックごとロックすることはできません）
     - **Device group**（デバイスグループ）–選択したデバイスグループに対する変更を制限しますが、その子孫のデバイスグループについては対象外です。
  4. （任意）ロックを設定する理由を示す **Comment**（コメント）を追加することをお勧めします。
  5. **OK**、**Close**（閉じる）の順にクリックします。

© 2019 Palo Alto Networks, Inc.

- 設定のロックを解除します。

  スーパーユーザーまたはロックをセットした管理者のみが手動でロックを解除することができます。しかし、ロックを開始した管理者が実行したコミット操作が完了すると、Panoramaは自動的にロックを解除します。

  1. Web インターフェイスの上部にある、ロックされた南京錠（  ）をクリックします。
  2. リストからロックのエントリを選択します。
  3. **Remove Lock**（ロック解除）、**OK**、**Close**（閉じる）の順にクリックします。

- 候補設定を変更した際、現在アクティブな設定をPanoramaが自動的にロックするよう設定します。この設定はすべてのPanorama管理者に適用されます。

  1. **[Panorama]** > [セットアップ] > [管理] の順に選択し、[一般設定] を編集します。
  2. **Automatically Acquire Commit Lock**（自動的にコミットをロック）を選択し、**OK** をクリックします。
  3. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

© 2019 Palo Alto Networks, Inc.

Panorama にカスタム ロゴを追加

イメージ ファイルをアップロードして、Panorama の以下のエリアをカスタマイズできます。

- ログイン画面の背景イメージ
- Web インターフェイスの左上隅にあるヘッダー。Panorama のデフォルトの背景を非表示にすることもできます。
- PDF レポートのタイトル ページおよびフッターのイメージ

.jpg、.gif、および .png などのイメージ タイプがサポートされています。PDF レポートで使用するイメージ ファイルには、アルファ チャネルを含めることはできません。イメージのサイズは、128 キロバイト（131,072 バイト）未満にする必要があります。推奨サイズが画面に表示されます。サイズが推奨サイズよりも大きい場合、イメージが自動的に切り取られます。

STEP 1 | **[Panorama]** > **[セットアップ]** > **[操作]** の順に選択します。

STEP 2 | Miscellaneous（その他）セクションで、**Custom Logos**（カスタム ロゴ）を選択します。

STEP 3 | ロゴのアップロード アイコンをクリックし、ログイン画面、主要なユーザー インターフェイスの左隅、PDF レポートのタイトル ページ、および PDF レポート フッターのいずれかのイメージを選択します。

STEP 4 | **Open**（開く）をクリックしてイメージを追加します。イメージをプレビューするには、ロゴのプレビュー アイコンをクリックします。

STEP 5 | （任意）Panorama Web インターフェイスの緑の背景のヘッダーをクリアするには、**Remove Panorama background header**（**Panorama** バックグラウンド ヘッダーの非表示）のチェックボックスをオンにします。

STEP 6 | **Close**（閉じる）をクリックして、変更内容を保存します。

STEP 7 | **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

© 2019 Palo Alto Networks, Inc.

Panorama タスク マネージャの使用

Web インターフェイス下部の**Tasks**（タスク）（Tasks）をクリックしてタスク マネージャを開くと、前回ファイアウォールを再起動してから管理者が開始したすべての操作（たとえば、手動コミットなど）や、Panorama あるいは管理対象のファイアウォールが開始したすべての操作（たとえば、スケジュール設定されたレポートの生成など）を表示できます。タスク マネージャを使用すれば、失敗した操作についてトラブルシューティングを行ったり、完了したコミットに関する警告について調査を行ったり、保留中のコミットをキャンセルしたりすることができます。



デバイス グループとテンプレートの管理者は、アクセス ドメイン内のタスクのみを表示できます。

STEP 1 | **Tasks**（タスク）をクリックします。

STEP 2 | 任意で種類に基づきフィルタリング（**Reports**（レポート）、**Log Requests**（ログ リクエスト）、あるいは **Jobs**（ジョブ）のコミット、ダウンロード、インストール）を行って、**Running**（実行中）（進行中）のタスクまたは **All**（すべて）のタスク（デフォルト）を **Show**（表示）し、タスクを表示したい **Panorama**（デフォルト）あるいはファイアウォールを選択します。

STEP 3 | 以下の中から選択して作業を行います。

- **Display or hide task details**（タスクの詳細を表示/非表示）— デフォルト設定では、タスク マネージャに各タスクの Type（タイプ）、Status（ステータス）、Start Time（開始時間）、Messages（メッセージ）が表示されます。タスクの End Time（終了時間）および Job ID（ジョブ ID）を確認するには、これらの列を手動で表示する必要があります。列の表示/非表示を行うには、列の見出しにあるドロップダウンを開き、**Columns**（列）を選択し、必要に応じて列を選択/削除します。
- **Investigate warnings or failures**（警告あるいは失敗を調査）— タスク詳細情報にある Messages（メッセージ）列の項目を読みます。列に `Too many messages`（メッセージが多すぎます）と表示されている場合、Type (タイプ)列で項目をクリックし、詳細な情報を表示します。
- **Display a commit description**（コミットの説明を表示）— 管理者がコミットの説明を入力している場合、Messages（メッセージ）列で **Commit Description**（コミットの説明）をクリックして説明を表示します。
- **Check the position of a commit in the queue**（コミットのキュー内の順番をチェック）— Messages（メッセージ）列に、進行中のコミットのキュー内の順番が表示されます。
- **Cancel pending commits**（保留中のコミットをキャンセル）— 保留中のコミットをすべてキャンセルするには **Clear Commit Queue**（コミット キューをクリア）を実行します（定義済みの管理ロールでのみ使用可能）。コミットを個々にキャンセルするには、Action（アクション）列にある **x** をクリックします（Panorama がこのコミットをキューから取り除くまで、コミットはキューに残ったままになります）。進行中のコミットはキャンセルできません。

© 2019 Palo Alto Networks, Inc.

ログおよびレポートのストレージ割り当ておよび有効期間を管理

- ログおよびレポートの保存
- ログおよびレポートの有効期間
- ログおよびレポートのストレージ割り当ておよび有効期間を設定
- Panorama レポートのランタイムの設定

ログおよびレポートの保存

各ログ タイプのデフォルトのストレージ割り当てを編集できます。ログ割り当てが最大サイズに達すると、Panorama は最も古いログ エントリから順に新しいログ エントリで上書きします。レポートのストレージ容量は、設定できません。ログ ストレージの場所とレポートのストレージ容量は、Panorama モデルごとに異なります。

- **Panorama** モードの **Panorama** バーチャル アプライアンス – レポートのストレージ スペースは 200MB です。アプライアンスは、その仮想システム ディスクを使用して、Panorama とログ コレクタが生成したシステム ログや設定ログを保存します。仮想システム ディスクは、Panorama がすべての管理対象ファイアウォールから 15 分間隔で自動的に受信したアプリケーション統計（App Stats）ログも保存します。Panorama は、それ以外のタイプのログは、仮想ロギング用ディスク（1 から 12）に保存します。
- 管理専用モードの **Panorama** バーチャル アプライアンス – レポートのストレージ スペースは 500MB です。アプライアンスは、その仮想システム ディスクを使用して、Panorama とログ コレクタが生成したシステム ログや設定ログを保存します。仮想システム ディスクは、Panorama がすべての管理対象ファイアウォールから 15 分間隔で自動的に受信したアプリケーション統計（App Stats）ログも保存します。管理専用モードの Panorama は他のログ タイプを保存できないため、管理対象ファイアウォールからログを転送するように管理対象のコレクタを設定する必要があります。
- レガシー モードの **Panorama** バーチャル アプライアンス – Panorama 8.0 以前のリリースの場合、レポートのストレージ スペースは 200MB です。Panorama 8.0.1 以降のリリースの場合、レポートのストレージ スペースは 500MB です。Panorama は、割り当てられた以下のいずれかのストレージ スペースにすべてのログを書き込みます。
  - 仮想システム ディスク – デフォルトでは、Panorama のインストール時に作成した仮想システム ディスクのログ ストレージには、約 11GB が割り当てられています。仮想ロギング用ディスクや NFS パーティションを追加しても、Panorama は、依然としてシステム ディスクを使用して、Panorama とログ コレクタが生成したシステム ログや設定ログと、ファイアウォールから収集された App Stats ログを保存します。
  - 専用の仮想ロギング用ディスク – システム ディスクに存在するタイプのログを除くすべてのタイプのログを保存します。
  - **NFS** パーティション – このオプションは、VMware ESXi サーバー上で稼働している Panorama に対してのみ使用できます。NFS パーティションは、システム ディスクに存在するタイプのログを除くすべてのタイプのログを保存します。
- **M-600**、**M-500** または **M-200** アプライアンス – レポートのストレージ容量は、Panorama 6.1以降のリリースでは500MB、それ以前のリリースでは200MBです。M-Series アプライアンスは、内部 SSD を使用して、Panorama とログ コレクタが生成した設定ログやシステム ログと、ファイアウォールから収集された App Stats を保存します。Panoramaはその他のすべてのログ タイプをRAIDが有効なディスクに保存します。RAIDディスクは、PanoramaモードのM-Seriesアプライアンスのローカルのものか、専用のログコレクタ内にあります（ログコレクタ モードのM-Seriesアプライアンス）。コレクタ グループの設定を行うときは、RAID ディスクのログ ストレージの割り当てを編集します。

© 2019 Palo Alto Networks, Inc.

ログ ストレージのオプションと容量の詳細は、Panorama モデルを参照してください。仮想ロギング ディスクまたは *NFS* ストレージを追加することで Panorama バーチャル アプライアンスでログ ストレージ容量を拡張することができます。*RAID* ドライブを追加、または *1TB* ドライブから *2TB* ドライブにアップグレードすることにより、M-Series アプライアンスのストレージの拡張を行うことができます。

ログおよびレポートの有効期間

Panorama管理サーバーおよびログコレクタがファイアウォールから収集するログの時間、およびPanoramaとログコレクタがローカルに生成するログおよびレポートの時間に基づいて自動検知を設定することができます。これは、モニタリングされた情報を定期的に削除したい、あるいは削除しなければならないような環境で役立ちます。例えば、法的な理由からお客様の組織では一定の期間後にユーザー情報を削除する必要があるかもしれません。次の項目に対して個別の有効期間を設定することができます。

- レポート — Panorama は、新しいレポートを生成するのと同時に、期限切れのレポートを削除します（「Panorama レポートのランタイムの設定」を参照）。
- 各ログ タイプ — Panorama はログを受信するとそれに対して評価を行い、設定済みの有効期間が過ぎたログは消去します。
- *Panorama*は高可用性（*HA*）ペア間で有効期間を同期します。アクティブ *HA* ピアのみがログを生成するため、パッシブ ピアでは、フェイルオーバーが発生してログの生成を開始しない限り、削除するログあるいはレポートはありません。

  有効期間を設定していない場合でも、ログ割り当てが最大サイズに達すると、*Panorama*は最も古いエントリから順に新しいログ エントリで上書きします。

ログおよびレポートのストレージ割り当ておよび有効期間を設定

STEP 1 | 次の項目に対してストレージ割り当ておよび有効期間を設定します。

- レガシー モードの Panorama バーチャル アプライアンスがファイアウォールから受信するすべてのタイプのログ。
- Panorama がファイアウォールから受信する App Stats ログ。
- Panorama およびログ コレクタがローカルで生成するシステムおよび設定ログ。

Panorama 管理サーバーはこれらのログをローカルで保存します。

ストレージ割り当てを現在のログ容量を下回る値に設定すると、変更をコミットした後に *Panorama* は新しい割り当てに合わせて古いログを削除します。

1. **[Panorama]** > [セットアップ] > [管理] の順に選択し、[ロギングおよびレポート設定] を編集します
2. **Log Storage**（ログ ストレージ）設定で、各ログ タイプのストレージの **Quota (%)**（割り当て（%））を入力します。

   パーセント値を変更するとページが更新されて、Panorama に割り当てられた合計ストレージに基づいて、対応する絶対値（割り当ての (GB)/(MB) 列）が表示されます。
3. 各ログ タイプの **Max Days**（最大日数）（有効期間）を入力します（範囲は 1 ~ 2,000）。

   デフォルトではこのフィールドは空白（ログは無期限）です。

割り当ておよび有効期間を工場出荷時設定にリセットする場合は、*Restore Defaults*（デフォルトを復元）します。

STEP 2 | Panorama が生成するレポートの有効期間を設定します。

© 2019 Palo Alto Networks, Inc.

1. **Log Export and Reporting**（ログのエクスポートとレポート）を選択して **Report Expiration Period**（レポートの有効期間）（日数）を入力します（範囲は 1 ~ 2,000）。

   デフォルトではこのフィールドは空白（レポートは無期限）です。
2. **OK** をクリックして変更内容を保存します。

STEP 3 | M-600、M-500、M-200 アプライアンス、または Panorama モードの Panorama バーチャル アプライアンスがファイアウォールから受信するすべてのタイプのログ（App Stats ログを除く）のストレージの割り当ておよび有効期間を設定します。

ローカルまたは専用ログ コレクタがこれらのログを保存します。

このストレージ割り当ては、個々のログ コレクタではなくコレクタ グループのレベルで設定します。

1. **Panorama** > **Collector Groups**（コレクタ グループ）の順に選択し、コレクタ グループを編集します。
2. **General**（全般）設定で、**Log Storage**（ログ ストレージ）の値をクリックします。

   ログ コレクタをコレクタ グループに割り当てていなければ、値は表示されません。ログ コレクタを割り当てた後でフィールドに「*0MB*」と表示される場合は、管理対象のコレクタを設定する際にディスク ペアを有効にして変更をコミットしていることを確認します（*Panorama* > *Managed Collectors*（管理対象コレクタ）> *Disks*（ディスク））。
3. ログ タイプごとにストレージ**Quota(%)**（割り当て（%）を入力します。

   パーセント値を変更するとページが更新されて、コレクタ グループに割り当てられた合計ストレージに基づいて、対応する絶対値（割り当ての (GB)/(MB) 列）が表示されます。
4. 各ログ タイプの **Max Days**（最大日数）（有効期間）を入力します（範囲は 1 ~ 2,000）。

   デフォルトではこのフィールドは空白（ログは無期限）です。

   割り当ておよび有効期間を工場出荷時設定にリセットする場合は、*Restore Defaults*（デフォルトを復元）します。
5. **OK** をクリックして変更内容を保存します。

STEP 4 | Panorama に対する変更をコミットして、変更をコレクタ グループにプッシュします。

1. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択し、Push Scope（プッシュ スコープ）で **Edit Selections**（選択内容の編集）を行います。
2. **Collector Groups**（コレクタ グループ）を選択し、変更したコレクタ グループを選択して、**OK** をクリックします。
3. 変更を **Commit and Push**（コミットしてプッシュ）します。

STEP 5 | Panorama によってストレージ割り当ての変更が適用されたことを確認します。

1. **Panorama** > **Setup** > **Management** (Panorama > セットアップ > 管理)を選択し、Logging and Reporting Settings (ログおよびレポート設定)にてPanorama管理サーバーが保存するログに対して**Log Storage** (ログ ストレージ)の値が正しく設定されていることを確認します。
2. **Panorama** > **Collector Groups** (Panorama > コレクタ グループ)を選択し、さらに変更したコレクタ グループを選択し、ログコレクタが保存するログに対して**General** (全般)タブの**Log Storage** (ログ ストレージ)の値が正しく設定されていることを確認します。

   また、ログコレクタの*CLI*にログインして操作コマンド***show log-diskquota-pct***を入力することでも、コレクタ グループのストレージ割り当てを確認することができます。

© 2019 Palo Alto Networks, Inc.

Panorama レポートのランタイムの設定

Panorama は、指定した時間に毎日レポートを生成します。Panorama は、新しいレポートを生成した後で有効期限が切れたレポートを削除します。

STEP 1 | **[Panorama]** > **[セットアップ]** > **[管理]** の順に選択し、[ロギングおよびレポート設定] を編集します

STEP 2 | **Log Export and Reporting**（ログのエクスポートとレポート）を選択して **Report Runtime**（レポートの実行時間）を 24 時間形式の時間に設定します（デフォルトは 02:00、範囲は 00:00（深夜）~ 23:00）。

STEP 3 | **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

© 2019 Palo Alto Networks, Inc.

Panorama のモニタリング

システムおよび設定ログ（タイプによるログのフィルタリング）を定期的に確認するか、SNMP マネージャーが Panorama の統計情報を定期的に収集（GET）するように設定するか、あるいは SNMP トラップやメール アラートを設定し、監視している指標の状態が変更された、あるいはしきい値に達した際に通知を受け取るよう Panorama で設定を行い、Panorama およびその管理対象のコレクタを監視します。電子メール アラートおよび SNMP トラップは、注意を必要とする重大なシステム イベントを即座に通知する場合に便利です。メール アラートあるいはSNMPトラップの設定についてはPanorama から外部の宛先へのログ転送を設定をご覧ください。

- Panorama のシステム ログと設定ログ
- SNMP を使用して Panorama およびログ コレクタの統計を監視

Panorama のシステム ログと設定ログ

システム イベントあるいは設定変更が発生した際に通知を送信するように Panorama を設定できます。Panorama では、デフォルトですべての設定変更が設定ログに記録されます。システム ログでは各イベントの重大度が示されるため、緊急度や影響度を判断しやすくなっています。「Panorama から外部の宛先へのログ転送を設定」を行うと、すべてのシステム ログと設定ログを転送したり、受信時刻や重大度レベル（システム ログのみ）などの属性に基づいてログを絞り込んだりすることができるようになります。以下の表にシステム ログの重大度レベルを要約して示します。

重大度	説明
重大	高可用性（HA）フェイルオーバーやリンク エラーのようなハードウェア障害など、迅速な対応が求められる障害。
High（高）	システムの動作に悪影響を与える深刻な問題（ログ コレクタの切断やコミット エラー）。
Medium（中）	アンチウイルス パッケージのアップグレードやコレクタ グループの設定のプッシュなどの中レベルの通知。
低	ユーザー パスワードの変更などそれほど重要ではない通知。
情報	ログイン/ログアウト、設定の変更、認証の成功および失敗の通知、コミットの成功、および他の重大度レベルでカバーされないその他のすべてのイベントなどの通知イベント。

Panorama はシステム ログと設定ログをローカルに保存します。正確な場所と保存容量は Panorama モデルによって異なります（「ログおよびレポートの保存」を参照）。容量の制限に達すると、Panorama は最も古いログを削除して、新しいログ用の領域を作成します。ローカル ストレージで許容されるよりも長い期間ログを保存する必要がある場合は、「Panorama から外部の宛先へのログ転送を設定」できます。

*Panorama*を使用してファイアウォールを監視する方法については「ネットワーク アクティビティのモニター」をご覧ください。

SNMP を使用して Panorama およびログ コレクタの統計を監視

SNMPマネージャがPanorama管理サーバーに情報をリクエストし、Panoramaが応答するよう設定できます。例えば、SNMPマネージャは高可用性（HA）モード、Panoramaの状態、Panoramaのバージョンをリ

© 2019 Palo Alto Networks, Inc.

クエストできます。Panorama 管理サーバーにローカル ログ コレクタがある場合、Panorama では、平均ログ/秒、保存期間、保持期間、ログのディスク使用量、各ファイアウォールから Panorama および外部サーバーへのログ転送の状態、ファイアウォールとログ コレクタの接続の状態などのロギング統計も提供されます。PanoramaはHAピア間でSNMP構成を同期しないため、SNMPリクエストおよび各ピアの応答を有効にする必要があります。

専用ログ コレクタを設定し、Panorama 管理サーバーと同じロギング統計の要求に応答することもできます。ログの保存容量を大きくする必要があるか検討する際にこの情報が役立ちます。

*SNMP*マネージャが（*SET* メッセージを使用した）*Panorama*あるいはログコレクタを制御するように設定することはできません。*SNMP*マネージャは統計収集のみを収集できます（*GET*メッセージを使用）。

*Panorama*が*SNMP*を実装する方法についての詳細は、SNMP サポートを参照してください。

STEP 1 | Panoramaおよびログコレクタから統計情報を取得するようにSNMPマネージャを設定

以下の手順では、SNMPマネージャで実行するタスクの概要を説明します。具体的な手順は、SNMP マネージャのドキュメントを参照してください。

1. SNMP マネージャを有効にして統計を解釈するには、サポートされたMIBをロードし、必要に応じてコンパイルします。
2. SNMP マネージャがモニターする Panorama アプライアンスごとに、その接続設定（IP アドレスとポート）および認証設定（SNMPv2c コミュニティ文字列または SNMPv3 ユーザー名およびパスワード）を定義します。すべての Panorama アプライアンスはポート 161 を使用します。

   SNMP マネージャでは、複数のPanorama管理サーバーおよびログコレクタに対して使用する接続設定と認証設定は同じでも違っていてもかまいません。設定は、Panorama で SNMP を設定するときに定義するものと一致する必要があります（SNMP マネージャからの統計要求に応答するようにPanorama 管理サーバーを設定するおよび専用ログ コレクタ（存在する場合）が SNMP リクエストに応答するように設定するを参照）。たとえば、SNMPv2c を使用する場合、Panorama設定時に定義するコミュニティ文字列が、SNMP マネージャでそのPanoramaに対して定義するコミュニティ文字列と一致する必要があります。
3. モニターする統計のオブジェクト識別子（OID）を判別します。例えばロギング率を監視するために、この統計情報がPAN-PRODUCT-MIB.myのOID 1.3.6.1.4.1.25461.2.3.30.1.1に対応するということがMIBブラウザに表示されます。詳細についてはSNMP マネージャを使用してMIB およびオブジェクトを探索をご覧ください。
4. SNMP マネージャを、目的の OID をモニターするように設定します。

STEP 2 | Panorama管理サーバーの管理（MGT）インターフェイスでSNMPトラフィックを有効化します。

1. **[Panorama]** > [セットアップ] > [管理] の順に選択し、[管理インターフェイス設定] を編集します。
2. Services（サービス）セクションで **SNMP** チェック ボックスをオンにして **OK** をクリックします。

STEP 3 | ログコレクタ モードのいずれかのM-Seriesアプライアンスの管理（MGT）インターフェイスでSNMPトラフィックを有効化します。

1. **Panorama** > **Managed Collectors**(Panorama > 管理対象コレクタ) の順に選択し、ログ コレクタを選択します。
2. **Management**（管理）タブを選択し、**SNMP**チェックボックスを選択して **OK** をクリックします。

STEP 4 | SNMP マネージャからの統計要求に応答するようにPanorama管理サーバーを設定します。

1. **Panorama** > **Setup** > **Operations** (Panorama > セットアップ > 操作)の順に選択し、Miscellaneous (その他)セクションで、**SNMP Setup** (SNMP のセットアップ)をクリックします。

© 2019 Palo Alto Networks, Inc.

2. SNMP の **Version**（バージョン）を選択し、認証値を以下のように設定します。バージョンの詳細については、SNMP サポートを参照してください。
   - **V2c**—SNMPマネージャおよびモニター対象デバイス(この場合はPanorama)のSNMPコミュニティを識別し、コミュニティメンバーを相互認証するためのパスワードとして機能する **SNMP Community String**（**SNMP**コミュニティ名）を入力します。

     デフォルトのコミュニティ名***public***は、広く公開されていて安全ではないので使用しないでください。
   - **V3** – 少なくとも 1 つの SNMP 表示グループと 1 つのユーザーを作成します。ユーザー アカウントと表示により、SNMP マネージャが統計を取得するときに、認証、プライバシー、およびアクセス制御を実現できます。

     Views（表示）– 各表示は、ペアになっている OID とビット単位のマスクです。OID で MIB を指定し、マスク（16 進数形式）で、その MIB 内（一致部分を含む）または MIB 外（一致部分を含まない）でアクセスできるオブジェクトを指定します。最初のリストで **Add**（追加）をクリックし、表示グループの **Name**（名前）を入力します。グループの各表示について、**Add**（追加）をクリックし、表示の **Name**（名前）、**OID**、一致の **Option**（オプション）（**include**（含む）たは **exclude**（除外））、および **Mask**（マスク）を設定します。

     Users [ユーザー]–2 つ目のリストで **Add** [追加]をクリックし、**Users** [ユーザー]列にユーザー名を入力し、ドロップダウンから View [表示]グループを選択し、SNMP マネージャへの認証に使用する認証パスワード（**Auth Password** [認証パスワード]）、SNMP マネージャへの SNMP メッセージの暗号化に使用する専用パスワード（**Priv Password** [専用パスワード]）を入力します。
3. **OK** をクリックして設定を保存します。

STEP 5 | 専用ログコレクタ（存在する場合）がSNMPリクエストに応答するように設定します。

各コレクタ グループについて：

1. **Panorama** > **Collector Groups**(Panorama > コレクタ グループ) の順に選択し、コレクタ グループを選択します。
2. **Monitor**（監視）タブを選択し、SNMP マネージャからの統計要求に応答するように Panorama 管理サーバーを設定すると同じ設定を行い、**OK** をクリックします。

STEP 6 | Panorama に変更をコミットし、その変更をコレクタ グループにプッシュします。

1. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択し、Push Scope（プッシュ スコープ）で **Edit Selections**（選択内容の編集）を行います。
2. **Collector Groups**（コレクタ グループ）を選択し、編集したコレクタ グループを選択して **OK** をクリックします。
3. 変更を **Commit and Push**（コミットしてプッシュ）します。

STEP 7 | SNMPマネージャ内のPanoramaおよびログコレクタの統計情報を監視します。

SNMP マネージャのドキュメントを参照してください。

© 2019 Palo Alto Networks, Inc.

Panorama の再起動またはシャットダウン

再起動オプションでは、Panorama のグレースフル リスタートが開始されます。シャットダウンでは、システムの停止後、電源がオフになります。Panorama を再起動するには、シャットダウンした後で、システムの電源コードを手動で取り外してから再度接続します。

STEP 1 | **[Panorama]** > [セットアップ] > [操作] の順に選択します。

STEP 2 | Device Operations（デバイスの操作）セクションで、**Reboot Panorama**（**Panorama** の再起動）または **Shutdown Panorama**（**Panorama** のシャットダウン）を選択します。

© 2019 Palo Alto Networks, Inc.

Panorama のパスワード プロファイルおよび複雑性の設定

ローカル管理者アカウントを保護するために、管理者がパスワードを変更したり、新規作成したりするときに適用されるパスワードの複雑性の要件を定義できます。個々のアカウントに適用可能なパスワード プロファイルとは異なり、パスワードの複雑性ルールはファイアウォール全体に影響し、すべてのパスワードに適用されます。

定期的なパスワードの更新を適用するには、パスワードの有効期間を定義するパスワード プロファイルを作成します。

STEP 1 | パスワード複雑性設定を設定します。

1. **[Panorama]** > [セットアップ] > [管理] の順に選択し、[パスワード複雑性設定] セクションを編集します。
2. **Enabled**（有効）を選択します。
3. **Password Format Requirements**（パスワード フォーマットの要件）を定義します。パスワードに含める必要のある大文字、小文字、数字、特殊文字の要件を適用できます。
4. アカウント ユーザー名がパスワードで使用されないようにするには（またはその逆）、**Block Username Inclusion (including reversed)**（ユーザー名を含むパスワードを禁止（逆順を含む））を選択します。
5. パスワードの **Functionality Requirements**（機能要件）を定義します。

   管理者のパスワード プロファイルを設定している場合、パスワード プロファイルで定義された値は、このセクションで定義された値よりも優先されます。

STEP 2 | パスワード プロファイルを作成します。

複数のパスワード プロファイルを作成し、必要に応じて管理者アカウントに適用してセキュリティを確保できます。

1. **[Panorama]** > [パスワード プロファイル] の順に選択し、 [追加] をクリックします。
2. パスワード プロファイルの **Name**（名前）を入力し、以下を定義します。
   1. **Required Password Change Period**（パスワード有効期限日数） – パスワードを変更する必要のある頻度（日数）。
   2. **Expiration Warning Period**（失効の警告期間） – 管理者がパスワードのリマインダーを受け取るまでの有効期限日数。
   3. **Post Expiration Grace Period**（失効後の猶予期間） – パスワードの失効後に管理者がシステムにログインできる日数。
   4. **Post Expiration Admin Login Count**（失効後の管理者ログイン回数） – パスワードの失効後に管理者がシステムにログインできる回数。

Panorama プラグイン

Panorama の拡張可能なプラグイン アーキテクチャにより、VMware NSX などのサードパーティ統合プラグインや、GlobalProtect クラウド サービスなどのその他の Palo Alto Networks 製品をサポートすることができます。このモジュラ アーキテクチャにより、新しい PAN-OS バージョンを待たずに新機能を利用できます。

Panorama から VM Series プラグインを構成することもできます。VM-Series プラグインは、Google Cloud Platform (GCP)、Azure、AWS などのパブリック クラウド環境、および KVM、ESXi などのプライベート クラウド ハイパーバイザとの統合を可能にする単一のプラグインです。VM-Series プラグインを使用すると、パブリック クラウドにデプロイされた VM-Series ファイアウォールからメトリックを公開することができます。Panorama を使用して、パブリック クラウドの VM-Series プラグイン設定を構成し、構成を管理対象のファイアウォールにプッシュすることができます。

> Panorama プラグインについて
> VM-Series プラグインおよび Panorama プラグイン

Panorama プラグインについて

Panorama は、拡張可能なプラグイン アーキテクチャをサポートしており、次の機能を統合・構成できます：

- **AWS**—AWS プラグインにより、AWS 上の EC2 ワークロードを監視できるようになります。このプラグインにより、（PAN-OS 8.1.3 以降のリリースが稼働する）Parnorama と AWS VPC の間の通信が可能となり、Panorama は、事前定義済みの 属性のセット（あるいはメタデータ要素のセット）を EC2 インスタンスのタグとして収集し、その情報を Palo Alto Networks のファイアウォールに登録することができます。ダイナミック アドレス グループ内でこれらのタグを参照してセキュリティポリシー ルール内の項目にマッチさせる際、VPC 内にデプロイしたすべてのアセットに対して一貫した形でポリシーを適用できます。
- **Azure**—Azure プラグインにより、Azure パブリック クラウド上のVirtual Machine (仮想マシン - VM) の監視が可能です。このプラグインにより、（PAN-OS 8.1.3 以降のリリースが稼働する）Parnorama と Azure サブスクリプション の間の通信が可能となり、Panorama は、事前定義済みの 属性のセット（あるいはメタデータ要素のセット）を Azure 仮想マシンのタグとして収集し、その情報を Palo Alto Networks のファイアウォールに登録することができます。これらのタグをダイナミック アドレス グループ内で参照し、セキュリティポリシー ルールにマッチさせる際、サブスクリプションの VNet 内にデプロイしたアセット全体に一貫したポリシーを適用できます。
- **Cisco ACI** — Cisco ACI プラグインを使用すると、Cisco ACI ファブリックでエンドポイントを監視することができます。このプラグインにより、（PAN-OS 8.1.3 以降のリリースが稼働する）Parnorama と Cisco APIC の間の通信が可能となり、Panorama はエンドポイントグループのタグとしてエンドポイント情報を収集し、その情報を Palo Alto Networks ファイアウォールに登録することができます。ダイナミック アドレス グループ内でこれらのタグを参照してセキュリティポリシー ルールでそれらとマッチさせる際、Cisco ACI ファブリック内にデプロイしたすべてのアセットに対して一貫した形でポリシーを適用することができます。
- **Cisco TrustSec** — Cisco TrustSec プラグインを使用すると、Cisco TrustSec 環境でエンドポイントを監視することができます。このプラグインにより、Panorama と Cisco pxGrid サーバ間の通信が可能となり、Panorama がエンドポイントのタグとしてエンドポイント情報を収集し、その情報を Palo Alto Networks ファイアウォールに登録することができます。ダイナミック アドレス グループ内でエンドポイントのタグを参照し、セキュリティポリシー ルールと照合する際、Cisco TrustSec の環境内で展開したアセットすべてに対して一貫した方法でポリシーを適用することができます。
- **Cloud Services** — Cloud Services プラグインにより、Cortex Data Lake および Prisma Access を使用できます。Cortex Data Lake は運用ロギングの課題を解決し、Prisma Access クラウドサービスによるセキュリティ基盤は、リモートネットワークロケーションやモバイルワーカーにまで拡大します。
- エンタープライズ データ損失防止 **(DLP)**— エンタープライズ データ損失防止（DLP）は、機密情報を不正なアクセス、誤用、入手、または共有から保護するための、一連のツールとプロセスです。エンタープライズ DLP はクラウドサービスを介して有効になっています。機密データを正確に識別、保護して、インシデントを防止するためにコンテンツを検査して、正しいコンテキスト内のデータを分析します。エンタープライズ DLP は、PAN-OS 10.0.2 以降のリリースを実行している、Panorama およびマネージド ファイアウォールでサポートされています。
- **GCP**-Google Kubernetes Engine (GKE) クラスタで Kubernetes サービスを保護することができます。Google Cloud Platform (GCP) の Panorama プラグインを設定して GKE クラスタに接続し、インターネットに公開されているサービスについて学習します。
- **Interconnect**—Interconnect プラグインを使用すると、大規模なファイアウォールのデプロイを管理ができます。（PAN-OS 8.1.3 以降のリリースが稼働する Panorama 上の）水平型スケールアウトのアーキテクチャで 2 階層の Panorama デプロイメントをセットアップする際は、この Interconnect プラグインを使用します。Interconnect プラグインの使用により、最大 64 の Panorama ノードあるいは 32 の Panorama HA ペアを備える Panorama Controller をデプロイし、多数のファイアウォールを集中管理が可能です。
- **Nutanix**—Nutanix 用の Panorama プラグインを使用すると、Nutanix 環境での VM モニタリングが可能です。Nutanix Prism Central内の仮想マシンのインベントリを追跡でき、Nutanix 環境内を変更に自動

© 2019 Palo Alto Networks, Inc.

的に適応するセキュリティ ポリシーを一貫して適用することができます。仮想マシンをプロビジョニング、プロビジョニング解除、または移動するので、このソリューションでは、IP アドレスと関連する属性のセット（またはメタデータ要素）をタグとして収集できます。次に、タグを使用してDynamic Address Group (ダイナミック アドレス グループ)を定義し、セキュリティ ポリシーで使用することができます。Nutanix 対応 Panorama プラグインは、Panorama 9.0.4 以降が必要です。

- **SD-WAN**—Software-Defined Wide Area Network（SD-WAN）プラグインを使用すると、複数のインターネットサービスおよびプライベートサービスを使用して、インテリジェントおよび動的なWANを構築でき、コストの削減およびアプリケーションの品質と使いやすさの最大化に役立ちます。ルーター、ファイアウォール、WAN パスコントローラー、WAN 最適化装置などのコンポートネントを使用した高コストで時間のかかる MPLS を採用して WAN をインターネットに接続する代わりに、Palo Alto Networks ファイアウォールで SD-WAN を採用することにより、より低コストのインターネットアクセスが実現でき、さらに機能統合によるデバイス数の削減が可能になります。
- **VMware NSX**—VMware NSX プラグインにより、VMware NSX 上の VM-Series ファイアウォール と VMware NSX Manager 間の統合が実現します。この統合により、VM-Series ファイアウォールをサービスとして ESXi サーバーのクラスタにデプロイすることができます。
- **VMware vCenter**—VMware vCenter の Panorama プラグインを使用すると、 vCenter 環境で仮想マシンを監視できます。プラグインは、vCenter 環境で仮想マシンの IP アドレスを取得し、動的アドレスグループを使用してポリシーを構築するために使用できるタグに変換します。
- ゼロタッチプロビジョニング—ゼロタッチプロビジョニング (ZTP)は、Panorama への新しいファイアウォールのオンボーディングを簡素化および自動化するように設計されています。ZTP は、ネットワーク管理者が管理対象ファイアウォールをブランチに直接出荷し、ファイアウォールを自動的に Panorama に追加できるようにすることで、ファイアウォールの初期導入プロセスを合理化し、新規ファイアウォールを導入する際に時間とリソースを節約します。ZTP は、PAN-OS 9.1.3 以降のリリースでサポートされています。
- **IPS** シグネチャ コンバータ—Panorama 用 IPS シグネチャ コンバータ プラグインは、サードパーティの侵入防御システム (Snort および Suricata) からカスタム設定の Palo Alto Networks 脅威シグネチャにルールを変換するための自動化されたソリューションを提供します。次に、指定したデバイスグループに属するファイアウォールにこれらのシグネチャを登録し、それらを使用して、脆弱性防御およびアンチスパイウェア セキュリティ プロファイルのポリシーを適用できます。

単一の Panorama インスタンスで、複数のプラグインをインストールし、複数のソースから IP アドレスの更新を取得できます。これにより、一貫性のあるセキュリティ ポリシーの作成および適用をして、複数のクラウド環境全体でアプリケーションとワークロードを保護することができます。取得された IP アドレスは、Dynamic Address Group (ダイナミック アドレス グループ) を通じてセキュリティ ポリシーで使用されます。ワークロードが環境に追加または環境から削除されると、Panorama はその変更を登録し、更新をファイアウォールにプッシュします。Panorama 上で複数のプラグインをデプロイする場合は、更新がファイアウォールに正しく渡されるように、デバイス グループ階層を慎重に計画する必要があります。

各プラグインのバージョンおよび互換性に関する詳細については、Palo Alto Networks の互換性一覧を参照してください。

Panorama プラグインをインストール

Panorama に 1以上の使用可能なプラグインをインストールし、GlobalProtect クラウドサービスおよび Cortex Data Lake、VMware NSX、 AWS や Azure パブリック クラウド上の仮想マシンの監視を統合できるようにします。

クラウド サービス プラグインの場合は、カスタマー サポート ポータルで有効な認証コードを有効にし、ログを送信する地域（アメリカ大陸またはヨーロッパ）を選択する必要があります。

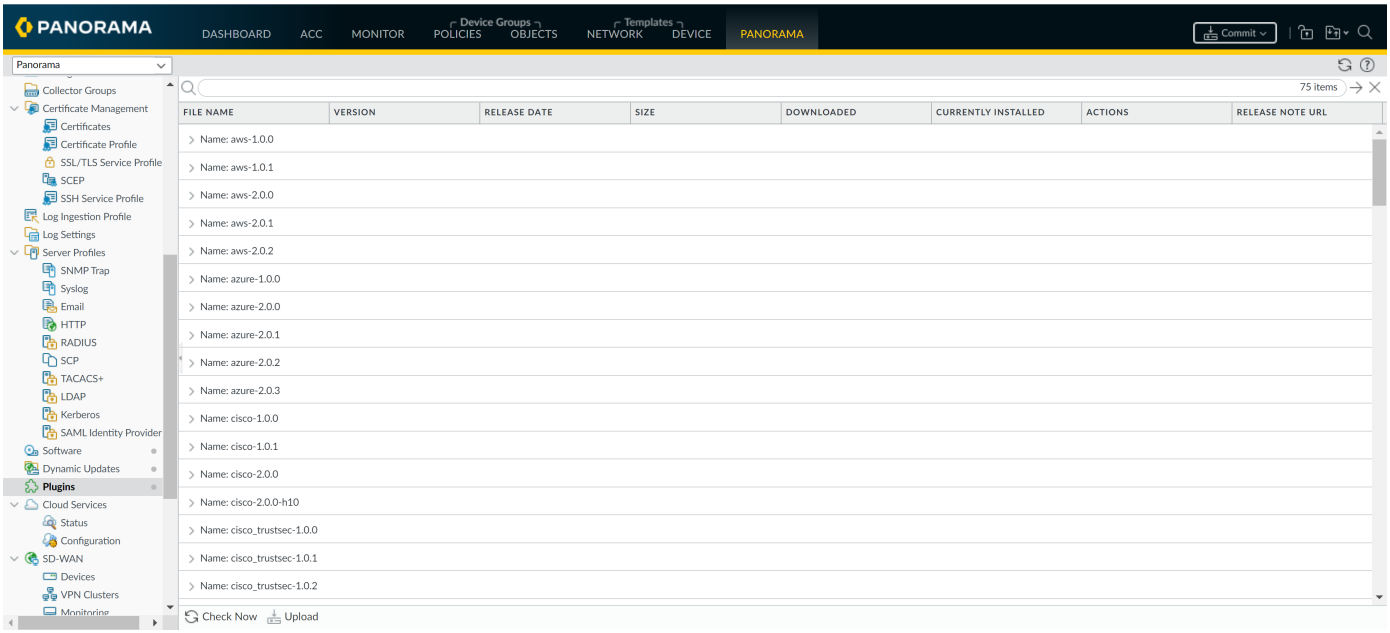


現在インストールされているプラグインのバージョンがあり、プラグインの新しいバージョンを*Install*（インストール）すると、現在インストールされているバージョンが置き換えられます。

STEP 1 | プラグインをダウンロードします。

© 2019 Palo Alto Networks, Inc.

1. **Panorama** > **Plugins**（プラグイン）を選択します。



2. **Check Now**（今すぐチェック）を選択して、利用可能な更新のリストを取得します。
3. Action（アクション）列にある **Download**（ダウンロード）をクリックしてインストールを実行します。

   各 Panorama プラグインの最低サポート PAN-OS バージョンについては、Compatability Matrix (互換性一覧) を参照してください。

STEP 2 | プラグインをインストールします。

プラグインのバージョンを選択し、Action（アクション）列にある**Install**（インストール）をクリックしてプラグインをインストールします。インストールが完了すると Panorama からメッセージが表示されます。詳細は、 VMware NSX プラグイン または クラウド サービス プラグインのインストールを参照します。

Panorama HA ペアでプラグインを初めてインストールする場合は、アクティブ ピアより前にパッシブ ピアにプラグインをインストールします。プラグインをパッシブ ピアにインストール中に、パッシブ ピアはノンファンクショナル状態に移行します。次に、アクティブなピアにプラグインを正常にインストールすると、パッシブ ピアは機能状態に戻ります。

© 2019 Palo Alto Networks, Inc.

VM-Series プラグインおよび Panorama プラグイン

VM-Series プラグインと Panorama の各種プラグインの違いは何でしょうか？

VM-Series プラグインは、VM-Series ファイアウォール用のプラグインで、Google Cloud Platform (GCP)、Azure、AWS などのパブリック クラウド環境、および KVM、ESXi などのプライベート クラウド ハイパーバイザとの統合を可能にする単一のプラグインです。ファイアウォールをデプロイする場合、ファイアウォールがデプロイされる仮想環境を内蔵のプラグインが自動的に検出して、そのクラウド環境との対話操作の管理を可能にする、プラグイン コンポーネントをロードします。たとえば、GCP に VM-Series をデプロイする場合、VM-Series ファイアウォールは GCP との統合を可能にするプラグイン コンポーネントをロードします。VM-Series プラグインを使って GCP 上の VM-Series ファイアウォールを設定して、メトリックを Google Stackdriver Monitoring に公開することができます。同様に、Azure 上の VM-Series ファイアウォールの VM-Series プラグインにより、ファイアウォールを設定してメトリックを Azure Application Insights に公開する、またはファイアウォールが HA ペアとして動作するために必要な詳細情報を設定することができます。VM-Series プラグインは VM-Series ファイアウォールにプレインストールされており、アップグレード/ダウングレードすることはできますが、削除することはできません。Panorama で VM-Series プラグインを利用できますが、プレインストールされてはいません。Panoramaを使ってファイアウォールの統合を管理する場合は、Panorama に VM-Series プラグインをインストールして、ファイアウォール上の VM-Series プラグインとの通信を確立します。

Panorama プラグインはハードウェア ベースの ファイアウォールと VM-Series ファイアウォールの両方に対応しています。Panorama プラグインはオプションで、Panorama上でプラグインを追加、削除、再インストール、またはアップグレードすることができます。Panorama プラグインは内蔵されていないため、必要な環境を管理するために通信を確立するには、プラグインをインストールする必要があります。たとえば、Panorama で Cloud Services プラグインを使用して、Panorama/ファイアウォールと Cortex Data Lake 間のセットアップを有効にします。GCP plugin on Panorama により、Panorama と GCP デプロイ環境間の通信が可能になり、Google Kubernetes Engine (GKE) クラスタにデプロイされているサービスとやり取りされるトラフィックを保護することができます。

Panorama への VM-Series プラグインのインストール

VM Series ファイアウォールにデプロイされたクラウド統合を表示および構成するには、Panorama と VM Series ファイアウォールの両方に VM Series プラグインをインストールする必要があります。プラグインはファイアウォールに自動的にインストールされますが、設定を デバイス グループ にプッシュするには、Panorama にプラグインを手動でインストールする必要があります。

VM Series プラグインはすべてのクラウドをサポートしているため、*VM Series* ファイアウォールにアップグレードが適用されない場合があります。プラグインをアップグレードする前に、リリースノートを参照してください。現在利用しているクラウドに関連する変更がある場合にのみ、プラグインを更新します。

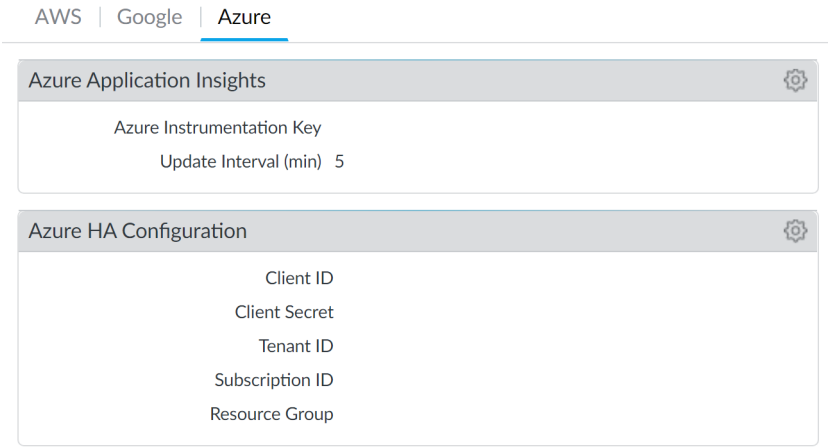
STEP 1 | VM-Series プラグインをダウンロードします。

1. **Panorama** > **Plugins** (プラグイン) を選択し、**Check Now** (今すぐチェック) を使用して新しいプラグインパッケージを検索します。VM Series のプラグイン名は `vm_series` です。
2. プラグインのリリースノートを参照して、どのバージョンが有用なアップグレードを提供しているかを判断します。
3. プラグインのバージョンを選択し、Action (アクション) 列にある **Download** (ダウンロード) を選択します。

STEP 2 | VM-Series プラグインをインストールします。

© 2019 Palo Alto Networks, Inc.

1. Action (アクション) 列の **Install (インストール)** をクリックします。インストールが完了すると Panorama から警告が表示されます。
2. プラグインを表示するには、**Device** > **VM-Series (デバイス VM-Series)** を選択します。
   - ファイアウォールがプライベートクラウドにインストールされており、ハイパーバイザまたはサービスに統合がない場合、VM Series という名前のタブに `VM Series plugin infrastructure support is installed to allow the firewall's functionality to be enhanced in response to new features launched by hypervisor, or to meet new security needs` というデフォルトメッセージが表示されます。
   - ファイアウォールがパブリック クラウドにデプロイされている場合、サポートされているすべてのクラウドのタブが Panorama に表示されます。



STEP 3 | (任意) 設定を保存し、管理対象のファイアウォールにプッシュします。

STEP 4 | (任意) VM-Series ファイアウォールで、**Device (デバイス)** > **VM-Series** を選択します。プラットフォームの統合を構成済みの場合は、ファイアウォールがデプロイされているクラウドのタブが 1 つ表示されます。統合を設定していない場合、VMSeries プラグイン インフラストラクチャに関するデフォルトメッセージが表示されます。

トラブルシューティング

以下のトピックでは、Panorama™ 管理サーバーおよび専用ログ コレクタの問題を解決します。

- Panorama システムの問題のトラブルシューティング
- ログ ストレージと接続に関する問題のトラブルシューティング
- RMA ファイアウォールの交換
- コミット エラーのトラブルシューティング
- 登録あるいはシリアル番号のエラーのトラブルシューティング
- レポート エラーのトラブルシューティング
- デバイス管理ライセンスエラーのトラブルシューティング
- 自動復帰ファイアウォール設定のトラブルシューティング
- Panorama HA ピアがダウンした際の完全なコンテンツ更新
- タスクの成否の確認
- 管理対象デバイスのポリシーマッチと接続のテスト
- Panorama 10.0 からのダウングレード

Panorama システムの問題のトラブルシューティング

- Panorama の診断ファイルの生成
- Panorama がサスペンド状態になっている場合の診断
- ファイル システム整合性チェックの監視
- ソフトウェア更新とコンテンツ更新が格納される Panorama ストレージの管理
- Panorama HA デプロイ環境でのスプリット ブレインからの回復

Panorama の診断ファイルの生成

診断ファイルは、システム アクティビティのモニタリングや、Panorama の問題の潜在的な原因を識別するのに役立ちます。Palo Alto Networks テクニカル サポートによる問題のトラブルシューティングを支援するために、サポート担当者からテクニカル サポート ファイルを求められる場合があります。以下の手順では、テクニカル サポート ファイルをダウンロードし、サポート ケースにアップロードする方法について説明します。

STEP 1 | **Panorama** > **Support** (Panorama > サポート)を選択し、**Generate Tech Support File** (テクニカル サポート ファイルの生成)をクリックします。

STEP 2 | ファイルをダウンロードしてコンピューターに保存します。

STEP 3 | ファイルをPalo Alto Networks カスタマーサポート ウェブサイトの事案にアップロードします。

Panorama がサスペンド状態になっている場合の診断

Panorama がサスペンド状態になっている場合は、以下の状態を確認します。

- シリアル番号 — 各 Panorama バーチャル アプライアンスのシリアル番号が一意であることを確認します。同じシリアル番号を使用して Panorama の複数のインスタンスを作成すると、同じシリアル番号を使用するすべてのインスタンスがサスペンド状態になります。
- モード — Panorama バーチャル アプライアンスを高可用性（HA）構成でデプロイする場合は、両方の HA ピアが同じモード（Panorama モードかレガシー モード）になっていることを確認します。
- **HA** 優先度 — 1 つのピアの HA 優先度がプライマリとして設定され、他がセカンダリとして設定されていることを確認します。両方のピアで同じ優先度が設定されていると、シリアル番号が高い Panorama ピアがサスペンド状態になります。
- **Panorama** ソフトウェア バージョン — 両方の Panorama HA ピアが同じ Panorama ソフトウェア バージョン（メジャーおよびマイナーのバージョン番号）で実行されていることを確認します。

ファイル システム整合性チェックの監視

Panorama システム ファイルの破損を回避するため、Panorama では定期的にファイル システムの整合性チェック (FSCK) が実行されます。このチェックは、再起動を 8 回行った後、または最後の FSCK が実行されてから 90 日経過した後の再起動で実行されます。Panorama で FSCK が実行されていると、FSCK が進行中であることを示す警告が Web インターフェイスおよびSSH（Secure Shell）ログイン画面に表示されます。この処理が完了するまで、ログインできません。この処理が完了する時間は、ストレージ システムのサイズによって異なり、Panorama にログインできるようになるまで数時間かかることもあります。

Panorama またはマネージドファイアウォールに PAN-OS ソフトウェア更新プログラムを正常にダウンロードしてインストールすると、ソフトウェア インストールプロセスの一部として Panorama または物理

© 2019 Palo Alto Networks, Inc.

ファイアウォールが再起動した後にソフトウェア更新プログラムが検証され、PAN-OS ソフトウェアの整合性が保証されます。これにより、現在実行中の新しいソフトウェア アップデートが正常に認識され、リモートまたは物理的なエクスプロイトによって Panorama またはマネージドファイアウォールが危険にさらされることがなくなります。

FSCK の進捗状況を表示するには、Panorama へのコンソール アクセスをセットアップします。

ソフトウェア更新とコンテンツ更新が格納される Panorama ストレージの管理

Panorama のコンテンツ更新とソフトウェア更新のインストール、およびPanorama を使用したファイアウォール、ログ コレクタ、および WildFire アプライアンスへの更新のデプロイを行うことができます。更新を保存するPanoramaの空き容量を設定することはできません。割り当て済みの領域の使用容量が 90% に達すると、新しいダウンロードあるいはアップロードを格納するための空き領域を確保する（格納されている更新を削除する）ように指示する警告が表示されます。更新の最大数は、Panorama に格納されるすべての更新に適用されるグローバル設定です。この設定を構成するには、CLI にアクセスする必要があります。デフォルトの値は、各タイプにつき更新2件です。

- 各タイプの更新の最大数を変更します。

  Panorama CLIにアクセスし、次のコマンド（*<number>*は2～64が可能）を入力します。

```
> set max-num-images count <number>
```

- Panoramaが現在保存している更新の数を確認します。

  入力コマンド：

```
> show max-num-images
```

- Webインターフェイスを使用して更新を削除し、Panoramaの空き容量を増やします。
  1. 削除したい更新のタイプを選択します。
     - ファイアウォールあるいはログコレクタの更新：

       PAN-OS/Panorama ソフトウェア イメージ — **Panorama** > **Device Deployment**（デバイスのデプロイ）> **Software**（ソフトウェア）を選択します。

       GlobalProtect™ エージェント/アプリ ソフトウェア更新 — **Panorama** > **Device Deployment**（デバイスのデプロイ）> **GlobalProtect Client**（**GlobalProtect** クライアント）を選択します。

       コンテンツ更新 — **Panorama** > **Device Deployment**（デバイスのデプロイ）> **Dynamic Updates**（動的更新）を選択します。
     - Panoramaソフトウェアイメージ—**Panorama** > **Software** (Panorama > ソフトウェア)を選択します。
     - Panoramaコンテンツ更新—**Panorama** > **Dynamic Updates** (Panorama > 動的更新)を選択します。
  2. かなり右の方にある列で、目的のイメージあるいは更新の**X**アイコンをクリックします。

- CLIを使用して更新を削除し、Panoramaの空き容量を増やします。

  バージョンに基づいてソフトウェア イメージを削除する場合：

```
> delete software version <version_number>
```


© 2019 Palo Alto Networks, Inc.

コンテンツ更新を削除する場合：

```
> delete content update <filename>
```

Panorama HA デプロイ環境でのスプリット ブレインからの回復

Panorama が高可用性（HA）構成でデプロイされている場合、管理対象ファイアウォールはアクティブとパッシブの両方の Panorama HA ピアに接続されます。アクティブとパッシブの Panorama 間の接続に障害が発生すると、パッシブ Panorama は、アクティブ を引き継ぐ前に、アクティブ とパッシブ の両方に接続されているファイアウォールが存在しないかチェックします。両方に接続されているファイアウォールが 1 台でも存在すると、フェイルオーバー処理は実行されません。

あまり発生することはありませんが、アクティブに接続されているファイアウォールのセットと、パッシブに接続されているファイアウォールのセットがあり、両方のピアに接続されているファイアウォールはない場合にフェイルオーバー処理が実行されることがあります。これがスプリット ブレインと呼ばれる現象です。スプリット ブレインが発生すると、以下の状態になります。

- どちらの Panorama も、相手の状態または HAの役割を認識しない。
- 両方の Panorama がアクティブになり、それぞれ異なるファイアウォールのセットを管理している。

スプリット ブレインを解決するには、ネットワークの問題を調査・解決し、Panorama HA ピア間の接続を復元します。

ただし、ピア間の接続を復元せずにファイアウォールの設定を変更する必要がある場合、いくつかの方法があります。

- 両方の Panorama に同じ設定変更を手動で追加します。これにより、リンクが再確立されたときに設定が同期されます。
- 1 つの Panorama の場所でのみ設定を追加/変更する必要がある場合、Panorama 間のリンクが再確立されたときに設定を変更して同期します（変更を行ったピアから同期を開始してください）。ピアを同期するには、**Dashboard**（ダッシュボード）タブを選択し、High Availability（高可用性）ウィジェット内の**Sync to peer**（ピアと同期）リンクをクリックします。
- 各場所の接続されたファイアウォールでのみ設定を追加/変更する必要がある場合、各 Panorama で別々に設定を変更できます。ピアは切断されているため、複製は行われず、各ピアは、それぞれ個別のの（同期していない）設定ファイルを持つことになります。したがって、接続の復元時に各ピアの設定の変更が失われないようにするために、設定が自動的に再同期されないようにします。この問題を解決するには、各 Panorama から設定をエクスポートして、外部の比較/マージ ツールを使用して、手動で変更をマージします。変更が統合されたら、統合された設定ファイルをプライマリ Panorama にインポートし、インポートされた設定ファイルをピアと同期できます。

© 2019 Palo Alto Networks, Inc.

ログ ストレージと接続に関する問題のトラブルシューティング

ログの移行は *M-Series* アプライアンスのみがサポートされます。*Panorama* バーチャル アプライアンスに移行するには、Panorama バーチャル アプライアンスから異なるハイパーバイザへの移行 を参照してください。

- Panorama　ポートの使用状況の確認
- コレクタ グループのログ保存エリアがゼロと表示される問題を解決する
- 故障した M-Series アプライアンスのディスクを交換
- ESXi サーバーの仮想ディスクを交換
- vCloud Air サーバーの仮想ディスクを交換
- ログ コレクタ モードでログを新しい M-Series アプライアンスに移行
- Panorama モードでログを新しい M-Series アプライアンスに移行
- 高可用性の Panorama モードで新しい M-Series アプライアンス モデルにログを移行
- 高可用性の Panorama モードで同じ M-Series アプライアンス モデルにログを移行
- 非 HA の Panorama で障害/RMA が発生した後のログ コレクタの移行
- M-Series アプライアンスの RAID ペアのメタデータを再生成
- ログ クエリ ジョブの閲覧

Panorama　ポートの使用状況の確認

Panorama が管理対象ファイアウォール、ログ コレクタ、WildFire アプライアンスおよびアプライアンス クラスタ、およびその高可用性（HA）ピアと通信できるようにするには、以下の表を使用して、ネットワークで開く必要のあるポートを確認します。Panorama はポート通信に TCP プロトコルを使用します。

デフォルトでは、Panorama は管理（MGT）インターフェイスを使用して管理対象デバイス（ファイアウォール、ログ コレクタ、WildFire アプライアンスおよびアプライアンス クラスタ）の管理、ログの収集、コレクタ グループとの通信、ソフトウェアおよびコンテンツ更新のデバイスへのデプロイを行います。ただし任意で、Panorama 6.1 から 7.1 を実行している M-600、M-500 または M-200 アプライアンスの Eth1 または Eth2 インターフェイスにログ収集機能とコレクタ グループ通信機能を割り当てることができます。アプライアンスが Panorama 8.0 以降のリリースを実行している場合、M-600、M-500、または M-200 アプライアンスの Eth1、Eth2、Eth3、Eth4 または Eth5 インターフェースに任意の機能を割り当てることができます。以下の表に示したポートは、機能とその割り当て先インターフェイスに関係なく適用されます。たとえば、ログ収集機能を MGT に、コレクタ グループ通信を Eth2 に割り当てると、MGT は 3978 番ポートを、Eth2 は 28270 番ポートを使用します（Panorama バーチャル アプライアンスでは、以下のすべての機能について、MGT インターフェイスのみを使用できます）。

システムとの通信と通信方向の確立	Panorama 5.x で使用するポート	Panorama 6.x と 7.x で使用するポート	Panorama 8.x 以降で使用するポート	説明
Panorama 間（HA） 方向：各ピアから他のピアに接続が開始される	28	28	28	HA 接続および同期（暗号化が有効になっている場合） ログ配信用のコレクタ グループ内のログ コレクタ間の通信で使用します。

© 2019 Palo Alto Networks, Inc.

システムとの通信と通信方向の確立	Panorama 5.x で使用するポート	Panorama 6.x と 7.x で使用するポート	Panorama 8.x 以降で使用するポート	説明
Panorama 間（HA） 方向：各ピアから他のピアに接続が開始される	28769 および 28260（5.1） 28769 および 49160 (5.0)	28260 および 28769	28260 および 28769	HA 接続および同期（暗号化が有効になっていない場合）
Panorama と管理対象ファイアウォール 方向：ファイアウォールから開始される	3978	3978	3978	双方向接続で、ログはファイアウォールから Panorama に転送され、設定の変更は Panorama から管理対象ファイアウォールにプッシュされます。コンテキストの切り替えコマンドは、同じ接続を使用して送信されます。
Panorama とログ コレクタ 方向：ログ コレクタから開始	3978	3978	3978	管理およびログ収集/レポート。 Panorama モードの Panorama でのローカル ログ コレクタ間の通信、および分散ログ収集のデプロイにおけるログ コレクタとの通信に使用されます。
Panorama および管理対象デバイス（ファイアウォール、ログ コレクタ、WildFire アプライアンスおよびアプライアンス クラスタ） 方向： • PAN-OS 8.x 以降のリリースを実行している管理対象デバイスによって開始されます。 • PAN-OS 7.x 以前のリリースを実行しているデバイスの Panorama によって開始されます。	3978	3978	28443	PAN-OS 8.x 以降のリリースを実行しているデバイスは、ポート 28443 を使用してソフトウェアおよびコンテンツ更新ファイルを Panorama から取得します。 7.x 以前のリリースを実行しているデバイスは、更新ファイルを Panorama から取得しません。Panorama はポート 3978 を介して更新ファイルをデバイスにプッシュします。 WildFire アプライアンスおよびアプライアンス クラスタの Panorama 管理のサポートには、PAN-OS 8.0.1 以降が管理対象 WildFire アプライアンスにインストールされていることが必要です。WildFire アプライアンスおよびアプライアンス クラスタを管理するには、Panorama で 8.0.1 以降

© 2019 Palo Alto Networks, Inc.

システムとの通信と通信方向の確立	Panorama 5.x で使用するポート	Panorama 6.x と 7.x で使用するポート	Panorama 8.x 以降で使用するポート	説明
				を実行することをお勧めします。
ログ コレクタ間 方向：各ログ コレクタからコレクタ グループ内の他のログ コレクタに接続が開始される	49190	28270	28270	ログ コレクタ間でのブロックおよびすべてのバイナリ データの配信。
Panorama を Cortex Data Lake へ	NA	NA	444 バージョン *8.0.5* 以降。	Cortex Data Lake との保護された通信チャネルのセットアップ用。 管理対象ファイアウォールはポート 3978 を使用して Cortex Data Lake と通信します。

コレクタ グループのログ保存エリアがゼロと表示される問題を解決する

ログコレクタ内でディスク ペアがロギング可能になっていない場合、コレクタ グループのログ ストレージ容量が 0MB と表示されることがあります。ディスク ペアを有効にするには、コレクタ グループのログ コレクタごとに次の手順を実行します。

STEP 1 | RAID ディスク ペアを追加します。

1. **Panorama** > **Managed Collectors**（管理対象コレクタ）の順に選択し、コレクタ名をクリックします。
2. **Disks**（ディスク）を選択し、各 RAID ディスク ペアを **Add**（追加）して **OK** をクリックします。

STEP 2 | Panorama に対する変更をコミットして、変更をコレクタ グループにプッシュします。

1. **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択し、Push Scope（プッシュ スコープ）で **Edit Selections**（選択内容の編集）を行います。
2. **Collector Groups**（コレクタ グループ）を選択し、変更したコレクタ グループを選択して、**OK** をクリックします。
3. 変更を **Commit and Push**（コミットしてプッシュ）します。

STEP 3 | ログ コレクタとディスク ペアの状態を確認します。

1. **Panorama** > **Managed Collectors** (Panorama > 管理対象コレクタ)を選択し、各ログコレクタの構成がPanoramaと同期していることを確認します。

   Configuration Status（設定ステータス）列は **In Sync**（同期）、Run Time Status（ランタイム ステータス）列は **connected**（接続済み）という表示でなければなりません。
2. 各ログコレクタについて、最後の列にある**Statistics**（統計）をクリックし、ディスク ペアが**Enabled**（有効）かつ**Available**（利用可能）になっていることを確認します。

© 2019 Palo Alto Networks, Inc.

故障した M-Series アプライアンスのディスクを交換

M-Seriesアプライアンスのディスクに障害が発生した場合、障害が発生したハードディスクを交換し、RAID 1をリビルドする必要があります。詳細については、M-Series アプライアンスのハードウェア リファレンス ガイドを参照してください。

ESXi サーバーの仮想ディスクを交換

仮想ディスクを VMware ESXi サーバー上で動作する Panorama バーチャル アプライアンスに追加した後は、その仮想ディスクのサイズを変更することはできません。レガシー モードの Panorama バーチャル アプライアンスはログの保存場所を 1 つしか許容しないため、次のように仮想ディスクを交換してログの保存容量を変更する必要があります。Panorama モードでは、単に別のディスクを追加して（最大 12 個）、「Panorama バーチャル アプライアンスでのログ ストレージ容量の拡張」を行います。

レガシー モードの *Panorama* バーチャル アプライアンスでは、既存のディスクを交換すると、そのログは失われます。既存のログを保持するオプションについては、「レガシー モードの Panorama バーチャル アプライアンスにストレージを追加するときに既存のログを保持」を参照してください。

STEP 1 | 古い仮想ディスクを取り外します。

1. VMware vSphereクライアントにアクセスして**Virtual Machines**（仮想マシン）タブを選択します。
2. Panorama バーチャル アプライアンスを右クリックし、**Power**（電源）> **Power Off**（電源オフ）を選択します。
3. Panorama バーチャル アプライアンスを右クリックし、**Edit Settings**（設定変更）を選択します。
4. **Hardware**（ハードウェア）タブで仮想ディスクを選択し、**Remove**（除去）をクリックします。
5. Removal Options (除去オプション)のいずれかを選択して**OK**をクリックします。

STEP 2 | 新しい仮想ディスクを追加します。

1. ESXi サーバー上の Panorama に仮想ディスクを追加.

   PanoramaがESXi 5.5以降のバージョンで動作している場合、最大8TBの仮想ディスクをサポートしていること。Panoramaが古いESXiのバージョンで動作している場合、最大2TBの仮想ディスクをサポートしていること。
2. vSphereクライアントでPanorama バーチャル アプライアンスを右クリックし、**Power** > **Power On** (電源 > 電源オン)を選択します。

   再起動プロセスは数分かかる場合があり、`cache data unavailable`というメッセージが画面に表示されます。

STEP 3 | 変更したログの保存容量が正しいことを確認します。

1. Panorama バーチャル アプライアンスにログインします。
2. **Panorama** > **Setup** > **Management**(Panorama > セットアップ > 管理) の順に選択し、Logging and Reporting Settings (ロギングおよびレポート設定) セクションのLog Storage (ログ ストレージ)フィールドに、変更したログ ストレージ容量が正確に表示されることを確認します。

vCloud Air サーバーの仮想ディスクを交換

仮想ディスクを VMware vCloud Air 上で動作する Panorama バーチャル アプライアンスに追加した後は、その仮想ディスクのサイズを変更することはできません。レガシー モードの Panorama バーチャル アプライアンスはログの保存場所を 1 つしか許容しないため、次のように仮想ディスクを交換してログの保存容量を変更する必要があります。Panorama モードでは、単に「vCloud Air の Panorama に仮想ディスクを追加」を行うことができます（最大 12 個）。

© 2019 Palo Alto Networks, Inc.

レガシー モードの *Panorama* バーチャル アプライアンスでは、既存のディスクを交換すると、そのログは失われます。既存のログを保持するオプションについては、「レガシー モードの Panorama バーチャル アプライアンスにストレージを追加するときに既存のログを保持」を参照してください。

STEP 1 | 古い仮想ディスクを取り外します。

1. vCloud AirのWebコンソールにアクセスし、ご自身の **Virtual Private Cloud OnDemand**（仮想プライベート クラウド オンデマンド）領域を選択します。
2. **Virtual Machines**（仮想マシン）タブで Panorama バーチャル アプライアンスを選択します。
3. **Actions** > **Edit Resources** (アクション > リソース編集)を選択します。
4. 取り除く仮想ディスクの**x**をクリックします。

STEP 2 | 新しい仮想ディスクを追加します。

1. **Add another disk**（別のディスクを追加）します。
2. **Storage**（ストレージ）を8TBまでの間で設定し、ストレージ層を **Standard**（標準）あるいは **SSD-Accelerated**（**SSD**アクセラレート）に設定します。
3. 変更を**Save**（保存）します。

STEP 3 | Panorama を再起動します。

1. Panorama バーチャル アプライアンスにログインします。
2. **Panorama** > **Setup**（セットアップ） > **Operations**（操作）を開き、**Reboot Panorama**（**Panorama** の再起動）をクリックします。

STEP 4 | 変更したログの保存容量が正しいことを確認します。

1. 再起動後、Panorama バーチャル アプライアンスにログインします。
2. **Panorama** > **Setup** > **Management**(Panorama > セットアップ > 管理) の順に選択し、Logging and Reporting Settings (ロギングおよびレポート設定) セクションのLog Storage (ログ ストレージ)フィールドに、変更したログ ストレージ容量が正確に表示されることを確認します。

ログ コレクタ モードでログを新しい M-Series アプライアンスに移行

ログ コレクタ モードの M-600、M-500、M-200 または M-100 アプライアンス（専用ログ コレクタ）を交換する必要がある場合、RAID ディスクを新しい M-Series アプライアンスに移動することで、ファイアウォールから収集したログを移行することができます。これにより、M-Series アプライアンスのシステム エラーが発生した後でログを復元したり、ハードウェアアップグレードの一環としてログを移行したりすることができます。（M-100 アプライアンスから M-500 アプライアンスへ）

M-Series アプライアンスからロギング ディスクを削除して*M-600 Panorama* 管理サーバにログを読み込むというログ移行方法は、サポートされていません。*M-600* アプライアンスに移行するには、*M-Series* アプライアンスに保存されるログへのアクセスが必要な間は、M-600 アプライアンスをセットアップし、新しい M-600 アプライアンスへのログ転送を設定し、 管理対象ログ コレクタである M-Series アプライアンスを設定します。

STEP 1 | 専用ログ コレクタにする新しい M-Series アプライアンスの初期セットアップを実行します。

1. M-Series アプライアンスをラック マウントします。方法については、M-Series アプライアンスのハードウェア リファレンス ガイドを参照してください。
2. M-Series アプライアンスの初期設定を行います。

インターフェイスを設定する際は、管理（*MGT*）インターフェイスのみを設定します。（この作業の後半で）ログ コレクタ モードに切り替えると、他のインターフェ

© 2019 Palo Alto Networks, Inc.

イスの設定が削除されます。ログ コレクタが *MGT* 以外のインターフェイスを使用する場合は、ログ コレクタの設定時に追加します (ステップ 2 参照)。

3. Panorama を登録します。
4. 購入してPanorama サポート ライセンスをアクティベートするか、新しい M-Series アプライアンスが以前の M-Series アプライアンスと同じハードウェア モデルである場合のみ、以下のようにしてライセンスを移行します。新しい M-Series アプライアンスのモデルが以前の M-Series アプライアンスと異なる場合、新しいライセンスを購入する必要があります。
   1. Palo Alto Networks カスタマーサポート Web サイトにログインします。
   2. **Assets** (アセット) タブを選択し、**Spares** (スペア) リンクをクリックします。
   3. 新しい M-Series アプライアンスの Serial Number (シリアル番号) をクリックします。
   4. **Transfer Licenses** (ライセンスを移行) をクリックします。
   5. 以前の M-Series アプライアンスを**Select** (選択) し、**Submit** (送信) をクリックします。
5. ファイアウォール管理ライセンスのアクティベーションを行います。M-100 アプライアンスから M-500 アプライアンスへ移行する場合、移行ライセンスの認証コードを入力します。
6. Panorama のコンテンツ更新とソフトウェア更新のインストールを行います。ソフトウェア バージョンに関する重要な詳細情報は、「Panorama、ログ コレクタ、ファイアウォール、および WildFire のバージョン互換性」を参照してください。
7. Panorama モードからログ コレクタ モードに切り替えます。
   1. ログ コレクタの CLI にアクセスし、ログ コレクタ モードに切り替えます。

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

   2. **y**を入力して、モード変更を確定します。M-Series アプライアンスが再起動します。再起動処理によってターミナル エミュレーション ソフトウェアのセッションが終了した場合は、M-Series アプライアンスに再接続し、Panorama のログイン画面を表示します。

      *(**CMS Login**)* プロンプトが表示された場合は、ユーザー名やパスワードを入力せずに *Enter* を押します。
8. ログ コレクタの CLI を使用してログ コレクタおよび Panorama 管理サーバー間の接続を有効にします。<IPaddress1 はプライマリ PanoramaのMGTインターフェイスのものであり、<IPaddress2>はセカンダリ PanoramaのMGTインターフェイスのものです。

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

STEP 2 | Panorama 管理サーバー上で新しいログ コレクタを管理対象コレクタとして追加します。

シリアル番号が必要になるコマンドを使用するステップでは、必ずシリアル番号全体を入力してください。*Tab* キーを押してもシリアル番号の一部が補完されることはありません。

1. Panorama Web インターフェイスを使用するか、次の CLI コマンドを使用してログ コレクタを管理対象コレクタとして設定します。

```
> configure
# set log-collector <LC_serial_number> deviceconfig system ホスト名 <log-
collector-ホスト名>
# exit
```


© 2019 Palo Alto Networks, Inc.

以前のログ コレクタがログ収集およびコレクタ グループ通信に *MGT* 以外のインターフェイスを使用していた場合、新しいログ コレクタを管理対象コレクタとして設定する際にそのインターフェイスを定義する必要があります（*Panorama* > *Managed Collectors*（管理対象コレクタ）> *Interfaces*（インターフェイス））。

2. ログ コレクタが Panorama に接続されており、そのディスク ペアのステータスが present/available であることを確認します。

```
> show log-collector serial-number <log-collector_SN>
```

復元プロセスのこの段階では、ディスク ペアが無効として表示されます。

3. 変更を Panorama にコミットします。まだ変更をコレクタ グループにコミットしないでください。

```
> configure
# commit
# exit
```

STEP 3 | 以前のログ コレクタから RAID ディスクを取り外します。

1. システムがシャットダウンするまで Power（電源）ボタンを押し続け、以前のログ コレクタの電源を切ります。
2. ディスク ペアを取り除きます。詳細についてはM-Series アプライアンスのハードウェア リファレンス ガイドに記載されたディスクの交換方法を参照してください。

STEP 4 | 移行用のディスクを準備します。

各ディスク ペアのメタデータを生成すると、インデックスが再構築されます。そのため、データ サイズによっては、プロセスの完了に長時間を要する場合があります。複数の *CLI* セッションを立ち上げ、各セッションでメタデータを再生成するコマンドを実行して各ペアのプロセスを同時に完了させれば、プロセスが迅速に進みます。詳細については、「M-Series アプライアンスの RAID ペアのメタデータを再生成」を参照してください。

1. 新しいログ コレクタにディスクを挿入します。詳細についてはM-Series アプライアンスのハードウェア リファレンス ガイドに記載されたディスクの交換方法を参照してください。

M-100 アプライアンスのディスク キャリアは *M-500* アプライアンスのものとは互換性がありません。そのため、これらのハードウェア モデル間で移行を行う際は、以前のキャリアのネジを外して各ディスクを取り出し、ディスクを新しいアプライアンスに格納する前に新しいキャリアに挿入しておく必要があります。

ディスクのペアの関係を崩さないようにしてください。以前のアプライアンスのスロット A1/A2 から新しいアプライアンスのスロット B1/B2 にディスク ペアを移動させることはできますが、ディスクのペアを一緒にして同じスロットに入れるようにしてください。そうしなければ Panorama が正常にデータを復元できなくなるおそれがあります。

2. 各ペアに対して次の CLI コマンドを実行し、ディスク ペアを有効にします。

```
> request system raid add <slot> force no-format
```

以下に例を示します。

```
> request system raid add A1 force no-format
```


© 2019 Palo Alto Networks, Inc.

```
> request system raid add A2 force no-format
```

引数 **force** および **no-format** は必須です。引数**force**は、ディスク ペアを新しいログコレクタに関連付けます。引数 **no-format** はドライブが再フォーマットされるのを回避し、ディスクに保存されたログを維持させます。

3. 各ディスク ペアのメタデータを生成します。

```
> request metadata-regenerate slot <slot_number>
```

以下に例を示します。

```
> request metadata-regenerate slot 1
```

STEP 5 | ディスクを持たないログ コレクタをコレクタ グループに追加します。

ここから、*Panorama* およびログ コレクタで移行プロセスを完了するために必要なコミットのみ実行します。他の変更を行うのは控えてください。

1. Panorama CLI にアクセスします。
2. Panorama の制限を上書きして、ディスクを持たないログ コレクタをコレクタ グループに追加できるようにします：**request log-migration-set-start**

STEP 6 | ログを移行します。

このステップでは、*Web* インターフェイスではなく *Panorama CLI* を使用する必要があります。

新しいログ コレクタは、以前のログ コレクタを含むコレクタ グループに割り当てる必要があります。

1. 新しいログ コレクタをコレクタ グループに割り当て、Panorama に加えた変更をコミットします。

```
> configure
# set log-collector-group <collector_group_name> logfwd-setting collectors
 <new_LC_serial_number>
# commit
# exit
```

2. 各ディスク ペアについて、ログを以前のログ コレクタから新しいログ コレクタに移行し、ディスク ペアを新しいログ コレクタに取り付けます。

```
> request log-migration from <old_LC_serial_number> old-disk-pair
 <log_disk_pair> to <new_LC_serial_number> new-disk-pair <log_disk_pair>
```

以下に例を示します。

```
> request log-migration from 003001000010 old-disk-pair A to 00300100038
 new-disk-pair A
```

STEP 7 | コレクタ グループを再設定します。

1. Web インターフェイスを使用し、ログを転送するファイアウォールに新しいログ コレクタを割り当てます（**Panorama** > **Collector Groups**（コレクタ グループ） > **Device Log Forwarding**（デバイ

© 2019 Palo Alto Networks, Inc.

ス ログ転送)) 。ファイアウォール優先度リストにて、以前のログ コレクタと同じ優先度を新しいログ コレクタに付与します。

CLI を使用してファイアウォール優先度リストの優先度の割り当てを変更することはできません。

2. コレクタ グループから以前のログ コレクタを削除します。

```
> configure
# delete log-collector-group <group_name> logfwd-setting collectors
 <old_LC_serial_number>
```

以下に例を示します。

```
# delete log-collector-group DC-Collector-Group logfwd-setting collectors
 003001000010
```

3. 以前のログ コレクタを Panorama 設定から削除し、変更を Panorama にコミットします。

```
# delete log-collector <old_LC_serial_number>
# commit
# exit
```

4. コレクタ グループの変更をコミットして、管理対象ファイアウォールがログを新しいログ コレクタに送信できるようにします。

```
> commit-all log-collector-config log-collector-
group <collector_group_name>
```

以下に例を示します。

```
> commit-all log-collector-config log-collector-group DC-Collector-Group
```

STEP 8 | 新しい専用ログ コレクタで新しい鍵を生成します。

このコマンドは新しいログ コレクタをコレクタ グループに追加するために必要であり、交換するログ コレクタのコレクタ グループについてのみ実行する必要があります。この手順により、既存の *RSA* 鍵が削除され、*Panorama* が新しい *RSA* 鍵を作成できます。

1. Panorama CLI にアクセスします。
2. 新しいログ コレクタですべての RSA 鍵を削除します。

   request logdb update-collector-group-after-replace collector-group *<collector-group-name>*

   このプロセスが完了するまで、最大 10 分間かかる場合があります。

STEP 9 | コレクタ グループのすべてのログ コレクタで SearchEngine Status (検索エンジン ステータス) が Active (アクティブ) であることを確認します。

コレクタ グループのすべてのログ コレクタで *SearchEngine Status* (検索エンジン ステータス) が *Active* (アクティブ) になるまで、続行しないでください。これにより、交換するログ コレクタからログが消去されます。

1. Panorama CLI にアクセスします。

© 2019 Palo Alto Networks, Inc.

2. 次のいずれかのコマンドを実行してログ コレクタの詳細を表示します。
   - Panorama 上のすべてのログ コレクタ：

     show log-collector all

     または、各専用ログ コレクタで次のコマンドを実行することもできます。

     ```
     show log-collector detail
     ```
3. SearchEngine Status（検索エンジン ステータス）が Active（アクティブ）であることを確認します。

```
Redistribution status:       none
```

```
Last commit-all: commit succeeded, current ring version 1
```

```
SearchEngine status:     Active
```

```
md5sum 4e5055a359f7662fab8f8c4f57e24525 updated at 2017/06/14 09:58:19
```

STEP 10 | 新しいログ コレクタで、以前のログ コレクタのシリアル番号を新しいログ コレクタのシリアル番号に置換します。

以前のログ コレクタのシリアル番号を新しいログ コレクタのシリアル番号に置換する必要があるのは、新しいログ コレクタの実行により消去の問題が発生し、消去する必要があるにもかかわらずログ コレクタが以前のデータを消去できなくなるのを防ぐためです。

1. ログ コレクタ CLI にアクセスします。
2. 以前のログ コレクタのシリアル番号を新しいログ コレクタのシリアル番号に置換します。

   request log-migration-update-logger from *<old-log-collector-serial-number>* to*<new-log-collector-serial-number>*

Panorama モードでログを新しい M-Series アプライアンスに移行

Panorama モードの M-600、M-500、M-200 または M-100 アプライアンス（Panorama 管理サーバー）を交換する必要がある場合、RAID ディスクを新しい M-Series アプライアンスに移動することで、ファイアウォールから収集したログを移行することができます。ディスクを移動させることにより、M-Series アプライアンスのシステム障害が発生した後でログを復元したり、ハードウェア更新の一環としてログを（M-100 アプライアンスから M-500 アプライアンスへ）移行したりすることができます。



M-Series アプライアンスからロギング ディスクを削除して*M-600 Panorama* 管理サーバにログを読み込むというログ移行方法は、サポートされていません。*M-600* アプライアンスに移行するには、*M-Series* アプライアンスに保存されるログへのアクセスが必要な間は、M-600 アプライアンスをセットアップし、新しい M-600 アプライアンスへのログ転送を設定し、 管理対象ログ コレクタである M-Series アプライアンスを設定します。

この移行作業は、HA 構成でない単一の M-Series アプライアンスを単一の コレクタ グループに含まれる管理対象コレクタ（ログコレクタ）と置き換える、次のようなケースを扱います。

STEP 1 | ログを維持したい場合、以前の M-Series アプライアンスの SSD に入っているログをすべて外部の宛先に転送します。

© 2019 Palo Alto Networks, Inc.

SSD は、Panorama およびログ コレクタが生成するシステムおよび設定ログを保存します。M-Series アプライアンス間で SSD を移動させることはできません。

Panorama から外部の宛先へのログ転送を設定します。

STEP 2 | Panorama モードのデコミッショニングされた M-Series アプライアンスから Panorama 設定をエクスポートします。

1. Panorama アプライアンスにログインし、**Panorama** > **Setup**（セットアップ）> **Operations**（操作）の順に選択します。
2. **Save named Panorama configuration snapshot**（名前を付けて **Panorama** 設定スナップショットを保存）をクリックし、設定を識別できる **Name**（名前）を入力して **OK** をクリックします。
3. **Export named Panorama configuration snapshot**（名前を付けて **Panorama** 設定スナップショットを保存）をクリックし、先ほど保存した設定の **Name**（名前）を選択して **OK** をクリックします。Panorama が XML ファイルの形式で設定をクライアント システムにエクスポートします。

STEP 3 | 以前の M-Series アプライアンスから RAID ディスクを取り外します。

1. システムがシャットダウンするまで Power（電源）ボタンを押し続け、以前の M-Series アプライアンスの電源を切ります。
2. ディスク ペアを取り除きます。詳細については M-Series アプライアンスのハードウェア リファレンス ガイドに記載されたディスクの交換方法を参照してください。

STEP 4 | 新しい M-Series アプライアンスの初期セットアップを実行します。

1. M-Series アプライアンスをラック マウントします。方法については、M-Series アプライアンスのハードウェア リファレンス ガイドを参照してください。
2. M-Series アプライアンスの初期設定を行います。
3. Panorama を登録します。
4. 購入して Panorama サポート ライセンスをアクティベートするか、新しい M-Series アプライアンスが以前の M-Series アプライアンスと同じハードウェア モデルである場合のみ、以下のようにしてライセンスを移行します。新しい M-Series アプライアンスのモデルが以前の M-Series アプライアンスと異なる場合、新しいライセンスを購入する必要があります。
   1. Palo Alto Networks カスタマーサポート Web サイトにログインします。
   2. **Assets**（アセット）タブを選択し、**Spares**（スペア）リンクをクリックします。
   3. 新しい M-Series アプライアンスの Serial Number（シリアル番号）をクリックします。
   4. **Transfer Licenses**（ライセンスを移行）をクリックします。
   5. 以前の M-Series アプライアンスを**Select**（選択）し、**Submit**（送信）をクリックします。
5. ファイアウォール管理ライセンスのアクティベーションを行います。M-100 アプライアンスから M-500 アプライアンスへ移行を行っている場合、移行ライセンスの認証コードを入力します。
6. Panorama のコンテンツ更新とソフトウェア更新のインストールを行います。ソフトウェア バージョンに関する重要な詳細情報は、「Panorama、ログ コレクタ、ファイアウォール、および WildFire のバージョン互換性」を参照してください。

STEP 5 | デコミッショニングされた M-Series アプライアンスからエクスポートした Panorama 設定スナップショットを Panorama モードの新しい M-Series アプライアンスに読み込みます。

1. Panorama Web インターフェイスへのログイン（新しい M-Series アプライアンスの）、さらに**Panorama** > **Setup**（セットアップ）> **Operations**（操作）の順に選択します。
2. **Import named Panorama configuration snapshot**（名前を付けて保存した **Panorama** 設定スナップショットをインポート）をクリックし、デコミッショニングした M-Series アプライアンスからエクスポートした設定ファイルを **Browse**（参照）し、**OK** をクリックします。
3. **Load named Panorama configuration snapshot**（名前を付けて保存した **Panorama** 設定スナップショットを読み込み）をクリックし、先ほどインポートした設定の**Name**（名前）を選択し、さらに **Decryption Key**（復号化鍵）（Panorama のマスター鍵）を選択して **OK** をクリックします。読

© 2019 Palo Alto Networks, Inc.

み込んだ設定で Panorama が現在の候補設定を上書きします。設定ファイルのロード時にエラーが発生すると Panorama が表示を行います。エラーが発生した場合は、それらのエラーをローカル ファイルに保存します。必ず各エラーを解決し、正常に設定が移行されるようにします。

RMA Panorama を置き換える場合、名前付きの *Panorama* 設定スナップショットを読み込む際に必ず *Retain Rule UUIDs (*ルールの *UUID* を維持*)* してください。このオプションを選択しない場合、*Panorama* は以前のルールの *UUID* をすべて設定スナップショットから削除し、新しい *UUID* を *Panorama* 上のルールに割り当てます。つまり、ポリシールール ヒット数など、以前の *UUID* に紐付いていた情報は保持されません。

4. 必要に応じて、追加の構成変更を実行します。

   以前の *M-Series* アプライアンスで *Panorama* サービス *(*ログ収集など*)*に *MGT* インターフェイス以外のインターフェイスを使用していた場合、新しい *M-Series* アプライアンスでこれらのインターフェイスを定義する必要があります *(Panorama > Setup (*セットアップ*) > Interfaces (*インターフェイス*))*。

5. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、**Validate Commit**（コミットの検証）を行います。次に進む前にすべてのエラーを解決します。
6. Panorama 設定に対する変更を **Commit**（コミット）します。

STEP 6 | 新しい M-Series アプライアンスにディスクを挿入します。詳細についてはM-Series アプライアンスのハードウェア リファレンス ガイドに記載されたディスクの交換方法を参照してください。

M-100 アプライアンスのディスク キャリアは *M-500* アプライアンスのものとは互換性がありません。そのため、これらのハードウェア モデル間で移行を行う際は、以前のキャリアのネジを外して各ディスクを取り出し、ディスクを新しいアプライアンスに格納する前に新しいキャリアに挿入しておく必要があります。

ディスクのペアの関係を崩さないようにしてください。以前のアプライアンスのスロット A1/A2 から新しいアプライアンスのスロット B1/B2 にディスク ペアを移動させることはできますが、ディスクのペアを一緒にして同じスロットに入れるようにしてください。そうしなければ Panorama が正常にデータを復元できなくなるおそれがあります。

STEP 7 | Palo Alto Networks カスタマーサポートに連絡し、デコミッショニングされた M-Series アプライアンスから新しい M-Series アプライアンスにログコレクタ グループのメタデータをコピーし、mgmtsrvrプロセスを再起動してください。

STEP 8 | M-Series アプライアンスがコレクタ グループの一部だった場合、以前の M-Series アプライアンスのシリアル番号が引き続き正しいコレクタ グループに含まれていることを確認します。

```
debug log-collector-group show name <Log Collector Group name>
```

以前の M-Series アプライアンスのシリアル番号が正しいコレクタ グループに含まれなくなっている場合、前のステップでテクニカル サポート フォルダのコピーに失敗したことになります。もう一度 Palo Alto Networks カスタマー サポートに連絡し、テクニカル サポート フォルダを正しい場所にコピーしてください。

STEP 9 | 移行用のディスクを準備します。

各ディスク ペアのメタデータを生成すると、インデックスが再構築されます。そのため、データ サイズによっては、プロセスの完了に長時間を要する場合があります。複数の *CLI* セッションを立ち上げ、各セッションでメタデータを再生成するコマンドを実行して各ペアのプロセスを同時に完了させれば、プロセスが迅速に進みます。詳細につい

© 2019 Palo Alto Networks, Inc.

ては、「M-Series アプライアンスの RAID ペアのメタデータを再生成」を参照してください。

1. 新しい M-Series アプライアンスにディスクを挿入します。詳細については M-Series アプライアンスのハードウェア リファレンス ガイドに記載されたディスクの交換方法を参照してください。

   M-100 アプライアンスのディスク キャリアは *M-500* アプライアンスのものとは互換性がありません。そのため、これらのハードウェア モデル間で移行を行う際は、以前のキャリアのネジを外して各ディスクを取り出し、ディスクを新しいアプライアンスに格納する前に新しいキャリアに挿入しておく必要があります。

   ディスクのペアの関係を崩さないようにしてください。以前のアプライアンスのスロット A1/A2 から新しいアプライアンスのスロット B1/B2 にディスク ペアを移動させることはできますが、ディスクのペアを一緒にして同じスロットに入れるようにしてください。そうしなければ Panorama が正常にデータを復元できなくなるおそれがあります。
2. 各ペアに対して次の CLI コマンドを実行し、ディスク ペアを有効にします。

   ```
   admin> request system raid add <slot> force no-format
   ```

   以下に例を示します。

   ```
   admin> request system raid add A1 force no-format
   admin> request system raid add A2 force no-format
   ```

   引数 **force** および **no-format** は必須です。引数 **force** は、ディスク ペアを新しいアプライアンスに関連付けます。引数 **no-format** はドライブが再フォーマットされるのを回避し、ディスクに保存されたログを維持させます。
3. 各ディスク ペアのメタデータを生成します。

   このステップは、ディスクにあるログデータの量に応じて最大 *6* 時間を要することがあります。

   ```
   admin> request metadata-regenerate slot <slot_number>
   ```

   以下に例を示します。

   ```
   admin> request metadata-regenerate slot 1
   ```

STEP 10 | 新しい M-Series アプライアンス用のローカル ログ コレクタを設定します。

シリアル番号が必要になるコマンドを使用するステップでは、必ずシリアル番号全体を入力してください。*Tab* キーを押してもシリアル番号の一部が補完されることはありません。

この段階ではまだ新しい M-Series アプライアンスのディスクを有効化しないでください。ログの移行が正常に完了したら、Panorama が自動的にディスクを有効化します。

1. Panorama Web インターフェイスを使用して、あるいは次の CLI コマンドを使用してローカル ログ コレクタを管理対象コレクタとして設定します。

   ```
   admin> configure
   ```


© 2019 Palo Alto Networks, Inc.

```
admin# set log-collector <log-collector_SN> deviceconfig system ホスト名
 <log-collector-ホスト名>
admin# exit
```

2. ローカル ログ コレクタが Panorama に接続されており、そのディスク ペアのステータスが present/available であることを確認します。

```
admin> show log-collector serial-number <log-collector_SN>
```

復元プロセスのこの段階では、ディスク ペアが無効として表示されます。

3. 変更を Panorama にコミットします。まだ変更をコレクタ グループにコミットしないでください。

```
admin> configure
admin# commit
```

STEP 11 | ディスクを持たないログ コレクタをコレクタ グループに追加します。

ここから、*Panorama* およびログ コレクタで移行プロセスを完了するために必要なコミットのみ実行します。他の変更を行うのは控えてください。

1. 新しい M-Series アプライアンスのPanorama CLI にアクセスします。
2. Panorama の制限を上書きして、ディスクを持たないログ コレクタをコレクタ グループに追加できるようにします：**request log-migration-set-start**
3. 上書きされた制限をコミットします：

```
admin> configure
admin# commit force
```

STEP 12 | ログを移行します。

1. 新しい M-Series アプライアンスのPanorama CLI にアクセスします。
2. 新しいローカル ログ コレクタをコレクタ グループのメンバーとして追加し、変更を Panorama にコミットします。

```
admin# set log-collector-group <collector_group_name> ogfwd-setting
 collectors <SN_managed_collector>
admin# commit
admin# exit
```

以前のローカル ログ コレクタは、まだ設定から削除していないため、引き続きメンバーのリストに表示されます。

3. ディスク ペアごとにログを新しいアプライアンスに移行します。

```
admin> request log-migration from <old_LC_serial_number> old-disk-pair
 <log_disk_pair> to <new_LC_serial_number> new-disk-pair <log_disk_pair>
```

以下に例を示します。

```
admin> request log-migration from 003001000010 old-disk-pair A to
 00300100038 new-disk-pair A
```

4. 変更を Panorama にコミットします。

© 2019 Palo Alto Networks, Inc.

```
admin> configure
admin# commit
```

STEP 13 | コレクタ グループを再設定します。

1. （新しい M-Series アプライアンスの）、そしてログを転送するファイアウォールに新しいログ コレクタを割り当てPanorama Web インターフェイスへのログインます（**Panorama** > **Collector Groups**（コレクタ グループ）> **Device Log Forwarding**（デバイス ログ転送））。ファイアウォール優先度リストにて、以前のログ コレクタと同じ優先度を新しいログ コレクタに付与します。

   CLI を使用してファイアウォール優先度リストの優先度の割り当てを変更することはできません。

2. 新しい M-Series アプライアンスのPanorama CLI にアクセスします。
3. コレクタ グループから以前のログ コレクタを削除します。

   ```
   admin# delete log-collector-group <group_name> logfwd-setting collectors
    <old_LC_serial_number>
   ```

   以下に例を示します。

   ```
   admin# delete log-collector-group DC-Collector-Group logfwd-setting
    collectors 003001000010
   ```

4. 以前のログ コレクタを Panorama 設定から削除し、変更を Panorama にコミットします。

   ```
   admin# delete log-collector <old_LC_serial_number>
   admin# commit
   admin# exit
   ```

5. コレクタ グループの変更をコミットして、管理対象ファイアウォールがログを新しいログ コレクタに送信できるようにします。

   ```
   admin> commit-all log-collector-config log-collector-
   group <collector_group_name>
   ```

   以下に例を示します。

   ```
   admin> commit-all log-collector-config log-collector-group DC-Collector-
   Group
   ```

STEP 14 | 新しいログ コレクタで新しい鍵を生成します。

このコマンドは新しいログ コレクタをコレクタ グループに追加するために必要であり、交換するログ コレクタのコレクタ グループについてのみ実行する必要があります。この手順により、既存の *RSA* 鍵が削除され、*Panorama* が新しい *RSA* 鍵を作成できます。

1. 新しい M-Series アプライアンスのPanorama CLI にアクセスします。
2. 新しいログ コレクタですべての RSA 鍵を削除します。

   ```
   request logdb update-collector-group-after-replace collector-group
   <collector-group-name>
   ```

   このプロセスが完了するまで、最大 10 分間かかる場合があります。

© 2019 Palo Alto Networks, Inc.

STEP 15 | コレクタ グループのすべてのログ コレクタで SearchEngine Status（検索エンジン ステータス）が Active（アクティブ）であることを確認します。

コレクタ グループのすべてのログ コレクタで *SearchEngine Status*（検索エンジン ステータス）が *Active*（アクティブ）になるまで、続行しないでください。これにより、交換するログ コレクタからログが消去されます。

1. 新しい M-Series アプライアンスのPanorama CLI にアクセスします。
2. 次のいずれかのコマンドを実行してログ コレクタの詳細を表示します。
   - Panorama 上のすべてのログ コレクタ：

     `show log-collector all`

     または、各専用ログ コレクタで次のコマンドを実行することもできます。

     ```
     show log-collector detail
     ```
3. SearchEngine Status（検索エンジン ステータス）が Active（アクティブ）であることを確認します。

```
Redistribution status:       none
```

```
Last commit-all: commit succeeded, current ring version 1
```

```
SearchEngine status:     Active
```

```
md5sum 4e5055a359f7662fab8f8c4f57e24525 updated at 2017/06/14 09:58:19
```

STEP 16 | 新しいログ コレクタで、以前のログ コレクタのシリアル番号を新しいログ コレクタのシリアル番号に置換します。

以前のログ コレクタのシリアル番号を新しいログ コレクタのシリアル番号に置換する必要があるのは、新しいログ コレクタの実行により消去の問題が発生し、消去する必要があるにもかかわらずログ コレクタが以前のデータを消去できなくなるのを防ぐためです。

1. ログ コレクタ CLI にアクセスします。
2. 以前のログ コレクタのシリアル番号を新しいログ コレクタのシリアル番号に置換します。

   `request log-migration-update-logger from <old-log-collector-serial-number> to<new-log-collector-serial-number>`

高可用性の Panorama モードで新しい M-Series アプライアンス モデルにログを移行

M-600、M-500、M-200 または M-100 アプライアンス（Panorama 管理サーバー）を、交換対象の M-Series アプライアンスとは別の M-Series アプライアンスを持つ Panorama モードと交換する必要がある場合、RAID ディスクを新しい M-Series アプライアンスに移動することで、ファイアウォールから収集したログを移行することができます。ディスクを移動させることにより、ハードウェア更新の一環としてログを（M-100 アプライアンスから M-500 アプライアンスへ）移行することができます。M-100 アプライアンスと M-500 アプライアンスとの間で移行が可能です。M-100 および M-500 アプライアンスは、M-200、M-600 アプライアンス間で移行を行うことはできません。

© 2019 Palo Alto Networks, Inc.

M-Series アプライアンスからロギング ディスクを削除して*M-600 Panorama* 管理サーバにログを読み込むというログ移行方法は、サポートされていません。*M-600* アプライアンスに移行するには、*M-Series* アプライアンスに保存されるログへのアクセスが必要な間は、M-600 アプライアンスをセットアップし、新しい M-600 アプライアンスへのログ転送を設定し、 管理対象ログ コレクタである M-Series アプライアンスを設定します。

ここで説明する移行作業は次の各状況を想定しています。

- 単体の Panorama HA ピアのコレクタ グループに管理対象コレクタ（ログコレクタ）がある。

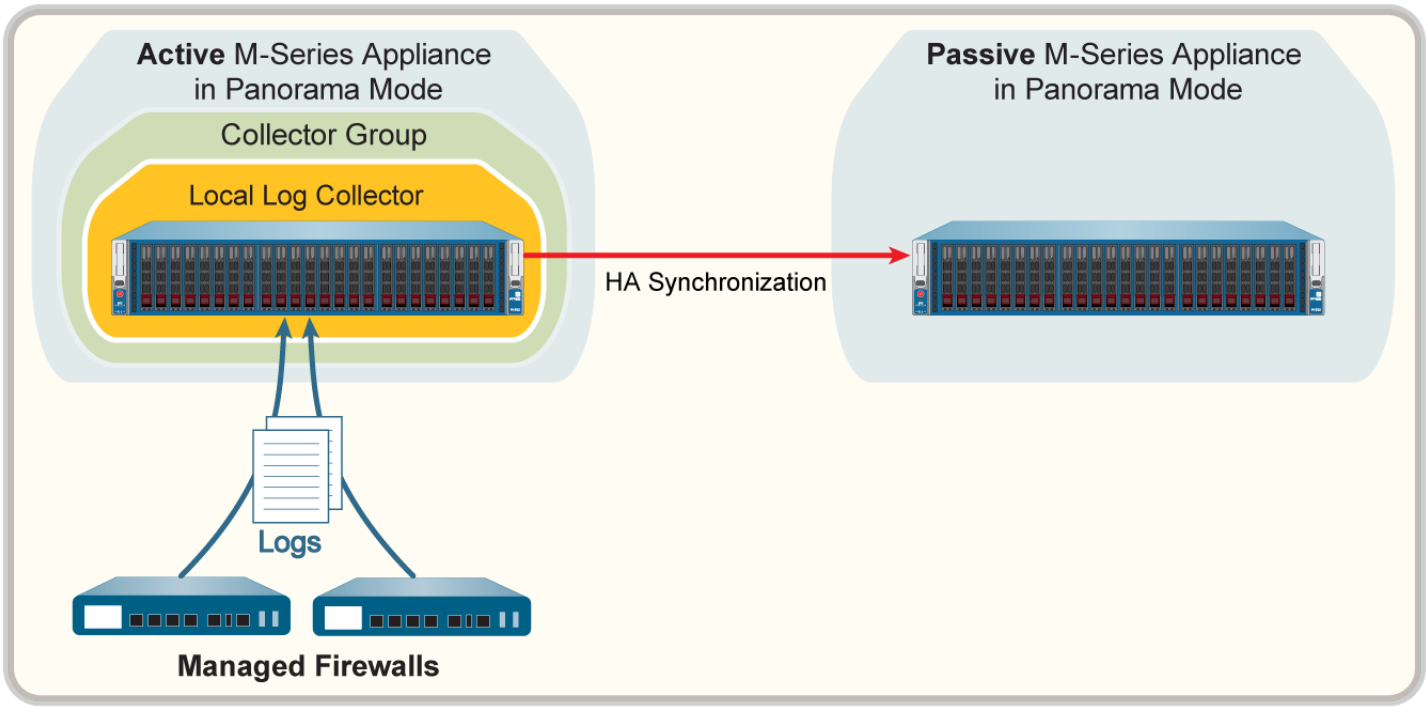


図 **30 :** コレクタ グループを持つ **Panorama HA** ピア

- 単一のコレクタ グループに所属する管理対象コレクタがどちらの Panorama HA ピアにもある。詳細は、「コレクタ グループごとに複数のローカル ログ コレクタ」を参照してください。
- どちらの Panorama HA ピアにも単一の管理対象コレクタがあり、それぞれ別のコレクタ グループに割り当てられている。詳細は、「コレクタ グループごとに 1 つのローカル ログ コレクタ」を参照してください。

STEP 1 | ログを維持したい場合、以前の M-Series アプライアンスの SSD に入っているログをすべて外部の宛先に転送します。

SSD は、Panorama およびログ コレクタが生成するシステムおよび設定ログを保存します。M-Series アプライアンス間で SSD を移動させることはできません。

Panorama から外部の宛先へのログ転送を設定します。

STEP 2 | Panorama モードのデコミッショニングされたプライマリ M-Series アプライアンスから Panorama 設定をエクスポートします。

1. Panorama Web インターフェイスへのログイン（置き換える M-Series アプライアンスの）、さらに**Panorama** > **Setup**（セットアップ）> **Operations**（操作）の順に選択します。
2. **Save named Panorama configuration snapshot**（名前を付けて **Panorama** 設定スナップショットを保存）をクリックし、設定を識別できる **Name**（名前）を入力して **OK** をクリックします。

© 2019 Palo Alto Networks, Inc.

3. **Export named Panorama configuration snapshot**（名前を付けて **Panorama** 設定スナップショットを保存）をクリックし、先ほど保存した設定の **Name**（名前）を選択して **OK** をクリックします。Panorama が XML ファイルの形式で設定をクライアント システムにエクスポートします。

STEP 3 | 以前の M-Series アプライアンスから RAID ディスクを取り外します。

1. システムがシャットダウンするまで Power（電源）ボタンを押し続け、以前の M-Series アプライアンスの電源を切ります。
2. ディスク ペアを取り除きます。詳細については M-Series アプライアンスのハードウェア リファレンス ガイドに記載されたディスクの交換方法を参照してください。

STEP 4 | 新しい M-Series アプライアンスの初期セットアップを実行します。

HA 構成で新しい M-Series アプライアンスのそれぞれに対してこのステップを繰り返します。

1. M-Series アプライアンスをラック マウントします。方法については、M-Series アプライアンスのハードウェア リファレンス ガイドを参照してください。
2. M-Series アプライアンスの初期設定を行います。
3. Panorama を登録します。
4. 購入して Panorama サポート ライセンスをアクティベートするか、新しい M-Series アプライアンスが以前の M-Series アプライアンスと同じハードウェア モデルである場合のみ、以下のようにしてライセンスを移行します。新しい M-Series アプライアンスのモデルが以前の M-Series アプライアンスと異なる場合、新しいライセンスを購入する必要があります。
   1. Palo Alto Networks カスタマーサポート Web サイトにログインします。
   2. **Assets**（アセット）タブを選択し、**Spares**（スペア）リンクをクリックします。
   3. 新しい M-Series アプライアンスの Serial Number（シリアル番号）をクリックします。
   4. **Transfer Licenses**（ライセンスを移行）をクリックします。
   5. 以前の M-Series アプライアンスを**Select**（選択）し、**Submit**（送信）をクリックします。
5. ファイアウォール管理ライセンスのアクティベーションを行います。M-100 アプライアンスから M-500 アプライアンスへ移行を行っている場合、移行ライセンスの認証コードを入力します。
6. Panorama のコンテンツ更新とソフトウェア更新のインストールを行います。ソフトウェア バージョンに関する重要な詳細情報は、「Panorama、ログ コレクタ、ファイアウォール、および WildFire のバージョン互換性」を参照してください。
7. Panorama での HA のセットアップ.新しい M-Series アプライアンスの優先度は、交換中の HA ピアと同じでなければなりません。

STEP 5 | デコミッショニングされたプライマリ M-Series アプライアンスからエクスポートした Panorama 設定スナップショットを Panorama モードの新しいプライマリ M-Series アプライアンスに読み込みます。

1. Panorama Web インターフェイスへのログイン（新しい M-Series アプライアンスの）、さらに**Panorama** > **Setup**（セットアップ）> **Operations**（操作）の順に選択します。
2. **Import named Panorama configuration snapshot**（名前を付けて保存した **Panorama** 設定スナップショットをインポート）をクリックし、デコミッショニングした M-Series アプライアンスからエクスポートした設定ファイルを **Browse**（参照）し、**OK** をクリックします。
3. **Load named Panorama configuration snapshot**（名前を付けて保存した **Panorama** 設定スナップショットを読み込み）をクリックし、先ほどインポートした設定の**Name**（名前）を選択し、さらに **Decryption Key**（復号化鍵）（Panorama のマスター鍵）を選択して **OK** をクリックします。読み込んだ設定で Panorama が現在の候補設定を上書きします。設定ファイルのロード時にエラーが発生すると Panorama が表示を行います。エラーが発生した場合は、それらのエラーをローカル ファイルに保存します。必ず各エラーを解決し、正常に設定が移行されるようにします。



RMA Panorama を置き換える場合、名前付きの *Panorama* 設定スナップショットを読み込む際に必ず *Retain Rule UUIDs (*ルールの *UUID* を維持*)* してください。このオ

© 2019 Palo Alto Networks, Inc.

プションを選択しない場合、*Panorama* は以前のルールの *UUID* をすべて設定スナップショットから削除し、新しい *UUID* を *Panorama* 上のルールに割り当てます。つまり、ポリシールール ヒット数など、以前の *UUID* に紐付いていた情報は保持されません。

4. 必要に応じて、追加の構成変更を実行します。



以前の *M-Series* アプライアンスで *Panorama* サービス *(*ログ収集など*)*に *MGT* インターフェイス以外のインターフェイスを使用していた場合、新しい *M-Series* アプライアンスでこれらのインターフェイスを定義する必要があります *(Panorama > Setup (*セットアップ*) > Interfaces (*インターフェイス*))*。

5. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、**Validate Commit**（コミットの検証）を行います。次に進む前にすべてのエラーを解決します。
6. Panorama 設定に対する変更を **Commit**（コミット）します。コミット後、HA ピア全体にかけて Panorama 設定が同期されます。

STEP 6 | 新しい M-Series アプライアンスにディスクを挿入します。詳細についてはM-Series アプライアンスのハードウェア リファレンス ガイドに記載されたディスクの交換方法を参照してください。

HA 構成で新しい M-Series アプライアンスのそれぞれに対してこのステップを繰り返します。



M-100 アプライアンスのディスク キャリアは *M-500* アプライアンスのものとは互換性がありません。そのため、これらのハードウェア モデル間で移行を行う際は、以前のキャリアのネジを外して各ディスクを取り出し、ディスクを新しいアプライアンスに格納する前に新しいキャリアに挿入しておく必要があります。

ディスクのペアの関係を崩さないようにしてください。以前のアプライアンスのスロット A1/A2 から新しいアプライアンスのスロット B1/B2 にディスク ペアを移動させることはできますが、ディスクのペアを一緒にして同じスロットに入れるようにしてください。そうしなければ Panorama が正常にデータを復元できなくなるおそれがあります。

STEP 7 | Palo Alto Networks カスタマーサポートに連絡し、デコミッショニングされた M-Series アプライアンスから新しい M-Series アプライアンスにログコレクタ グループのメタデータをコピーし、mgmtsrvrプロセスを再起動してください。

STEP 8 | M-Series アプライアンスがコレクタ グループの一部だった場合、以前の M-Series アプライアンスのシリアル番号が引き続き正しいコレクタ グループに含まれていることを確認します。

```
debug log-collector-group show name <Log CollectorGroup name>
```

以前の M-Series アプライアンスのシリアル番号が正しいコレクタ グループに含まれなくなっている場合、前のステップでテクニカル サポート フォルダのコピーに失敗したことになります。もう一度 Palo Alto Networks カスタマー サポートに連絡し、テクニカル サポート フォルダを正しい場所にコピーしてください。

STEP 9 | 移行用のディスクを準備します。



各ディスク ペアのメタデータを生成すると、インデックスが再構築されます。そのため、データ サイズによっては、プロセスの完了に長時間を要する場合があります。複数の *CLI* セッションを立ち上げ、各セッションでメタデータを再生成するコマンドを実行して各ペアのプロセスを同時に完了させれば、プロセスが迅速に進みます。詳細については、「M-Series アプライアンスの RAID ペアのメタデータを再生成」を参照してください。

© 2019 Palo Alto Networks, Inc.

1. 各ペアに対して次の CLI コマンドを実行し、ディスク ペアを有効にします。

```
admin> request system raid add <slot> force no-format
```

以下に例を示します。

```
admin> request system raid add A1 force no-format
admin> request system raid add A2 force no-format
```

引数 **force** および **no-format** は必須です。引数 **force** は、ディスク ペアを新しいアプライアンスに関連付けます。引数 **no-format** はドライブが再フォーマットされるのを回避し、ディスクに保存された口グを維持させます。

2. 各ディスク ペアのメタデータを生成します。



このステップは、ディスクにある口グデータの量に応じて最大 *6* 時間を要することがあります。

```
admin> request metadata-regenerate slot <slot_number>
```

以下に例を示します。

```
admin> request metadata-regenerate slot 1
```

STEP 10 | 新しい M-Series アプライアンス用のローカル ログ コレクタを設定します。



シリアル番号が必要になるコマンドを使用するステップでは、必ずシリアル番号全体を入力してください。*Tab* キーを押してもシリアル番号の一部が補完されることはありません。

この段階ではまだ新しい M-Series アプライアンスのディスクを有効化しないでください。ログの移行が正常に完了したら、Panorama が自動的にディスクを有効化します。

1. Panorama Web インターフェイスを使用して、あるいは次の CLI コマンドを使用してローカル ログ コレクタを管理対象コレクタとして設定します。

```
admin> configure
admin# set log-collector <log-collector_SN> deviceconfig system ホスト名
 <log-collector-ホスト名>
admin# exit
```

2. 変更を Panorama にコミットします。まだ変更をコレクタ グループにコミットしないでください。

```
admin> configure
admin# commit
```

3. ローカル ログ コレクタが Panorama に接続されており、そのディスク ペアのステータスが present/available であることを確認します。

```
admin> show log-collector serial-number <log-collector_SN>
```

復元プロセスのこの段階では、ディスク ペアが無効として表示されます。

© 2019 Palo Alto Networks, Inc.

STEP 11 | ディスクを持たないログ コレクタをコレクタ グループに追加します。

ここから、*Panorama* およびログ コレクタで移行プロセスを完了するために必要なコミットのみ実行します。他の変更を行うのは控えてください。

1. 新しい M-Series アプライアンスのPanorama CLI にアクセスします。
2. Panorama の制限を上書きして、ディスクを持たないログ コレクタをコレクタ グループに追加できるようにします： **requestlog-migration-set-start**要求
3. 変更を Panorama にコミットします。

```
admin> configure
admin# commit force
```

STEP 12 | ログを移行します。

1. 新しい M-Series アプライアンスのPanorama CLI にアクセスします。
2. 新しいローカル ログ コレクタをコレクタ グループのメンバーとして追加し、変更を Panorama にコミットします。

```
admin# set log-collector-group <collector_group_name> ogfwd-setting
 collectors <SN_managed_collector>
admin# commit
admin# exit
```

以前のローカル ログ コレクタは、まだ設定から削除していないため、引き続きメンバーのリストに表示されます。

3. ディスク ペアごとにログを新しいアプライアンスに移行します。

```
admin> request log-migration from <old_LC_serial_number> old-disk-pair
 <log_disk_pair> to <new_LC_serial_number> new-disk-pair <log_disk_pair>
```

以下に例を示します。

```
admin> request log-migration from 003001000010 old-disk-pair A to
 00300100038 new-disk-pair A
```

4. 変更を Panorama にコミットします。

```
admin> configure
admin# commit
```

STEP 13 | コレクタ グループを再設定します。

1. Panorama Web インターフェイスへのログイン（新しい M-Series アプライアンスの）、そしてログを転送するファイアウォールに新しいログ コレクタを割り当てます（**Panorama** > **Collector Groups**（コレクタ グループ）> **Device Log Forwarding**（デバイス ログ転送））。ファイアウォール優先度リストにて、以前のログ コレクタと同じ優先度を新しいログ コレクタに付与します。

CLI を使用してファイアウォール優先度リストの優先度の割り当てを変更することはできません。

2. 新しい M-Series アプライアンスのPanorama CLI にアクセスします。
3. コレクタ グループから以前のログ コレクタを削除します。

© 2019 Palo Alto Networks, Inc.

```
admin# delete log-collector-group <group_name> logfwd-setting collectors
 <old_LC_serial_number>
```

以下に例を示します。

```
admin# delete log-collector-group DC-Collector-Group logfwd-setting
 collectors 003001000010
```

4. 以前のログ コレクタを Panorama 設定から削除し、変更を Panorama にコミットします。

```
admin# delete log-collector <old_LC_serial_number>
admin# commit
admin# exit
```

5. コレクタ グループの変更をコミットして、管理対象ファイアウォールがログを新しいログ コレクタに送信できるようにします。

```
admin> commit-all log-collector-config log-collector-
group <collector_group_name>
```

以下に例を示します。

```
admin> commit-all log-collector-config log-collector-group DC-Collector-
Group
```

STEP 14 | 新しいログ コレクタで新しい鍵を生成します。

このコマンドは新しいログ コレクタをコレクタ グループに追加するために必要であり、交換するログ コレクタのコレクタ グループについてのみ実行する必要があります。この手順により、既存の *RSA* 鍵が削除され、*Panorama* が新しい *RSA* 鍵を作成できます。

1. 新しい M-Series アプライアンスのPanorama CLI にアクセスします。
2. 新しいログ コレクタですべての RSA 鍵を削除します。

   request logdb update-collector-group-after-replacecollector-group *<collector-group-name>*

   このプロセスが完了するまで、最大 10 分間かかる場合があります。

STEP 15 | コレクタ グループのすべてのログ コレクタで SearchEngine Status (検索エンジン ステータス) が Active (アクティブ) であることを確認します。

コレクタ グループのすべてのログ コレクタで *SearchEngine Status* (検索エンジン ステータス) が *Active* (アクティブ) になるまで、続行しないでください。これにより、交換するログ コレクタからログが消去されます。

1. 新しい M-Series アプライアンスのPanorama CLI にアクセスします。
2. 次のいずれかのコマンドを実行してログ コレクタの詳細を表示します。
   - Panorama 上のすべてのログ コレクタ :

     show log-collector all

© 2019 Palo Alto Networks, Inc.

または、各専用ログ コレクタで次のコマンドを実行することもできます。

```
show log-collector detail
```

3. SearchEngine Status（検索エンジン ステータス）が Active（アクティブ）であることを確認します。

```
Redistribution status:       none
```

```
Last commit-all: commit succeeded, current ring version 1
```

```
SearchEngine status:     Active
```

```
md5sum 4e5055a359f7662fab8f8c4f57e24525 updated at 2017/06/14 09:58:19
```

STEP 16 | 新しいログ コレクタで、以前のログ コレクタのシリアル番号を新しいログ コレクタのシリアル番号に置換します。

以前のログ コレクタのシリアル番号を新しいログ コレクタのシリアル番号に置換する必要があるのは、新しいログ コレクタの実行により消去の問題が発生し、消去する必要があるにもかかわらずログ コレクタが以前のデータを消去できなくなるのを防ぐためです。

1. ログ コレクタ CLI にアクセスします。
2. 以前のログ コレクタのシリアル番号を新しいログ コレクタのシリアル番号に置換します。

   request log-migration-update-logger from *<old-log-collector-serial-number>* to*<new-log-collector-serial-number>*

STEP 17 | 新しいセカンダリ Panorama 高可用性ピアをセットアップします。

1. ログを維持したい場合、すべて外部の宛先に以前の M-Series アプライアンスの SSD に入っているログを転送します。
2. 以前の M-Series アプライアンスから RAID ディスクを取り外します。
3. 新しい M-Series アプライアンスの初期セットアップを実行します。
4. 新しい M-Series アプライアンスにディスクを挿入します。
5. ステップ7から16を繰り返し、以前の M-Series アプライアンスから新しい M-Series アプライアンスにログを移行します。
6. Panorama での HA のセットアップ.新しい M-Series アプライアンスの優先度は、交換中の HA ピアと同じでなければなりません。
7. Panorama Web インターフェイスへのログイン（プライマリ HA ピアの）、そして**Dashboard (ダッシュボード)** > **High Availability (高可用性)** > **Sync to peer (ピアに同期)**をクリックして M-Series アプライアンスの HA ピアの設定を同期します。

高可用性の Panorama モードで同じ M-Series アプライアンス モデルにログを移行

高可用性（HA）構成でデプロイされた M-600、M-500、M-200 または M-100 アプライアンス（Panorama 管理サーバー）を、交換対象の M-Series アプライアンスと同じ M-Series アプライアンスを持つ Panorama モードと交換する必要がある場合、RAID ディスクを新しい M-Series アプライアンスに移動することで、ファイアウォールから収集したログを移行することができます。ディスクを移動させる

© 2019 Palo Alto Networks, Inc.

ことにより、M-Series アプライアンスのシステム エラーが発生した後でログを復元できるようになります。

ここで説明する移行作業は次の各状況を想定しています。

- 単体の Panorama HA ピアのコレクタ グループに管理対象コレクタ（ログコレクタ）がある。

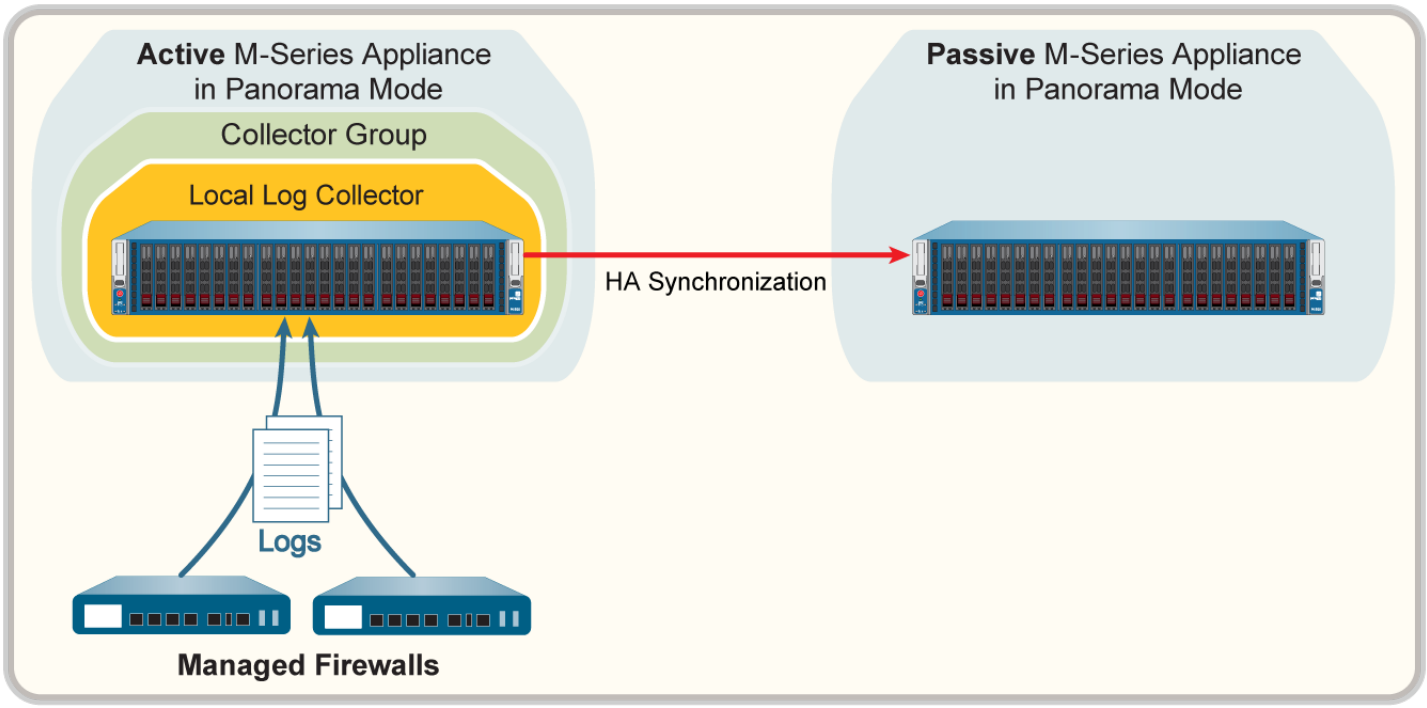


図 **31 :** コレクタ グループを持つ **Panorama HA** ピア

- 単一のコレクタ グループに所属する管理対象コレクタがどちらの Panorama HA ピアにもある。詳細は、「コレクタ グループごとに複数のローカル ログ コレクタ」を参照してください。
- どちらの Panorama HA ピアにも単一の管理対象コレクタがあり、それぞれ別のコレクタ グループに割り当てられている。詳細は、「コレクタ グループごとに 1 つのローカル ログ コレクタ」を参照してください。

STEP 1 | ログを維持したい場合、以前の M-Series アプライアンスの SSD に入っているログをすべて外部の宛先に転送します。

SSD は、Panorama およびログ コレクタが生成するシステムおよび設定ログを保存します。M-Series アプライアンス間で SSD を移動させることはできません。

Panorama から外部の宛先へのログ転送を設定します。

STEP 2 | 以前の M-Series アプライアンスから RAID ディスクを取り外します。

1. システムがシャットダウンするまで Power（電源）ボタンを押し続け、以前の M-Series アプライアンスの電源を切ります。
2. ディスク ペアを取り除きます。詳細については M-Series アプライアンスのハードウェア リファレンス ガイドに記載されたディスクの交換方法を参照してください。

STEP 3 | 新しい M-Series アプライアンスの初期セットアップを実行します。

1. M-Series アプライアンスをラック マウントします。方法については、M-Series アプライアンスのハードウェア リファレンス ガイドを参照してください。
2. M-Series アプライアンスの初期設定を行います。

© 2019 Palo Alto Networks, Inc.

以前の *M-Series* アプライアンスで *Panorama* サービス (ログ収集など) に *MGT* インターフェイス以外のインターフェイスを使用していた場合、新しい *M-Series* アプライアンスの初期設定中にこれらのインターフェイスを定義する必要があります (*Panorama* > *Setup* (セットアップ) > *Interfaces* (インターフェイス))。

3. Panorama を登録します。
4. 購入してPanorama サポート ライセンスをアクティベートするか、新しい M-Series アプライアンスが以前の M-Series アプライアンスと同じハードウェア モデルである場合のみ、以下のようにしてライセンスを移行します。新しい M-Series アプライアンスのモデルが以前の M-Series アプライアンスと異なる場合、新しいライセンスを購入する必要があります。
   1. Palo Alto Networks カスタマーサポート Web サイトにログインします。
   2. **Assets** (アセット) タブを選択し、**Spares** (スペア) リンクをクリックします。
   3. 新しい M-Series アプライアンスの Serial Number (シリアル番号) をクリックします。
   4. **Transfer Licenses** (ライセンスを移行) をクリックします。
   5. 以前の M-Series アプライアンスを**Select** (選択) し、**Submit** (送信) をクリックします。
5. ファイアウォール管理ライセンスのアクティベーションを行います。M-100 アプライアンスから M-500 アプライアンスへ移行を行っている場合、移行ライセンスの認証コードを入力します。
6. Panorama のコンテンツ更新とソフトウェア更新のインストールを行います。ソフトウェア バージョンに関する重要な詳細情報は、「Panorama、ログ コレクタ、ファイアウォール、および WildFire のバージョン互換性」を参照してください。
7. 必要に応じて、追加の構成変更を実行します。

   以前の *M-Series* アプライアンスで *Panorama* サービス *(*ログ収集など*)*に *MGT* インターフェイス以外のインターフェイスを使用していた場合、新しい *M-Series* アプライアンスでこれらのインターフェイスを定義する必要があります *(Panorama* > *Setup (*セットアップ*)* > *Interfaces (*インターフェイス*))*。
8. Panorama での HA のセットアップ.新しい M-Series アプライアンスの優先度は、交換中の HA ピアと同じでなければなりません。

STEP 4 | 新しい M-Series アプライアンスにディスクを挿入します。詳細についてはM-Series アプライアンスのハードウェア リファレンス ガイドに記載されたディスクの交換方法を参照してください。

M-100 アプライアンスのディスク キャリアは *M-500* アプライアンスのものとは互換性がありません。そのため、これらのハードウェア モデル間で移行を行う際は、以前のキャリアのネジを外して各ディスクを取り出し、ディスクを新しいアプライアンスに格納する前に新しいキャリアに挿入しておく必要があります。

ディスクのペアの関係を崩さないようにしてください。以前のアプライアンスのスロット A1/A2 から新しいアプライアンスのスロット B1/B2 にディスク ペアを移動させることはできますが、ディスクのペアを一緒にして同じスロットに入れるようにしてください。そうしなければ Panorama が正常にデータを復元できなくなるおそれがあります。

STEP 5 | M-Series アプライアンスがコレクタ グループの一部だった場合、以前の M-Series アプライアンスのシリアル番号が引き続き正しいコレクタ グループに含まれていることを確認します。

```
debug log-collector-group show name <Log CollectorGroup name>
```

STEP 6 | 移行用のディスクを準備します。

© 2019 Palo Alto Networks, Inc.

各ディスク ペアのメタデータを生成すると、インデックスが再構築されます。そのため、データ サイズによっては、プロセスの完了に長時間を要する場合があります。複数の *CLI* セッションを立ち上げ、各セッションでメタデータを再生成するコマンドを実行して各ペアのプロセスを同時に完了させれば、プロセスが迅速に進みます。詳細については、「M-Series アプライアンスの RAID ペアのメタデータを再生成」を参照してください。

1. 各ペアに対して次の CLI コマンドを実行し、ディスク ペアを有効にします。

```
admin> request system raid add <slot> force no-format
```

以下に例を示します。

```
admin> request system raid add A1 force no-format
admin> request system raid add A2 force no-format
```

引数 **force** および **no-format** は必須です。引数 **force** は、ディスク ペアを新しいアプライアンスに関連付けます。引数 **no-format** はドライブが再フォーマットされるのを回避し、ディスクに保存された口グを維持させます。

2. 各ディスク ペアのメタデータを生成します。

```
admin> request metadata-regenerate slot <slot_number>
```

以下に例を示します。

```
admin> request metadata-regenerate slot 1
```

STEP 7 | 新しい M-Series アプライアンス用のローカル ログ コレクタを設定します。

シリアル番号が必要になるコマンドを使用するステップでは、必ずシリアル番号全体を入力してください。*Tab* キーを押してもシリアル番号の一部が補完されることはありません。

この段階ではまだ新しい M-Series アプライアンスのディスクを有効化しないでください。ログの移行が正常に完了したら、Panorama が自動的にディスクを有効化します。

1. Panorama Web インターフェイスを使用して、あるいは次の CLI コマンドを使用してローカル ログ コレクタを管理対象コレクタとして設定します。

```
admin> configure
admin# set log-collector <log-collector_SN> deviceconfig system ホスト名
 <log-collector-ホスト名>
admin# exit
```

2. 変更を Panorama にコミットします。まだ変更をコレクタ グループにコミットしないでください。

```
admin> configure
admin# commit
```

3. ローカル ログ コレクタが Panorama に接続されており、そのディスク ペアのステータスが present/available であることを確認します。

© 2019 Palo Alto Networks, Inc.

```
admin> show log-collector serial-number <log-collector_SN>
```

復元プロセスのこの段階では、ディスク ペアが無効として表示されます。

STEP 8 | ディスクを持たないログ コレクタをコレクタ グループに追加します。

ここから、*Panorama* およびログ コレクタで移行プロセスを完了するために必要なコミットのみ実行します。他の変更を行うのは控えてください。

1. Panorama CLI にアクセスします。
2. Panorama の制限を上書きして、ディスクを持たないログ コレクタをコレクタ グループに追加できるようにします：**request log-migration-set-start**
3. 上書きされた制限をコミットします：

```
admin> configure
admin# commit force
```

STEP 9 | ログを移行します。

1. Panorama CLI にアクセスします。
2. 新しいローカル ログ コレクタをコレクタ グループのメンバーとして追加し、変更を Panorama にコミットします。

```
admin# set log-collector-group <collector_group_name> ogfwd-setting
 collectors <SN_managed_collector>
admin# commit
admin# exit
```

以前のローカル ログ コレクタは、まだ設定から削除していないため、引き続きメンバーのリストに表示されます。

3. ディスク ペアごとにログを新しいアプライアンスに移行します。

```
admin> request log-migration from <old_LC_serial_number> old-disk-pair
 <log_disk_pair> to <new_LC_serial_number> new-disk-pair <log_disk_pair>
```

以下に例を示します。

```
admin> request log-migration from 003001000010 old-disk-pair A to
 00300100038 new-disk-pair A
```

4. 変更を Panorama にコミットします。

```
admin> configure
admin# commit
```

STEP 10 | コレクタ グループを再設定します。

1. Web インターフェイスを使用し、ログを転送するファイアウォールに新しいログ コレクタを割り当てます（**Panorama** > **Collector Groups**（コレクタ グループ）> **Device Log Forwarding**（デバイス ログ転送））。ファイアウォール優先度リストにて、以前のログ コレクタと同じ優先度を新しいログ コレクタに付与します。

© 2019 Palo Alto Networks, Inc.

CLI を使用してファイアウォール優先度リストの優先度の割り当てを変更することはできません。

2. コレクタ グループから以前のログ コレクタを削除します。

```
admin# delete log-collector-group <group_name> logfwd-setting collectors
 <old_LC_serial_number>
```

以下に例を示します。

```
admin# delete log-collector-group DC-Collector-Group logfwd-setting
 collectors 003001000010
```

3. 以前のログ コレクタを Panorama 設定から削除し、変更を Panorama にコミットします。

```
admin# delete log-collector <old_LC_serial_number>
admin# commit
admin# exit
```

4. M-Series アプライアンス HA ピアの設定を同期します。

```
admin> request high-availability sync-to-remote running-config
```

5. コレクタ グループの変更をコミットして、管理対象ファイアウォールがログを新しいログ コレクタに送信できるようにします。

```
admin> commit-all log-collector-config log-collector-
group <collector_group_name>
```

以下に例を示します。

```
admin> commit-all log-collector-config log-collector-group DC-Collector-
Group
```

STEP 11 | 新しいログ コレクタで新しい鍵を生成します。

このコマンドは新しいログ コレクタをコレクタ グループに追加するために必要であり、交換するログ コレクタのコレクタ グループについてのみ実行する必要があります。この手順により、既存の *RSA* 鍵が削除され、*Panorama* が新しい *RSA* 鍵を作成できます。

1. Panorama CLI にアクセスします。
2. 新しいログ コレクタですべての RSA 鍵を削除します。

   request logdb update-collector-group-after-replacecollector-group <collector-group-name>

   このプロセスが完了するまで、最大 10 分間かかる場合があります。

STEP 12 | コレクタ グループのすべてのログ コレクタで SearchEngine Status (検索エンジン ステータス) が Active (アクティブ) であることを確認します。

コレクタ グループのすべてのログ コレクタで *SearchEngine Status* (検索エンジン ステータス) が *Active* (アクティブ) になるまで、続行しないでください。これにより、交換するログ コレクタからログが消去されます。

© 2019 Palo Alto Networks, Inc.

1. Panorama CLI にアクセスします。
2. 次のいずれかのコマンドを実行してログ コレクタの詳細を表示します。
   - Panorama 上のすべてのログ コレクタ：

     show log-collector all

     または、各専用ログ コレクタで次のコマンドを実行することもできます。

     ```
     show log-collector detail
     ```
3. SearchEngine Status（検索エンジン ステータス）が Active（アクティブ）であることを確認します。

```
Redistribution status:       none
```

```
Last commit-all: commit succeeded, current ring version 1
```

```
SearchEngine status:     Active
```

```
md5sum 4e5055a359f7662fab8f8c4f57e24525 updated at 2017/06/14 09:58:19
```

STEP 13 | 新しいログ コレクタで、以前のログ コレクタのシリアル番号を新しいログ コレクタのシリアル番号に置換します。

以前のログ コレクタのシリアル番号を新しいログ コレクタのシリアル番号に置換する必要があるのは、新しいログ コレクタの実行により消去の問題が発生し、消去する必要があるにもかかわらずログ コレクタが以前のデータを消去できなくなるのを防ぐためです。

1. ログ コレクタ CLI にアクセスします。
2. 以前のログ コレクタのシリアル番号を新しいログ コレクタのシリアル番号に置換します。

   request log-migration-update-logger from *<old-log-collector-serial-number>* to*<new-log-collector-serial-number>*

非 HA の Panorama で障害/RMA が発生した後のログ コレクタの移行

高可用性（HA）設定でデプロイされていない Panorama 管理サーバーでシステム障害が発生し、Panorama サーバーが HA 設定で導入されていない場合、この手順を使用して、代替 Panorama の設定を復元し、専用ログ コレクタが管理するログへ再びアクセスできるようにします。移行方法の選択肢は Panorama 管理サーバーのモデルによって異なります。

古い/故障した Panorama	新しい/交換用の Panorama
Panorama バーチャル アプライアンス	• Panorama バーチャル アプライアンス • M-200アプライアンス • M-500 アプライアンス • M-600 アプライアンス

© 2019 Palo Alto Networks, Inc.

古い/故障した Panorama	新しい/交換用の Panorama
M-100 アプライアンス	• Panorama バーチャル アプライアンス • M-200アプライアンス • M-500 アプライアンス • M-600 アプライアンス
M-500 アプライアンス	• Panorama バーチャル アプライアンス • M-200アプライアンス • M-500 アプライアンス • M-600 アプライアンス

Panorama は、専用ログ コレクタがログの保存に使用するセグメントおよびパーティションをマッピングするリング ファイルを保持します。Panorama モードの M-Series アプライアンスがリング ファイルを内部の SSD に保存する一方、Panorama バーチャル アプライアンスはリング ファイルを内部ディスクに保存します。システム障害が発生した場合、非 HA の Panorama はリング ファイルを自動的に復元できません。そのため、Panorama を交換する際にリング ファイルを復元し、専用ログ コレクタのログにアクセスできるようにしなくてはなりません。

この作業を行うには、システム障害が発生する前に Panorama 設定をバックアップおよびエクスポートしておかなければなりません。

Palo Alto Networks は *HA* 設定で *Panorama* をデプロイすることをお勧めします。ピアのいずれかを交換する必要があっても、アクティブ *Panorama* ピアは *HA* 設定のパッシブ ピアとリング ファイルを同期するため、専用ログ コレクタにアクセスできる状態が維持されます。

STEP 1 | 新しい Panorama アプライアンスの初期セットアップを実行します。

1. 必要に応じてM-Series アプライアンスをセットアップするか Panorama バーチャル アプライアンスをセットアップします。新しい M-Series アプライアンスをセットアップ中の場合は、M-Series アプライアンスのハードウェア リファレンス ガイドを参照して M-Series アプライアンスのラック マウント方法をお読みください。
2. M-Series アプライアンスの初期設定あるいは Panorama バーチャル アプライアンスの初期設定を行います。

   以前の *M-Series* アプライアンスで *Panorama* サービス (ログ収集など) に *MGT* インターフェイス以外のインターフェイスを使用していた場合、新しい *M-Series* アプライアンスの初期設定中にこれらのインターフェイスを定義する必要があります (*Panorama* > *Setup* (セットアップ) > *Interfaces* (インターフェイス))。*Panorama* バーチャル アプライアンスでは、*MGT* 以外のインターフェイスはサポートされません。
3. Panorama を登録します。
4. 新しい Panorama アプライアンスが以前のアプライアンスと同じモデルである場合のみ、以下のようにしてライセンスを移行します。そうでない場合、新しいライセンスを購入する必要があります。
   1. Palo Alto Networks カスタマーサポート Web サイトにログインします。
   2. **Assets** (アセット) タブを選択し、**Spares** (スペア) リンクをクリックします。
   3. 新しい M-Series アプライアンスの Serial Number (シリアル番号) をクリックします。
   4. **Transfer Licenses** (ライセンスを移行) をクリックします。
   5. 以前のアプライアンスを **Select** (選択) し、**Submit** (送信) をクリックします。
5. Panorama サポート ライセンスのアクティベーションを行います。

© 2019 Palo Alto Networks, Inc.

6. ファイアウォール管理ライセンスのアクティベーションを行います。
7. Panorama のコンテンツ更新とソフトウェア更新のインストールを行います。

> *M-500* アプライアンスの場合、*Panorama 7.0* 以降のバージョンでなければなりません。*M-200* および *M-600* アプライアンスは *Panorama 8.1* が必要です。ソフトウェア バージョンに関する重要な詳細情報は、「Panorama、ログ コレクタ、ファイアウォール、および WildFire のバージョン互換性」を参照してください。

STEP 2 | 古い Panorama から交換 Panorama に設定を復元します。

1. 新しい Panorama にログインし、**Panorama** > **Setup**（セットアップ）> **Operations**（操作）の順に選択します。
2. **Import named Panorama configuration snapshot**（名前を付けて保存した **Panorama** 設定スナップショットのインポート）をクリックし、バックアップ設定ファイルを **Browse**（参照）して **OK** をクリックします。
3. **Load named Panorama configuration snapshot**（名前を付けて保存した **Panorama** 設定スナップショットの読み込み）をクリックし、先ほどインポートしたファイルの **Name**（名前）を選択して **OK** をクリックします。

   > *RMA Panorama* を置き換える場合、名前付きの *Panorama* 設定スナップショットを読み込む際に必ず *Retain Rule UUIDs (*ルールの *UUID* を維持*)* してください。このオプションを選択しない場合、*Panorama* は以前のルールの *UUID* をすべて設定スナップショットから削除し、新しい *UUID* を *Panorama* 上のルールに割り当てます。つまり、ポリシールール ヒット数など、以前の *UUID* に紐付いていた情報は保持されません。
4. **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。
5. **Panorama** > **Managed Collectors** (Panorama > 管理対象コレクタ)を選択し、Connected (接続済み)列の専用ログコレクタにチェックマークが付いていることを確認します。

   専用ログコレクタが表示されない場合、次のステップに従って専用ログコレクタおよびそのコレクタ グループを設定し直す必要があります。それ以外の場合、ステップをリング ファイルを取得して、専用ログ コレクタに保存されているログへのアクセスを復元するまでスキップします。

STEP 3 | Panorama で専用ログ コレクタおよびコレクタ グループが表示されない場合はそれらを設定し直します。

1. 専用ログ コレクタの CLI にアクセスして以下のコマンドを実行し、コレクタ グループの名前を表示します。
   1. 次のコマンドを入力します。

      ```
      > request fetch ring from log-collector <serial_number>
      ```

      以下のエラーが表示されます。

      ```
      Server error: Failed to fetch ring info from <serial_number>
      ```
   2. 次のコマンドを入力します。

      ```
      > less mp-log ms.log
      ```

      以下のエラーが表示されます。

© 2019 Palo Alto Networks, Inc.

```
Dec04 11:07:08 Error:
 pan_cms_convert_resp_ring_to_file(pan_ops_cms.c:3719): Current
 configuration does not contain group CA-Collector-Group
```

この例のエラー メッセージは、CA-Collector-Group という名前のコレクタ グループが欠落していることを示します。

2. コレクタ グループを設定し、専用ログ コレクタをそのグループに割り当てます。

```
> configure
# set log-collector-group <collector-group-name>
# set log-collector-group <collector-group-name> logfwd-setting
コレクタのシリアル番号
```

3. 変更を Panorama にコミットしますが、コレクタ グループにはコミットしません。

```
# commit
# exit
```

STEP 4 | リング ファイルを取得して、専用ログ コレクタに保存されているログへのアクセスを復元します。

1. 新しい Panorama の CLI にアクセスします。
2. リング ファイルを取得します。

```
> request fetch ring from log-collector <serial-number>
```

以下に例を示します。

```
> request fetch ring from log-collector 009201000343
```



専用ログコレクタのシリアル番号が分からない場合は、*CLI*にログインして操作コマンド***show system info***を入力します。

3. 変更をコレクタ グループにコミットします。

```
> commit-all log-collector-config log-collector-group <collector-group-
name>
```

M-Series アプライアンスの RAID ペアのメタデータを再生成

M-600、M-500、または M-200 アプライアンスでシステム障害が発生した場合、アプライアンス間で物理的にディスクを移動し、必要に応じてメタデータを再生成する必要があります。メタデータは、ディスクのログを特定するために必要になります。ユーザーがログ クエリを発行した場合、クエリはこのメタデータを参照して、要求されたログ データにアクセスします。

M-Seriesアプライアンスの設定済みのRAIDディスク ペアごとに、アプライアンスのCLIにアクセスして次のコマンドを実行し、メタデータを再び生成する必要があります。

```
> request metadata-regenerate slot <slot_number>
```


© 2019 Palo Alto Networks, Inc.

以下に例を示します。

```
> request metadata-regenerate slot 1
```

メタデータの再生成にかかる時間はRAIDディスクのサイズによります。100GBごとに平均で1時間かかります。コマンドを実行する場合、コマンドが完全に実行されるまでの間、CLI セッションがロックされます。複数のCLIセッションを使用して処理を効率化することもできます。例えば、合計 4TB のログ データを持つ、1TB ドライブの 4 つの RAID ペアを交換する際、4 つの CLI セッションを立ち上げて各セッションに対してコマンドを実行し、すべてのペア/スロットでメタデータを同時に再生成する場合は約 10 時間かかります。

メタデータの再生成中は、これらの RAID ディスクが属するコレクタ グループは使用できず、ディスク ペアはロギングやレポート操作 (書き込み/クエリ) に使用できません。ただし、他のタスク (新しいファイアウォール接続の処理や管理対象ファイアウォールの設定変更の管理など) は実行できます。Panorama が管理する、この RMA プロセスの一部ではない他のすべてのコレクタ グループは、割り当てられたロギングおよびレポート機能を通常どおり実行できます。

ログ クエリ ジョブの閲覧

ログ クエリ ジョブを表示して、ログ データのクエリに予想よりも時間がかかる理由を調査して理解を深めることができます。開始するには、Panorama で実行されるすべてのログ クエリ ジョブを最初に表示する必要があります。調査の必要があるログ クエリ ジョブを特定した後は、ジョブ ID を使用してクエリに関する詳細情報を表示し、ログ クエリで問題が発生している理由をより深く理解します。Panorama でログ データをクエリする時、新しいログ クエリ ジョブが実行されると、詳細なジョブ ID 情報が上書きされます。

STEP 1 | Panorama CLI へのログイン.

STEP 2 | Panorama で実行されるログ クエリ ジョブを表示します。

CLI 出力には、ジョブ ID、クエリ実行日時、クエリのステータス、クエリされたログ データベース、クエリが結果を返すまでに要した時間 (ミリ秒単位)、クエリを実行した管理者、およびクエリに適用されたフィルタなどの、実行されるそれぞれのログ クエリに関する一般情報が含まれます。

```
admin@Panorama> show query jobs
```

```
admin@bingdot34> show query jobs

ID        Enqueue Time         State       Database  nlogs     Runtime(ms)    Us
er            Filter
------------------------------------------------------------------------------
------------------------------------------------------------------------------
42        2020/01/02 14:35:46  COMPLETE    threat    110       166.27         ad
min           ((((receive_time leq 'now')) and (((subtype eq 'file')) or ((subty
pe eq 'data')))) and ((receive_time in 'last-hour')))


41        2020/01/02 14:35:46  COMPLETE    system    110       163.84         ad
min           (((receive_time leq now)) and (receive_time in last-hour))

40        2020/01/02 14:35:46  COMPLETE    config    110       158.23         ad
min           (((receive_time leq now)) and (receive_time in last-hour))

39        2020/01/02 14:35:36  COMPLETE    config    110       162.58         ad
min           (((receive_time leq now)) and (receive_time in last-hour))

38        2020/01/02 14:35:36  COMPLETE    system    110       172.68         ad
min           (((receive_time leq now)) and (receive_time in last-hour))

37        2020/01/02 14:35:36  COMPLETE    threat    110       188.80         ad
min           ((((receive_time leq 'now')) and (((subtype eq 'file')) or ((subty
pe eq 'data')))) and ((receive_time in 'last-hour')))
```


© 2019 Palo Alto Networks, Inc.

STEP 3 | ジョブ ID を使用する特定のジョブに関する、詳細なログ クエリ情報を表示します。

```
admin@Panorama> show query jobid <Job ID>
```

```
admin@bingdot34> show query jobid 42

Serial          ID        State     Num Req   Num Proc  RTT(Max)      Avg Recs/R
TTSoftware Ver    CG                              Last Update Time
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
LOGDB           42        DONE      110       0         0.00      0.00
9.2.0           LOCAL                           2020/01/02 14:35:46

PODABCD12       42        FAILED    110       0         0.00      0.00
9.2.0           PODABCD12                       2020/01/02 14:35:46
```


© 2019 Palo Alto Networks, Inc.

RMA ファイアウォールの交換

RMA時の管理対象ファイアウォールの設定復元に必要な作業を最小限にするために、Panorama で古いファイアウォールのシリアル番号を新規ファイアウォールのシリアル番号と置き換えることができます。その後、交換用のファイアウォールに設定を復元するには、以前にファイアウォールで生成し、エクスポートしたファイアウォールステートをインポートするか、Panorama を使用して PAN-OS v5.0 以降のバージョンの管理対象ファイアウォールの部分的なデバイスステートを生成します。シリアル番号を置き換えてファイアウォールステートをインポートすることで、Panorama を使用したファイアウォールの管理を再開できます。

- ファイアウォールの部分的なデバイス状態の生成
- RMA ファイアウォール交換の前準備
- 交換後のファイアウォール設定の復元

ファイアウォールの部分的なデバイス状態の生成

Panorama では、部分的なデバイス状態を作成する際、Large Scale VPN（LSVPN）のセットアップの若干の例外を除き、管理対象ファイアウォールの設定を複製します。部分的なデバイス状態は、ファイアウォールの設定の 2 つの側面を組み合わせて作成します。

- Panorama が一元管理する設定 – Panorama は、共有ポリシールールとテンプレートのスナップショットを保持しており、これをファイアウォールにプッシュします。
- ファイアウォール側のローカル設定 – ファイアウォール設定の変更をコミットすると、ファイアウォールはローカル設定ファイルのコピーを Panorama に送信します。このファイルは Panorama に保存され、部分的なデバイス状態のバンドルをまとめるときに使用されます。

> *LSVPN* セットアップでは、*Panorama* で生成する部分的なデバイス状態のバンドルは、ファイアウォールからのエクスポート（*[Device]* > *[*セットアップ*]* > *[*操作*]* の順に選択し、*[*デバイス状態のエクスポート*]* をクリック）によって生成されるバージョンとは異なります。手動でデバイス状態のエクスポートを実行したか、*XML API* スクリプトでファイルをリモート サーバーにエクスポートするようにスケジュール設定した場合、エクスポートされたデバイス状態をファイアウォール交換ワークフローで使用できます。
>
> デバイス状態をエクスポートしていない場合、ワークフローで生成するデバイス状態には、証明書の詳細や登録済みファイアウォールなど、ダイナミック設定情報は含まれません。この設定情報は、*LSVPN* ポータルとして機能するファイアウォールの完全な設定を復元する場合に必要になります。詳細は、「RMA ファイアウォール交換の前準備」を参照してください。

デバイス状態は Panorama に保存されず、「交換後のファイアウォール設定の復元」に挙げた CLI コマンドを使用して要求されると生成されます。

RMA ファイアウォール交換の前準備

- 交換するファイアウォールのバージョンは PAN-OS 5.0.4 以降でなければなりません。Panorama は、これより古い PAN-OS バージョンを実行するファイアウォールのデバイス状態を生成できません。
- 交換するファイアウォールについて、以下の詳細事項を記録しておきます。
  - シリアル番号 – ライセンスを古いファイアウォールから交換用のファイアウォールに転送するには、Palo Alto Networks カスタマーサポート Web サイトにシリアル番号を入力する必要があります。古いシリアル番号へのすべての参照を、交換用ファイアウォールの新しいシリアル番号に置き換えるために、この情報を Panorama にも入力する必要があります。
  - （推奨）**PAN-OS** バージョンとコンテンツ データベース バージョン – 同じバージョンのソフトウェアおよびコンテンツ データベース（URL データベース ベンダーを含む）をインストールする

© 2019 Palo Alto Networks, Inc.

と、交換ファイアウォールに同じ状態を作成できます。コンテンツ データベースの最新バージョンをインストールする場合は、データベースへの更新と追加による差異がある可能性があります。ファイアウォールにインストールされているバージョンを確認するには、Panorama に保存されたファイアウォールのシステム ログにアクセスします。

- 交換ファイアウォールのデプロイを準備します。デバイス状態を一括インポートして設定を復元する間に、以下の手順を実行する必要があります。
  - 交換用のファイアウォールが古いファイアウォールと同じモデルであり、同様の操作機能が有効になっていることを確認します。各機能（交換用のファイアウォールに複数の仮想システムが必要か、ジャンボ フレームをサポートしなければならないか、CC あるいは FIPS モードで動作しなければならないか）について検討を行います。
  - ネットワーク アクセスを設定し、ライセンスを転送して、適切なバージョンの PAN-OS とコンテンツ データベースをインストールします。
- このファイアウォール交換プロセスを完了するには Panorama CLI を使用する必要があります。つまり、スーパーユーザーあるいは panorama-admin のユーザーロールがある管理者アカウントが必要になります。
- LSVPN 設定があり、サテライトまたは LSVPN ポータルとしてデプロイされている Palo Alto Networks ファイアウォールを置き換える場合、LSVPN 接続の復元に必要なダイナミック設定情報は、Panorama で生成された部分的なデバイス状態を復元するときには使用できません。推奨事項に従って LSVPN 設定のファイアウォールのデバイス状態を頻繁に生成してエクスポートした場合は、Panorama でデバイス状態を生成するのではなく、ファイアウォール自体から以前にエクスポートしたデバイス状態を使用します。

  ファイアウォールから手動でデバイス状態をエクスポートしたことがなく、Panorama で部分的なデバイス状態を生成する必要がある場合、ダイナミック設定が欠落しているとファイアウォール交換プロセスに以下のような影響があります。

  - 交換するファイアウォールが**GlobalProtect**ポータルで、サテライトのシリアル番号が明示的に設定されている場合（**Network** > **GlobalProtect** > **Portals** > **Satellite Configuration**(ネットワーク > GlobalProtect > ポータル > サテライト設定)）、ファイアウォール設定を復元するときに、ダイナミック設定が欠落していても、ポータル ファイアウォールはサテライトを正常に認証できます。認証が成功するとダイナミック設定情報が入力され、LSVPN 接続が回復します。
  - サテライト ファイアウォールを交換する場合、ポータルに接続して認証を受けることはできません。このエラーは、シリアル番号がファイアウォールに明示的に設定されていないか（**Network** > **GlobalProtect** > **Portals** > **Satellite Configuration**(ネットワーク > GlobalProtect > ポータル > サテライト設定)）、シリアル番号が明示的に設定されていない場合は、交換ファイアウォールのシリアル番号が古いファイアウォールのシリアル番号と一致しないために発生します。接続を復元するには、デバイス状態を一括インポートした後に、サテライト管理者がファイアウォールにログインし、認証情報（ユーザー名とパスワード）を入力してポータルの認証を受ける必要があります。認証後、LSVPN 接続に必要なダイナミック設定がポータルに生成されます。

  ただし、ファイアウォールが高可用性設定で構成されていた場合、設定を復元した後、ファイアウォールは実行中の設定をピアと自動的に同期して、シームレスに機能するために必要な最新のダイナミック設定を取得します。

交換後のファイアウォール設定の復元

新しいファイアウォールでファイアウォールの設定を復元するには、操作モードを設定したり、古いファイアウォールにインストールされていたものに合わせてコンテンツ リリース バージョンおよびPAN-OSソフトウェアを更新するなど、まずは新しいファイアウォールで初期設定を行う必要があります。次に古いファイアウォールのデバイス状態をPanoramaからエクスポートし、新しいファイアウォールにインポートします。最後にPanoramaに戻り、新しいファイアウォールがPanoramaに接続したことを確認してから、Panoramaとの同期を行います。

STEP 1 | 新しいファイアウォールで初期設定を実行し、ネットワーク接続を確認します。

© 2019 Palo Alto Networks, Inc.

シリアル ポート接続か SSH（Secure Shell）接続を使用して、IP アドレスと DNS サーバーの IP アドレスを追加し、新しいファイアウォールが Palo Alto Networks 更新サーバーにアクセスできることを確認します。

STEP 2 | （任意）新しいファイアウォールの操作モードが古いファイアウォールの操作モードと同じになるように設定します。

このタスクには、シリアル ポート接続が必要です。

1. 以下の CLI コマンドを入力して、ファイアウォールのメンテナンス モードにアクセスします。

```
> debug system maintenance-mode
```

2. Operational (操作)モードについては、メイン メニューで**Set FIPS Mode** (FIPS モードを設定) または**Set CCEAL 4 Mode** (CCEAL 4モードを設定)を選択します。

STEP 3 | 新しいファイアウォールでライセンスを取得します。

ライセンスを取得するには、以下のコマンドを入力します。

```
> request license fetch
```

STEP 4 | （任意）新しいファイアウォールの操作状態を古いファイアウォールの操作状態と同じになるように設定します。たとえば、古いファイアウォールでマルチ仮想システム（マルチ-vsys）機能が有効だった場合は、マルチ-vsys 機能を有効にします。

ファイアウォール設定に関連するコマンドを入力します。

```
> set system setting multi-vsys on
> set system setting jumbo-frame on
```

STEP 5 | 新しいファイアウォールの PAN-OS バージョンをアップグレードします。

古いファイアウォールにインストールされていたものと同じ PAN-OS にアップグレードする必要があります。コンテンツリリースのバージョンを古いファイアウォールにインストールされていたものと同じかそれ以降のものにアップグレードする必要があります。

以下のコマンドを入力します。

1. コンテンツ リリース バージョンをアップグレードします。

```
> request content upgrade download latest
> request content upgrade install version latest
```

2. ウイルス対策 リリース バージョンをアップグレードする方法：

```
> request anti-virus upgrade download latest
> request anti-virus upgrade install version latest
```

3. PAN-OS ソフトウェア バージョンをアップグレードします。

```
> request system software download version <version>
> request system software install version <version>
```


© 2019 Palo Alto Networks, Inc.

STEP 6 | Panorama の CLI に移動し、Secure Copy（SCP）または TFTP を使用して、デバイス状態バンドルを古いファイアウォールからコンピュータにエクスポートします（Web インターフェイスからはこれを実行できません）。



ファイアウォールから手動でデバイス状態をエクスポートした場合は、このステップを省略できます。

エクスポート コマンドは、デバイス状態バンドルを tar 圧縮ファイルとして生成し、指定された場所にエクスポートします。このデバイス状態には、LSVPN ダイナミック設定（サテライト情報と証明書の詳細）は含まれません。

以下のいずれかのコマンドを入力します。

```
> scp export device-state device <old serial#> to <login> @ <serverIP>:
 <path>
```

or

```
> tftp export device-state device <old serial#> to <login> @ <serverIP>:
 <path>
```

STEP 7 | Panorama で、古いファイアウォールのシリアル番号を新しい交換ファイアウォールのシリアル番号で置き換えます。

Panorama でシリアル番号を置き換えることで、新しいファイアウォール上に設定を復元した後、そのファイアウォールから Panorama に接続できます。

1. 操作モードで以下のコマンドを入力します。

```
> replace device old <old SN#> new <new SN#>
```

2. 設定モードに切り替え、変更をコミットします。

```
> configure
# commit
```

3. 設定モードを終了します。

```
# exit
```

STEP 8 | 新しいファイアウォールでデバイス状態をインポートし、変更をコミットします。

1. 新しいファイアウォールのWebインターフェイスにアクセスします。
2. **[Device]** > [セットアップ] > [操作] の順に選択し、[設定の管理] セクションの[デバイス状態のインポート] リンクをクリックします。
3. ファイルを参照して見つけ、**OK** をクリックします。
4. ファイアウォールで現在アクティブな設定に、変更を **Commit**（コミット）します。

STEP 9 | ファイアウォールの設定を正常に復元できたことをPanoramaから確認します。

1. Panorama Web インターフェイスにアクセスして、**Panorama** > **Managed Devices**（管理対象デバイス）の順に選択します。
2. 新しいファイアウォールの Connected（接続済み）列にチェック マークが表示されていることを確認します。

© 2019 Palo Alto Networks, Inc.

STEP 10 | ファイアウォールをPanoramaと同期します。

1. Panorama Web インターフェイスにアクセスし、**Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）の順に選択し、プッシュ スコープで **Edit Selections**（選択内容の編集）を行います。
2. **Device Groups**（デバイス グループ）を選択し、ファイアウォールを含むデバイス グループを選択して **Include Device and Network Templates**（デバイスおよびネットワーク テンプレートを含める）によってデバイスとネットワーク テンプレートを含めます。
3. **Collector Groups**（コレクタ グループ）を選択し、ファイアウォールを含むコレクタ グループを選択します。
4. **OK** をクリックして、プッシュ スコープに対する変更を保存します。
5. 変更を **Commit and Push**（コミットしてプッシュ）します。



新しいファイアウォールをインストールした後で以前のファイアウォールがまだ機能している期間についてのレポートを生成する必要がある場合は、*Panorama* のシリアル番号を置き換えてもログの情報は上書きされないため、それぞれのファイアウォールのシリアル番号について別個にクエリを生成する必要があります。

© 2019 Palo Alto Networks, Inc.

コミット エラーのトラブルシューティング

Panorama でコミットまたはプッシュ操作のエラーが発生した場合、次の条件をチェックしてください。

症状	条件	解決策
テンプレートあるいはデバイス グループのプッシュ エラー	Panorama からテンプレートおよびデバイス グループ設定の変更を受信する機能がファイアウォールで無効になっています。	ファイアウォールの Web インターフェイスにアクセスし、**Device**（デバイス）> **Setup**（セットアップ）の順に選択して、Panorama Settings（Panorama 設定）を編集し、**Enable Device and Network Template**（デバイスとネットワーク テンプレートを有効にする）および **Enable Panorama Policy and Objects**（**Panorama** ポリシーとオブジェクトを有効にする）をクリックします。
Panorama のコミット エラー、またはテンプレート、デバイス グループ、またはコレクタ グループのプッシュ エラー	Panorama 管理サーバーのソフトウェア バージョンが、管理対象の専用ログ コレクタあるいはファイアウォールのものよりも古くなっています。	Panorama 管理サーバーのソフトウェア バージョンを管理対象のファイアウォール、ログ コレクタ、WildFire アプライアンスおよびアプライアンス クラスタと同じかそれ以降のバージョンにアップグレードしてください。詳細は、「Panorama、ログ コレクタ、ファイアウォール、および WildFire のバージョン互換性」を参照してください。

© 2019 Palo Alto Networks, Inc.

登録あるいはシリアル番号のエラーのトラブルシューティング

Panoramaの登録を行った後でも M-600、M-500、または M-200 アプライアンスの**Panorama** > **Support** (Panorama > サポート)ページにサポート ライセンスの詳細が表示されない、あるいは**Panorama** > **Setup** > **Management** (Panorama > セットアップ > 管理)ページで**Serial Number** (シリアル番号)が「Unknown」と表示される場合は、次の作業を行ってください。

STEP 1 | Palo Alto Networks から送信されてきた注文処理メールに記載されている Panorama のシリアル番号を控えます。

STEP 2 | **[Panorama]** > **[セットアップ]** > **[管理]** の順に選択し、[一般設定] を編集します。

STEP 3 | **Serial Number**（シリアル番号）を入力し、**OK** をクリックします。

STEP 4 | **Commit**（コミット）> **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

© 2019 Palo Alto Networks, Inc.

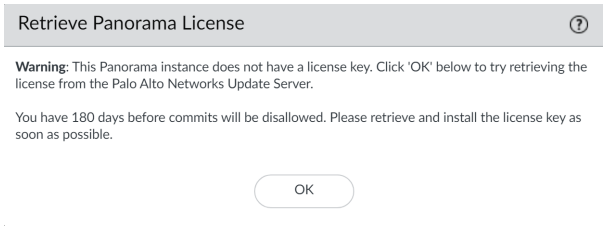
レポート エラーのトラブルシューティング

Panorama がレポートの生成に失敗した、あるいはレポートにあるはずのデータが欠けている場合は、そのコンテンツ バージョン (アプリケーション データベースなど) が管理対象コレクタおよびファイアウォールのバージョンと異なっている可能性があります。Panorama のコンテンツ バージョンは、管理対象コレクタおよびファイアウォールのコンテンツ バージョンと同じかそれより古いバージョンでなければなりません。詳細は、「Panorama、ログ コレクタ、ファイアウォール、および WildFire のバージョン互換性」を参照してください。

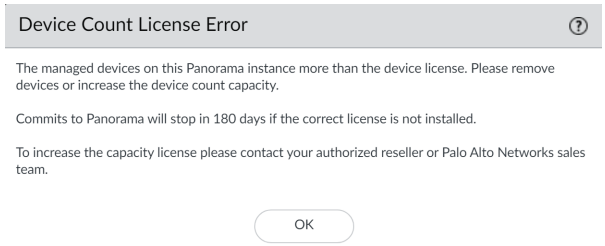
© 2019 Palo Alto Networks, Inc.

デバイス管理ライセンスエラーのトラブルシューティング

PAN-OS 8.1 にアップグレードした後、Panorama バーチャル アプライアンスによりデバイス管理ライセンスが正常にインストールされているかどうかが確認されます。デバイス管理ライセンスが正常にインストールされていないか、Panorama バーチャル アプライアンスによって管理されているファイアウォールの数がデバイス管理ライセンスの制限を超えている場合、有効なデバイス管理ライセンスをインストールするのに 180 日間かかります。有効なデバイス管理ライセンスがインストールされていない場合は、Panorama Web インターフェイスにログインするたびに次のアラートが表示されます：



Panorama バーチャル アプライアンスによって管理されるファイアウォールの数がデバイス管理ライセンスの制限を超えると、Panorama Web インターフェイスにログインするたびに次のアラートが表示されます：



解決するには、有効なデバイス管理ライセンスをインストールしてください：

STEP 1 | 適切なデバイス管理ライセンスを購入するには、Palo Alto Networks 営業担当者または認定小売業者にお問い合わせください。

STEP 2 | Panorama Web インターフェイスへのログイン。

STEP 3 | Panorama バーチャル アプライアンスがオンラインであるかオフラインであるかに基づいて、デバイス管理ライセンスを有効化/取得します。

- Panorama バーチャル アプライアンスがインターネットに接続している時のファイアウォール管理ライセンスのアクティベーション/取得。
- Panorama バーチャル アプライアンスがインターネットに接続していない時のファイアウォール管理ライセンスのアクティベーション/取得。

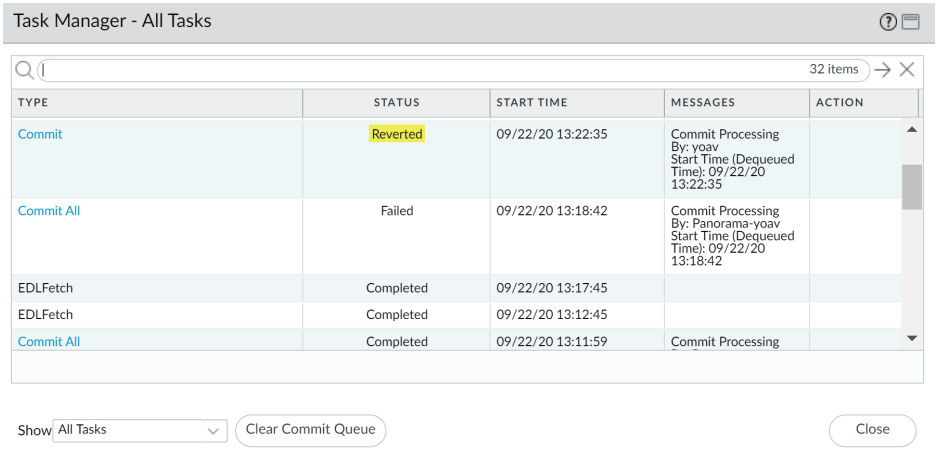
© 2019 Palo Alto Networks, Inc.

自動復帰ファイアウォール設定のトラブルシューティング

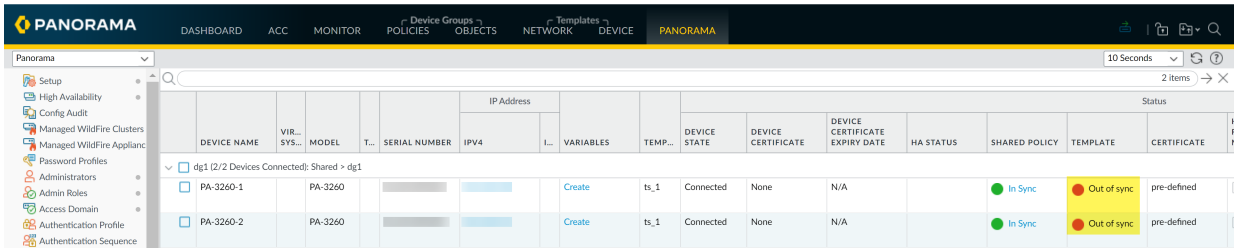
Panorama™ 管理サーバとファイアウォールの間の接続が切断される原因となった設定変更により、管理対象ファイアウォールが設定を自動で元に戻す場合、どんな変更があったかを特定し、またファイアウォールが設定を元に戻した原因となった最後の設定プッシュがどのような内容だったかを特定し、非同期のファイアウォールのトラブルシューティングを行うことができます。

STEP 1 | 管理対象ファイアウォールが、最後に実行した設定に自動で戻ったことを確認します。

- ファイアウォール側
  1. ファイアウォール Web インターフェースを起動します。
  2. （Web インターフェースの右下隅の）**Tasks**（タスク）をクリックします。
  3. 最後のコミット操作（Panorama からのプッシュまたはローカルのコミットのいずれか）が、`Reverted`（リバート済み）ステータスを示していることを確認します。



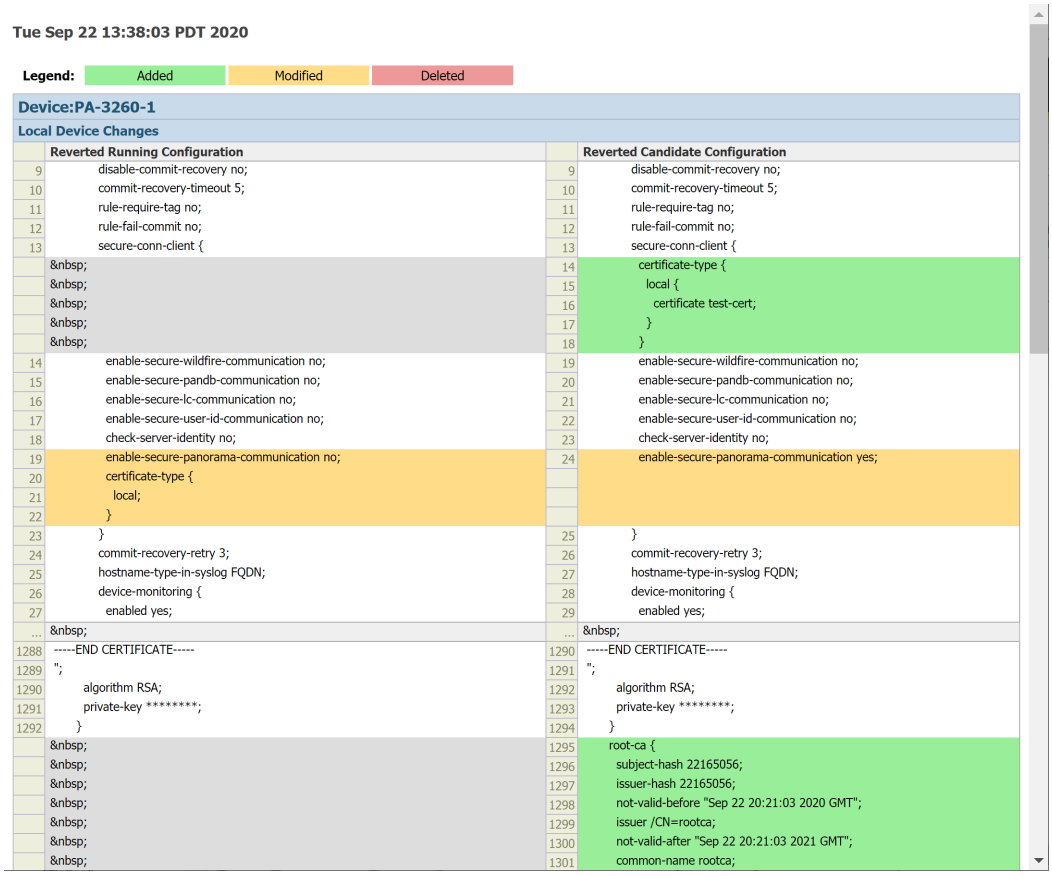
- Panorama 側
  1. Panorama Web インターフェイスへのログイン.
  2. **Panorama** > **Managed Devices**（管理対象デバイス）> **Summary**（サマリー）を選択します。
  3. 共有ポリシーとテンプレートの同期ステータスを表示します。最近 Panorama から管理対象ファイアウォールに設定をプッシュして、それが元に戻された場合、共有ポリシーまたはテンプレートは `Out of Sync`（非同期）として表示されます（設定の変更内容によって異なります）。



STEP 2 | 管理対象ファイアウォールの Last Merged Diff（最後にマージした差分）の列で、**Show Last Merged Config Diff**（最後にマージされた設定の差分を表示）（ ）を比較して、現在実行中の設定と元に戻された設定を比較します。この例では、Panorama からプッシュされたポリ

© 2019 Palo Alto Networks, Inc.

シールールにより、管理対象ファイアウォールと Panorama の間のすべてのトラフィックが拒否されたため、ファイアウォール設定が自動で元に戻っています。



Tue Sep 22 13:38:03 PDT 2020

Legend: Added Modified Deleted

Device:PA-3260-1

Local Device Changes

	Reverted Running Configuration		Reverted Candidate Configuration
9	disable-commit-recovery no;	9	disable-commit-recovery no;
10	commit-recovery-timeout 5;	10	commit-recovery-timeout 5;
11	rule-require-tag no;	11	rule-require-tag no;
12	rule-fail-commit no;	12	rule-fail-commit no;
13	secure-conn-client {	13	secure-conn-client {
		14	certificate-type {
		15	local {
		16	certificate test-cert;
		17	}
		18	}
14	enable-secure-wildfire-communication no;	19	enable-secure-wildfire-communication no;
15	enable-secure-pandb-communication no;	20	enable-secure-pandb-communication no;
16	enable-secure-lc-communication no;	21	enable-secure-lc-communication no;
17	enable-secure-user-id-communication no;	22	enable-secure-user-id-communication no;
18	check-server-identity no;	23	check-server-identity no;
19	enable-secure-panorama-communication no;	24	enable-secure-panorama-communication yes;
20	certificate-type {		
21	local;		
22	}		
23	}	25	}
24	commit-recovery-retry 3;	26	commit-recovery-retry 3;
25	hostname-type-in-syslog FQDN;	27	hostname-type-in-syslog FQDN;
26	device-monitoring {	28	device-monitoring {
27	enabled yes;	29	enabled yes;
...		...	
1288	-----END CERTIFICATE-----	1290	-----END CERTIFICATE-----
1289	";	1291	";
1290	algorithm RSA;	1292	algorithm RSA;
1291	private-key ********;	1293	private-key ********;
1292	}	1294	}
		1295	root-ca {
		1296	subject-hash 22165056;
		1297	issuer-hash 22165056;
		1298	not-valid-before "Sep 22 20:21:03 2020 GMT";
		1299	issuer /CN=rootca;
		1300	not-valid-after "Sep 22 20:21:03 2021 GMT";
		1301	common-name rootca;

STEP 3 | 設定を再度プッシュする前に、管理対象ファイアウォールと Panorama の間の接続を切断しないように、必要に応じて設定オブジェクトを変更します。

© 2019 Palo Alto Networks, Inc.

Panorama HA ピアがダウンした際の完全なコンテンツ更新

Panorama™ が高可用性 (HA) 設定になっている際に管理対象デバイスにコンテンツ更新をデプロイすると、Panorama は HA ピア間でコンテンツ更新ジョブのバランスを取り、各 Panorama の負荷を軽減します。コンテンツの更新中に HA ピアにアクセス不能になった場合、ダウン HA ピアが通常コンテンツ更新をプッシュする管理対象デバイスのコンテンツ更新ジョブは失敗します。これは、スケジュールされたコンテンツ更新と手動のコンテンツ更新の両方で発生します。コンテンツの更新を完了するには、上記の管理対象デバイスにコンテンツの更新を手動でプッシュする必要があります。

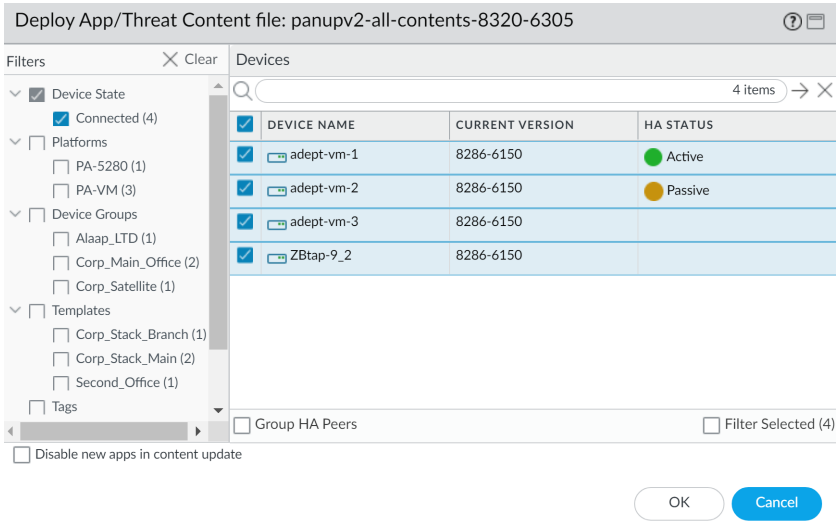
STEP 1 | Panorama CLI へのログインさらに、コンテンツ更新の負荷分散を無効にします。

```
admin> set dlsrvr distribute no
```

STEP 2 | Panorama Web インターフェイスへのログイン.

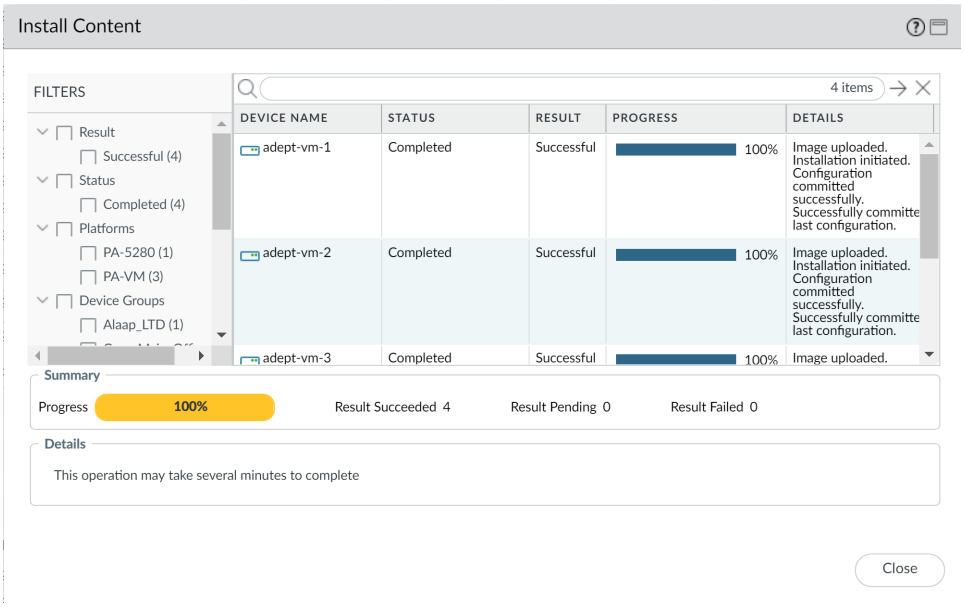
STEP 3 | **Panorama** > **Device Deployment** (デバイスのデプロイ) > **Dynamic Updates** (動的更新) を選択して、動的更新を **Install** (インストール) します。

STEP 4 | コンテンツの更新に失敗した管理対象デバイスを選択し、**OK** をクリックします。



STEP 5 | 選択した管理対象デバイスにコンテンツの更新が正常にプッシュされたことを確認します。

© 2019 Palo Alto Networks, Inc.



STEP 6 | Panorama CLI へのログインさらに、コンテンツ更新の負荷分散を有効にします。

```
admin> set dlsrvr distribute yes
```


© 2019 Palo Alto Networks, Inc.

タスクの成否の確認

Panorama Web インターフェイスの右下隅にあるタスク マネージャのアイコン  をクリックすると、タスクの成否を確認できます。タスク マネージャには、問題のデバッグに役立つ詳細メッセージも表示されます。詳細は、「Panorama タスク マネージャの使用」を参照してください。

© 2019 Palo Alto Networks, Inc.

管理対象デバイスのポリシーマッチと接続のテスト

デバイス グループおよびテンプレート スタック構成をファイアウォール、ログ コレクタ、および WF-500 アプライアンスにプッシュしたら、正しいトラフィックが管理対象デバイスにプッシュされたポリシー ルールとマッチし、ファイアウォールがすべての適切なネットワーク リソースに正常に接続することができるかをテストします。

- ポリシー ルールのトラフィックマッチのトラブルシューティング
- ネットワーク リソースへの接続のトラブルシューティング

ポリシー ルールのトラフィックマッチのトラブルシューティング

管理対象ファイアウォールのポリシーマッチテストを実行するには、管理対象デバイスのポリシー ルール構成をテストして、実行中の構成が正しいトラフィックを許可または拒否してネットワークを適切に保護していることを確認します。設定したルールにマッチしたトラフィックの結果が生成されたら、監査のため **Export to PDF (PDF** にエクスポート) することができます。

STEP 1 | Panorama Web インターフェイスへのログイン.

STEP 2 | **Panorama** > **Managed Devices (**管理対象デバイス) > **Troubleshooting (**トラブルシューティング) を選択して、ポリシーマッチを実施します。

*Policies (*ポリシー) タブからポリシーマッチテストを実行することもできます。

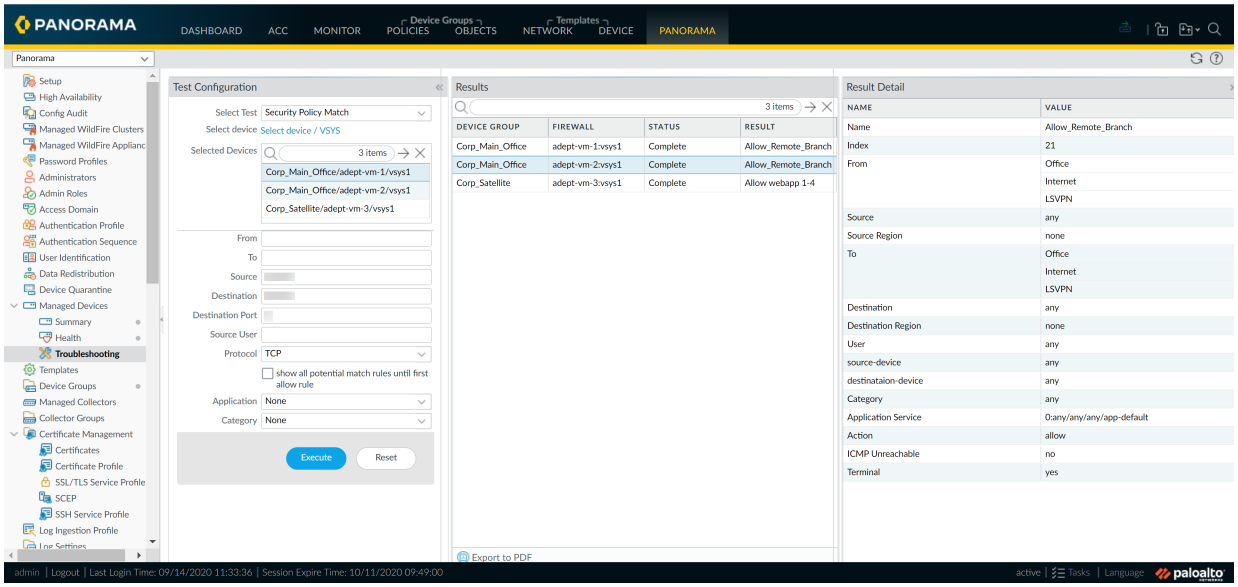
STEP 3 | ポリシーマッチテストを実行するために必要な情報を入力します。この例では、セキュリティポリシーのマッチテストが実行されます。

1. **Select Test (**テストを選択)ドロップダウンからセキュリティポリシー マッチ **(Security Policy Match)** を選択します。
2. **Select device/VSYS (**デバイス/**VSYS** を選択) し、テストする管理対象ファイアウォールを選択します。
3. トラフィックの発信元のソース IP アドレスを入力します。
4. トラフィックのターゲットデバイスの宛先 IP アドレスを入力します。
5. トラフィックに使用されるプロトコル IP を入力します。
6. 必要に応じて、セキュリティポリシー ルールのテストに関連する追加情報を入力します。

STEP 4 | セキュリティ ポリシー マッチテストを **Execute (**実行) します。

STEP 5 | セキュリティポリシーのマッチ結果を選択して、テスト条件にマッチするポリシー ルールを確認します。

© 2019 Palo Alto Networks, Inc.



ネットワーク リソースへの接続のトラブルシューティング

管理対象ファイアウォールの接続性テストを実行して、管理対象デバイスがすべての適切なネットワーク リソースに接続できていることを確認します。管理対象デバイスのデバイス構成をテストして、管理対象デバイスにプッシュされた構成により、デバイスがログ コレクタ、構成済みの外部動的リスト、Palo Alto Networks 更新サーバーなどのリソースに接続できることを確認し、実行構成がネットワークを適切に保護するようにします。さらに、ルーティング、WildFire®、Threat Vault、ping、およびトレースルート接続性テストを実行して、Panorama™ および管理対象デバイスがネットワークの運用とセキュリティに重要な外部ネットワーク リソースにアクセス可能であるかを確認することができます。結果が生成されたら、監査のため **Export to PDF (PDF にエクスポート)** することができます。

この *Ping* の接続性テストは、*PAN-OS 9.0* 以降で動作するファイアウォールのみでサポートされています。

STEP 1 | Panorama Web インターフェイスへのログイン.

STEP 2 | **Panorama** > **Managed Devices (管理対象デバイス)** > **Troubleshooting (トラブルシューティング)** を選択し、接続性テストを実行します。

Policies (ポリシー) タブからポリシーマッチテストを実行することもできます。

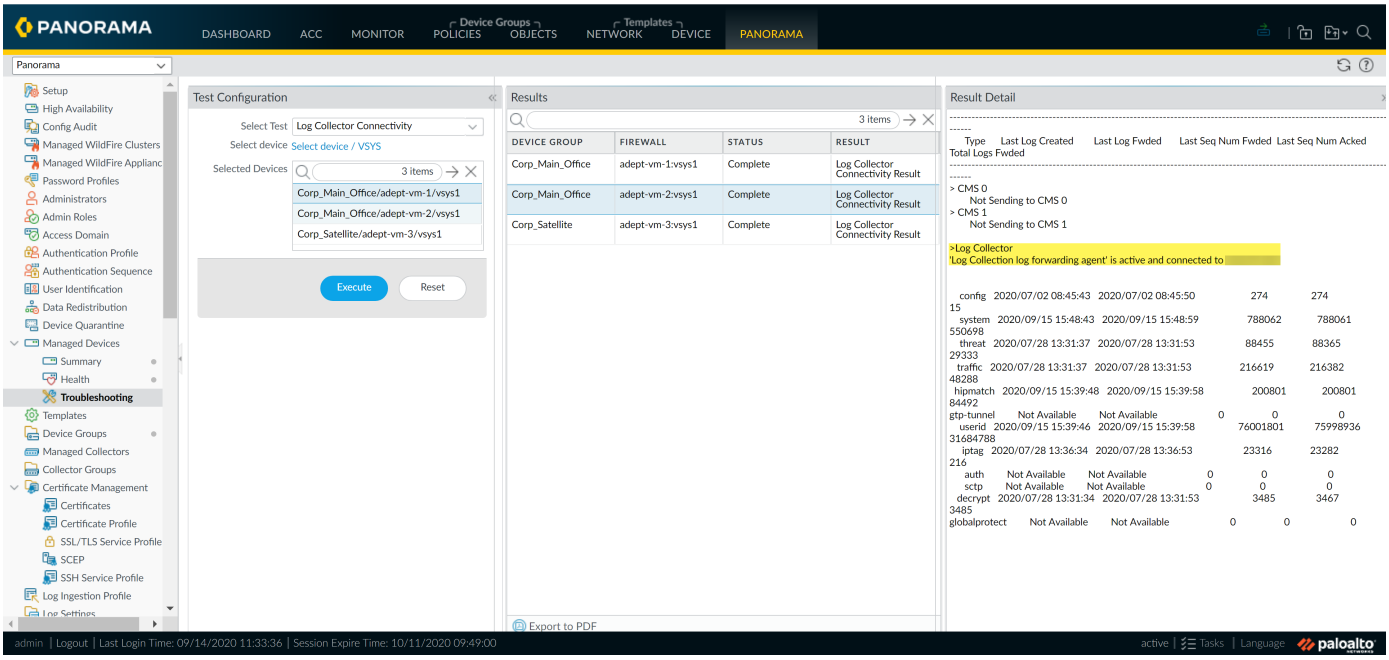
STEP 3 | 接続性テストを実行するために必要な情報を入力します。この例では、ログ コレクタ接続性テストが実行されます。

1. **Select Test (テストを選択)** ドロップダウンから **Log Collector Connectivity (ログ コレクタの接続性)** を選択します。
2. **Select device/VSYS (デバイス/VSYS を選択)** し、テストする管理対象ファイアウォールを選択します。
3. 必要に応じて、接続性テストに関連する追加情報を入力します。

STEP 4 | ログ コレクタ接続性テストを **Execute (実行)** します。

STEP 5 | 選択したデバイスのログ コレクタ接続ステータスを確認するには、ログ コレクタ接続結果を選択します。

© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

Panorama 10.0 からのダウングレード

PAN-OS® 10.0 は、専用のログ コレクタと WildFire アプライアンスのローカル管理者と Panorama 管理者を設定する機能、イーサネット インターフェースを介したログの機能、エアグリップされた Panorama™ 管理サーバーの自動動的更新、ポリシー オプティマイザでフィルタ処理されたルールに対してアクションを実行する機能、および監視、ACC、オンデマンド レポート用の追加の 60 日および 90 日フィルタ機能を導入します。ただし、これらの機能は PAN-OS 9.1 以前のリリースを実行する Panorama との互換性がありません。次のワークフローに従い、ファイアウォールをダウングレードしてから、Panorama 10.0 リリースを実行しているログ コレクタと Panorama を以前のリリースにダウングレードします。この手順は、ローカル ログ コレクタを管理するときの Panorama と、1 つ以上の専用ログ コレクタを管理するときの Panorama の両方で機能します。

Palo Alto Networks Compatibility Matrix (Palo Alto Networks 互換性マトリックス) を参照し、ダウングレード対象のファイアウォールとアプライアンスが、ダウングレード対象の *PAN-OS* リリースと互換性があることを確認します。ダウングレード可能なファイアウォールとアプライアンスについては、『Upgrade/Downgrade Considerations (アップグレードとダウングレードの考慮事項)』も参照し、ダウングレード後に変更されたり使用できなくなったりする、すべての機能と設定を考慮したことを確認してください。

STEP 1 | Panorama および管理対象デバイスの構成ファイルのバックアップを保存します。

1. **Export Panorama and device configuration snapshot** (**Panorama** とデバイスの設定スナップショットをエクスポート) (**Panorama** > **Setup** (セットアップ) > **Operations** (操作)) により、設定スナップショットをエクスポートします。
2. エクスポートされた .tgz ファイルを、Panorama、ログ コレクタ、ファイアウォール以外の場所に保存します。問題が発生して最初からやり直さなければならなくなった場合は、このバックアップを使用して設定を復元できます。

STEP 2 | 専用のログ コレクタの認証を設定済みで、**admin** 管理者を削除した場合は、新しい **admin** ユーザーを設定して専用のログ コレクタにプッシュします。

PAN-OS 9.1 以前のリリースにダウングレードするためには、専用のログ コレクタに `admin` ユーザーを設定する必要があります。

STEP 3 | PAN-OS 10.0 リリースを実行している各ファイアウォールをダウングレードします。

複数のファイアウォールをダウングレードする場合は、各ファイアウォール固有の *PAN-OS 9.1* イメージを *Panorama* にダウンロードしてからダウングレードを開始し、プロセスを効率化します。たとえば、*PA-220* のファイアウォールを *PAN-OS 9.1.0* にダウングレードするには、*`PanOS_220-9.1.0`* または *`PanOS_3000-9.1.0`* イメージをダウンロードします。

Panorama では、すべてのファイアウォールが同じかそれ以下の PAN-OS リリースを実行している必要があります。そのため、Panorama をダウングレードする前に、環境に従って次のうち適切なタスクを利用して繰り返し、必要に応じてすべての管理対象ファイアウォールをダウングレードします。

1. **Check Now** (今すぐチェック) により、使用可能なイメージを確認します (**Panorama** > **Device Deployment** (デバイスのデプロイ) > **Software** (ソフトウェア))。
2. ダウングレードするファイアウォールのモデルまたはシリーズごとに、PAN-OS 9.1 イメージを探します。イメージをまだダウンロードしていない場合は、**Download** (ダウンロード) します。

非 **HA** ファイアウォール

© 2019 Palo Alto Networks, Inc.

適切な PAN-OS 9.1 バージョンを（アクション列）**Install**（インストール）し、ダウングレードするすべてのファイアウォールを選択してから **Reboot device after install**（インストール後にデバイスを再起動）を選択して **OK** をクリックします。

アクティブ/アクティブ **HA** ファイアウォール

1. **Install**（インストール）をクリックし、**Group HA Peers**（グループ **HA** ピア）をオフにし、いずれかの HA ピアを選択し、さらに **Reboot device after install**（インストール後にデバイスを再起動）を選択して **OK** をクリックします。ファイアウォールの再起動が完了するのを待ってから、続行してください。
2. **Install**（インストール）をクリックし、**Group HA Peers**（グループ **HA** ピア）をオフにし、前の手順でアップデートしていない HA ピアを選択し、さらに**Reboot device after install**（インストール後にデバイスを再起動）を選択して **OK** をクリックします。

アクティブ/パッシブ **HA** ファイアウォール

この例では、アクティブ ファイアウォールの名前が fw1、パッシブ ファイアウォールの名前が fw2 です。

1. 適切なアップデートを **Install** (インストール) (アクション列) して **Group HA Peers** (グループ **HA** ピア) を無効 (クリア) にし、fw2 を選択した後に **Reboot device after install** (インストール後にデバイスを再起動) を選択してから **OK** をクリックします。
2. fw2 の再起動が完了したら、fw1 (**Dashboard** (ダッシュボード) > **High Availability** (高可用性)ウィジェット) が現在もアクティブピアであり、fw2 がパッシブ ピアであること (ローカル ファイアウォールの状態が `active`、Peer-fw2 が `passive` であること) を確認します。
3. fw1 にアクセスし、**Suspend local device**（ローカル デバイスをサスペンド）（**Device**（デバイス）> **High Availability**（高可用性）> **Operational Commands**（操作コマンド））を選択します。
4. fw2 にアクセス (**Dashboard** (ダッシュボード) > **High Availability** (高可用性)) し、ローカル ファイアウォールの状態が `active` で、ピア ファイアウォール fw1 が `suspended` になっていることを確認します。
5. Panorama にアクセスして **Panorama** > **Device Deployment** (デバイスのデプロイ) > **Software** (ソフトウェア) を選択し、適切な更新を **Install** (インストール) (アクション列) した後に **Group HA Peers** (グループ **HA** ピア) を無効 (クリア) にし、fw1 を選択して **Reboot device after install** (インストール後にデバイスを再起動) を選択して、**OK** をクリックします。fw1 の再起動が完了するまで待ってから、続行します。
6. fw1 にアクセス (**Dashboard** (ダッシュボード) > **High Availability** (高可用性)ウィジット) し、ローカル ファイアウォールの状態が `passive` で、ピア fw2 が `active` になっていることを確認します。



選択設定でプリエンプションを有効にした場合（*Device*（デバイス）> *High Availability*（高可用性）> *General*（全般））、*fw1* は再起動後にアクティブ ピアとして復帰します。

STEP 4 | Panorama 10.0 を実行している各ログ コレクタをダウングレードします。

1. **Check Now**（今すぐチェック）により、使用可能なイメージを確認します（**Panorama** > **Device Deployment**（デバイスのデプロイ）> **Software**（ソフトウェア））。
2. Panorama 9.1 イメージを探します。イメージをまだダウンロードしていない場合は、**Download**（ダウンロード）します（Action（アクション）列）。
3. ダウンロードが完了したら、Panorama 10.0 を実行している各ログ コレクタにイメージを **Install**（インストール）します。アップグレードの完了時に、デバイスを自動的に再起動するには、**Reboot device after install** (インストール後にデバイスを再起動) を選択します。

STEP 5 | Panorama をダウングレードします。

1. **Check Now**（今すぐチェック）により、使用可能なイメージを確認します（**Panorama** > **Device Deployment**（デバイスのデプロイ）> **Software**（ソフトウェア））。

© 2019 Palo Alto Networks, Inc.

2. Panorama 9.1 イメージを探します。イメージをまだダウンロードしていない場合は、**Download**（ダウンロード）します。
3. ダウンロードが完了したら、Panorama にイメージを **Install**（インストール）します。
4. 次のように Panorama を再起動します。
   - 再起動を促されたら、**Yes**（はい）をクリックします。**CMS Login**（**CMS** ログイン）画面が表示された場合は、ユーザー名やパスワードを入力せずに Enter を押します。Panorama のログインプロンプトが表示されたら、初期設定時に設定したユーザー名およびパスワードを入力します。
   - 再起動を促されなかったら、**Panorama** > **Setup**（セットアップ）> **Operations**（操作）の順に選択し、**Reboot Panorama**（**Panorama** の再起動）をクリックします（デバイスの操作）。

STEP 6 | Panorama ログを PAN-OS 8.1 ログ形式へ移行します。

移行中、ログデータは *ACC* またはモニタータブには表示されません。さらに、移行が完了するまで、新しいログデータはログ コレクタに転送されることはありません。

1. 着信ログギング レートを確認します。

   着信ログ率が低いときに、ログの移行を開始することをお薦めします。率を確認するには、ログ コレクタの CLI から次のコマンドを実行します。

```
admin@FC-M500-1> debug log-collector log-collection-stats show incoming-logs
```

   ログの移行中は *CPU* 利用率が高くなる（*100%* に迫る）ことが予想されますが、操作は通常どおりに機能し続けます。リソースが競合する場合は、着信ログとその他のプロセスが優先されて、ログ移行は抑制されます。
2. 各ログ コレクタで、以前の形式へのログ移行を開始します。

   移行を開始するには、各ログ コレクタの CLI から次のコマンドを入力します。

```
admin@FC-M500-1> request logdb migrate lc serial-number <ser_num> 開始日:
```

3. ログ移行の状態を確認し、以前の形式への既存のすべてのログが移行にかかる時間を見積もります。

```
admin@FC-M500-1> request logdb migrate lc serial-number <ser_num>
 Status（状態） Slot: all
Migration State: In Progress
Percent Complete: 0.04
Estimated Time Remaining: 451 hour(s) 47 min(s)
```