paloalto TECHDOCS

PAN-OS アップグレード ガイド

Version 11.1 & later

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Last Revised

May 22, 2024

Table of Contents

ソフトウェアおよびコンテンツ更新

PAN-OS は、すべての Palo Alto Networks 次世代ファイアウォールを実行するソフトウェアです。また、Palo Alto Networks は、最新のセキュリティ機能をファイアウォールに装備するためのアップデートも頻繁に発行しています。ファイアウォールは、ファイアウォールの設定を更新しなくても、コンテンツの更新が提供するアプリケーションや脅威のシグネチャ (など) に基づいてポリシーを適用することができます。

物理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環として物理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、実行中の新しいソフトウェア更新が正常に認識され、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。

PAN-OS ソフトウェア更新

PAN-OS は、すべての Palo Alto Networks 次世代ファイアウォールを実行するソフトウェアです。PAN-OS ソフトウェアのバージョンは、ファイアウォール **Dashboard (**ダッシュボード**)** に表示されます。

ファイアウォールで直接、または Palo Alto Networks サポートポータルで、新しい PAN-OS リリースを確認できます。ファイアウォールを最新バージョンの PAN-OS にアップグレードするには、次の手順を実行します。

STEP 1 | 最新情報については、最新の PAN-OS リリースノートを確認してください。また、アップグレード/ダウングレードに関する考慮事項を見て、PAN-OS リリースで導入される可能性のあるすべての変更を理解していることを確認してください。

STEP 2 | PAN-OS の新しいリリースを確認します。

- **On the support portal (**サポートポータルの場合**)**– support.paloaltonetworks.com へアクセスし、左側のメニューバーで、**Updates** > **Software Updates (**ソフトウェアアップデートの更新**)** を選択します。ファイアウォールをアップグレードするために使用したいリリースをダウンロードして保存します。
- **On the firewall (**ファイアウォールの場合**)**–ファイアウォールで、**Device** > **Software (**デバイスソフトウェア**)** と **Check Now (**今すぐチェック**)** を選択して、新しい PAN-OS リリースバージョンについて Palo Alto Networks Update Server で確認します。

ソフトウェアアップデートの確認に問題がありますか?一般的な接続の問題の解決策については、この記事を参照してください。

STEP 3 | 必要なリリース バージョンを決定したら、完全なワークフローに従ってFirewall を PAN-OS 11.1 にアップグレードするします。実行する手順は、現在実行しているリリースバージョン、HA を使用しているかどうか、および Panorama を使用して firewall を管理しているかどうかによって異なります。

動的コンテンツ更新

Palo Alto Networks は、ファイアウォールがセキュリティポリシーを適用するために使用する更新を頻繁に発行しており、PAN-OS ソフトウェアをアップグレードしたり、ファイアウォールの設定を変更したりする必要はありません。これらのアップデートにより、ファイアウォールが最新のセキュリティ機能と脅威インテリジェンスを得られます。

アプリケーションの更新プログラムと一部のウイルス対策更新 (ファイアウォールが受け取ることができるもの) を除いて、使用可能な動的コンテンツの更新は サブスクリプション に依存する可能性があります。各動的コンテンツ更新のスケジュールを設定すると、ファイアウォールが新しい更新の有無を確認し、ダウンロードまたはインストールする頻度を定義することができます (**Device (デバイス) > Dynamic Updates (動的更新)**)。

動的コンテンツ更新	このパッケージの中身とは？
Antivirus [アンチウイルス]	ウイルス対策の更新プログラムは 24 時間ごとにリリースされ、新たに検出されたマルウェアの • WildFire シグネチャが含まれます。これらの更新プログラムを 1 日1回ではなく 5 分ごとに取得するには、WildFire サブスクリプション が必要です。 • (脅威防止が必要)C2 トラフィックの特定のパターンを検出する自動生成されたコマンド アンド コントロール(C2)シグネチャ。これらのシグネチャにより、firewall は、C2 ホストが不明であるか、急速に変化する場合でも、C2 アクティビティを検出できます。 • (脅威防止が必要)組み込みの外部動的リストの新規および更新されたリストエントリ。これらのリストには、悪意のある、危険度が高く、防弾のホスト提供の IP アドレスが含まれており、悪意のあるホストからユーザーを保護するのに役立ちます。 • (脅威防止が必要)firewall が既知の悪意のあるドメインを識別するために使用する DNS 署名のローカル セットの更新。DNS シンクホールをセットアップしている場合、ファイアウォールは、これらのドメインに接続しようとするネットワーク上のホストを識別できます。firewall がドメインを DNSシグネチャの完全なデータベースと照合できるようにするには、DNS Security を設定します。
アプリケーション	アプリケーション更新は、新規あるいは更新されたアプリケーション シグネチャまたは App-ID を提供します。この更新に追加のサブスクリプションは不要ですが、有効なメンテナンス/サポートの連絡先が必要です。新しいアプリケーションの更新は、必要なポリシーの更新を事前に準備する時間を与えるために、毎月第 3 火曜日にのみ発行されます。 まれに、新しい *App-ID* を含む更新プログラムの公開が *1* 日または *2* 日遅れる場合があります。

動的コンテンツ更新	このパッケージの中身とは？
	アプリケーション ID の変更は、より頻繁にリリースされます。新規および変更済みの App-ID により、ファイアウォールはセキュリティ ポリシーの精度を常に向上させることができますが、その結果として、セキュリティ ポリシーの適用の変更がアプリケーションの可用性に影響します。アプリケーションの更新を最大限に活用するには、のヒントに従って、新しいアプリ ID と変更されたアプリ ID を管理します。
アプリケーションおよび脅威	新規および更新されたアプリケーション、および脅威シグネチャを含みます。この更新は、脅威防御サブスクリプションを購入している場合 (この場合、プリケーション更新の代わりにこの更新を取得) に入手できます。新しい脅威更新は、時に週に複数回など、更新された App-ID と共に頻繁に発行されます。新しいアプリ ID は、毎月第 3 火曜日にのみ発行されます。 まれに、新しい *App-ID* を含む更新プログラムの公開が *1* 日または *2* 日遅れる場合があります。 ファイアウォールは、可用性の 30 分以内に最新の脅威とアプリケーションの更新を取得できます。 アプリケーションと脅威の更新を有効にして、アプリケーションの可用性と最新の脅威に対する保護の両方を確保する最適な方法については、アプリケーションおよび脅威コンテンツ更新のベストプラクティスを確認してください。
Device Dictionary **Device Dictionary**	デバイス ディクショナリは、Device-ID に基づくセキュリティ ポリシー ルールで使用する firewall 用の XML ファイルです。さまざまなデバイス属性のエントリが含まれており、定期的に完全に更新され、更新サーバーに新しいファイルとして投稿されます。辞書エントリに変更があった場合、改訂されたファイルが更新サーバーに投稿され、Panorama と firewall が次回更新サーバーをチェックするときに自動的にダウンロードしてインストールします。
GlobalProtect データファイル	GlobalProtect アプリによって返されるホスト情報プロファイル (HIP) データを定義および評価するためのベンダー固有情報を含みます。これらの更新を取得するには、GlobalProtect ゲートウェイのサブスクリプションが必要です。さらに、GlobalProtect を機能させるには、更新のためのスケジュールを作成しておく必要があります。
GlobalProtect クライアントレス **VPN**	GlobalProtect ポータルから一般的なウェブアプリケーションへのクライアントレス VPN アクセスを可能にする新しいおよび更新されたアプリケーション シグネチャが含まれます。これらの更新を取得するには、GlobalProtect サブスクリプションが必要です。さらに、GlobalProtect クライアントレス VPN を機能させるには、更新のためのスケジュールを作成しておく必要があります。ベストプラクティス

動的コンテンツ更新	このパッケージの中身とは？
	として、GlobalProtect Clientless VPN の最新のコンテンツ更新を常にインストールすることをお勧めします。
WildFire	リアルタイムで WildFire パブリック クラウドにより生成されたマルウェアとウイルス対策のシグネチャへのアクセスを提供します。オプションで、PAN-OS が WildFire シグネチャ更新パッケージを取得するように設定することができます。最速で 1 分に一度という頻度で新しい更新を確認するようにファイアウォールを設定し、最新の WildFire シグネチャが利用できるようになってから 1 分以内にファイアウォールが更新を受信するように設定することができます。WildFire サブスクリプションがない場合、シグネチャがアンチウイルス アップデートで提供されるまで 24 時間以上待つ必要があります。
WF プライベート	WildFire アプライアンスで分析を実行し、その結果として作成したマルウェアおよびアンチウイルス シグネチャをほぼリアルタイムに提供します。WildFire アプライアンスからコンテンツ更新を受信するために、ファイアウォールおよびアプライアンスの両方が PAN-OS 6.1 以降のバージョンを実行しており、ファイアウォールがファイルおよびメールリンクを WildFire プライベート クラウドに転送するように設定する必要があります。

コンテンツ更新のインストール

常に最新の脅威 (まだ発見されていない脅威を含む) から保護されるようにするため、Palo Alto Networks から公開される最新のコンテンツ/ソフトウェア アップデートにより、使用するファイアウォールが常に最新の状態に維持されるようにする必要があります。使用できる動的コンテンツ更新は、所有している subscriptions によって異なります。

各ステップに従い、コンテンツ更新をインストールします。また、コンテンツ更新のスケジュールを設定し、ファイアウォールが更新を取得してインストールする間隔を定義することもできます。

アプリケーションと脅威のコンテンツの更新は、他の種類の更新とは動作が少し異なります。最新のアプリケーション知識と脅威防止を最大限に活用するには、こちらの手順ではなく、ガイドラインに従ってアプリケーションのデプロイと脅威コンテンツの更新してください。

STEP 1 | ファイアウォールが更新サーバーにアクセスできることを確認します。

1. 既定では、ファイアウォールは **updates.paloaltonetworks.com** の **Update Server** にアクセスし、ファイアウォールが最も近いサーバーからコンテンツの更新を受信するようにします。ファイアウォールでインターネットへのアクセスが制限されている場合は、更新プログラムのダウンロードに関連するサーバーへのアクセスを有効にする許可一覧を構成する必要があります。コンテンツ更新サーバーの詳細については、動的更新用のコンテンツ配信ネットワーク インフラストラクチャを参照してください。参照情報を追加したい場合、または接続が発生してダウンロードの問題が発生している場合は、https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000001UtRCAUを参照してください。

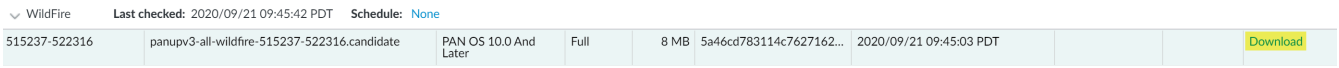
   デバイスが中国本土にある場合、*Palo Alto Networks*では、アップデートダウンロードに ***updates.paloaltonetworks.cn*** サーバーを使用することをお勧めします。

2. （任意）サーバーのSSL証明書が信頼できる機関によって署名されているかどうかファイアウォールに確認させ、さらに厳重な検証を行いたい場合は**Verify Update Server Identity**[更新サーバーの身元を検証]をクリックします。これはデフォルトで有効になっています。
3. （任意）ファイアウォールがプロキシ サーバーを使用して Palo Alto Networks アップデート サービスにアクセスする必要がある場合は、**Proxy Server (**プロキシ サーバー**)** ウィンドウで以下の情報を入力します。
   - **Server** [サーバー] – プロキシ サーバーの IP アドレスまたはホスト名。
   - **Port** [ポート] – プロキシ サーバーのポート。範囲:1～65535
   - **User** [ユーザー] – サーバーにアクセスするユーザー名。
   - **Password** [パスワード] – プロキシ サーバーにアクセスするユーザーのパスワード。**Confirm Password** [再入力 パスワード]にパスワードを再入力します。
4. (任意) 接続障害が発生した場合、最大3回の再接続試行を設定します。**debug set-content-download-retry attempts** を使用して、接続試行回数を設定します。デフォルトは 0 です。

STEP 2 | 最新のコンテンツ アップデートがあるかどうか確認します。

Device (デバイス) > Dynamic Updates (動的更新) を選択し、ウィンドウの左下にある **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]列のリンクは、更新が入手可能かどうかを示します。

- **Download** [ダウンロード] – 新しい更新ファイルが入手可能なことを示します。リンクをクリックし、ファイアウォールへのファイルの直接ダウンロードを開始します。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。



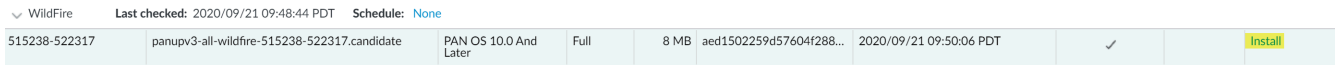
アプリケーションおよび脅威アップデートをインストールするまでは、アンチウイルス アップデートをダウンロードできません。

- **Revert** [戻す] – 以前にインストールしたバージョンのコンテンツまたはソフトウェアバージョンが入手可能なことを示します。以前にインストールしたバージョンに戻すことができます。

STEP 3 | コンテンツ更新をインストールします。

インストールには最長で、*PA-220* ファイアウォールの場合には *10* 分、*PA-5200 Series*、*PA-7000 Series*、または *VM Series* のファイアウォールの場合には *2* 分かかります。

Action[アクション] 列の **Install**[インストール] リンクをクリックします。インストールが完了すると、**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。



STEP 4 | 各コンテンツ アップデートのスケジュール設定を行います。

スケジュールする更新ごとにこの手順を繰り返します。

ファイアウォールが一度にダウンロードできる更新は *1* つのみであるため、スケジュールが重ならないように調整します。複数の更新を同じ期間にダウンロードするようにスケジュールすると、最初のダウンロードだけが成功します。

1. **None** [なし]リンクをクリックすることにより、各更新タイプのスケジュールを設定します。

2. [繰り返し] ドロップダウン リストから値を選択して更新の頻度を指定します。利用できる値はコンテンツのタイプによって異なります (WildFire 更新は、**Real-time (リアルタイム)**、**Every Minute (毎分)**、**Every 15 Minutes (15分毎)**、**Every 30 minutes (30分毎)**、または**Every Hour (1時間毎)** で利用でき、アプリケーションおよび脅威の更新は、**Weekly (毎週)**、**Daily (毎日)**、**Hourly (毎時)**、**Every 30 Minutes (30分毎)** で

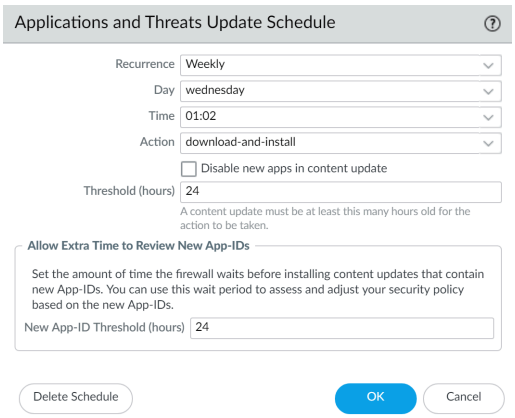
スケジュール設定でき、アンチウイルスの更新は、**Hourly** (毎時)、**Daily** (毎日)、または**Weekly** (毎週) でスケジュール設定できます)。

アプリケーションと脅威またはウイルス対策の更新プログラムに対して**None**(手動)を選択することもできます。つまり、このアイテムには定期的なスケジュールはなく、更新プログラムを手動でインストールする必要があります。スケジュール ノードを完全に削除するには、スケジュールの削除 を選択します。

3. **Time** [日時]（または、WildFire の場合には経過分数）、および該当する場合は、選択した **Recurrence** [繰り返し]値に応じて更新する **Day** [曜日]を指定します。
4. システムで **Download Only** (ダウンロードのみ) を実行するか、またはベスト プラクティスとして更新を **Download And Install** (ダウンロードおよびインストール) するかを指定します。
5. リリースされてからコンテンツ更新を実行するまでの待機時間を**Threshold (Hours)** [しきい値（時間）]に入力します。まれに、コンテンツ更新の中でエラーが見つかることがあります。このため、リリースされてから一定の時間が経過するまで、新しい更新のインストールを延期することが可能です。

   100% 使用可能である必要があるミッション クリティカルなアプリケーションがある場合は、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のしきい値を最低 *24* 時間以上に設定し、アプリケーションおよび脅威コンテンツ更新のベストプラクティスに従います。さらに、スケジュールを設定した後、コンテンツの更新の予約は *1* 回限りまたは低頻度ですが、スケジュール設定後は、コンテンツ リリースに含まれている新規および変更済みの App-ID の管理を続行する必要があります。これは、こうした *App-ID* によりどのようにセキュリティ ポリシーが実施されるかを変更できるためです。

6. (任意) **New App-ID Thresholds** (新規 **App-ID** しきい値) を時間単位で入力して、新しい App-ID を含むコンテンツ更新をインストールする前に、ファイアウォールが待機する時間を設定します。



7. **[OK]** をクリックしてスケジュールの設定を保存します。
8. **Commit** [コミット]をクリックして、現在アクティブな設定に対する設定値を保存します。

STEP 5 | PAN-OS をアップデートします。

*PAN-OS*のアップデートを行う前に、必ずコンテンツをアップデートしてください。*PAN-OS*の各バージョンにはサポートされているコンテンツリリースの最低バージョンが指定されています。

1. リリースノートを確認します。
2. PAN-OS ソフトウェアのアップデートを行います。

アプリケーションおよび脅威コンテンツの更新

アプリケーションおよび脅威コンテンツの更新により、最新のアプリケーションおよび脅威のシグネチャがファイアウォールに配信されます。パッケージのアプリケーション部分には、新しく変更された App-ID が含まれており、ライセンスは必要ありません。新しい脅威シグネチャと変更された脅威シグネチャを含む完全なアプリケーションと脅威のコンテンツ パッケージには、脅威防止ライセンスが必要です。ファイアウォールは、カスタム設定に基づいて最新のアプリケーションと脅威シグネチャを自動的に取得してインストールするため、追加の設定なしで最新の App-ID と脅威の保護に基づいてセキュリティ ポリシーを適用し始めます。

新しい脅威シグネチャや変更された脅威シグネチャ、および変更された App-ID は、少なくとも週に 1 回、頻繁にリリースされます。新しい App-ID は各月の第 3 火曜日にリリースされます。

まれに、新しい *App-ID* を含む更新プログラムの公開が *1* 日または *2* 日遅れる場合があります。

新しい App-ID はセキュリティ ポリシーがトラフィックをどのように適用するかを変更することができるため、セキュリティ ポリシーを準備して更新するための予測可能なウィンドウを提供することを目的としています。さらに、コンテンツの更新は累積的です。つまり、最新のコンテンツ更新には、常に以前のバージョンでリリースされたアプリケーションおよび脅威シグネチャが含まれています。

アプリケーション シグネチャでアプリケーションを識別し、脅威シグネチャでトラフィックを検査できるようにする同じデコーダであるアプリケーションと脅威シグネチャが 1 つのパッケージで提供されるため、シグネチャを一緒に配布するか個別に配布するかを検討する必要があります。コンテンツの更新をデプロイする方法は、組織のネットワーク セキュリティとアプリケーションの可用性要件によって異なります。出発点として、あなたの組織が以下のいずれかの姿勢をとっていることを確認します（または、おそらくどちらの場合でも、ファイアウォールの場所によって異なります）。

- セキュリティ ファーストを重視する組織は、アプリケーションの可用性よりも、最新の脅威シグネチャを使用することによって保護を優先します。脅威防止機能を確保するために使用するのは、主にファイアウォールです。セキュリティ ポリシーがアプリケーション トラフィックをどのように強制するかに影響を与える App-ID の変更はすべてセカンダリです。
- ミッション クリティカルなネットワークは、最新の脅威シグネチャによって保護を行うことよりも、アプリケーションの可用性を優先します。ネットワークはダウンタイムを許容しません。ファイアウォールはインラインでデプロイされてセキュリティポリシーを適用します。セキュリティポリシーで App-ID を使用している場合、App-ID に影響するコンテンツ リリース導入にどのような変更を加えても、ダウンタイムが生じるおそれがあります。

コンテンツ更新のデプロイを行うにあたり、ミッション クリティカルあるいはセキュリティ ファーストのアプローチ、あるいは両方のアプローチを組み合わせてビジネスニーズを満たすことができます。アプリケーションおよび脅威コンテンツ更新のベストプラクティスを確認して検討し、アプリケーションと脅威の更新を実装する方法を決定します。それから：

- アプリケーションのデプロイと脅威コンテンツの更新を行います。
- コンテンツ更新に関するヒントに従ってください。

スケジュールを設定した後、コンテンツの更新の予約は *1* 回限りまたは低頻度ですが、スケジュール設定後は、コンテンツ リリースに含まれている新規および変更済みの App-ID の管理を続行する必要があります。これは、こうした *App-ID* によりどのようにセキュリティ ポリシーが実施されるかを変更できるためです。

アプリケーションのデプロイと脅威コンテンツの更新

アプリケーションと脅威コンテンツの更新を構成する手順を実行する前に、アプリケーションおよび脅威コンテンツの更新しくみを理解し、アプリケーションおよび脅威コンテンツ更新のベストプラクティスの実装方法を決定します。

さらに、Panorama を使用すると、コンテンツの更新をファイアウォールに簡単かつ迅速にデプロイできます。Panorama を使用してファイアウォールを管理している場合は、以下で紹介する方法の代わりに、 コンテンツの更新をデプロイするためのステップ に従ってください。

STEP 1 | アプリケーションと脅威の完全なコンテンツ パッケージのロックを解除するには、脅威防止ライセンスを入手し、ファイアウォールでライセンスを有効にします。

1. **Device > Licenses (**デバイス **>** ライセンス**)**を選択します。
2. 手動でライセンス キーをアップロードするか、Palo Alto Networks ライセンス サーバーから取得します。
3. 脅威防止ライセンスがアクティブであることを確認します。

STEP 2 | ファイアウォールがコンテンツ更新を取得してインストールするスケジュールを設定します。

次の手順を完了するときは、組織が mission-critical or security-first (またはその両方の組み合わせ) であるかどうかを検討し、アプリケーションおよび脅威コンテンツ更新のベストプラクティスを確認することが特に重要です。

1. **Device**（デバイス） > **Dynamic Updates**（動的更新）を選択します。
2. アプリケーションの**Schedule**（スケジュール）と脅威コンテンツの更新を選択します。
3. ファイアウォールが Palo Alto Networks アップデート サーバーで新しいアプリケーションと脅威のコンテンツ リリース、および **Day**（本日）と **Time**（時刻）を確認する頻度（ **Recurrence**（繰返し）） を設定します。
4. 新しいコンテンツ リリースを検出して取得するときに、ファイアウォールが実行する **Action**（操作）を設定します。
5. コンテンツ リリースのインストールの **Threshold**（しきい値）を設定します。ファイアウォールがリリースを取得して最後のステップで設定したアクションを実行するには、少なくとも Palo Alto Networks アップデート サーバーでコンテンツ リリースを利用できるようにする必要があります。
6. アプリケーションのダウンタイム（アプリケーションの可用性が最新の脅威防止であっても同様）を許容しないミッション クリティカルなネットワークの場合は、 **New App-ID Threshold**（新しい **App-ID** しきい値）を設定できます。ファイアウォールは、

この時間内に新しい App-ID が使用可能になった後でのみ、新しい App-ID を含むコンテンツ更新を取得します。

7. **OK** をクリックして、アプリケーションおよび脅威のコンテンツ更新スケジュールを保存し、**Commit**（コミット）をクリックします。

STEP 3 | ネットワークとファイアウォールの活動を監視するために使用する外部サービスに Palo Alto Networks の重要なコンテンツ アラートを送信するために、ログ転送を設定します。これにより、適切な個人に重要なコンテンツの問題が通知され、必要に応じて対処できるようになります。重大なコンテンツ アラートは、次のタイプとイベントを持つシステム ログ エントリとして記録されます。（subtype eq content）と（eventid eq palo-alto-networks-message）。

STEP 4 | スケジュールを設定した後、コンテンツの更新の予約は 1 回限りまたは低頻度ですが、スケジュール設定後は、コンテンツ リリースに含まれている新規および変更済みの App-ID の管理を続行する必要があります。これは、こうした App-ID によりどのようにセキュリティ ポリシーが実施されるかを変更できるためです。

コンテンツ更新に関するヒント

Palo Alto Networks アプリケーションおよび脅威のコンテンツ リリースは、厳密なパフォーマンスと品質の検査を受けています。しかし、顧客環境には非常に多くの変数が存在するため、予期しない方法でコンテンツのリリースがネットワークに影響を及ぼすことが稀にあります。これらのヒントに従い、できるだけネットワークに与える影響が少なくなるように、コンテンツ リリースの問題を小さくする、あるいはそのトラブルシューティングを行います。

- アプリケーションおよび脅威コンテンツ更新のベストプラクティスに準拠してください。

  アプリケーションおよび脅威コンテンツ更新のベストプラクティスを確認して実装します。コンテンツの更新をデプロイする方法は、ネットワーク セキュリティとアプリケーションの可用性要件によって異なる場合があります。

- 最新のコンテンツを実行していることを確認してください。

  ファイアウォール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していない場合は、最新のコンテンツ更新を入手してください。

  ファイアウォールは、ダウンロードしたコンテンツの更新がインストール時に Palo Alto Networks で推奨されているかどうかを検証します。ファイアウォールがデフォルトで実行するこのチェックは、インストール前に Palo Alto Networks アップデート サーバーから（手動またはスケジュールで）コンテンツの更新をダウンロードする場合に役立ちます。Palo Alto Networks がコンテンツの更新を可用性から削除する稀なケースがあるため、このオプションは、ファイアウォールが既にダウンロードしたとしても、Palo Alto Networks が削除したコンテンツ更新をファイアウォールがインストールするのを防ぎます。インストールを試みるコンテンツ更新がすでに有効ではないというエラーメッセージが表示される場合は、**Check Now**（今すぐチェック）を行い、最新のコンテンツ更新を取得してそのバージョンをインストールします（**Device**（デバイス） > **Dynamic Updates**（動的更新））。

- 脅威インテリジェンス テレメトリーをオンにします。

  ファイアウォールが Palo Alto Networks に送信する脅威情報テレメトリーをオンにします。テレメトリー データを使用して、コンテンツの更新に関する問題の特定とトラブルシューティングを行います。

  テレメトリー データは、Palo Alto Networks の顧客基盤全体で、ファイアウォールのパフォーマンスやセキュリティ ポリシーの実施に予期しない影響を及ぼすコンテンツ更新を迅速に認識するのに役立ちます。問題を特定するまでの時間が短いほど、速やかに問題を回避したり、ネットワークへの影響を軽減しやすくなります。

  ファイアウォールが Palo Alto Networks と遠隔測定データを収集して共有できるようにするには：

  1. [デバイス > セットアップ > テレメトリ] を選択します。
  2. **Telemetry**（テレメトリー）設定を編集して、**Select All**（すべて選択）を行います。
  3. **OK** および **Commit (コミット)** をクリックして変更を保存します。

- **Palo Alto Networks** のコンテンツ更新アラートを適切な担当者に転送します。

  Palo Alto Networks の重要なコンテンツ アラートのログ転送を有効にすることで、コンテンツ リリースに関する重要なメッセージが適切な担当者に直接送信されるようにします。

  Palo Alto Networks は、ファイアウォールの Web インターフェイスに直接コンテンツ更新の問題に関するアラートを発行したり、ログ転送を有効にしている場合は、監視に使用する外部サービスにアラートを発行することができます。重要コンテンツ アラートでは、問題がどのように影響を与えるか、そして必要に応じた処置方法を理解できるように、問題が記述されます。

  ファイアウォール Web インターフェイスでは、コンテンツの問題に関する重要なアラートが、本日のメッセージと同様に表示されます。Palo Alto Networks がコンテンツの更新に関する重要なアラートを発行する際に、ファイアウォールの Web インターフェイスにログインするとアラートがデフォルトで表示されます。ファイアウォール Web インターフェイスにすでにログインしている場合は、Web インターフェイスの下部にあるメニューバーのメッセージ アイコンの上に感嘆符が表示されます。メッセージ アイコンをクリックすると警告が表示されます。

  重要なコンテンツ更新アラートは、**dynamic-updates**タイプおよびイベント **palo-alto-networks-message** イベントのシステム ログ エントリとしても記録されます。これらのログ エントリを表示するには、次のフィルタを使用します。(subtype eq dynamic-updates) および (eventid eq palo-alto-networks-message)。

- 必要に応じて、**Panorama** を使用して過去のコンテンツ リリースにロールバックします。

  コンテンツ更新の問題に関する通知を受け取った後、Panorama を使用して、個々の firewall のコンテンツ バージョンを手動で元に戻す代わりに、管理されている firewall を最新のコンテンツ更新バージョンにすばやく戻すことができますPanorama でコンテンツのアップデートを元に戻す。

アプリケーションおよび脅威コンテンツ更新のベストプラクティス

コンテンツ更新のデプロイのベストプラクティスは、ファイアウォールに新しいアプリケーションと脅威の署名が継続的に備わっているため、ポリシーの施行を円滑に行うのに役立ちます。アプリケーションと脅威のシグネチャは 1 つのコンテンツ更新パッケージでまとめて提供されますが (アプリケーションおよび脅威コンテンツの更新 の詳細をご覧ください)、ネットワーク セキュリティと可用性の要件に基づいて異なる方法で展開する柔軟性があります。

- セキュリティ ファーストを重視する組織は、アプリケーションの可用性よりも、最新の脅威シグネチャを使用することによって保護を優先します。脅威防止機能を確保するために使用するのは、主にファイアウォールです。
- ミッション クリティカルなネットワークは、最新の脅威シグネチャによって保護を行うことよりも、アプリケーションの可用性を優先します。ネットワークはダウンタイムを許容しません。ファイアウォールはインラインでデプロイされてセキュリティポリシーを適用します。セキュリティポリシーで App-ID を使用している場合、App-ID に影響するコンテンツにどのような変更を加えても、ダウンタイムが生じるおそれがあります。

コンテンツ更新のデプロイを行うにあたり、ミッション クリティカルあるいはセキュリティ ファーストのアプローチ、あるいは両方のアプローチを組み合わせてビジネスニーズを満たすことができます。新しく変更された脅威とアプリケーションのシグネチャを最も効果的に活用するために、次のベストプラクティスを適用する際のアプローチを検討してください。

- コンテンツ更新のベストプラクティス–ミッション クリティカル
- コンテンツ更新のベストプラクティス–セキュリティ第一優先

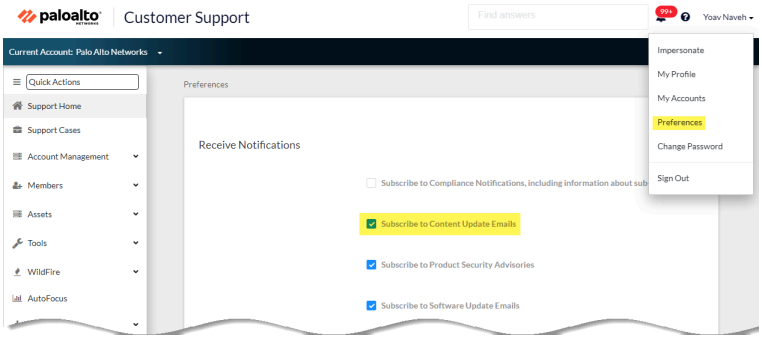
コンテンツ更新のベストプラクティス–ミッション クリティカル

このアプリケーションおよび脅威コンテンツ更新のベストプラクティスは、新しいアプリケーションと脅威シグネチャがリリースされたときにシームレスなポリシー適用を保証するのに役立ちます。以下のベストプラクティスに従って、アプリケーションのダウンタイムに対する耐性がゼロの、ミッションクリティカルなネットワークにコンテンツ更新をデプロイしてください。。

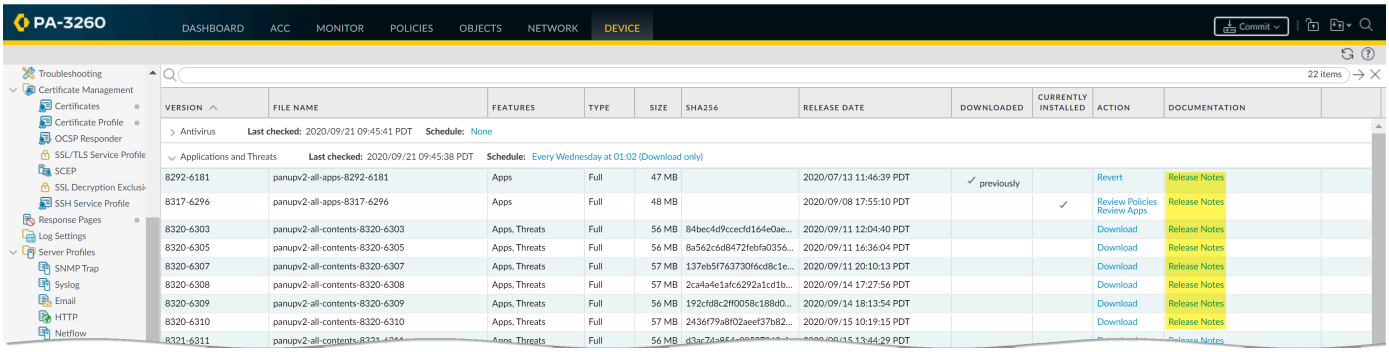
- 必ずコンテンツ リリースノートを確認し、そのコンテンツ リリースで導入される、新たに特定・修正されたアプリケーションおよび脅威シグネチャのリストをチェックしてください。また、コンテンツ リリースノートには、更新によって既存のセキュリティポリシーが受ける

おそれがある影響についての説明や、更新を最大限活用するためにセキュリティポリシーをどのように修正すれば良いかといった推奨内容も記載されています。

新しいコンテンツ更新の通知を購読するには、カスタマーサポートポータルにアクセスし、**Preferences** (設定)を編集し**Subscribe to Content Update Emails** (更新コンテンツのメールを購読する) を選択します。



また、Palo Alto Networks のサポート ポータル上、あるいはファイアウォールの Webインターフェースで直接、アプリケーションおよび脅威に関するコンテンツ リリースノートを確認できます。**Device** (デバイス) > **Dynamic Updates** (ダイナミック更新) を選択し、特定のコンテンツ リリースのバージョンについての **Release Note** (リリースノート) を開いてください。

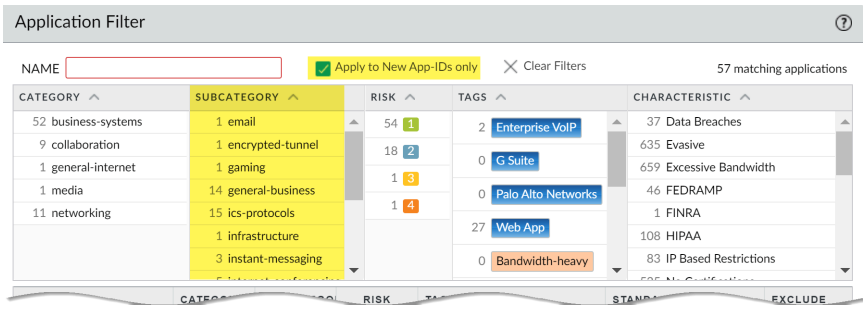


コンテンツ リリースノートの *Notes* (ノート) セクションは、後に *Palo Alto Networks* が極めて影響が大きい可能性があると判断した更新（例：新しい *App-ID* やデコーダ）を中心に取り扱います。これらの将来の更新を確認し、リリース前にポリシーが受ける影響を把握しておくようにしてください。

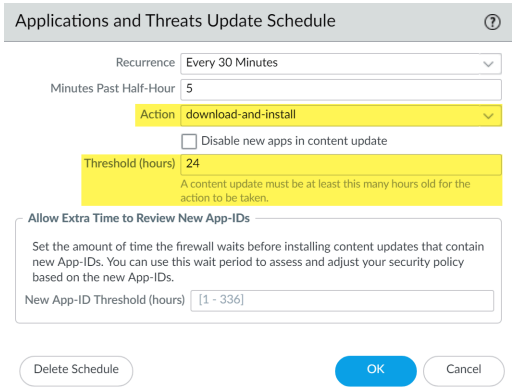
- 重要なビジネス機能が依存する認証やソフトウェア開発アプリケーションなどの新しい App-ID の特定のカテゴリを常に許可するセキュリティ ポリシー ルールを作成します。つまり、コンテンツのリリースで重要なビジネス アプリケーションの対象範囲がデプロイまたは変更された場合、ファイアウォールは引き続きシームレスにアプリケーションを許可し、セキュリティ ポリシーを更新する必要はありません。これにより、重要なカテゴリの App-ID に対する潜在的な影響が排除され、ミッション クリティカルな App-ID を許可するようにセキュ

リティ ポリシーを調整するために 30 日になります（新しい App-ID は毎月リリースされるため）。

これを行うには、重要カテゴリ内の新規 App-ID へのアプリケーション フィルタ（**Objects**（オブジェクト） > **Application Filters**（アプリケーション フィルタ））を作成してから、アプリケーション フィルタをセキュリティ ポリシー ルールに追加します。



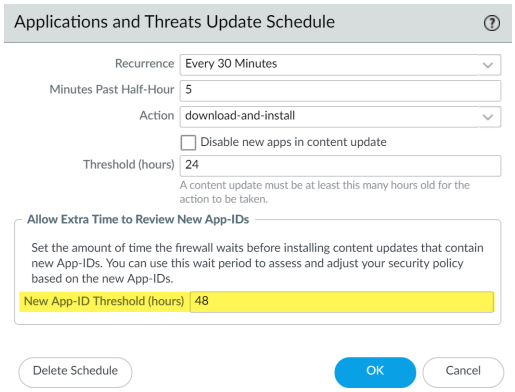
- 新しいアプリケーションと脅威シグネチャを有効にすることに関連するセキュリティ ポリシーの適用への影響を軽減するには、新しいコンテンツのロールアウトを調整します。新しいコンテンツは、ビジネス リスクが大きいロケーション（重要なアプリケーションがあるロケーションなど）にデプロイする前に、ビジネス リスクが小さいロケーション（ユーザー数が少ないサテライト オフィスなど）に提供するようにします。最新のコンテンツ更新をネットワーク全体にデプロイする前に、一部のファイアウォールに制限してデプロイすることで、あらゆる問題のトラブルシューティングも行いやすくなります。Panorama を使用して、組織や場所を基準に、ファイアウォールやデバイス グループに調整済みのスケジュールやインストールのしきい値をプッシュできます（ Panorama を使用してファイアウォールへのアップデートをデプロイする ）。
- コンテンツの更新が自動的に **download-and-install**（ダウンロードおよびインストール）されるようにスケジュールします。次に、ファイアウォールが最新のコンテンツをインストールするまでに待機する時間を決定する**Threshold**（しきい値）を設定します。ミッション クリティカルなネットワークでは、最大 48 時間のしきい値をスケジュール設定します。



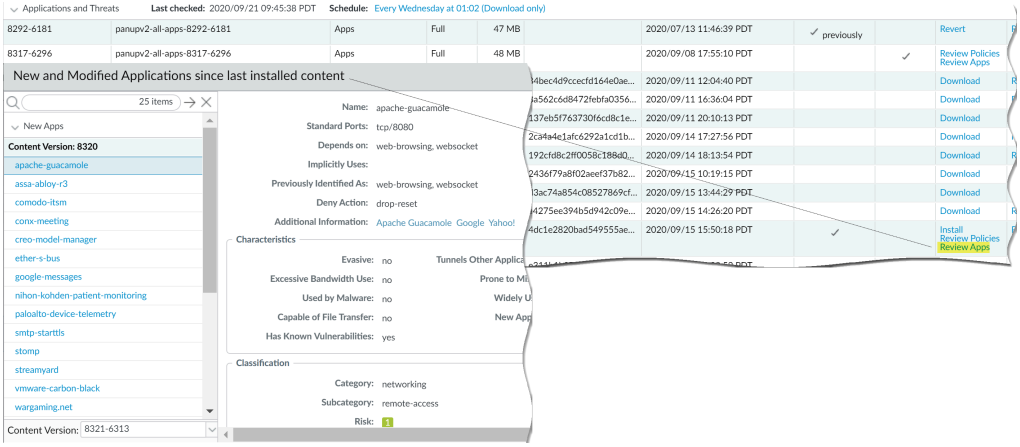
インストールの遅延は、ファイアウォールが指定された時間だけ利用可能であり、顧客環境で機能しているコンテンツが確実にインストールされます。コンテンツ更新のスケジュールを設定するには、**Device** (デバイス) > **Dynamic Updates** (動的更新) > **Schedule** (スケジュール) を選択します。

- インストールする前に、新しい App-ID に基づいてセキュリティ ポリシーを調整するための予備時間を設けてください。これを行うには、新しい App-ID を含むコンテンツの更新にの

み適用されるインストールのしきい値を設定します。新しい App-ID を使用したコンテンツの更新は 1 か月に 1 回のみリリースされ、インストールのしきい値はその時点でのみ発生します。**New App-ID Threshold**（新しい **App-ID** のしきい値）（**Device**（デバイス）> **Dynamic Updates**（動的更新）> **Schedule**（スケジュール））を設定するには、コンテンツ更新のスケジュールを設定します。

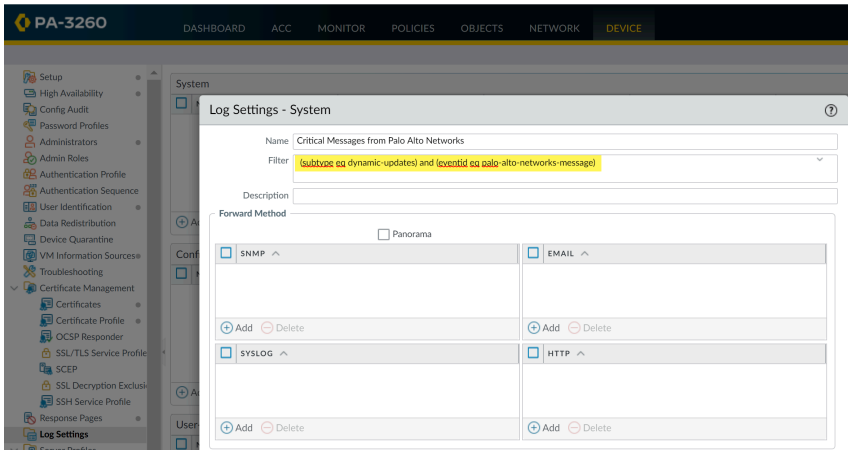


- 変更がセキュリティ ポリシーにどのように影響するかを評価するために、コンテンツのリリースで導入された新規または変更済みの App-ID を常に確認してください。次のトピックでは、新しい App-ID をインストールする前後にセキュリティ ポリシーを更新するために使用できるオプションについて説明します。新規および変更済みの App-ID の管理 。



- ネットワークとファイアウォールの活動を監視するために使用する外部サービスに Palo Alto Networks の重要なコンテンツ アラートを送信するために、ログ転送を設定します。これにより、適切な個人に重要なコンテンツの問題が通知され、必要に応じて対処できるようになります。重大なコンテンツ アラートは、次のタイプとイベントを持つシステム ログ エ

ントリとして記録されます。**(subtype eq dynamic-updates)** および **(eventid eq palo-alto-networks-message)**.



PAN-OS 8.1.2 では、重要なコンテンツ アラートのログタイプが***general (***全般***)***から***dynamic-updates (***動的更新***)***に変わっています。*PAN-OS 8.1.0* あるいは *PAN-OS 8.1.1* を使用している場合、重要なコンテンツが次のタイプとイベントを持つシステム ログ エントリとして記録されます。次のフィルターを使用し、これらのアラートを転送する設定を行う必要があります：***(subtype eq general)*** および ***(eventid eq palo-alto-networks-message)***

- 本番環境で新しいアプリケーションおよび脅威コンテンツ更新を有効化する前に、専用の準備環境でコンテンツをテストします。新しいアプリケーションおよび脅威をテストする最も簡単な方法は、試験用のファイアウォールを使って本番環境のトラフィックを利用することです。最新のコンテンツを試験用のファイアウォールにインストールし、本番環境からコピーしたトラフィックをファイアウォールが処理する間、ファイアウォールを監視します。また、試験用のクライアントおよびファイアウォールあるいはパケット キャプチャ（PCAP）を使い、本番環境のトラフィックを再現することもできます。PCAP を使用することで、ファイアウォールのセキュリティポリシーがロケーション毎に異なる、多彩なデプロイ環境のトラフィックを上手く再現することができます。

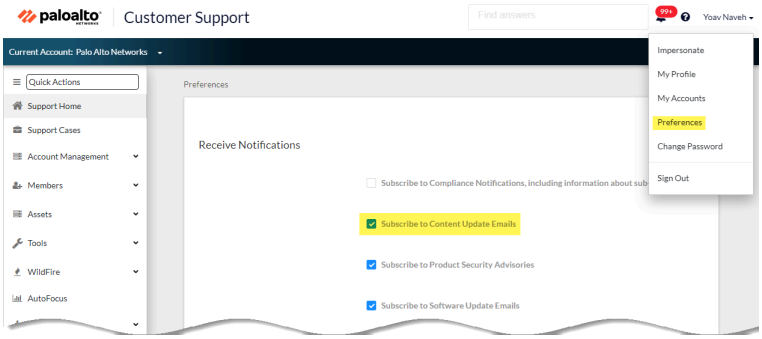
コンテンツ更新のベストプラクティス—セキュリティ第一優先

このアプリケーションおよび脅威コンテンツ更新のベストプラクティスは、新しいアプリケーションと脅威シグネチャがリリースされたときにシームレスなポリシー適用を保証するのに役立ちます。これらのベストプラクティスに従い、ファイアウォールを主に脅威防止機能に使用し、第一の優先順位は攻撃からの防御であるセキュリティ優先のネットワークにコンテンツ更新をデプロイします。

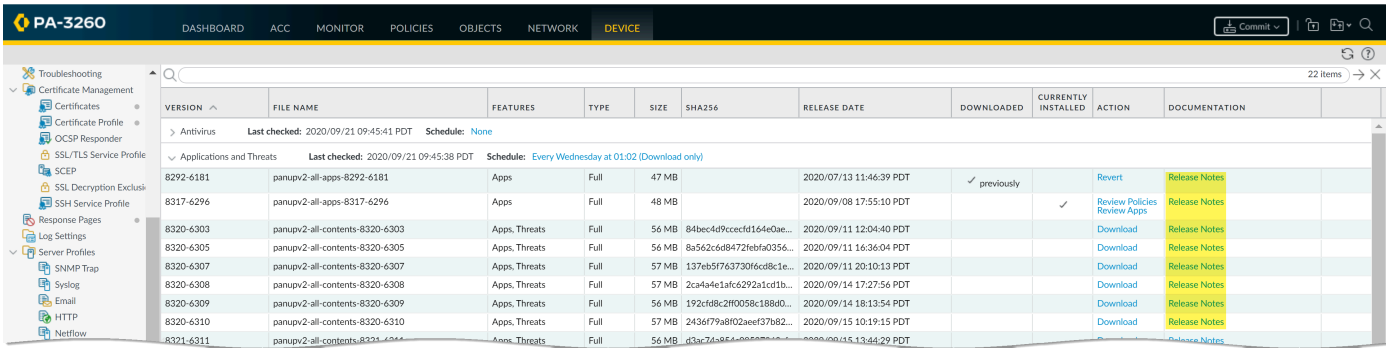
- 必ずコンテンツ リリースノートを確認し、そのコンテンツ リリースで導入される、新たに特定・修正されたアプリケーションおよび脅威シグネチャのリストをチェックしてください。また、コンテンツ リリースノートには、更新によって既存のセキュリティポリシーが受ける

おそれがある影響についての説明や、更新を最大限活用するためにセキュリティポリシーをどのように修正すれば良いかといった推奨内容も記載されています。

新しいコンテンツ更新の通知を購読するには、カスタマーサポートポータルにアクセスし、**Preferences (設定)**を編集し**Subscribe to Content Update Emails (更新コンテンツのメールを購読する)** を選択します。



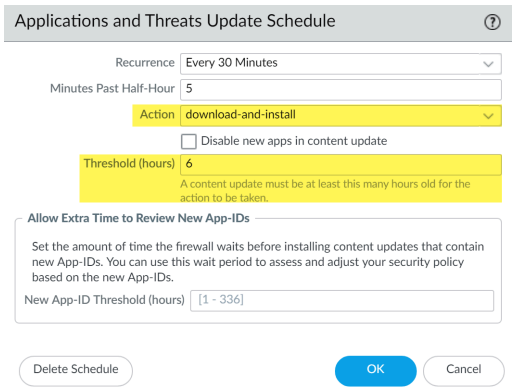
また、Palo Alto Networks のサポート ポータル上、あるいはファイアウォールの Webインターフェースで直接、アプリケーションおよび脅威に関するコンテンツ リリースノートを確認できます。**Device (デバイス) > Dynamic Updates (ダイナミック更新)** を選択し、特定のコンテンツ リリースのバージョンについての **Release Note (リリースノート)** を開いてください。



コンテンツ リリースノートの *Notes (ノート)* セクションは、後に *Palo Alto Networks* が極めて影響が大きい可能性があると判断した更新（例：新しい *App-ID* やデコーダ）を中心に取り扱います。これらの将来の更新を確認し、リリース前にポリシーが受ける影響を把握しておくようにしてください。

- 新しいアプリケーションと脅威シグネチャを有効にすることに関連するセキュリティ ポリシーの適用への影響を軽減するには、新しいコンテンツのロールアウトを調整します。新しいコンテンツは、ビジネス リスクが大きいロケーション（重要なアプリケーションがあるロケーションなど）にデプロイする前に、ビジネス リスクが小さいロケーション（ユーザー数が少ないサテライト オフィスなど）に提供するようにします。最新のコンテンツ更新をネットワーク全体にデプロイする前に、一部のファイアウォールに制限してデプロイすることで、あらゆる問題のトラブルシューティングも行いやすくなります。Panorama を使用して、組織や場所を基準に、ファイアウォールやデバイス グループに調整済みのスケジュールやインストールのしきい値をプッシュできます（ Panorama を使用してファイアウォールへのアップデートをデプロイする ）。

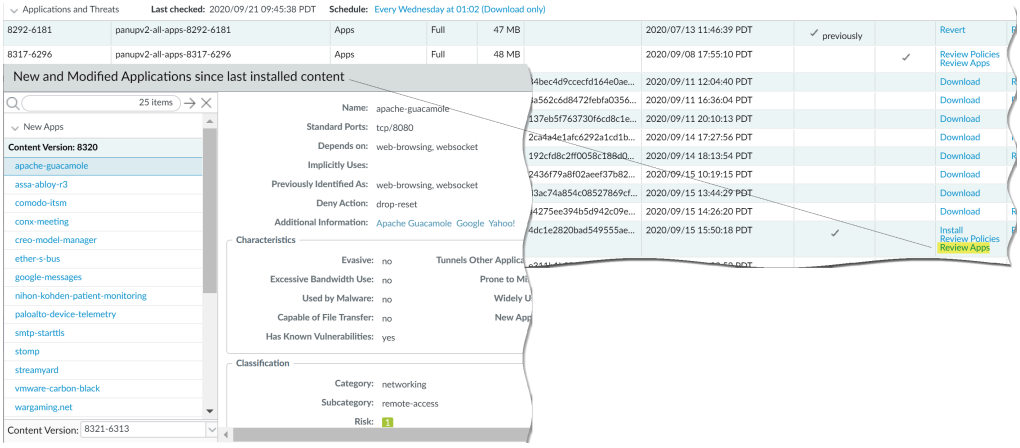
- コンテンツの更新が自動的に **download-and-install**（ダウンロードおよびインストール）されるようにスケジュールします。次に、ファイアウォールが最新のコンテンツをインストールするまでに待機する時間を決定する**Threshold**（しきい値）を設定します。セキュリティ第一優先のネットワークでは、6～12 時間のしきい値をスケジュールします。



インストールの遅延は、ファイアウォールが指定された時間だけ利用可能であり、顧客環境で機能しているコンテンツが確実にインストールされます。コンテンツ更新のスケジュールを設定するには、**Device (**デバイス**) > Dynamic Updates (**動的更新**) > Schedule (**スケジュール**)** を選択します。

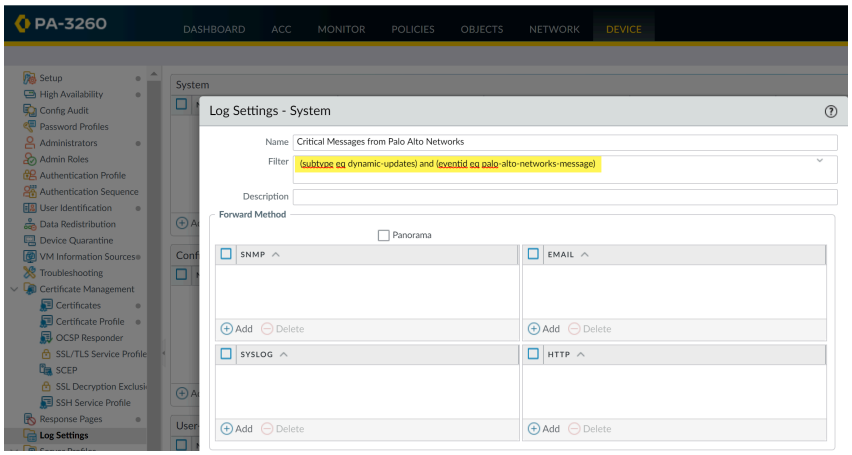
> ***New App-ID Threshold***（新しい ***App-ID*** のしきい値）をスケジュール設定しないでください。このしきい値により、ミッション クリティカルな組織は、新しい *App-ID* に基づいてセキュリティ ポリシー適用を調整するための予備時間を確保できます。ただし、このしきい値は最新の脅威防止更新の配信も遅延させるため、セキュリティの優先順位を持つ組織には推奨されません。

- 変更がセキュリティ ポリシーにどのように影響するかを評価するために、コンテンツのリリースで導入された新規または変更済みの App-ID を確認してください。次のトピックでは、新しい App-ID をインストールする前後にセキュリティ ポリシーを更新するために使用できるオプションについて説明します。新規および変更済みの App-ID の管理 。



- ネットワークとファイアウォールの活動を監視するために使用する外部サービスに Palo Alto Networks の重要なコンテンツ アラートを送信するために、ログ転送を設定します。これにより、適切な個人に重要なコンテンツの問題が通知され、必要に応じて対処できるようになります。重大なコンテンツ アラートは、次のタイプとイベントを持つシステム ログ エント

リとして記録されます。(`subtype eq dynamic-updates`) および (`eventid eq palo-alto-networks-messagee`)。



PAN-OS 8.1.2 では、重要なコンテンツ アラートのログタイプが***general (***全般***)***から***dynamic-updates (***動的更新***)***に変わっています。*PAN-OS 8.1.0* あるいは *PAN-OS 8.1.1* を使用している場合、重要なコンテンツが次のタイプとイベントを持つシステム ログ エントリとして記録されます。次のフィルターを使用し、これらのアラートを転送する設定を行う必要があります：***(subtype eq general)*** および ***(eventid eq palo-alto-networks-message)***

コンテンツ配信ネットワークのインフラストラクチャ

Palo Alto Networks は、Palo Alto Networks のファイアウォールにコンテンツの更新を提供するための CDN （Content Delivery Network）インフラストラクチャを管理しています。このファイアウォールは CDN 内の Web リソースにアクセスしてさまざまなコンテンツおよびアプリケーション ID 機能を実行します。

以下の表に、ファイアウォールが機能やアプリケーションのために利用できる Web リソースを示します。

リソース	URL	スタティック アドレス（スタティック サーバーが必要な場合）
アプリケーション データベース	• updates.paloaltonetworks.com (Global, except China) • updates.paloaltonetworks.cn (中国本土のみ) firewall のインターネットへのアクセスが制限されている場合は、次の URL を firewall 許可リストに追加します: • downloads.paloaltonetworks.com:443 • proditpdownloads.paloaltonetworks.com:443 ベスト プラクティスとして、更新サーバーを updates.paloaltonetworks.com に設定します。これにより、Palo Alto Networks firewall は、CDN インフラストラクチャ内で最も近いサーバーからコンテンツの更新を受信できます。	us-static.updates.paloaltonetworks.co ファイアウォール許可リストに次の IPv4 または IPv6 静的サーバー アドレス セットを追加します。 • **IPv4**— 35.186.202.45:443 および 34.120.74.244:443 • **IPv6**) - [2600:1901:0:669::]:443 と [2600:1901:0:5162::]:443
脅威/アンチウイルス データベース		

リソース	URL	スタティック アドレス（スタティック サーバーが必要な場合）
	追加の参照情報が必要な場合、または接続と更新プログラムのダウンロードの問題が発生している場合は、https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000001UtRCAU を参照してください Palo Alto Networks ThreatVault データベースには、脆弱性、エクスプロイト、ウイルス、およびスパイウェアの脅威に関する情報が含まれています。DNS セキュリティやウイルス対策プロファイルなどの Firewall 機能は、次のリソースを使用して脅威 ID 情報を取得し、例外を作成します: • data.threatvault.paloaltonetworks.com	適切な機能を実現するには、特定のプロトコルタイプに対して提供される両方の *IP* アドレスを許可リストに追加する必要があります。
PAN-DB URL フィルタリング |高度な URL フィルタリング	*.urlcloud.paloaltonetworks.com プライマリ URL s0000.urlcloud.paloaltonetworks.com に解決され、最も近い地域サーバーにリダイレクトされます。 • s0100.urlcloud.paloaltonetworks.com • s0200.urlcloud.paloaltonetworks.com • s0300.urlcloud.paloaltonetworks.com • s0500.urlcloud.paloaltonetworks.com	スタティック IP アドレスは使用できません。ただし、手動で URL を IP アドレスに解決して、地域サーバー IP アドレスへのアクセスを許可することはできます。
クラウドサービス	hawkeye.services-edge.paloaltonetworks.com に解決され、最も近い地域サーバーにリダイレクトされます。 • US—**us.hawkeye.services-edge.paloaltonetworks.com** • **EU — eu.hawkeye.services-edge.paloaltonetworks.com**	スタティック IP アドレスは使用できません。

リソース	URL	スタティック アドレス（スタティック サーバーが必要な場合）
	• UK—**uk.hawkeye.services-edge.paloaltonetworks.com** • アジア太平洋—apac.hawkeye.services-edge.paloaltonetworks.com	
DNS セキュリティ	• Cloud—dns.service.paloaltonetworks.com:443 • Telemetry—io.dns.service.paloaltonetworks.com:443 許可リストをダウンロードすると、dns.service.paloaltonetworks.com 次のサーバーに解決されます。 • static.dns.service.paloaltonetworks.com:443 • data.threatvault.paloaltonetworks.com (DNS 例外の作成に使用)	スタティック IP アドレスは使用できません。
ファイアウォールベースのインライン ML: • URL Filtering Inline ML（URL フィルタリング インライン ML） • WildFire インライン ML	• ml.service.paloaltonetworks.com:443	スタティック IP アドレスは使用できません。
WildFire	• クラウド (レポート取得) - wildfire.paloaltonetworks.com:443 WildFire クラウド領域: • グローバルI—wildfire.paloaltonetworks.com • 欧州—eu.wildfire.paloaltonetworks.com • 日本—jp.wildfire.paloaltonetworks.com • シンガポール—sg.wildfire.paloaltonetworks.com • 英国—uk.wildfire.paloaltonetworks.com	スタティック IP アドレスは使用できません。

リソース	URL	スタティック アドレス（スタティック サーバーが必要な場合）
	• カナダ—ca.wildfire.paloaltonetworks.com • オーストラリア—au.wildfire.paloaltonetworks.com • ドイツ—de.wildfire.paloaltonetworks.com • インド—in.wildfire.paloaltonetworks.com • スイス—ch.wildfire.paloaltonetworks.com • ポーランド—pl.wildfire.paloaltonetworks.com • インドネシア—id.wildfire.paloaltonetworks.com • 台湾—tw.wildfire.paloaltonetworks.com • フランス—fr.wildfire.paloaltonetworks.com • カタール—qatar.wildfire.paloaltonetworks.com • 韓国—krv.wildfire.paloaltonetworks.com • イスラエル—il.wildfire.paloaltonetworks.com • サウジアラビア—sa.wildfire.paloaltonetworks.com • スペイン—es.wildfire.paloaltonetworks.com	

アップグレード Panorama

- Panorama のコンテンツの更新とソフトウェア アップグレードのインストール
- Panorama アップグレードのトラブルシューティング
- 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 のコンテンツの更新とソフトウェア アップグレードのインストール

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。

- インターネット接続で Panorama をアップグレードする
- インターネット接続なしでPanoramaをアップグレード
- インターネット接続のない Panorama のコンテンツ更新プログラムを自動的にインストールする
- HA 構成で Panorama をアップグレードする
- PAN-OSソフトウェアパッチのインストール
- Panorama ログの新しいログ形式への移行
- Panorama をアップグレードしてデバイス管理能力を強化
- FIPS-CC モードでの Panorama デバイスと管理対象デバイスのアップグレード
- Panorama 11.1 からのダウングレード

インターネット接続で Panorama をアップグレードする

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)構成で実行されている場合は、各ピアの Panorama ソフトウェアをアップグレードします(HA 構成で Panorama をアップグレードする を参照)。FIPS-CC モードの Panorama および管理対象デバイスを PAN-OS 10.2 以前のリリースから PAN-OS® 11.1 にアップグレードする場合、PAN-OS 10.2 リリースの実行中に Panorama 管理に追加された場合は、FIPS-CC モードでデバイスのセキュア接続ステータスをリセットする追加の手順を実行する必要があります。FIPS-CC モードでの Panorama および FIPS-CC デバイスのアップグレードの詳細については、FIPS-CC モードでの Panorama デバイスと管理対象デバイスのアップグレードを参照してください。

Panorama 仮想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、ローカル ログ コレクタ で Panorama 仮想アプライアンスをセットアップする場合に説明されているように、追加の設定が必要な手動タスクです。

Palo Alto Networks は、アップグレード元の *PAN-OS* バージョンに応じて、アップグレード パスのさまざまなポイントで新しいログ データ形式を導入しました。

- ***PAN-OS 8.1*** から ***PAN-OS 9.0*** へのアップグレード:*PAN-OS 9.0* では、ローカルおよび専用 *Log Collector* 用の新しいログ データ形式が導入されました。*PAN-OS 11.1* へのアップグレード パスでは、*PAN-OS 8.1* から *PAN-OS 9.0* にアップグレードすると、既存のログ データが自動的に新しい形式に移行されます。
- ***PAN-OS 10.0*** から ***PAN-OS 10.1*** へのアップグレード:*PAN-OS 10.1* では、ローカルおよび専用 *Log Collector* 用の新しいログ形式が導入されました。*PAN-OS 11.1* へのアップグレード パスでは、*PAN-OS 8.1* 以前で生成されたログは使用できなくなりました。これには、*PAN-OS 9.0* へのアップグレードの一部として移行されたログが含まれます。*PAN-OS 10.1* にアップグレードした後、これらのログを回復して *PAN-OS 10.1* ログ形式に移行するオプションがあります。

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、PAN-OS® 11.1に必要な最小コンテンツリリースバージョンについてリリースノートを参照してください。

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。

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。

- 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 | 「PAN-OS 11.1 へのアップグレード パスを決定する」を行います。

現在実行中の PAN-OS バージョンから PAN-OS 11.1 へのパスにある機能リリース 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。

Release Notes のPAN-OS アップグレード チェックリスト、既知の問題、既定の動作の変更点を確認し、アップグレード パスの一部として渡す各リリースアップグレード/ダウングレードに関する考慮事項を確認します。

STEP 3 | (Panorama Interconnectプラグインのみ) PanoramaノードをPanoramaコントローラーと同期します。

Panoramaノードのアップグレードを開始する前に、Panoramaコントローラーとの Panoramaノードの設定を同期する必要があります。これは、アップグレードが正常に完了した後に、一般的なPanoramaコントローラーの構成をPanoramaノードに正常にプッシュするために必要です。

STEP 4 | 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. Panorama Web インターフェースにログインします。
2. 名前の **Panorama** 構成スナップショット (**P1anorama** > セットアップ > 操作)、構成に名前 を入力し、**OK** をクリックします。
3. **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 5 | (ベスト プラクティス) Cortex データ レイク (CDL) を活用している場合は、Panorama デバイス証明書 をインストールします。

Panorama は、PAN-OS 11.1 へのアップグレード時に、CDL 取り込みおよびクエリ エンドポイントでの認証にデバイス証明書を使用するように自動的に切り替わります。

PAN-OS 11.1 にアップグレードする前にデバイス証明書をインストールしない場合、*Panorama* は認証に既存のロギング サービス証明書を引き続き使用します。

STEP 6 | ネットワークで次の TCP ポートを有効にします。

Log Collector 間通信を可能にするには、これらの TCP ポートをネットワーク上で有効にする必要があります。

- TCP/9300
- TCP/9301
- TCP/9302

STEP 7 | 最新の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 (18を参照してください)。

1. 最新の更新プログラムの **Panorama** > 動的更新 と 今すぐチェック を選択します。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. (Panoramaでコンテンツリリースバージョンを更新する前に、必ずLog Collectors(Panorama がインターネットに接続されている場合はLog Collectorsをアップグレードするを参照)を同じ(またはそれ以降の)コンテンツリリースバージョンにファイアウォールを Panorama から PAN-OS 11.1 にアップグレードするしてから更新してください。

   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 8 | **[Panorama] > [Plugins (プラグイン)]**を選択し、Panoramaにインストールされている PAN-OS 11.1 でサポートされるプラグイン バージョンを ダウンロードします。

ターゲットの PAN-OS 11.1 リリースでサポートされている Panorama プラグインのバージョンについては、互換性マトリックス を参照してください。

これは、Panorama を PAN-OS 11.0 から PAN-OS 11.1 に正常にアップグレードするために必要です。サポートされているプラグインバージョンがダウンロードされていない場合、PAN-OS 11.1へのアップグレードはブロックされます。

PAN-OS 11.1 へのアップグレードに必要なダウンロード済みプラグインは、*Panorama* が *PAN-OS 11.1* に正常にアップグレードされると自動的にインストールされます。ダウンロードしたプラグインが自動的にインストールされない場合は、*PAN-OS 11.1* へのアップグレード後に影響を受けるプラグインを手動でインストールする必要があります。

STEP 9 | Pan-OS 11.1 へのアップグレード パスに沿って、Panorama を PAN-OS リリースにアップグレードします。

1. インターネット接続を使用する Panorama を PAN-OS 9.1 にアップグレード にアップグレードします。
2. インターネット接続を使用する Panorama をアップグレード を PAN-OS 10.0 にアップグレードします。

   (Panorama in Legacy モードのみ) ***Download*** *PAN-OS 10.0.0* と ***Download*** および ***Install*** *PAN-OS 10.0.8* 以降のリリースを続行する前に、アップグレード パスを続行します。

   これは、*NFS* ストレージパーティションに保存されているすべてのログを保持するために必要です。レガシー モードの *Panorama* の *NFS* ストレージ パーティションに保存されている一部のログは、*PAN-OS 10.0.7* 以前の *PAN-OS 10.0* リリースをインストールすると削除されます。
3. PAN-OS 10.1へインターネット接続されているPanoramaをアップグレードします。

   PAN-OS 10.1 では、新しいログ形式が導入されました。PAN-OS 10.0 から PAN-OS 10.1 へのアップグレードでは、PAN-OS 8.1 以前のリリースで生成されたログを移行することを選択できます。それ以外の場合、PAN-OS 10.1 へのアップグレードが正常に完了すると、これらのログは自動的に削除されます。移行中、ログ データは [ACC] タブまたは [監視] タブに表示されません。移行が行われている間、ログ データは適切

なログ コレクタに転送され続けますが、パフォーマンスに影響が生じる場合があります。

> *(Panorama レガシーモードのみ) PAN-OS 10.1.0* のダウンロードと*PAN-OS 10.1.3* 以降のリリースを ダウンロード および インストール します。
>
> これは、*NFS* ストレージパーティションに保存されているすべてのログを保持するために必要です。レガシー モードで *Panorama* の *NFS* ストレージ パーティションに保存されている一部のログは、*PAN-OS 10.1.2* 以前の *PAN-OS 10.1* リリースをインストールすると削除されます。

4. Upgrade Panorama with an Internet Connection to PAN-OS 10.2.
5. PAN-OS 11.0へインターネット接続されているPanoramaをアップグレードします。

STEP 10 | Panorama を PAN-OS 11.1 にアップグレードします。

1. 最新のリリースを **Check Now (**今すぐチェック**)**します **([Panorama] > [Software (**ソフトウェア**)])** 。

   （PAN-OS 11.1.3以降）デフォルトでは、優先リリースと対応する基本リリースが表示されます。優先リリースのみを表示するには、**[Base Releases (**基本リリース**)]**チェックボックスをオフ(選択解除)にします。同様に、基本リリースのみを表示するには、**[Preferred Releases (**優先リリース**)]** チェックボックスを無効 (クリア) にします。
2. PAN-OS 11.1.0 イメージを見つけて 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. (Panoramaモードのみ) PAN-OS 10.0 以前のリリースで生成されたログを含むローカルログコレクターがある場合は、通知が表示されます。

   この通知は、PAN-OS 11.1.2以降の11.1リリースを最初にインストールしようとしたときに表示され、通知が閉じられた後の2回目には表示されません。PAN-OS 10.0以前のリリースを実行しているときにPanoramaまたは管理対象デバイスによって生成された

ログが検出され、アップグレード時に削除されることを警告します。つまり、アップグレードが正常に終了した後は、影響を受けたログは表示または検索できません。

ただし、これらの影響を受けたログはアップグレード後に復元できます。通知では、次の情報も提供されます。

- 影響を受けるログの種類。
- 各ログタイプの影響を受けるタイムフレーム。
- 影響を受けたログをログタイプごとにリカバリするために必要な各`debug logdb migrate-lc`コマンド。

  通知を閉じる前に、リストされている`debug logdb migrate-lc`をコピーします。

通知を閉じます。

4. 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））。

   Panorama が正常に再起動したら、次のステップに進みます。

STEP 11 | （PAN-OS 11.1.2以降のリリース、Panoramaモードのみ）Panorama CLIにログインし 、前のステップで示した `debug logdb migrate-lc`コマンド を使用して影響を受けるログを復旧します。

これらのコマンドは順番に実行する必要があり、同時に実行することはできません。通知ウィンドウから`debug logdb migrate-lc`コマンドをコピーしていない場合は 、 **[Tasks (タスク)**］をクリックし、失敗した`Install (インストール)`ジョブの詳細を表示します。

STEP 12 | お使いのPanoramaプラグインのバージョンがPAN-OS 11.1をサポートしていることを確認してください。

Panorama を正常にアップグレードした後、PAN-OS 11.1 でサポートされている Panorama プラグインのバージョンを確認してインストールする必要があります。PAN-OS 11.1 でサ

ポートされているサポートされている Panorama プラグインの詳細については、互換性マトリックス を参照してください。

1. Panorama Web インターフェイス にログインし、**Dashboard** の一般情報ウィジェットを確認して、PAN-OS 11.1 互換プラグイン バージョンが正常にインストールされたことを確認します。

   また、Panorama CLI にログインし、コマンド `show plugins installed` を入力して、現在インストールされているプラグインのリストを表示することもできます。
2. **[Panorama]** > **[Plugins (プラグイン)]** を選択し、インストールされなかったプラグインを検索します。
3. PAN-OS 11.1 でサポートされているプラグイン バージョンをインストールします 。
4. Panorama にインストールされているすべてのプラグインが PAN-OS 11.1 でサポートされているバージョンを実行するまで、上記の手順を繰り返します。

STEP 13 | (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 14 | (Panorama および FIPS-CC モードの管理対象デバイス)FIPS-CC モードでの Panorama デバイスと管理対象デバイスのアップグレード.

FIPS-CC モードで Panorama および管理対象デバイスをアップグレードするには、PAN-OS 11.1 リリースの実行中に Panorama 管理に追加された場合、FIPS-CC モードのデバイスのセキュアな接続ステータスをリセットする必要があります。デバイス登録認証キーを使用して、次の管理対象デバイスを Panorama 管理に再オンボードする必要があります:

- FIPS-CC モードの管理対象デバイスが Panorama に追加されました。
- デバイス登録認証キーを使用して Panorama に追加されました

管理対象デバイスが PAN-OS 10.0 以前のリリースを実行している間に、Panorama 管理に追加された管理対象デバイスを再オンボーディングする必要はありません。

STEP 15 | OpenSSL セキュリティー・レベル 2 に準拠するために、すべての証明書を再生成または再インポートします。

この手順は、PAN-OS 10.1 以前のリリースから PAN-OS 11.1 にアップグレードする場合に必要です。PAN-OS 10.2 からアップグレードし、証明書をすでに再生成または再インポートしている場合は、この手順をスキップします。

すべての証明書が次の最小要件を満たしている必要があります。

- RSA 2048 ビット以上、または ECDSA 256 ビット以上
- SHA256 以上のダイジェスト

証明書の再生成または再インポートの詳細については、PAN-OS Administrator's Guide または Panorama Administrator's Guide を参照してください。

STEP 16 | (Panorama モード に推奨) Panorama 仮想アプライアンスのメモリを 64 GB に増やします

Panorama モードの Panorama 仮想アプライアンスを PAN-OS 11.1 に正常にアップグレードした後、Palo Alto Networks では、プロビジョニング不足の Panorama 仮想アプライアンスに関連するロギング、管理、および運用パフォーマンスの問題を回避するために、増加したシステム要件 を満たすために、Panorama 仮想アプライアンスのメモリを 64GB に増やすことをお勧めします。

STEP 17 | **[Commit (コミット)]** > **[Commit and Push (コミットとプッシュ)]** を選択し、Panorama管理対象の設定をすべての管理対象デバイスにコミットしてプッシュします。

Panoramaおよび管理対象デバイスをPAN-OS 11.1に正常にアップグレードしたら、選択した構成を管理対象デバイスにプッシュし、Panoramaが管理するマルチvsysファイアウォールの改善された共有構成オブジェクト管理を活用する前に、Panorama管理対象構成を完全にコミットしてプッシュする必要があります。

STEP 18 | （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。
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。

インターネット接続なしでPanoramaをアップグレード

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)構成で展開されている場合は、各ピアをアップグレードする必要があります(HA 構成で Panorama をアップグレードするを参照)。FIPS-CC モードの Panorama および管理対象デバイスを PAN-OS 10.2 以前のリリースから PAN-OS 11.1 にアップグレードする場合、PAN-OS 10.2 リリースの実行中に Panorama 管理に追加した場合は、FIPS-CC モードでデバイスのセ

キュア接続ステータスをリセットする追加手順を実行する必要があります。FIPS-CC モードでの Panorama および FIPS-CC デバイスのアップグレードの詳細については、FIPS-CC モードでの Panorama デバイスと管理対象デバイスのアップグレードを参照してください。

Panorama 仮想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、ローカル ログ コレクタ で Panorama 仮想アプライアンスをセットアップする場合に説明されているように、追加の設定が必要な手動タスクです。

Palo Alto Networks は、アップグレード元の *PAN-OS* バージョンに応じて、アップグレード パスのさまざまなポイントで新しいログ データ形式を導入しました。

- ***PAN-OS 8.1*** から ***PAN-OS 9.0*** へのアップグレード:*PAN-OS 9.0* では、ローカルおよび専用 *Log Collector* 用の新しいログ データ形式が導入されました。*PAN-OS 11.1* へのアップグレード パスでは、*PAN-OS 8.1* から *PAN-OS 9.0* にアップグレードすると、既存のログ データが自動的に新しい形式に移行されます。
- ***PAN-OS 10.0*** から ***PAN-OS 10.1*** へのアップグレード:*PAN-OS 10.1* では、ローカルおよび専用 *Log Collector* 用の新しいログ形式が導入されました。*PAN-OS 11.1* へのアップグレード パスでは、*PAN-OS 8.1* 以前で生成されたログは使用できなくなりました。これには、*PAN-OS 9.0* へのアップグレードの一部として移行されたログが含まれます。*PAN-OS 10.1* にアップグレードした後、これらのログを回復して *PAN-OS 10.1* ログ形式に移行するオプションがあります。

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、PAN-OS® 11.1 に必要な最小コンテンツ リリース バージョンについては、リリース ノート を参照してください。

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。

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。

- 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 | 「PAN-OS 11.1 へのアップグレード パスを決定する」を行います。

現在実行中の PAN-OS バージョンから PAN-OS 11.1 へのパスにある機能リリース 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。

Release Notes のPAN-OS アップグレード チェックリスト、既知の問題、既定の動作の変更点を確認し、アップグレード パスの一部として渡す各リリースアップグレード/ダウングレードに関する考慮事項を確認します。

STEP 3 | (Panorama Interconnectプラグインのみ) PanoramaノードをPanoramaコントローラーと同期します。

Panoramaノードのアップグレードを開始する前に、Panoramaコントローラーとの Panoramaノードの設定を同期する必要があります。これは、アップグレードが正常に完了した後に、一般的なPanoramaコントローラーの構成をPanoramaノードに正常にプッシュするために必要です。

STEP 4 | 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. Panorama Web インターフェースにログインします。
2. 名前の **Panorama** 構成スナップショット (**P1anorama** > セットアップ > 操作)、構成に名前 を入力し、**OK** をクリックします。
3. **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 5 | SCP または HTTPS 経由で Panorama にコンテンツを接続してアップロードできるホストに、最新のコンテンツの更新をダウンロードします。

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。

STEP 6 | ネットワークで次の TCP ポートを有効にします。

Log Collector 間通信を可能にするには、これらの TCP ポートをネットワーク上で有効にする必要があります。

- TCP/9300
- TCP/9301
- TCP/9302

STEP 7 | 最新のコンテンツ更新をインストールします。

ソフトウェア更新プログラムの前にコンテンツ更新プログラムをインストールし、*Panorama* 管理サーバーにインストールする前に、最初にファイアウォールを Panorama から PAN-OS 11.1 にアップグレードするしてから upgrade Log Collectors をインストールする必要があります。

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 Web インターフェイス にログインし、コンテンツ タイプごとに次の手順を実行します。

1. **Panorama** > 動的更新 を選択します。
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、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。
3. **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 8 | Panoramaに現在インストールされているすべてのプラグインについて、PAN-OS 11.1でサポートされているプラグインバージョンをアップロードします。

ターゲットの PAN-OS 11.1 リリースでサポートされている Panorama プラグインのバージョンについては、互換性マトリックス を参照してください。

これは、Panorama を PAN-OS 11.0 から PAN-OS 11.1 に正常にアップグレードするために必要です。サポートされているプラグインバージョンがダウンロードされていない場合、PAN-OS 11.1へのアップグレードはブロックされます。

PAN-OS 11.1 へのアップグレードに必要なダウンロード済みプラグインは、*Panorama* が *PAN-OS 11.1* に正常にアップグレードされると自動的にインストールされます。ダウンロードしたプラグインが自動的にインストールされない場合は、*PAN-OS 11.1* へのアップグレード後に影響を受けるプラグインを手動でインストールする必要があります。

1. PAN-OS 11.1 でサポートされているプラグインのバージョン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、ドロップダウンメニューからプラグインを選択します。
   3. PAN-OS 10.2 でサポートされているプラグインのバージョンをダウンロードします。
   4. Panoramaに現在インストールされているすべてのプラグインについて、この手順を繰り返します。
2. Panorama ウェブインターフェイスにログインします。
3. **Panorama** > **Plugins** と、前の手順でダウンロードしたプラグイン バージョンの **Upload** を選択します。

   Panoramaに現在インストールされているすべてのプラグインについて、この手順を繰り返します。

STEP 9 | Pan-OS 11.1 へのアップグレード パスに沿って、Panorama を PAN-OS リリースにアップグレードします。

1. インターネットに接続していない場合は Panorama をアップグレード を PAN-OS 9.1 にアップグレードします。
2. インターネットに接続していない場合は Panorama をアップグレード を PAN-OS 10.0 にアップグレードします。

   *(Panorama レガシーモードのみ) PAN-OS 10.0.0*をダウンロードし、アップグレード パスを続行する前に *PAN-OS 10.0.8* 以降のリリースをダウンロード および インストールします。

   これは、*NFS* ストレージパーティションに保存されているすべてのログを保持するために必要です。レガシー モードの *Panorama* の *NFS* ストレージ パーティションに保存されている一部のログは、*PAN-OS 10.0.7* 以前の *PAN-OS 10.0* リリースをインストールすると削除されます。
3. アップグレード Panorama When Not Internet Connected を PAN-OS 10.1.

   PAN-OS 10.1 では、新しいログ形式が導入されました。PAN-OS 10.0 から PAN-OS 10.1 へのアップグレードでは、PAN-OS 8.1 以前のリリースで生成されたログを移行することを選択できます。それ以外の場合、PAN-OS 10.1 へのアップグレードが正常に完了すると、これらのログは自動的に削除されます。移行中、ログ データは [ACC] タブまたは [監視] タブに表示されません。移行が行われている間、ログ データは適切なログ コレクタに転送され続けますが、パフォーマンスに影響が生じる場合があります。

   (Panorama レガシーモードのみ) PAN-OS 10.1.0 のダウンロードと*PAN-OS 10.1.3* 以降のリリースを ダウンロード および インストール します。

   これは、*NFS* ストレージパーティションに保存されているすべてのログを保持するために必要です。レガシー モードで *Panorama* の *NFS* ストレージ パーティションに保存されている一部のログは、*PAN-OS 10.1.2* 以前の *PAN-OS 10.1* リリースをインストールすると削除されます。
4. PAN-OS 10.2へインターネットに接続されていない Panorama をアップグレード。
5. PAN-OS 11.0へインターネットに接続されていない Panorama をアップグレード。

STEP 10 | 最新の PAN-OS 11.1 リリース イメージを、SCP または HTTPS 経由で Panorama に接続してコンテンツをアップロードできるホストに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. 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. 最新の PAN-OS 11.1 リリース イメージのモデル固有のモデルを見つけます。たとえば、M シリーズ アプライアンスを Panorama 11.1.0 にアップグレードするには、`Panorama_m-11.1.0` イメージをダウンロードします。 Panorama 仮想アプライアンスを Panorama 11.1.0 にアップグレードするには、`Panorama_pc-11.1.0` イメージをダウンロードします。

      Content By（コンテンツ別）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。

      (PAN-OS 11.1.3 以降のリリース) デフォルトでは、結果には優先リリースが表示されます。***[Release type (リリースタイプ)]***フィールドで、***[Other (その他)]***をクリックすると、利用可能な他のリリースを表示できます。
   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。

STEP 11 | Panorama を PAN-OS 11.1 にアップグレードします。

1. Panorama Web インターフェースにログインします。
2. **[Panorama] > [Software (ソフトウェア)]** と **[Upload (アップロード)]** 前の手順でダウンロードした PAN-OS 11.1 イメージを選択します。
3. 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。
4. (Panoramaモードのみ) PAN-OS 10.0 以前のリリースで生成されたログを含むローカル ログコレクターがある場合は、通知が表示されます。

   この通知は、PAN-OS 11.1.2以降の11.1リリースを最初にインストールしようとしたときに表示され、通知が閉じられた後の2回目には表示されません。PAN-OS 10.0以前のリリースを実行しているときにPanoramaまたは管理対象デバイスによって生成された

ログが検出され、アップグレード時に削除されることを警告します。つまり、アップグレードが正常に終了した後は、影響を受けたログは表示または検索できません。

ただし、これらの影響を受けたログはアップグレード後に復元できます。通知では、次の情報も提供されます。

- 影響を受けるログの種類。
- 各ログタイプの影響を受けるタイムフレーム。
- 影響を受けたログをログタイプごとにリカバリするために必要な各`debug logdb migrate-lc`コマンド。

  通知を閉じる前に、リストされている`debug logdb migrate-lc`をコピーします。

通知を閉じます。

5. 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 構成で Panorama をアップグレードする。または：

   1. インストール アップロードされたイメージ。
   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））。

   Panorama が正常に再起動したら、次のステップに進みます。

STEP 12 | （PAN-OS 11.1.2以降のリリース、Panoramaモードのみ）Panorama CLIにログインし 、前のステップで示した `debug logdb migrate-lc`コマンド を使用して影響を受けるログを復旧します。

これらのコマンドは順番に実行する必要があり、同時に実行することはできません。通知ウィンドウから`debug logdb migrate-lc`コマンドをコピーしていない場合は 、 **[Tasks (タスク)**］をクリックし、失敗した`Install (インストール)`ジョブの詳細を表示します。

STEP 13 | お使いのPanoramaプラグインのバージョンがPAN-OS 11.1をサポートしていることを確認してください。

Panorama を正常にアップグレードした後、PAN-OS 11.1 でサポートされている Panorama プラグインのバージョンを確認してインストールする必要があります。PAN-OS 11.1 でサ

ポートされているサポートされている Panorama プラグインの詳細については、互換性マトリックス を参照してください。

1. Panorama Web インターフェイス にログインし、**Dashboard** の一般情報ウィジェットを確認して、PAN-OS 11.1 互換プラグイン バージョンが正常にインストールされたことを確認します。

   また、Panorama CLI にログインし、コマンド `show plugins installed` を入力して、現在インストールされているプラグインのリストを表示することもできます。
2. **[Panorama]** > **[Plugins (プラグイン)]** を選択し、インストールされなかったプラグインを検索します。
3. PAN-OS 11.1 でサポートされているプラグイン バージョンをインストールします 。
4. Panorama にインストールされているすべてのプラグインが PAN-OS 11.1 でサポートされているバージョンを実行するまで、上記の手順を繰り返します。

STEP 14 | (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。

STEP 15 | (Panorama モード に推奨) Panorama 仮想アプライアンスのメモリを 64 GB に増やします

Panorama モードの Panorama 仮想アプライアンスを PAN-OS 11.1 に正常にアップグレードした後、Palo Alto Networks では、プロビジョニング不足の Panorama 仮想アプライアンスに関連するロギング、管理、および運用パフォーマンスの問題を回避するために、増加したシステム要件 を満たすために、Panorama 仮想アプライアンスのメモリを 64GB に増やすことをお勧めします。

STEP 16 | (Panorama および FIPS-CC モードの管理対象デバイス)FIPS-CC モードでの Panorama デバイスと管理対象デバイスのアップグレード.

FIPS-CC モードで Panorama および管理対象デバイスをアップグレードするには、PAN-OS 11.1 リリースの実行中に Panorama 管理に追加された場合、FIPS-CC モードのデバイスのセキュアな接続ステータスをリセットする必要があります。次の管理対象デバイスをPanorama管理に再度オンボードする必要があります。

- FIPS-CC モードの管理対象デバイスが、デバイス登録認証キーを使用して Panorama に追加されました。
- デバイス登録認証キーを使用して Panorama に追加されました

管理対象デバイスが PAN-OS 10.0 以前のリリースを実行している間に、Panorama 管理に追加された管理対象デバイスを再オンボーディングする必要はありません。

STEP 17 | (PAN-OS 10.2 以降のリリース)OpenSSL Security レベル 2 に準拠するように、すべての証明書を再生成または再インポートします。

この手順は、PAN-OS 10.1 以前のリリースから PAN-OS 11.1 にアップグレードする場合に必要です。PAN-OS 10.2 からアップグレードし、証明書をすでに再生成または再インポートしている場合は、この手順をスキップします。

すべての証明書が次の最小要件を満たしている必要があります。

- RSA 2048 ビット以上、または ECDSA 256 ビット以上
- SHA256 以上のダイジェスト

証明書の再生成または再インポートの詳細については、PAN-OS Administrator's Guide または Panorama Administrator's Guide を参照してください。

STEP 18 | **[Commit (コミット)]** > **[Commit and Push (コミットとプッシュ)]** を選択し、[パノラマ] 管理対象の設定をすべての管理対象デバイスにコミットしてプッシュします。

Panoramaおよび管理対象デバイスをPAN-OS 11.1に正常にアップグレードしたら、選択した構成を管理対象デバイスにプッシュし、Panoramaが管理するマルチvsysファイアウォールの改善された共有構成オブジェクト管理を活用する前に、Panorama管理対象構成を完全にコミットしてプッシュする必要があります。

インターネット接続のない Panorama のコンテンツ更新プログラムを自動的にインストールする

Panorama™ 管理サーバー、管理ファイアウォール、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 ネットワークのファイアウォール、Log Collectors、WildFire® アプライアンスにコンテンツの更新を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。インターネットアクセスを使用して Panorama を展開した後、コンテンツの更新を SCP サーバーに自動的にダウンロードするように、インターネットに接続された Panorama を構成します。SCP サーバーから、エア ギャップ Panorama は、コンテンツの更新スケジュールに従ってコンテンツの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構成されています。Panoramaは、インターネットアクセスを持つPanoramaがSCPサーバーにコンテンツの更新をダウンロードするとき、またはエアギャップPanoramaがSCPサーバーからコンテンツの更新をダウンロードしてインストールするときに、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 からインターネック接続のないパノラマへの以下のコンテンツ更新スケジュールのみがサポートされます。

コンテンツ更新ファイル名を *SCP* サーバーに正常にダウンロードした後は、操作したり変更したりしないでください。*Panorama* は、変更されたファイル名を含むコンテンツの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、コンテンツの自動更新を成功させるには、*SCP* サーバーに十分なディスク領域があること、ダウンロードが開始しようとしているときに *SCP* サーバーが実行していること、および両方の *Panoramas* の電源が入っており、再起動の途中で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コンテンツ更新のコンテンツの自動更新を構成する方法を示します。

STEP 1 | SCP サーバーをデプロイします。

管理対象ファイアウォール、ログコレクター、および WildFire アプライアンスのコンテンツ更新は、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。空隙状態の Panorama は、SCP サーバーからコンテンツの更新をダウンロードし、管理されたファイアウォール、WildFire アプライアンス、およびログ コレクターに更新をインストールします。

コンテンツ更新用のフォルダ ディレクトリを作成する場合は、コンテンツの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、大量のコンテンツ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コンテンツ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 アップデート サーバーと通信し、コンテンツの更新を 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

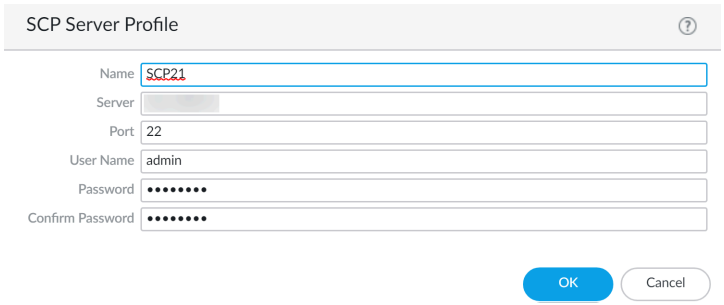
STEP 3 | インターネット接続せずに Panorama をデプロイします。

この Panorama は、SCP サーバーと通信して、管理対象のファイアウォール、ログ コレクター、および WildFire アプライアンスでコンテンツの更新をダウンロードしてインストールします。

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
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 | SCP サーバーにコンテンツの更新をダウンロードするように、インターネットに接続された Panorama を構成します。

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。



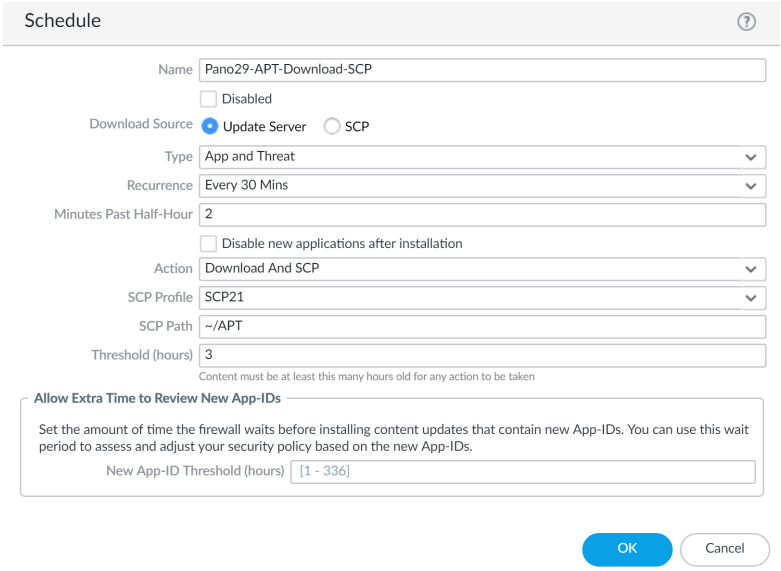
3. コンテンツ更新スケジュールを作成して、コンテンツの更新を SCP サーバーに定期的にダウンロードします。

   管理されたファイアウォール、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てインストールするコンテンツ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** > デバイス展開 > 動的更新を選択し、[スケジュール、コンテンツ更新スケジュール **Add** を選択します。
   2. コンテンツ更新スケジュールの説明的な 名 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. コンテンツ更新 **Type** を選択します。
   5. Panorama が Palo Alto Networks 更新サーバーをチェックして新しいコンテンツの更新を行う間隔を設定するには、繰り返し を選択します。

      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。同じ繰り返し間隔でダウンロードするように複数のコンテンツ更新をスケジュールしている場合は、パノラマおよび *SCP* サーバーの過負荷を避けるために、それらをずらして調整します。

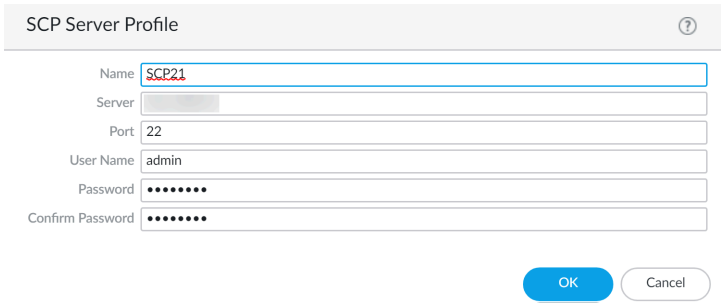
6. **Action (**アクション**)** に対して、**Download And SCP (**ダウンロードと **SCP)** を選択します。
7. 前のステップで設定した **SCP Profile (SCP** プロファイル**)** を選択します。
8. コンテンツ更新タイプの **SCP** パス を入力します。
9. (オプション) コンテンツの更新に **Threshold**を時間単位で入力します。Panorama は、この時間 (またはそれ以前) のコンテンツ更新プログラムのみをダウンロードします。
10. **OK** をクリックして変更内容を保存します。



4. 変更を **Commit (**コミット**)** します。

STEP 5 | SCP サーバーからコンテンツの更新をダウンロードするように、エア ギャップ Panorama を設定し、管理されたファイアウォール、ログ コレクター、および WildFire アプライアンスに更新プログラム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. SCP サーバーからコンテンツの更新を定期的にダウンロードしてインストールするコンテンツ更新スケジュールを作成します。

   管理されたファイアウォール、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てインストールするコンテンツ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** > デバイス展開 > 動的更新を選択し、[スケジュール、コンテンツ更新スケジュール **Add** を選択します。
   2. コンテンツ更新スケジュールの説明的な 名 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. コンテンツ更新タイプの **SCP** パス を入力します。
   6. コンテンツ更新 **Type** を選択します。
   7. Panorama が Palo Alto Networks 更新サーバーをチェックして新しいコンテンツの更新を行う間隔を設定するには、繰り返し を選択します。

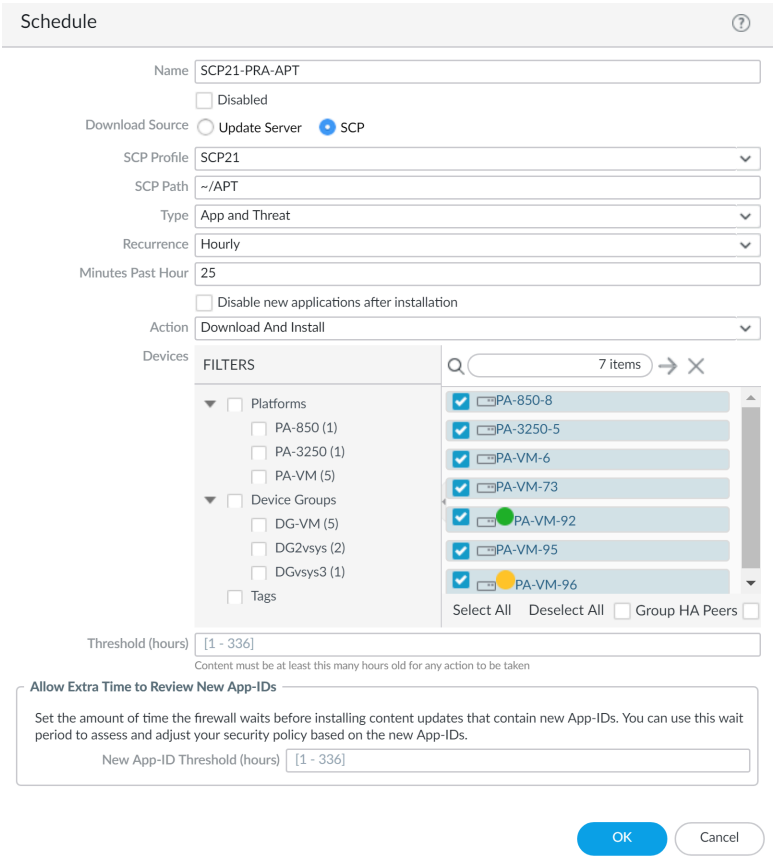
より正確な繰り返しスケジュールを設定するには、選択した繰り返し間隔を過ぎた分数を入力します。同じ繰り返し間隔を使用してダウンロードするように複数のコンテンツ更新をスケジュールしている場合は、*Panorama* および *SCP* サーバーの過負荷を避けるために、それらの更新をずらしてください。

8. アクションの場合は、[ダウンロードまたはダウンロードしてインストール を選択します。

***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。*

ダウンロードを選択した場合は、管理されたファイアウォールでコンテンツ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. コンテンツ更新プログラムをインストールする **Devices** を選択します。
10. (オプション) コンテンツの更新に **Threshold**を時間単位で入力します。Panorama は、この時間 (またはそれ以前) のコンテンツ更新プログラム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。



4. 変更を**Commit** (コミット) します。

HA 構成で Panorama をアップグレードする

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。

FIPS-CC モードの Panorama および管理対象デバイスを PAN-OS 10.2 以前のリリースから PAN-OS 11.1 にアップグレードする場合、PAN-OS 10.2 リリースの実行中に Panorama 管理に追加した場合は、FIPS-CC モードでデバイスのセキュア接続ステータスをリセットする追加手順を実行する必要があります。FIPS-CC モードでの Panorama および FIPS-CC デバイスのアップグレードの詳細については、FIPS-CC モードでの Panorama デバイスと管理対象デバイスのアップグレードを参照してください。

Panorama を更新する前に、PAN-OS 11.0 に必要な最小コンテンツ リリース バージョンについては、リリース ノート を参照してください。

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。

- インターネット接続で Panorama をアップグレードする
- インターネット接続なしでPanoramaをアップグレード

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 | (Panorama Interconnectプラグインのみ) PanoramaノードをPanoramaコントローラーと同期します。

Panoramaノードのアップグレードを開始する前に、Panoramaコントローラーとの Panoramaノードの設定を同期する必要があります。これは、アップグレードが正常に完了した後に、一般的なPanoramaコントローラーの構成をPanoramaノードに正常にプッシュするために必要です。

STEP 3 | (ベスト プラクティス)Cortex データ レイク (CDL) を活用している場合は、をインストールして、Panorama の各 HA ピアに Panorama デバイス証明書 をインストールします。

Panorama は、PAN-OS 11.0 へのアップグレード時に、CDL 取り込みおよびクエリ エンドポイントでの認証にデバイス証明書を使用するように自動的に切り替わります。

PAN-OS 11.0 にアップグレードする前にデバイス証明書をインストールしない場合、*Panorama* は認証に既存のロギング サービス証明書を引き続き使用します。

STEP 4 | 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** セクション (**Panorama** > **High Availability**), **Suspend local Panorama**.
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 5 | 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。

- インターネット接続で Panorama をアップグレードする
- インターネット接続なしでPanoramaをアップグレード

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 6 | 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 7 | (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

STEP 8 | (Panorama モード に推奨) Panorama 仮想アプライアンスのメモリを 64 GB に増やします

Panorama モードの Panorama 仮想アプライアンスを PAN-OS 11.1 に正常にアップグレードした後、Palo Alto Networks では、プロビジョニング不足の Panorama 仮想アプライアンスに関連するロギング、管理、および運用パフォーマンスの問題を回避するために、増加したシステム要件 を満たすために、Panorama 仮想アプライアンスのメモリを 64GB に増やすことをお勧めします。

STEP 9 | **[Commit (コミット)]** > **[Commit and Push (コミットとプッシュ)]** を選択し、Panorama管理対象の設定をすべての管理対象デバイスにコミットしてプッシュします。

Panoramaおよび管理対象デバイスをPAN-OS 11.1に正常にアップグレードしたら、選択した構成を管理対象デバイスにプッシュし、Panoramaが管理するマルチvsysファイアウォールの改善された共有構成オブジェクト管理を活用する前に、Panorama管理対象構成を完全にコミットしてプッシュする必要があります。

STEP 10 | (Panorama および FIPS-CC モードの管理対象デバイス)FIPS-CC モードでの Panorama デバイスと管理対象デバイスのアップグレード.

FIPS-CC モードで Panorama および管理対象デバイスをアップグレードするには、PAN-OS 11.1 リリースの実行中に Panorama 管理に追加された場合、FIPS-CC モードのデバイスのセキュアな接続ステータスをリセットする必要があります。次の管理対象デバイスをPanorama管理に再度オンボードする必要があります。

- FIPS-CC モードの管理対象デバイスが、デバイス登録認証キーを使用して Panorama に追加されました。
- デバイス登録認証キーを使用して Panorama に追加されました

管理対象デバイスが PAN-OS 10.0 以前のリリースを実行している間に、Panorama 管理に追加された管理対象デバイスを再オンボーディングする必要はありません。

STEP 11 | OpenSSL セキュリティー・レベル 2 に準拠するために、すべての証明書を再生成または再インポートします。

この手順は、PAN-OS 10.1 以前のリリースから PAN-OS 11.1 にアップグレードする場合に必要です。PAN-OS 10.2 からアップグレードし、証明書をすでに再生成または再インポートしている場合は、この手順をスキップします。

すべての証明書が次の最小要件を満たしている必要があります。

- RSA 2048 ビット以上、または ECDSA 256 ビット以上
- SHA256 以上のダイジェスト

証明書の再生成または再インポートの詳細については、PAN-OS Administrator's Guide または Panorama Administrator's Guide を参照してください。

PAN-OSソフトウェアパッチのインストール

どこで使用できますか?	何が必要ですか?
• PAN-OS 11.1.3以降のリリースを実行しているパノラマ	☐ デバイス管理ライセンス ☐ サポートライセンス ☐ PAN-OS 11.1.3 以降もしくは 11.1 リリース ☐ アウトバウンドインターネットアクセス

「PAN-OS 11.1リリースノート」を確認してから、次の手順に従ってPAN-OSソフトウェアパッチをインストールし、現在Panorama™ 管理サーバーで実行されているPAN-OSリリースのバグと共通脆弱性および暴露（CVE）に対処します。PAN-OSソフトウェアパッチをインストールすると、長期間のメンテナンスをスケジュールしなくてもバグやCVEに対する修正が適用され、新しいPAN-OSリリースのインストールに伴う新たな既知の問題やデフォルト動作の変更をもたらすことなく、すぐにセキュリティ体制を強化できます。さらに、現在インストールされているソフトウェアパッチを元に戻して、ソフトウェアパッチをインストールしたときに適用されたバグやCVEの修正をアンインストールすることもできます。

PAN-OSのソフトウェアパッチをインストールまたは元に戻すと、システムログが生成されます（**[Monitor (モニター)]** > **[Logs (ログ)]** > **[System (システム)]**）。パロアPalo Alto Networks カスタマーサポートポータルからPAN-OSソフトウェアパッチをダウンロードするには、アウトバウンドインターネット接続が必要です。

- インストール
- 元に戻す

インストール

STEP 1 | Panorama Web インターフェースにログインします。

STEP 2 | Palo Alto Networksの更新サーバーから最新のPAN-OSソフトウェアパッチを取得するには、「**[Panorama]** > **[Software (ソフトウェア)]** **[Check Now (今すぐチェック)]** 」を順に選択します。

STEP 3 | ［**Include Patch (パッチを含める)**］をオンに（有効に）すると、使用可能なすべての PAN-OS ソフトウェア パッチが表示されます。

STEP 4 | 現在PanoramaにインストールされているPAN-OSリリースのソフトウェアパッチを探します。

ソフトウェアパッチは、**[Version (バージョン)]**名の横に表示される `[Patch (パッチ)]` ラベルで示されます。

STEP 5 | 「**More Info (詳細情報)**」を参照して、重大なバグや CVE の修正などのソフトウェアパッチの詳細、および修正を適用するために次世代ファイアウォールの再起動が必要かどうかを確認してください。

STEP 6 | ソフトウェアパッチをダウンロードします。

（HA のみ）PAN-OS ソフトウェアパッチをダウンロードするには、[HA ピアに同期] をチェック（有効化）して **[Continue Download (ダウンロードを続行)]** を選択します。

ソフトウェアパッチが正常にダウンロードされたら、**[Close (閉じる)]** をクリックします。

STEP 7 | ソフトウェアパッチをインストールする

ソフトウェアパッチが正常にインストールされたら、**[Close (閉じる)]** をクリックします。

STEP 8 | ソフトウェアパッチを適用します。

インストールされているPAN-OSソフトウェアパッチをPanoramaに適用するかどうかを確認するメッセージが表示されたら、［**Apply (適用)**］をクリックします。

ステータスバーに、PAN-OS ソフトウェアパッチアプリケーションの現在の進行状況が表示されます。パッチが正常に適用されたら、**[Close (閉じる)]** をクリックします。

この時点で、PanoramaへのPAN-OSソフトウェアパッチの適用を完了するために再起動が必要な場合、Panoramaは自動的に再起動します。

STEP 9 | （HAのみ）PAN-OSソフトウェアパッチをPanorama HAピアにインストールします。

1. HA ピアの Panorama の Web インターフェイス にログインします。
2. **[Panorama]** > **[Software (ソフトウェア)]** **[Check Now (今すぐチェック)]** の順に選択します。
3. ソフトウェアパッチを**Install (インストール)**します
4. 必要に応じてPanoramaを再起動します。

元に戻す

STEP 1 | Panorama Web インターフェースにログインします。

STEP 2 | **[Panorama]** > **[Software (ソフトウェア)]**を選択し、元に戻すPAN-OSソフトウェアパッチを探します。

STEP 3 | ソフトウェアパッチを元に戻します。

PanoramaにインストールされているPAN-OSソフトウェアパッチを元に戻すかどうかを確認するメッセージが表示されたら、**[Revert (元に戻す)]**をクリックします。

PAN-OSソフトウェアパッチ適用の現在の進捗状況を示すステータスバーが表示されます。パッチが正常に適用されたら、**[Close (閉じる)]** をクリックします。

この時点で、PanoramaへのPAN-OSソフトウェアパッチの適用を完了するために再起動が必要な場合、ファイアウォールは自動的に再起動します。

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。

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 シリアル番号 <ser_num>
 start
```

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 移行 LC シリアル番号 <ser_num> 状態 ス
ロット: すべて 移行状態:進行中の完了率:0.04 推定残り時間:451 時間 47 分
```

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 シリアル番号 <ser_num> stop
```

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 仮想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満たしていない場合は、Panorama 仮想アプライアンス の CPU とメモリを増やします。

増加したデバイス管理容量要件 を確認して、既存の Panorama 仮想アプライアンスがアップグレード前に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 へのログインを行います。

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 で始めて、M-Series アプライアンスを管理専用モード でセットアップします。

もしくは

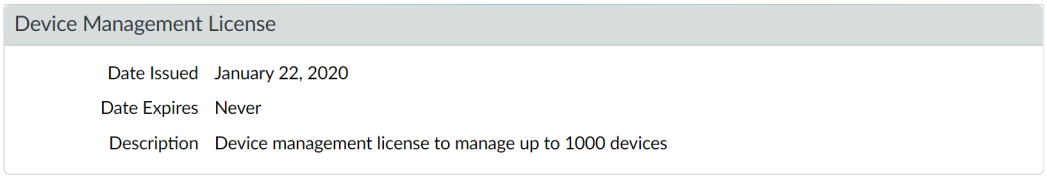
- Panorama 仮想アプライアンスを管理専用モード に設定します。

STEP 4 | Panorama Web インターフェースにログインします。

STEP 5 | Panorama 管理サーバーをアップグレードします。

- 「インターネット接続で Panorama をアップグレードする」を行います。
- 「インターネット接続なしでPanoramaをアップグレード」を行います。
- 「HA 構成で Panorama をアップグレードする」を行います。

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。

FIPS-CC モードでの Panorama デバイスと管理対象デバイスのアップグレード

PAN-OS 11.1 へのアップグレードが成功したら、FIPS-CC モードのすべての管理対象デバイスと、デバイスが PAN-OS 11.0 リリースを実行していたときに Panorama に追加されたすべての管理対象デバイスを Panorama 管理に再オンボードする必要があります。これには、FIPS-CC モードの Panorama と FIPS-CC モードのすべての管理対象デバイスの安全な接続ステータスをリセットする必要があります。安全な接続ステータスをリセットした後、 デバイス登録認証キーを使用して Panorama に追加されたファイアウォール、ログ コレクター、および WildFire アプライアンスを Panorama 管理に戻す必要があります。この手順は、PAN-OS 10.0 以前のリリースの実行中に Panorama に追加された管理対象デバイスには必要なく、影響もありません。これは、サポートされているすべての パノラマ モデル 、 次世代ファイアウォール ハードウェア、および FIPS-CC モードの VM シリーズ モデル に必要です。

STEP 1 | FIPS-CC モードで管理対象デバイスのリストを作成し、デバイス登録認証キーを使用して Panorama に追加された管理対象デバイスを作成します。これにより、後でマネージド デバイスを Panorama 管理に再オンボードするときに、作業に集中することができます。

STEP 2 | Panorama と管理対象デバイスを PAN-OS 11.1 にアップグレードします。

- インターネット接続で Panorama をアップグレードする
- インターネット接続なしでPanoramaをアップグレード
- HA 構成で Panorama をアップグレードする

STEP 3 | PAN-OS 11.1 へのアップグレードが成功したら、パノラマのシステム ログを確認して、FIPS-CC モードのどの管理対象デバイスがパノラマに接続できないかを特定します。

STEP 4 | Panoramaで安全な接続状態をリセットします。

この手順は、PAN-OS 11.1 リリースの実行中に Panorama 管理に追加された管理対象デバイスの接続をリセットし、元に戻すことはできません。この手順は、PAN-OS 11.1 にアップグレードされた PAN-OS 10.0 以前のリリースを実行しているときに追加されたファイアウォールの接続状態には影響しません。

1. Panorama CLI へのログインを行います。
2. 安全な接続ステータスをリセットします。

```
admin> request sc3 reset
```

3. Panoramaで管理サーバーを再起動します。

```
admin> debug software restart process management-server
```

4. (HA のみ) 高可用性 (HA) 構成のピアごとにこの手順を繰り返します。

STEP 5 | FIPS-CC モードで管理対象デバイスの安全な接続状態をリセットします。

このコマンドは管理対象デバイス接続をリセットし、元に戻すことはできません。

1. 管理対象デバイス CLI にログインします。
   - ファイアウォール CLI へのログイン
   - Log Collector CLI にログインします。
   - ワイルドファイア アプライアンス CLI にログインします。
2. セキュリティで保護された接続状態をリセットします。

```
admin> request sc3 reset
```

3. 管理対象デバイスで管理サーバーを再起動します。

```
admin> debug software restart process management-server
```


STEP 6 | 影響を受ける管理対象デバイスをPanoramaに追加します。

- 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 7 | OpenSSL セキュリティー・レベル 2 に準拠するために、すべての証明書を再生成または再インポートします。

PAN-OS 11.1 へのアップグレードでは、すべての証明書が次の最小要件を満たしている必要があります。

- RSA 2048 ビット以上、または ECDSA 256 ビット以上
- Digest of SHA256 以上

証明書の再生成または再インポートの詳細については、PAN-OS Administrator's Guide または Panorama Administrator's Guide を参照してください。

Panorama 11.1 からのダウングレード

PAN-OS 11.1では、インラインディープラーニングを活用するゼロデイエクスプロイト防止の高度な脅威防止サポート、Panoramaと管理対象デバイスの簡素化されたソフトウェアアップグレードとダウングレードにより、複数のPAN-OS®リリース間で管理対象デバイスをアップグレードする運用上の負担を軽減し、AIOpsを使用して侵害されたセキュリティ体制からの露出をさらに排除するプロアクティブなベストプラクティス評価(BPA)、セキュリティを犠牲にすることなくクラウドへの移行を支援するオンプレミスWebプロキシが導入されています。 または効率、IPv6 アドレスを取得するためのステートフル DHCPv6 クライアントの firewall サポート、Cloud Identity Engine (CIE) のユーザー コンテキストの可視性の強化、管理アクセスの TLSv1.3 サポート、およびポリシー ルールの推奨事項のスケーリングと管理を容易にするための IoT セキュリティ ポリシー ルールの推奨事項が強化されています。Panorama 11.1 リリースを実行している Log Collectors および Panorama を以前の機能リリースにダウングレードする前に、次のワークフローを使用して firewall を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。

PAN-OS 11.1 から以前の *PAN-OS* リリースにダウングレードするには、ターゲットの *PAN-OS* リリースへのダウングレード パスを続行する前に、優先する *PAN-OS 11.0* 以降の *PAN-OS 11.0* リリースをダウンロードしてインストールする必要があります。*PAN-OS 11.0* 以前の *PAN-OS* リリースにダウングレードしようとすると、*PAN-OS 10.2* からのダウングレードは失敗します。

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。ダウングレードできる *firewall* およびアプライアンスについては、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、ダウングレード後に異なる、または使用できなくなるすべての機能と構成設定を考慮していることを確認する必要があります。

PAN-OS 11.1 の実行時に生成されるログは、*PAN-OS 11.0* 以前のリリースと互換性がなく、ダウングレード時に削除されます。*PAN-OS 11.1.1* または *PAN-OS 11.1.0* の実行時に生成されたログを保持するには、対象の *PAN-OS* リリースへのダウングレードを開始する前に、まず *PAN-OS 11.1.2* に アップグレードする 必要があります。これは、ダウングレード後に *PAN-OS 11.1* で生成されたログを正常に回復するために必要です。

STEP 1 | Panorama Web インターフェースにログインします。

STEP 2 | 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 3 | 専用ログコレクターの構成された認証があり、`admin` 管理者を削除した場合は、新しい `admin`ユーザーを構成して専用ログ コレクターにプッシュします。

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 4 | **[Panorama]** > **[Plugins]**を順に選択し、Panoramaにインストールされている PAN-OS 11.0 でサポートされるプラグイン バージョンを ダウンロードします。

PAN-OS 11.0 以前のリリースでサポートされている Panorama プラグインのバージョンについては、[Panorama Plugins Compatibility Matrix (Panorama プラグイン互換性マトリックス)] を参照してください。

これは、Panorama を PAN-OS 11.1 から PAN-OS 11.0 以前のリリースに正常にダウングレードするために必要です。ダウンロードしたプラグインのバージョンは、PAN-OS 11.0 へのダウングレード中に自動的にインストールされます。サポートされているプラグインのバージョンがダウンロードされていない場合、PAN-OS 11.0 へのダウングレードはブロックされます。

(ZTP プラグインのみ) Panorama を *PAN-OS 11.0* に正常にダウングレードするには、ダウングレード プロセスを開始する前に ZTP プラグイン をアンインストールする必要があります。*PAN-OS 11.0* へのダウングレードに成功したら、*Panorama* に *ZTP* プラグインを再インストールする必要があります。

STEP 5 | PAN-OS 11.1 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。

PAN-OS 11.1 から以前の機能リリースにダウングレードするには、まず優先する *PAN-OS 11.0* リリースまたはそれ以降の *PAN-OS 11.0* リリースにダウングレードする必要があります。優先 *PAN-OS 11.0* 以降の *PAN-OS 11.0* リリースに正常にダウングレードした後、ターゲットの *PAN-OS* バージョンへのダウングレードを続行できます。

複数の *firewall* をダウングレードする場合は、ダウングレードを開始する前に、各 *firewall* 固有の *PAN-OS 11.0* イメージを *Panorama* にダウンロードして、プロセスを合理化します。たとえば、*PA-220 firewall* を *PAN-OS 11.0* にダウングレードするには、*PanOS_220-11.0.0* または *PanOS_3000-11.0.0* 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））。

   （PAN-OS 11.1.3以降）デフォルトでは、優先リリースと対応する基本リリースが表示されます。優先リリースのみを表示するには、**[Base Releases (基本リリース)]**チェックボックスをオフ(選択解除)にします。同様に、基本リリースのみを表示するには、**[Preferred Releases (優先リリース)]** チェックボックスを無効 (クリア) にします。
2. ダウングレードする各モデルまたは一連の firewall の PAN-OS 11.0 イメージを見つけます。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

Install (アクション列) 適切な PAN-OS 11.0 バージョンを選択し、ダウングレードするすべての firewall を選択し、インストール後にデバイスを再起動する 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 6 | Panorama 11.0を実行している各Log Collectorをダウングレードします。

PAN-OS 11.1 から以前の機能リリースにダウングレードするには、まず優先する *PAN-OS 11.0* 以降の *PAN-OS 11.0* リリースにダウングレードする必要があります。優先 *PAN-OS 11.0* 以降の *PAN-OS 11.0* リリースに正常にダウングレードした後、ターゲットの *PAN-OS* バージョンへのダウングレードを続行できます。

1. ログ コレクター CLI にログインし 、すべての `esdata` ディレクトリを削除します。

   `admin>` デバッグ **`elasticsearch`** データを消去する

   ダウングレードするコレクター グループ内のすべてのログ コレクターに対してこの手順を繰り返します。
2. 利用可能なイメージを今すぐチェック (**panorama** > **Device Deployment** > **Software**).

   （PAN-OS 11.1.3以降）デフォルトでは、優先リリースと対応する基本リリースが表示されます。優先リリースのみを表示するには、**[Base Releases (**基本リリース**)]**チェックボックスをオフ(選択解除)にします。同様に、基本リリースのみを表示するには、**[Preferred Releases (**優先リリース**)]** チェックボックスを無効 (クリア) にします。
3. PAN-OS 11.0 イメージを見つけます。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）。
4. ダウンロードが完了したら、Panorama 11.1 を実行している各 Log Collector 上のイメージを 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 7 | Panorama をダウングレードします。

PAN-OS 11.1 から以前の機能リリースにダウングレードするには、まず優先する *PAN-OS 11.0* 以降の *PAN-OS 11.0* リリースにダウングレードする必要があります。優先 *PAN-OS 11.0* 以降の *PAN-OS 11.0* リリースに正常にダウングレードした後、ターゲットの *PAN-OS* バージョンへのダウングレードを続行できます。

1. (Panorama モードのみ)Panorama CLI にログインし 、すべての `esdata` ディレクトリを削除します。

   `admin>` デバッグ **`elasticsearch`** データを消去する
2. Panorama Web インターフェイスにログインし 、**[Panorama]** > **[Software (**ソフトウェア**)]** と **[Check Now (**今すぐ確認**)]**を選択して、利用可能な画像を確認します 。

   （PAN-OS 11.1.3以降）デフォルトでは、優先リリースと対応する基本リリースが表示されます。優先リリースのみを表示するには、**[Base Releases (**基本リリース**)]**チェックボックスをオフ(選択解除)にします。同様に、基本リリースのみを表示す

るには、**[Preferred Releases (優先リリース)]** チェックボックスを無効 (クリア) にします。

3. ターゲットの PAN-OS イメージを見つけます。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。
4. 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。
5. 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 8 | (ZTP プラグインのみ)ZTP プラグインを再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. ZTP プラグインをインストールします。
3. **Panorama** > **Zero Touch Provisioning** を選択し **ZTP**(enable)を確認します.

STEP 9 | (Enterprise DLP only) Enterprise DLP データ フィルタリング設定 を編集して、**Max File Size** を 20 MB 以下に減らします。

これは、Enterprise DLP 4.0.1 以降のリリースの Panorama プラグインからダウングレードする場合に必要です。大きなファイル サイズの検査は、Enterprise DLP 4.0.1 以降のリリースでサポートされています。

STEP 10 | (エンタープライズ DLP のみ) Panorama 上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 DLP クラウド サービスと同期します。

これは、Panorama を PAN-OS 11.0.2 および Enterprise DLP プラグイン 4.0.1 から PAN-OS 11.0.1 またはそれ以前の 11.1 リリースおよび Enterprise DLP プラグイン 4.0.0 にダウングレードする場合に必要です。

1. Panorama CLI にログインします。
2. Panorama から DLP クラウド サービスにエンタープライズ DLP 構成をプッシュします。

   ```
   admin> プラグインのリクエスト dlp push-dlp-config
   ```

3. Enterprise DLP プラグインをリセットします。

   ```
   admin> プラグインのDLPリセットをリクエストする
   ```

4. Panorama にコミットし、Enterprise DLP を使用して管理対象ファイアウォールにプッシュします。
   1. Panorama Web インターフェースにログインします。
   2. **[Commit (コミット)]** > **[Commit to Panorama (Panorama へのコミット)]** を順に選択し、**[Commit (コミット)]**します。
   3. **[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。
   4. **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。
   5. **OK** をクリックします。
   6. エンタープライズ DLP を使用している管理対象ファイアウォールに構成の変更をプッシュします 。

STEP 11 | Panorama CLI にログインし 、PAN-OS 11.1 で生成されたログを回復します。

```
admin> debug logdb migrate-lc start log-type all
```

ログ移行ステータスを表示するには:

```
admin> debug logdb migrate-lc status
```


Panorama アップグレードのトラブルシューティング

Panorama のアップグレードのトラブルシューティングを行うには、次の表を使用して、考えられる問題とその解決方法を確認してください。

症状	解決策
ソフトウェア保証ライセンスの期限が切れています。	CLI から、期限切れのライセンス キーを削除します。 1. ライセンス キーの削除 **<software license key>** を入力します。 2. ライセンス キーの削除 **Software_Warranty<expiredate>.key** を入力します。
最新の PAN-OS ソフトウェア バージョンは使用できませんでした。	現在インストールされているバージョンより 1 つ先の機能リリースのソフトウェア バージョンのみが表示されます。たとえば、8.1 リリースがインストールされている場合、9.0 リリースのみが使用できます。9.1 リリースを表示するには、最初に 9.0 にアップグレードする必要があります。
(レガシーモードのPanorama仮想アプライアンスのみ)アップグレード バージョンは、ソフトウェア マネージャにプリロードできませんでした。	この問題は、十分なリソースが不足している場合に発生します。仮想マシンの容量を増やすか、レガシーモードからPanoramaモードに移行できます。

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。

- どのような更新プログラム Panorama は他のデバイスにプッシュできますか。
- 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 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
- 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
- インターネット接続を使用して Panorama から WildFire クラスターをアップグレードする
- インターネット接続なしで Panorama から WildFire クラスターをアップグレードする

- ZTP ファイアウォールのアップグレード
- PAN-OSソフトウェアパッチのインストール
- Panorama でコンテンツのアップデートを元に戻す

どのような更新プログラム Panorama は他のデバイスにプッシュできますか。

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。

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] 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] 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。

Panorama では、同じ種類の更新プログラムに対して一度に *1* つの更新プログラムしかダウンロードできません。同じ種類の複数の更新プログラムを同じ時間の繰り返し中にダウンロードするようにスケジュールすると、最初のダウンロードのみが成功します。

firewall が *Palo Alto Networks® Update Server* に直接接続している場合は、パノラマ テンプレート *(**Device** > **Dynamic Updates**)* を使用して content Update schedules を *firewall* にプッシュ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。

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、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。詳細については、 Panorama Management Compatibility を参照してください。

  firewall を PAN-OS 11.0 にアップグレードする前に、まず Panorama を 11.0 にアップグレードする必要があります。
- 専用ログコレクタは、管理対象のファイアウォールがログを転送するバージョンと同じまたはそれ以降のPAN-OSバージョンを実行している必要があります。
- PAN-OS 11.1 を実行している Panorama は、同じまたは以前の PAN-OS リリースを実行している WildFire® アプライアンスおよび WildFire アプライアンス クラスタを管理できます。詳細については、 Panorama Management Compatibility を参照してください。

  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。詳細については、 Panorama Management Compatibility を参照してください。

  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。

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。

PAN-OS 8.1 からアップグレードする場合、*PAN-OS 9.0* では、ローカルおよび専用のログ コレクタ用の新しいログ データ形式が導入されました。*PAN-OS 10.1* へのアップグレード パスでは、*PAN-OS 8.1* から *PAN-OS 9.0* にアップグレードすると、既存のログ データが自動的に新しいログ データ形式に移行されます。

ログ データが失われないように、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。

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®Panorama と *Log Collectors* は同じソフトウェア リリース バージョンを実行し、*Panorama*、*Log Collectors*、および管理対象ファイアウォールはすべて同じコンテンツ 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 は、Log Collectors と同じ (またはそれ以降の) ソフトウェア・リリースを実行している必要がありますが、同じまたはそれ以降のコンテンツ・リリース・バージョンを持っている必要があります。

- ソフトウェア リリース バージョン - Panorama 管理サーバーが、Log Collector を更新するリリースと同じかそれ以降のソフトウェア リリースをまだ実行していない場合は、Log Collector を更新する前に、Panorama (Panorama のコンテンツの更新とソフトウェア アップグレードのインストール を参照) に同じかそれ以降の Panorama リリースをインストールする必要があります。
- コンテンツ リリース バージョン - コンテンツ リリース バージョンの場合、すべての Log Collector が最新のコンテンツ リリース バージョンを実行しているか、少なくとも Panorama で実行されているバージョンよりも新しいバージョンを実行していることを確認する必要があります。そうでない場合は、Panorama 管理サーバーでコンテンツ リリー

ス バージョンを更新する前に、まず Log Collectors ファイアウォールを Panorama から PAN-OS 11.1 にアップグレードするしてから更新します。

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 コレクター—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 | ネットワーク上の以下のTCPポートを有効にします。

ログコレクタ間通信を可能にするには、ネットワーク上でこれらのTCPポートを有効にする必要があります。

- TCP/9300
- TCP/9301
- TCP/9302

STEP 3 | 「PAN-OS 11.1 へのアップグレード パスを決定する」を行います。

現在実行中の PAN-OS バージョンから PAN-OS 11.1.0へのパスにある機能リリース 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。

Release Notes のPAN-OS アップグレード チェックリスト、既知の問題、既定の動作の変更点を確認し、アップグレード パスの一部として渡す各リリースアップグレード/ダウングレードに関する考慮事項を確認します。

STEP 4 | 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. Panorama Web インターフェースにログインします。
2. **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。

3. 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。
4. インストール コンテンツの更新 (アプリケーションと脅威の更新) を他のユーザーの前にインストールします。

   サブスクリプションにアプリケーションと脅威の両方のコンテンツが含まれている場合は、まず アプリ コンテンツをインストールします。これにより、アプリケーションと脅威の両方のコンテンツが自動的にインストールされます。

   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。
5. 必要に応じて、他の更新プログラム(ウイルス対策、WildFire、または URL フィルタリング)に対して、上記のサブステップを繰り返し、一度に 1 つずつ、任意の順序で実行します。

STEP 5 | PAN-OS 11.1 へのアップグレード パスに沿って、Log Collector を PAN-OS リリースにアップグレードします。

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。

1. Panorama がインターネットに接続されている場合 のログ コレクタを PAN-OS 9.1 にアップグレードします。
2. Panorama がインターネットに接続されている場合 のログ コレクタを PAN-OS 10.0 にアップグレードします。
3. Log Collectors When Panorama is Internet-Connected を PAN-OS 10.1 にアップグレードします。

   PAN-OS 11.1 では、新しいログ形式が導入されています。PAN-OS 11.1 から PAN-OS 10.1 へのアップグレードでは、PAN-OS 8.1 以前のリリースで生成されたログを移行することを選択できます。それ以外の場合、PAN-OS 10.1 へのアップグレードが正常に完了すると、これらのログは自動的に削除されます。移行中、ログ データは [ACC] タブまたは [監視] タブに表示されません。移行が行われている間、ログ データは適切なログ コレクタに転送され続けますが、パフォーマンスに影響が生じる場合があります。
4. Panorama がインターネットに接続されている場合 のログ コレクタを PAN-OS 10.2 にアップグレードします。
5. Panorama がインターネットに接続されている場合 のログ コレクタを PAN-OS 11.0 にアップグレードします。

STEP 6 | Log Collector を PAN-OS 11.1 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. ダウンロード PAN-OS 10.1 リリースのリリース バージョンのモデル固有のファイルです。たとえば、M シリーズ アプライアンスを Panorama 11.1.0 にアップグレードするには、`Panorama_m-11.1.0` 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. インストールPAN-OS 11.1 をクリックし、適切な Log Collector を選択します。
4. 選択された1つ以上のログコレクタにPAN-OS 10.0以前のリリースで生成されたログが含まれている場合、通知が表示されます。

   この通知は、PAN-OS 11.1.2以降の11.1リリースを最初にインストールしようとしたときに表示され、通知が閉じられた後の2回目には表示されません。PAN-OS 10.0以前のリリースを実行しているときにPanoramaまたは管理対象デバイスによって生成されたログが検出され、アップグレード時に削除されることを警告します。つまり、アップグレードが正常に終了した後は、影響を受けたログは表示または検索できません。

   ただし、これらの影響を受けたログはアップグレード後に復元できます。通知では、次の情報も提供されます。複数のログコレクタを選択した場合は、**[Tasks (**タスク**)]**をクリックし、各ログコレクタの失敗したインストールジョブの詳細を表示して、必要な移行コマンドを表示およびコピーします。

   - 影響を受けるログの種類。
   - 各ログタイプの影響を受けるタイムフレーム。
   - 影響を受けたログをログタイプごとにリカバリするために必要な各`debug logdb migrate-lc`コマンド。

     通知を閉じる前に、リストされている`debug logdb migrate-lc`をコピーします。

   通知を閉じます。
5. 必要に応じて、次のいずれかを選択します。
   - **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** をクリックしてアップロードまたはインストールを開始します。

   選択したログコレクタが正常に再起動したら、次のステップに進みます。

STEP 7 | 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:11.1.0 app-version:8750-8261 app-release-date:2023/08/31
 03:57:2
```

STEP 8 | （PAN-OS 11.1.2以降のリリース、Panoramaモードのみ）影響を受ける各 ログコレクタのログコレクタCLIにログインし 、前のステップで示した `debug logdb migrate-lc`コマンド を使用して影響を受けるログを復旧します。

これらのコマンドは順番に実行する必要があり、同時に実行することはできません。通知ウィンドウから`debug logdb migrate-lc`コマンドをコピーしていない場合は 、 **[Tasks (タスク)**］をクリックし、特定のログコレクタの失敗した`Install (インストール)`ジョブの詳細を表示します。

STEP 9 | (FIPS-CC モードのみ)FIPS-CC モードでの Panorama デバイスと管理対象デバイスのアップグレード.

専用 Log Collector が PAN-OS 11.1 リリースを実行しているときに、専用 Log Collector を Panorama 管理に追加した場合、FIPS-CC モードで専用 Log Collector をアップグレードするには、セキュア接続ステータスをリセットする必要があります。

専用Log CollectorがPAN-OS 10.0以前のリリースを実行している間は、Panorama管理に追加された専用Log Collectorを再オンボードする必要はありません。

STEP 10 | OpenSSL セキュリティー・レベル 2 に準拠するために、すべての証明書を再生成または再インポートします。

この手順は、PAN-OS 10.1 以前のリリースから PAN-OS 11.0 にアップグレードする場合に必要です。PAN-OS 10.2 からアップグレードし、証明書をすでに再生成または再インポートしている場合は、この手順をスキップします。

すべての証明書が次の最小要件を満たしている必要があります。

- RSA 2048 ビット以上、または ECDSA 256 ビット以上
- SHA256 以上のダイジェスト

証明書の再生成または再インポートの詳細については、PAN-OS Administrator's Guide または Panorama Administrator's Guide を参照してください。

STEP 11 | (Recommended for Panorama Virtual Appliance) Panorama Virtual Appliance のメモリを 64GB に増やします。

Panorama 仮想アプライアンスを Log Collector モードで PAN-OS 11.1 に正常にアップグレードした後、Palo Alto Networks では、プロビジョニング不足の Panorama 仮想アプライアンスに関連するロギング、管理、および運用パフォーマンスの問題を回避するために、増加したシステム要件 を満たすために、Panorama 仮想アプライアンスのメモリを 64 GB に増やすことをお勧めします。

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 8.1 からアップグレードする場合、*PAN-OS 9.0* では、ローカルおよび専用のログ コレクタ用の新しいログ データ形式が導入されました。*PAN-OS 10.1* へのアップグレード パスでは、*PAN-OS 8.1* から *PAN-OS 9.0* にアップグレードすると、既存のログ データが自動的に新しい形式に移行されます。

ログ データが失われないように、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。

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®Panorama と *Log Collectors* は同じソフトウェア リリース バージョンを実行し、*Panorama*、*Log Collectors*、および管理対象ファイアウォールはすべて同じコンテンツ 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 は、Log Collectors と同じ (またはそれ以降の) ソフトウェア・リリースを実行している必要がありますが、同じまたはそれ以降のコンテンツ・リリース・バージョンを持っている必要があります。

- 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 バージョン - コンテンツ リリース バージョンの場合、すべての Log Collector が最新のコンテンツ リリース バージョンを実行しているか、少なくともインストールするバージョンよりも新しいバージョンを実行しているか、Panorama で実行されていることを確認する必要があります。そうでない場合は、Panorama 管理サーバーでコンテンツ リリース バージョンを更新する前に、まず Log Collectors ファイアウォールを

Panorama から PAN-OS 11.1 にアップグレードするを更新します (Panorama のコンテンツの更新とソフトウェア アップグレードのインストール 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 コレクター—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 | 「PAN-OS 11.1 へのアップグレード パスを決定する」を行います。

Release Notes のPAN-OS アップグレード チェックリスト、既知の問題、既定の動作の変更点を確認し、アップグレード パスの一部として渡す各リリースのアップグレード/ダウングレードに関する考慮事項を確認します。

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 3 | ネットワーク上の以下のTCPポートを有効にします。

ログコレクタ間通信を可能にするには、ネットワーク上でこれらのTCPポートを有効にする必要があります。

- TCP/9300
- TCP/9301
- TCP/9302

STEP 4 | SCP または HTTPS 経由で Panorama にファイルを接続してアップロードできるホストに、最新のコンテンツとソフトウェアの更新をダウンロードします。

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. 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. 最新のコンテンツ更新プログラムをダウンロードします。
   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. **Download** は最新のコンテンツ更新を行い、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. ソフトウェア更新プログラムをダウンロードします。
   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 シリーズ アプライアンスを Panorama 11.1.0 にアップグレードするには、`Panorama_m-11.1.0` 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 | 最新の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 Web インターフェースにログインします。
2. **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。
3. **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。
4. **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。
5. ログ コレクタを選択します。
6. **OK** をクリックしてインストールを開始します。
7. 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 | PAN-OS 11.1 へのアップグレード パスに沿って、Log Collector を PAN-OS リリースにアップグレードします。

1. P1anorama がインターネットに接続されていない場合 のログ コレクタを PAN-OS 9.1 にアップグレードします。
2. Panorama がインターネットに接続されていない場合の場合は、ログ コレクタを PAN-OS 10.0 にアップグレードします。
3. Panorama がインターネットに接続されていない場合に Log Collectors をアップグレード を PAN-OS 10.1 にアップグレードします。

   PAN-OS 10.0 では、新しいログ形式が導入されています。PAN-OS 10.0 から PAN-OS 10.1 へのアップグレードでは、PAN-OS 8.1 以前のリリースで生成されたログを移行することを選択できます。それ以外の場合、PAN-OS 10.1 へのアップグレードが正常に完了すると、これらのログは自動的に削除されます。移行中、ログ データは [ACC] タブまたは [監視] タブに表示されません。移行が行われている間、ログ データは適切

なログ コレクタに転送され続けますが、パフォーマンスに影響が生じる場合があります。

4. panorama がインターネットに接続されていない場合に log collectors を PAN-OS 10.2 にアップグレード
5. panorama がインターネットに接続されていない場合に log collectors を PAN-OS 11.0 にアップグレード

STEP 7 | Log Collector を PAN-OS 11.1 にアップグレードします。

1. **[Panorama] > [Device Deployment**（デバイスのデプロイ）**] > [Software**（ソフトウェア）**]**の順に選択します。
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. **Install**PAN-OS 11.1 をクリックし、適切な Log Collector を選択します。
5. 選択された1つ以上のログコレクタにPAN-OS 10.0以前のリリースで生成されたログが含まれている場合、通知が表示されます。

   この通知は、PAN-OS 11.1.2以降の11.1リリースを最初にインストールしようとしたときに表示され、通知が閉じられた後の2回目には表示されません。PAN-OS 10.0以前のリリースを実行しているときにPanoramaまたは管理対象デバイスによって生成されたログが検出され、アップグレード時に削除されることを警告します。つまり、アップグレードが正常に終了した後は、影響を受けたログは表示または検索できません。

   ただし、これらの影響を受けたログはアップグレード後に復元できます。通知では、次の情報も提供されます。複数のログコレクタを選択した場合は、**[Tasks (**タスク**)]**をクリックし、各ログコレクタの失敗したインストールジョブの詳細を表示して、必要な移行コマンドを表示およびコピーします。

   - 影響を受けるログの種類。
   - 各ログタイプの影響を受けるタイムフレーム。
   - 影響を受けたログをログタイプごとにリカバリするために必要な各`debug logdb migrate-lc`コマンド。

     通知を閉じる前に、リストされている`debug logdb migrate-lc`をコピーします。

   通知を閉じます。
6. 必要に応じて、次のいずれかを選択します。
   - **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）。
7. **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。

   選択したログコレクタが正常に再起動したら、次のステップに進みます。

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:11.1.0 app-version:8750-8261 app-release-date:2023/08/31
 03:57:2
```

STEP 9 | （PAN-OS 11.1.2以降のリリース、Panoramaモードのみ）影響を受ける各 ログコレクタのログコレクタCLIにログインし 、前のステップで示した `debug logdb migrate-lc`コマンド を使用して影響を受けるログを復旧します。

これらのコマンドは順番に実行する必要があり、同時に実行することはできません。通知ウィンドウから`debug logdb migrate-lc`コマンドをコピーしていない場合は 、 **[Tasks (タスク)**］をクリックし、特定のログコレクタの失敗した`Install (インストール)`ジョブの詳細を表示します。

STEP 10 | (FIPS-CC モードのみ)FIPS-CC モードでの Panorama デバイスと管理対象デバイスのアップグレード.

専用 Log Collector が PAN-OS 11.1 リリースを実行しているときに、専用 Log Collector を Panorama 管理に追加した場合、FIPS-CC モードで専用 Log Collector をアップグレードするには、セキュア接続ステータスをリセットする必要があります。

専用Log CollectorがPAN-OS 10.0以前のリリースを実行している間は、Panorama管理に追加された専用Log Collectorを再オンボードする必要はありません。

STEP 11 | (PAN-OS 10.2 以降のリリース)OpenSSL Security レベル 2 に準拠するように、すべての証明書を再生成または再インポートします。

この手順は、PAN-OS 10.1 以前のリリースから PAN-OS 11.0 にアップグレードする場合に必要です。PAN-OS 10.2 からアップグレードし、証明書をすでに再生成または再インポートしている場合は、この手順をスキップします。

すべての証明書が次の最小要件を満たしている必要があります。

- RSA 2048 ビット以上、または ECDSA 256 ビット以上
- SHA256 以上のダイジェスト

証明書の再生成または再インポートの詳細については、PAN-OS Administrator's Guide または Panorama Administrator's Guide を参照してください。

STEP 12 | (Recommended for Panorama Virtual Appliance) Panorama Virtual Appliance のメモリを 64GB に増やします。

Panorama 仮想アプライアンスを Log Collector モードで PAN-OS 11.1 に正常にアップグレードした後、Palo Alto Networks では、プロビジョニング不足の Panorama 仮想アプライアンスに関連するロギング、管理、および運用パフォーマンスの問題を回避するために、増加したシステム要件 を満たすために、Panorama 仮想アプライアンスのメモリを 64 GB に増やすことをお勧めします。

インターネット接続を使用して Panorama から WildFire クラスターを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、同じまたはそれ以前の*PAN-OS*ソフトウェアバージョンを実行している*WildFire*アプライアンスとアプライアンスクラスタを管理できます。

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 | 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 9.1 から PAN-OS 11.0 にアップグレードする場合は、最初に PAN-OS 10.0、PAN-OS 10.1、および PAN-OS 10.2 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. [インストール後にデバイスを再起動する] 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。

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 11.0.0 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なしで Panorama から WildFire クラスターを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。

*Panorama*は、同じまたはそれ以前の*PAN-OS*ソフトウェアバージョンを実行している*WildFire*アプライアンスとアプライアンスクラスタを管理できます。

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。

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 9.1 から PAN-OS 11.0 にアップグレードする場合は、最初に PAN-OS 10.0、PAN-OS 10.1、および PAN-OS 10.2 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. [インストール後にデバイスを再起動する] 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。

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 11.0.0 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
   ```

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 11.1 リリース ノート を確認し、次の手順を使用して、Panorama で管理する firewall 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。

複数の機能 PAN-OS リリース間で HA firewall をアップグレードする場合は、続行する前に、アップグレード パスで各 HA ピアを同じ機能 PAN-OS リリースにアップグレードする必要があります。たとえば、HA ピアを PAN-OS 10.2 から PAN-OS 11.1 にアップグレードするとします。ターゲットの PAN-OS 11.0 リリースへのアップグレードを続行する前に、両方の HA ピアを PAN-OS 11.1 にアップグレードする必要があります。HA ピアが 2 つ以上の機能リリース離れている場合、古いリリースがインストールされている firewall は suspended 状態になり、Peer version too long というメッセージが表示されます。

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。

新しい Skip Software Version Upgrade 機能を使用すると、PAN-OS 11.0 上の Panorama アプライアンスから PAN-OS 11.1 以降のバージョンのファイアウォールへのアップグレードを展開するときに、最大 3 つのリリースをスキップできます。

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。管理対象の firewall をこのバージョンにアップグレードする

前に、Panoramaのアップグレード とその Log Collectors を 11.1 に アップグレードする必要があります。さらに、Log Collector を 11.1 にアップグレードする場合は、ロギング インフラストラクチャの変更により、すべての Log Collector を同時にアップグレードする必要があります。

- 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。
- Panorama 仮想アプライアンスが PAN-OS 11.1 へのアップグレード時にレガシー モードである場合は、レガシー モードのままにするかどうかを決定します。レガシ モードは、PAN-OS 9.1 以降のリリースを実行する新しい Panorama 仮想アプライアンスの展開ではサポートされません。Panorama 仮想アプライアンスを PAN-OS 9.0 以前のリリースから PAN-OS 11.1 にアップグレードする場合、Palo Alto Networks では、Panorama仮想アプライアンスの Setup 前提条件 を確認し、必要に応じて Panorama mode または 管理専用モード に変更することをお勧めします。

  Panorama 仮想アプライアンスをレガシー モードのままにする場合は、Panorama 仮想アプライアンスに割り当てられた CPU とメモリの増加 を最小 16 CPU と 32 GB メモリに割り当てて、PAN-OS 11.1 に正常にアップグレードします。詳細については、「セットアップの前提条件 Panorama 仮想アプライアンス を参照してください。
- （マルチvsysマネージドファイアウォール推奨）マルチvsysマネージドファイアウォールのすべてのvsysをPanoramaに移行します。

  これは、マルチvsysマネージドファイアウォールでのコミットの問題を回避するために推奨され、Panoramaから最適化された共有オブジェクトプッシュを利用できます。

  これは、Skip Software Version Upgradeのみを使用してPAN-OS 10.1からPAN-OS 11.1にアップグレードしたマルチvsysファイアウォールに適用されます。
- (マルチvsysマネージド ファイアウォール) ローカルで構成されたものを削除または名前変更シェアード パノラマ内のオブジェクトと同じ名前のオブジェクト シェアード 構成。それ以外の場合、Panoramaからの設定プッシュはアップグレード後に失敗し、エラー`<object-name>`がすでに使用されています。

  これは、Skip Software Version Upgradeのみを使用してPAN-OS 10.1からPAN-OS 11.1にアップグレードしたマルチvsysファイアウォールに適用されます。

STEP 1 | Panorama Web インターフェースにログインします。

STEP 2 | `ssl`アプリケーショントラフィックを許可するようにセキュリティポリシールールを変更しました。

これは、スキップソフトウェアバージョンのアップグレードのみを使用してPAN-OS 10.1からPAN-OS 11.1にアップグレードしたファイアウォールに適用されます。

これは、`Panorama`App-IDを使用してPanoramaと管理対象デバイス間のトラフィックを制御している場合、PAN-OS 11.1へのアップグレード後に管理対象デバイスがPanoramaから切断されるのを防ぐために必要です。アップグレード前に`ssl`アプリケーションが許可されていない場合、管理対象デバイスはPanoramaから切断されます。

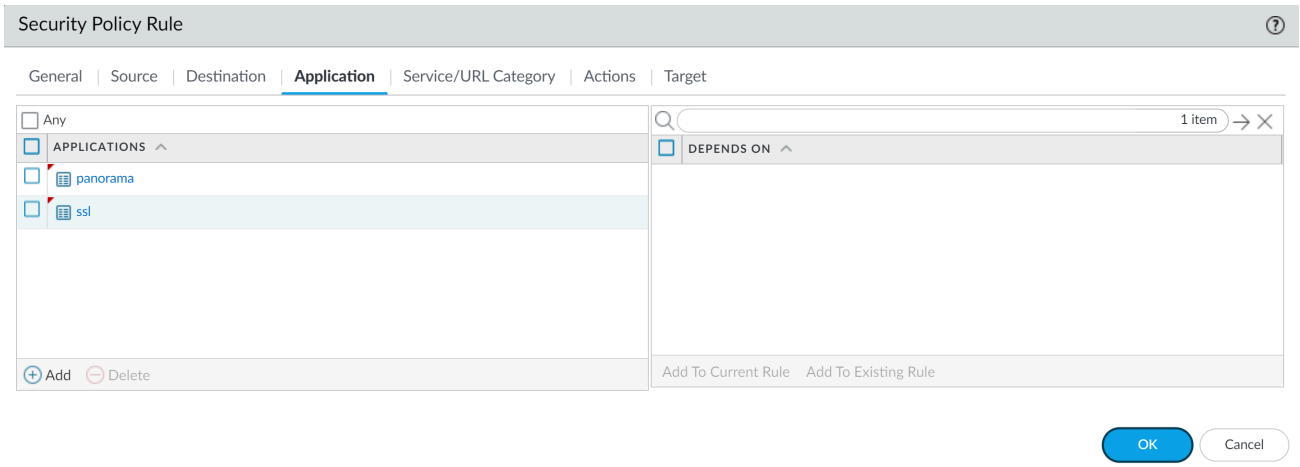
PAN-OS 11.1はTLSバージョン1.3を使用して、Panoramaとマネージドファイアウォール間のサービス証明書とハンドシェイクメッセージを暗号化します。これにより、マネージドファイアウォールからPanoramaへのトラフィックのApp-IDが`Panorama`から`ssl`に再分類されます。Panoramaと管理対象デバイス間の通信を継続するには、Panoramaと管理対象デバイス間のトラフィックを制御するセキュリティポリシールールを変更して、`ssl`アプリケーションも許可する必要があります。

Panoramaと管理対象デバイス間のトラフィックを制御するセキュリティポリシールールで任意のアプリケーションを許可している場合、またはPanoramaと管理対象デバイス間のトラフィックを制御するセキュリティポリシールールをすでに変更している場合は、この手順をスキップします。

1. **[Policies**（ポリシー）**] > [Security**（セキュリティ）**] > [Pre Rules**（プレルール）**]**を順に選択します。
2. Panoramaと管理対象ファイアウォール間のトラフィックを制御するセキュリティポリシールールを含む**[Device Group (**デバイスグループ**)]**を選択します。
3. セキュリティポリシー規則を選択します。

4. **[Application (アプリケーション)]**を選択し、`ssl`を**[Add (追加)]**します。

   *Panorama*アプリケーションを削除しないでください。これにより、変更をプッシュした後、すべての管理対象ファイアウォールが*Panorama*から切断されます。

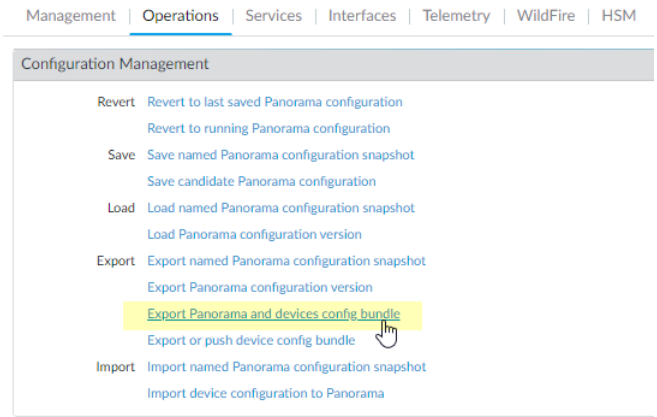


5. **OK** をクリックします。
6. **[Commit（コミット）] > [Commit and Push（コミットおよびプッシュ配信）]**を順に選択して、設定内容を**[Commit and Push（コミットしてプッシュ配信）]**します。

STEP 3 | 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. **Panorama > Setup > Operations** を選択し、**Export Panorama and Devices config bundle** をクリックして、Panorama および各管理対象アプライアンスの最新の構成バックアップを生成してエクスポートします。

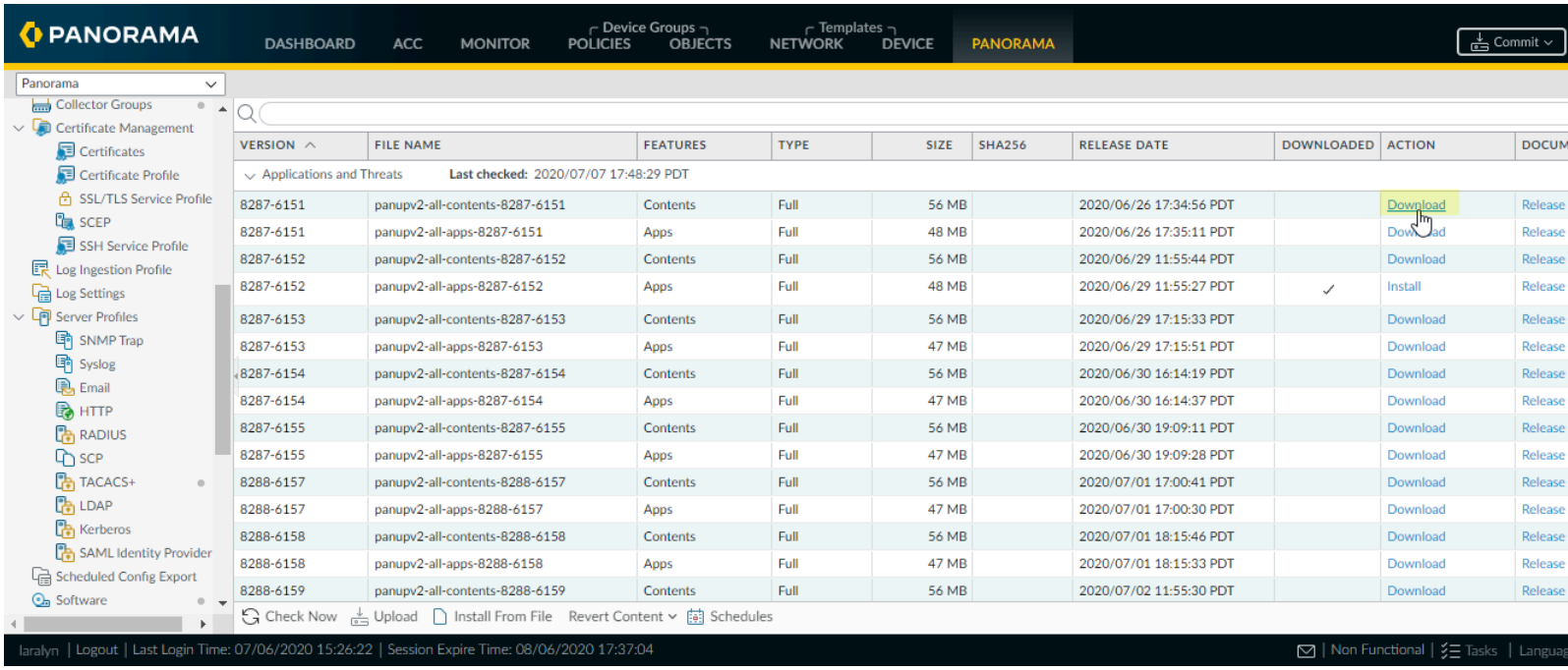


2. エクスポート ファイルをファイアウォールの外部に保存します。アップグレードで問題が発生した場合は、このバックアップを使用して設定を復元することができます。

STEP 4 | 最新のコンテンツ更新プログラムをインストールします。

PAN-OS 11.1 に必要な最小コンテンツ リリース バージョンについては、リリース ノート を参照してください。Panorama と管理された firewall にコンテンツの更新をデプロイするときは、必ずアプリケーションおよび脅威コンテンツ更新のベストプラクティスに従ってください。

1. 最新の更新プログラムについては、パノラマ > **Device Deployment** > **Dynamic Updates** および **Check Now** を選択します。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. インストール をクリックし、更新プログラムをインストールする firewall を選択します。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。
3. **[OK]** をクリックします。

STEP 5 | 「PAN-OS 11.1 へのアップグレード パスを決定する」を行います。

PAN-OS アップグレード チェックリスト、アップグレード パスの一部として渡す各リリースの リリース ノート および アップグレード/ダウングレードに関する考慮事項 の既知の問題と既定の動作の変更点を確認します。

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。

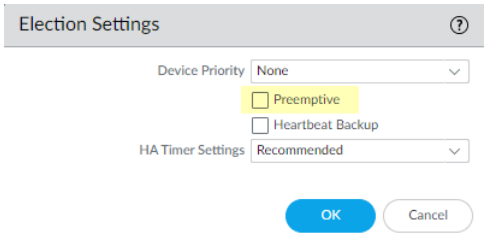
STEP 6 | (ベスト プラクティス) Cortex データ レイク (CDL) を活用している場合は、デバイス証明書をインストールします。

firewall は、PAN-OS 11.1 へのアップグレード時に、CDL 取り込みおよびクエリ エンドポイントでの認証にデバイス証明書を使用するように自動的に切り替わります。

PAN-OS 11.1 にアップグレードする前にデバイス証明書をインストールしない場合、ファイアウォールは認証に既存のロギング サービス証明書を引き続き使用します。

STEP 7 | （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。



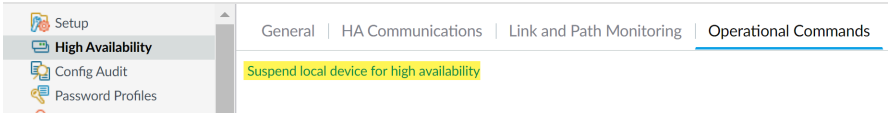
3. 変更を **Commit**（コミット）します。アップグレードを続行する前に、コミットが成功していることを確認してください。

STEP 8 | (HA firewall upgrades only)プライマリ HA ピアを一時停止して、フェールオーバーを強制します。

(Active/passive firewalls)アクティブ/パッシブ HA 構成の firewall の場合は、最初にアクティブ HA ピアを一時停止してアップグレードします。

(Active/active firewalls)アクティブ/アクティブ HA 構成の firewalls の場合は、最初にアクティブ/プライマリ HA ピアを一時停止してアップグレードします。

1. アクティブなプライマリ firewall HA ピアの firewall web interface にログインします。
2. 選ぶ **Device** > **High Availability** > **Operational Commands** and **Suspend local device for high availability**.



3. 右下隅で、状態が `suspended` であることを確認します。

   結果として生じるフェイルオーバーにより、セカンダリ・パッシブ HA ピアは `active` 状態に移行します。

   結果のフェイルオーバーは、アップグレードする前に *HA* フェイルオーバーが正常に機能していることを確認します。

STEP 9 | (Optional) Upgrade your managed firewalls to PAN-OS 10.1.

ソフトウェア バージョンのスキップ アップグレード機能は、PAN-OS 10.1 以降のリリースを実行している管理対象 firewall をサポートします。管理対象の firewall が PAN-OS 10.0 以前のリリースにある場合は、まず PAN-OS 10.1 以降のリリースにアップグレードします。

STEP 10 | (Optional) **Export** ファイルを構成済みの SCP サーバーに保存します。

PAN-OS 11.1 では、管理対象 firewall へのアップグレードを展開するときに、SCP サーバをダウンロード ソースとして使用できます。次の手順でソフトウェアとコンテンツイメージをダウンロードする前に、ファイルをエクスポートします。

STEP 11 | ターゲット リリースに必要なソフトウェアとコンテンツ バージョンを検証してダウンロードします。

この手順では、PAN-OS 11.1 へのアップグレードに必要な中間ソフトウェアとコンテンツ イメージの表示とダウンロードの両方を行うことができます。

マルチイメージダウンロードを使用したソフトウェアおよびコンテンツイメージのダウンロードはオプションです。画像を 1 つずつダウンロードできます。

1. クリック **panorama** > **Device Deployment** > **Software** > **Action** > **Validate**.
2. ダウンロードする必要がある中間ソフトウェアとコンテンツのバージョンを表示します。
3. アップグレードする firewall を選択し、デプロイ をクリックします。
4. ダウンロード元を選択し、ダウンロードをクリックします。

STEP 12 | PAN-OS 11.1.0 を firewalls にインストールします。

*(SD-WAN のみ)SD-WAN リンクの正確なステータスを維持するには、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 firewall を PAN-OS 11.1 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、誤った監視データ **([Panorama] > [SD-WAN] > [Monitoring (モニタリング)]*** が発生し、*SD-WAN リンクが誤って down（ダウン）*と表示されることがあります。

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。たとえば、PA-440ファイアウォールをアップグレードする場合は、PanOS_440-11.1.0 に対応する行で **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。

   (HA firewall upgrades only)ダウンタイムを短縮するには、各 HA ペアでピアを 1 つだけ選択します。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. firewalls のリブートが完了したら、**[Panorama] > [Managed Devices (管理対象外デバイス)]** 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 11.1.0 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 13 | (HA firewall upgrades only)HA 機能をプライマリ HA ピアに復元します。

1. 中断されたプライマリ firewall HA ピアの firewall web インターフェイス にログインします。
2. 選択します。 **Device > High Availability > Operational Commands** and **Make local device function for high availability**.
3. 右下隅で、状態が パッシブ であることを確認します。アクティブ/アクティブ構成の firewall の場合は、状態が `Active` であることを確認します。
4. HA ピア実行コンフィギュレーションが同期するのを待ちます。

   Dashboard で、高可用性ウィジェットで実行構成の状態を監視します。

STEP 14 | (HA firewall upgrades only)セカンダリ HA ピアを一時停止して、プライマリ HA ピアへのフェイルオーバーを強制します。

1. アクティブなセカンダリ firewall HA ピアの firewall web interface にログインします。
2. 選ぶ **Device** > **High Availability** > **Operational Commands** and **Suspend local device for high availability**.
3. 右下隅で、状態が `suspended` であることを確認します。

   結果として生じるフェイルオーバーにより、プライマリ・パッシブ HA ピアは `active` 状態に移行します。

   結果のフェイルオーバーは、アップグレードする前に *HA* フェイルオーバーが正常に機能していることを確認します。

STEP 15 | （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. Panorama web interface で、**Panorama** > **Device Deployment** > **Software**を選択します。
2. 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。
3. 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。
4. **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。
5. **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。
6. アップグレードを開始するには、**OK** をクリックします。
7. 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。

STEP 16 | (HA firewall upgrades only)HA 機能をセカンダリ HA ピアに復元します。

1. 中断されたセカンダリ firewall HA ピアの firewall web interface にログインします。
2. 選択します。 **Device** > **High Availability** > **Operational Commands** and **Make local device function for high availability**.
3. 右下隅で、状態が パッシブ であることを確認します。アクティブ/アクティブ構成の firewall の場合は、状態が `Active` であることを確認します。
4. HA ピア実行コンフィギュレーションが同期するのを待ちます。

   Dashboard で、高可用性ウィジェットで実行構成の状態を監視します。

STEP 17 | (FIPS-CC モードのみ)FIPS-CC モードでの Panorama デバイスと管理対象デバイスのアップグレード.

管理対象 firewall が PAN-OS 11.1 リリースを実行しているときに専用 Log Collector を Panorama 管理に追加した場合、FIPS-CC モードで管理対象 firewall をアップグレードするには、セキュア接続ステータスをリセットする必要があります。

管理対象 firewall が PAN-OS 10.0 以前のリリースを実行している間は、Panorama 管理に追加された管理対象 firewall を再オンボードする必要はありません。

STEP 18 | 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。

	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 19 | （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。

STEP 20 | Panorama ウェブインターフェイス で、Panorama 管理対象構成全体を管理対象の firewall にプッシュします。

この手順は、デバイス グループとテンプレート スタックの構成変更を Panorama から管理対象の firewall に選択的にコミットしてプッシュできるようにするために必要です。

これは、PAN-OS 10.1 以前のリリースから PAN-OS 11.1 へのアップグレードが正常に行われた後、Panorama によって管理されるマルチvsysファイアウォールに設定変更を正常にプッシュするために必要です。詳細については、Panorama によって管理されるマルチ vsys firewall の 共有構成オブジェクトの既定の動作の変更を参照してください。

1. **Commit** > **Push to Devices**を選択します。
2. **Push**.

STEP 21 | OpenSSL セキュリティー・レベル 2 に準拠するために、すべての証明書を再生成または再インポートします。

PAN-OS 11.1 以降のリリースにアップグレードする場合は、すべての証明書が次の最小要件を満たしている必要があります。PAN-OS 10.2 からアップグレードしていて、証明書をすでに再生成または再インポートしている場合は、この手順をスキップします。

- RSA 2048 ビット以上、または ECDSA 256 ビット以上
- Digest of SHA256 以上

証明書の再生成または再インポートの詳細については、PAN-OS Administrator's Guide または Panorama Administrator's Guide を参照してください。

STEP 22 | ファイアウォールのソフトウェア アップグレード履歴を表示します。

1. Panorama インターフェイスにログインします。
2. パノラマ > **Managed Devices** > **Summary** に移動し、[**Device History**] をクリックします。

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。

新しい Skip Software Version Upgrade 機能を使用すると、PAN-OS 11.0 上の Panorama アプライアンスから PAN-OS 11.1 以降のバージョンのファイアウォールへのアップグレードを展開するときに、最大 3 つのリリースをスキップできます。

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。管理対象の firewall をこのバージョンにアップグレードする前に、Panoramaのアップグレード とその Log Collectors を 11.1 に アップグレードする必要があります。さらに、Log Collector を 11.1 にアップグレードする場合は、ロギング インフラストラクチャの変更により、すべての Log Collector を同時にアップグレードする必要があります。
- 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。
- Panorama 仮想アプライアンスが PAN-OS 11.1 へのアップグレード時にレガシー モードである場合は、レガシー モードのままにするかどうかを決定します。レガシ モードは、PAN-OS 9.1 以降のリリースを実行する新しい Panorama 仮想アプライアンスの展開ではサポートされません。Panorama 仮想アプライアンスを PAN-OS 9.0 以前のリリースから PAN-OS 11.1 にアップグレードする場合、Palo Alto Networks では、Panorama仮想アプライアンスの Setup 前提条件 を確認し、必要に応じて Panorama mode または 管理専用モード に変更することをお勧めします。

  Panorama 仮想アプライアンスをレガシー モードのままにする場合は、Panorama 仮想アプライアンスに割り当てられた CPU とメモリの増加 を最小 16 CPU と 32 GB メモリに割り当て

て、PAN-OS 11.1 に正常にアップグレードします。詳細については、「セットアップの前提条件 Panorama 仮想アプライアンス を参照してください。

- （マルチvsysマネージドファイアウォール推奨）マルチvsysマネージドファイアウォールのすべてのvsysをPanoramaに移行します。

  これは、マルチvsysマネージドファイアウォールでのコミットの問題を回避するために推奨され、Panoramaから最適化された共有オブジェクトプッシュを利用できます。

  これは、Skip Software Version Upgradeのみを使用してPAN-OS 10.1からPAN-OS 11.1にアップグレードしたマルチvsysファイアウォールに適用されます。

- （マルチvsysマネージドファイアウォール）ローカルに設定された共有オブジェクトのうち、Panorama共有設定のオブジェクトと同じ名前を持つものを削除するか、名前を変更します。それ以外の場合、Panoramaからの設定プッシュはアップグレード後に失敗し、エラー`<object-name>`がすでに使用されています。

  これは、Skip Software Version Upgradeのみを使用してPAN-OS 10.1からPAN-OS 11.1にアップグレードしたマルチvsysファイアウォールに適用されます。

STEP 1 | Panorama Web インターフェースにログインします。

STEP 2 | `ssl`アプリケーショントラフィックを許可するようにセキュリティポリシールールを変更しました。

これは、スキップソフトウェアバージョンのアップグレードのみを使用してPAN-OS 10.1からPAN-OS 11.1にアップグレードしたファイアウォールに適用されます。

これは、*Panorama*App-IDを使用して*Panorama*と管理対象デバイス間のトラフィックを制御している場合、*PAN-OS 11.1*へのアップグレード後に管理対象デバイスが*Panorama*から切断されるのを防ぐために必要です。アップグレード前に`ssl`アプリケーションが許可されていない場合、管理対象デバイスは*Panorama*から切断されます。

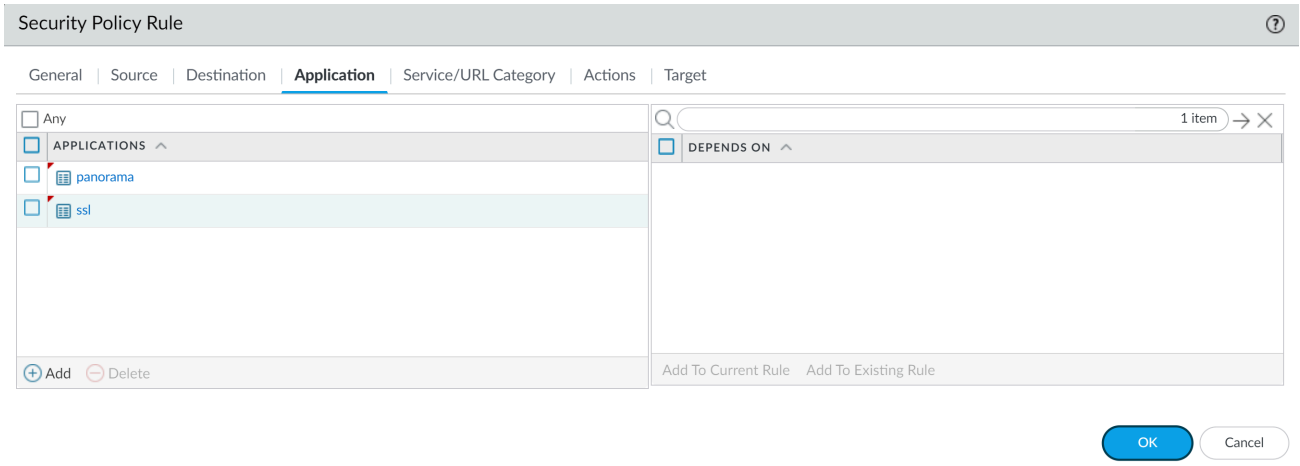
PAN-OS 11.1はTLSバージョン1.3を使用して、Panoramaとマネージドファイアウォール間のサービス証明書とハンドシェイクメッセージを暗号化します。これにより、マネージドファイアウォールからPanoramaへのトラフィックのApp-IDが`Panorama`から`ssl`に再分類されます。Panoramaと管理対象デバイス間の通信を継続するには、Panoramaと管理対象デバイス間のトラフィックを制御するセキュリティポリシールールを変更して、`ssl`アプリケーションも許可する必要があります。

Panoramaと管理対象デバイス間のトラフィックを制御するセキュリティポリシールールで任意のアプリケーションを許可している場合、またはPanoramaと管理対象デバイス間のトラフィックを制御するセキュリティポリシールールをすでに変更している場合は、この手順をスキップします。

1. **[Policies**（ポリシー）**]** > **[Security**（セキュリティ）**]** > **[Pre Rules**（プレルール）**]**を順に選択します。

2. Panoramaと管理対象ファイアウォール間のトラフィックを制御するセキュリティポリシールールを含む**[Device Group (デバイスグループ)]**を選択します。
3. セキュリティポリシー規則を選択します。
4. **[Application (アプリケーション)]**を選択し、`ssl`を**[Add (追加)]**します。

   *`Panorama`*アプリケーションを削除しないでください。これにより、変更をプッシュした後、すべての管理対象ファイアウォールが*Panorama*から切断されます。



5. **OK** をクリックします。
6. **[Commit（コミット）] > [Commit and Push（コミットおよびプッシュ配信）]**を順に選択して、設定内容を**[Commit and Push（コミットしてプッシュ配信）]**します。

STEP 3 | 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 4 | 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。

コンテンツアップデートごとに、更新が必要かどうかを判断し、次の手順でダウンロードする必要があるコンテンツアップデートをメモします。

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。

STEP 5 | Panorama 11.1 に更新する予定の firewalls のソフトウェア アップグレード パスを決定 します。

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。

Release Notes のPAN-OS アップグレード チェックリスト、既知の問題、既定の動作の変更点を確認し、アップグレード パスの一部として渡す各リリースアップグレード/ダウングレードに関する考慮事項を確認します。

STEP 6 | (Optional) Upgrade your managed firewalls to PAN-OS 10.1.

ソフトウェア バージョンのスキップ アップグレード機能は、PAN-OS 10.1 以降のリリースを実行している管理対象 firewall をサポートします。管理対象の firewall が PAN-OS 10.0 以前のリリース上にある場合は、まず PAN-OS 10.1 以降のリリースにアップグレードします。

STEP 7 | リリースの検証チェックを行います。

この手順では、11.1 へのアップグレードに必要な中間ソフトウェアとコンテンツ イメージを表示できます。

1. **Panorama > Device Deployment > Software > Action > Validate**を選択。
2. ダウンロードする必要があるソフトウェアとコンテンツのバージョンを表示します。

STEP 8 | コンテンツとソフトウェアの更新を、SCP または HTTPS 経由で Panorama または設定された SCP サーバーに接続してファイルをアップロードできるホストに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。2 つ以上のソフトウェア更新プログラムまたは 1 つのタイプのコンテンツ更新プログラムをアップロード

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。

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-440 および PA-5430ファイアウォールを PAN-OS 11.1.0 にアップグレードするには、`Pan0S_440-11.1.0` および `Pan0S_5430-11.1.0` イメージをダウンロードします。

      PAN-OS*用の*PA-<series/model> を選択するには、***Filter By*** ドロップダウンから特定の *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 9 | 中間ソフトウェア バージョンと最新のコンテンツ バージョンをダウンロードします。

PAN-OS 11.0 では、マルチイメージ ダウンロード機能を使用して複数の中間リリースをダウンロードできます。

1. アップグレードする firewalls (**Required Deployment** > **Deploy**) を選択します。
2. ダウンロード元を選択し、**Download**をクリックします。

STEP 10 | 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 11 | （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。
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 12 | PAN-OS 11.1 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。

(SD-WAN のみ)SD-WAN リンクの正確なステータスを維持するには、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 *firewall* を *PAN-OS 11.1* 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、誤った監視データ *([Panorama] > [SD-WAN] > [Monitoring (*モニタリング*)]* が発生し、*SD-WAN* リンクが誤って *down (*ダウン*)* と表示されることがあります。

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。各 HA ペアの 1 つの firewall でこの設定を無効にするだけで済みますが、続行する前にコミットが成功したことを確認してください。
  2. 該当する更新プログラムの [Action (アクション)] 列の **[Install (インストール)]** をクリックし、**Group HA Peers** を無効化 (クリア) し、fw2を選択し、**[Reboot device after install (インストール後にデバイスを再起動)]**し 、**OK** をクリックします。続行する前に、fw2 の再起動が完了するのを待ちます。
  3. fw2 の再起動が完了したら、fw1 (**[Dashboard (ダッシュボード)]** >高可用性) で、fw2 がまだパッシブ 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状態は `[active（アクティブ）]` で、ピア (fw2) は `[passive（パッシブ）]`)。
  4. fw1 にアクセスし ローカルデバイスをサスペンドします(**[Device (デバイス)]** > **[High Availability (高可用性)]** > **[Operational Commands (オペレーショナルコマンド)]**)。
  5. fw2 にアクセスし (**[Dashboard (ダッシュボード)]** > [High Availability (高可用性)]) をクリックし、ローカルファイアウォールの状態が `[アクティブ（active）]` であり、ピアが `[suspended（サスペンド）]` であることを確認します。
  6. Panoramaにアクセスし、**[Panorama]** > **[Device Deployment (デバイスの開発)]** > **[Software (ソフトウェア)]** を選択し、該当するリリースの[アクション]列で**[Install (インストール)]**をクリックし、**Group HA Peers**を無効化(クリア)し、fw1を選択し、インストール後にデバイスを再起動して、[OK]をクリックします。続行する前に、fw1 の再起動が完了するのを待ちます。
  7. fw1 にアクセスし (**[Device (デバイス)]** > **[High Availability (高可用性)]** > **[Operational Commands (オペレーショナルコマンド)]**)をクリックし、**[Make local device functional (ローカル デバイスを機能させる)]**をクリックし、2 分間待ってから続行します。
  8. fw1の (**[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（パッシブ）]` であり、ピア (fw2) が `[active（アクティブ）]` であることを確認します。

STEP 13 | (FIPS-CC モードのみ)FIPS-CC モードでの Panorama デバイスと管理対象デバイスのアップグレード.

管理対象 firewall が PAN-OS 11.1 リリースを実行しているときに専用 Log Collector を Panorama 管理に追加した場合、FIPS-CC モードで管理対象 firewall をアップグレードするには、セキュア接続ステータスをリセットする必要があります。

管理対象 firewall が PAN-OS 10.0 以前のリリースを実行している間は、Panorama 管理に追加された管理対象 firewall を再オンボードする必要はありません。

STEP 14 | 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 15 | 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。

STEP 16 | Panorama ウェブ インターフェイス で、Panorama 管理対象構成全体を管理対象の firewall にプッシュします。

この手順は、デバイス グループとテンプレート スタックの構成変更を Panorama から管理対象の firewall に選択的にコミットしてプッシュできるようにするために必要です。

これは、PAN-OS 11.1 へのアップグレードが成功した後、Panorama によって管理されるマルチ vsys firewall に設定変更を正常にプッシュするために必要です。詳細については、Panorama によって管理されるマルチ vsys firewall の 共有構成オブジェクトの既定の動作の変更を参照してください。

1. **Commit** > **Push to Devices**を選択します。
2. **Push**.

STEP 17 | OpenSSL セキュリティー・レベル 2 に準拠するために、すべての証明書を再生成または再インポートします。

PAN-OS 11.1 へのアップグレードでは、すべての証明書が次の最小要件を満たしている必要があります。

- RSA 2048 ビット以上、または ECDSA 256 ビット以上
- Digest of SHA256 以上

証明書の再生成または再インポートの詳細については、PAN-OS Administrator's Guide または Panorama Administrator's Guide を参照してください。

STEP 18 | ファイアウォールのソフトウェア アップグレード履歴を表示します。

1. Panorama インターフェイスにログインします。
2. パノラマ > **Managed Devices** > **Summary** に移動し、[**Device History**] をクリックします。

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 Webインターフェイスに管理者ユーザとしてログインします。

STEP 2 | Panorama に ZTP ファイアウォールを追加します。

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。

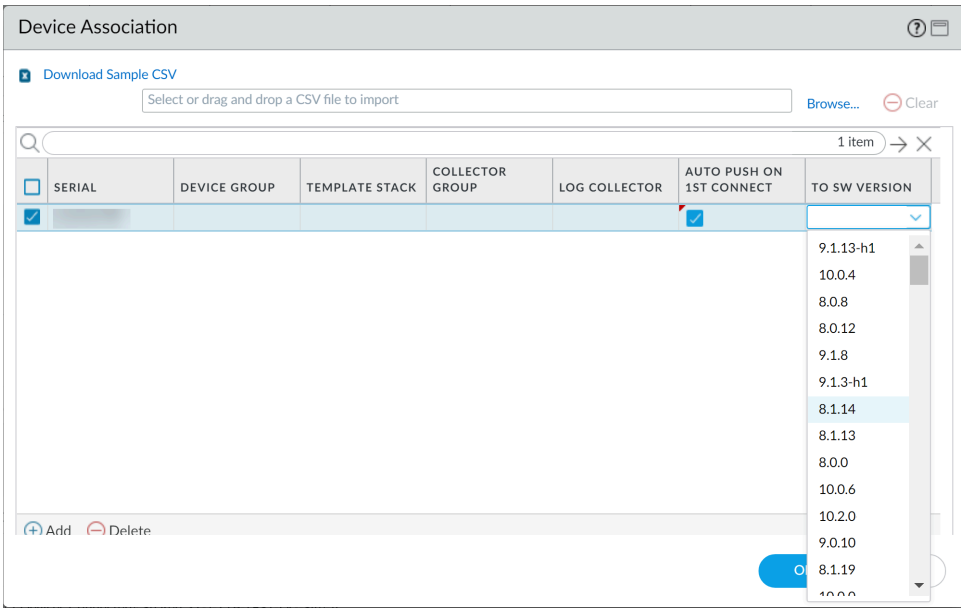
STEP 4 | **Panorama**（**Panorama**） > **Managed Devices**（管理対象デバイス） > **Summary**（概要）の順に選択して、次に 1 つ以上の ZTP ファイアウォールを選択します。

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 | Check (enable) **Auto Push on 1st Connect**.

STEP 7 | **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 8 | **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)** および **Commit to Panorama (Panorama** へのコミット**)** をクリックします。

STEP 10 | ZTP ファイアウォールの電源を入れます。

ZTP firewall が初めて Panorama に接続すると、選択した PAN-OS バージョンに自動的にアップグレードされます。

- **Panorama** が **PAN-OS 11.1.0** を実行している場合:PAN-OS メジャー リリースまたはメンテナンス リリース間で管理対象の firewall をアップグレードする場合、ターゲットの PAN-OS リリースがインストールされる前に、アップグレード パス上の中間 PAN-OS リリースが最初にインストールされます。

  たとえば、管理対象 firewall のターゲット **To SW** バージョンを PAN-OS 11.1.0 として設定し、ファイアウォールが PAN-OS 10.2 を実行しているとします。Panorama への最初の接続時に、PAN-OS 11.0.0 が最初に管理対象のファイアウォールにインストールされます。PAN-OS 11.0.0 が正常にインストールされると、ファイアウォールは自動的にターゲットの PAN-OS 11.1.0 リリースにアップグレードされます。

- **Panorama** が **PAN-OS 11.0.1** 以降のリリースを実行している:PAN-OS メジャー リリースまたはメンテナンス リリース間で管理対象 firewall をアップグレードする場合、アップグレード パス上の中間の PAN-OS メジャー リリースがインストールされ、ターゲットの PAN-OS メンテナンス リリースがインストールされる前にベース PAN-OS メジャー リリースがダウンロードされます。

  たとえば、管理対象の firewall のターゲット **To SW** バージョン を PAN-OS 11.0.1 として設定し、firewall が PAN-OS 10.0 で動作しているとします。Panorama への最初の接続時に、PAN-OS 10.1.0 および PAN-OS 10.2.0 が管理対象の firewall にインストールされます。管理対象の firewall がリブートすると、PAN-OS 11.0.0 がダウンロードされ、firewall がターゲットの PAN-OS 11.0.1 リリースに自動的にインストールされます。

STEP 11 | 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 Web インターフェイスへのログイン。
2. **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。
3. **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。

STEP 12 | 今後のすべての PAN-OS アップグレードについては、ファイアウォールを Panorama から PAN-OS 11.1 にアップグレードするを参照してください。

PAN-OSソフトウェアパッチのインストール

どこで使用できますか?	何が必要ですか?
• Panoramaで管理される次世代ファイアウォール CNシリーズのファイアウォールはサポートされていません • Panorama > Managed WildFire Appliances（管理対象 WildFire アプライアンス）	☐ デバイス管理ライセンス ☐ サポートライセンス ☐ PAN-OS 11.1.3 以降もしくは 11.1 リリース ☐ アウトバウンドインターネットアクセス

「PAN-OS 11.1リリースノート」を確認してから、次の手順に従ってPAN-OSソフトウェアパッチをインストールし、Panorama™ 管理サーバーの管理対象デバイスで現在実行されているPAN-OSリリースのバグと共通脆弱性および暴露（CVE）に対処します。PAN-OSソフトウェアパッチをインストールすると、長期間のメンテナンスをスケジュールしなくてもバグやCVEに対する修正が適用され、新しいPAN-OSリリースのインストールに伴う新たな既知の問題やデフォルト動作の変更をもたらすことなく、すぐにセキュリティ体制を強化できます。さらに、現在インストールされているソフトウェアパッチを元に戻して、ソフトウェアパッチをインストールしたときに適用されたバグやCVEの修正をアンインストールすることもできます。

PAN-OSのソフトウェアパッチをインストールまたは元に戻すと、システムログが生成されます（**[Monitor (モニター)]** > **[Logs (ログ)]** > **[System (システム)]**）。パロアPalo Alto Networks カスタマーサポートポータルからPAN-OSソフトウェアパッチをダウンロードするには、アウトバウンドインターネット接続が必要です。エアギャップ管理対象デバイスの場合、PAN-OSソフトウェアパッチをダウンロードするにはPanoramaがインターネットにアクセスできる必要がありますが、管理対象デバイスへのインストールと適用にはアウトバウンドインターネット接続は必要ありません。

- インストール
- 元に戻す

インストール

STEP 1 | Panorama Web インターフェースにログインします。

STEP 2 | **[Panorama] > [Device Deployment (デバイスデプロイメント)] > [Software (ソフトウェア)]**および **[Check Now (今すぐチェック)]** を選択して、パロアルトネットワークスの更新サーバから最新の PAN-OS ソフトウェアパッチを取得します。

STEP 3 | ［**Include Patch (パッチを含める)**］をオンに（有効に）すると、使用可能なすべての PAN-OS ソフトウェア パッチが表示されます。

STEP 4 | 管理対象デバイスに現在インストールされているPAN-OSリリースのソフトウェアパッチを探します。

ソフトウェアパッチは、**[Version (バージョン)]**名の横に表示される [Patch （パッチ）] ラベルで示されます。

STEP 5 | 詳細情報を表示して、重大なバグやCVEの修正、修正を適用するには管理対象デバイスの再起動が必要かどうかなど、ソフトウェアパッチの詳細を確認してください。

STEP 6 | ソフトウェアパッチをダウンロードします。

（HA のみ）PAN-OS ソフトウェアパッチをダウンロードするには、[HA ピアに同期] をチェック（有効化）して **[Continue Download (ダウンロードを続行)]** を選択します。

ソフトウェアパッチが正常にダウンロードされたら、**[Close (閉じる)]** をクリックします。

STEP 7 | ソフトウェアパッチをインストールする

ソフトウェアパッチが正常にインストールされたら、**[Close (閉じる)]** をクリックします。

STEP 8 | PAN-OSソフトウェアパッチをインストールする管理対象デバイスを選択し、［**OK**］をクリックします。

（HA のみ）高可用性（HA）構成の管理対象デバイスのペアにソフトウェア パッチをインストールする場合は、両方の HA ピアにソフトウェア パッチを選択してインストールする必要があります。

STEP 9 | ソフトウェアパッチを適用します。

インストールされているPAN-OSソフトウェアパッチを管理対象デバイスに適用するかどうかを確認するメッセージが表示されたら、［**Apply (適用)**］をクリックします。

PAN-OSソフトウェアパッチ適用の現在の進捗状況を示すステータスバーが表示されます。パッチが正常に適用されたら、**[Close (閉じる)]** をクリックします。

管理対象デバイスへのPAN-OSソフトウェアパッチの適用を完了するために再起動が必要な場合は、この時点でファイアウォールが自動的に再起動します。

元に戻す

STEP 1 | Panorama Web インターフェースにログインします。

STEP 2 | **[Panorama] > [Device Deployment (デバイスデプロイメント)] > [Software (ソフトウェア)]**および **[Check Now (今すぐチェック)]** を選択して、パロアルトネットワークスの更新サーバから最新の PAN-OS ソフトウェアパッチを取得します。

STEP 3 | ソフトウェアパッチを元に戻します。

STEP 4 | PAN-OSソフトウェアパッチを元に戻す管理対象デバイスを選択し、［**OK**］をクリックします。

対象となる管理対象デバイスだけが表示されます。

（HA のみ）高可用性（HA）構成の管理対象デバイスのペアにソフトウェア パッチをインストールする場合は、両方の HA ピアにソフトウェア パッチを選択してインストールする必要があります。

STEP 5 | 選択した管理対象デバイスからインストール済みのPAN-OSソフトウェアパッチを復元するかどうかを確認するメッセージが表示されたら、［**Revert (**元に戻す**)**］をクリックします。

PAN-OSソフトウェアパッチ適用の現在の進捗状況を示すステータスバーが表示されます。パッチが正常に適用されたら、**[Close (**閉じる**)]** をクリックします。

この時点で、PanoramaへのPAN-OSソフトウェアパッチの適用を完了するために再起動が必要な場合、ファイアウォールは自動的に再起動します。

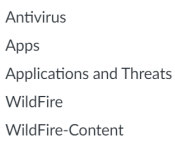
Panorama でコンテンツのアップデートを元に戻す

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コンテンツの更新を展開するときは、必ず アプリケーションおよび脅威コンテンツ更新のベストプラクティス を使用してください。

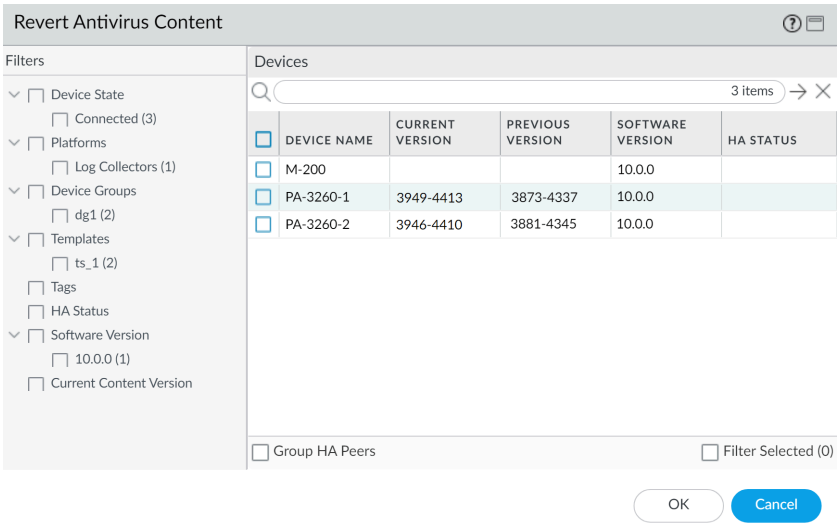
STEP 1 | Panorama Web インターフェースにログインします。

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。



PAN-OS をアップグレードする

PAN-OS アップグレード チェックリスト

PAN-OS のアップグレードを計画することで、Panorama またはファイアウォール用に新しいバージョンの PAN-OS へのスムーズな移行を確実に行うことができます。

- デバイスが登録され、ライセンスが付与されていることを確認します。
- 使用可能なディスク領域を確認します。

  必要なディスク容量は、PAN-OS リリースによって異なります。**2>**デバイス > ソフトウェアを選択し、ターゲット PAN-OS リリース **Size** を確認して必要なディスク領域を決定します。

  - を実行すると、システム ディスク領域 が表示されます。
- コンテンツリリースの最小バージョンを確認します。
- 優先リリースを特定します。

  - (PAN-OS 11.1.3以降)

    [Device (デバイス)] > **[Software (ソフトウェア)]**を選択します。デフォルトでは、[Release Type (リリースタイプ)]列に優先リリースと基本リリースが表示されます。優先リリースのみを表示するには、**[Base Releases (基本リリース)]**チェックボックスをオフ(選択解除)にします。
  - （PAN-OS 11.1.3以降のリリース）

    実行要求システムソフトウェア情報優先

  詳細については、Palo Alto Networks サポート ソフトウェア リリース ガイダンス および 終業の概要 を参照してください。さらに、PAN-OS アップグレードがユーザーにどのような影響を与える可能性があるかを理解するために、既知の問題と対処された問題、アップグレードとダウングレードに関する考慮事項、およびターゲット PAN-OS リリースの制限を確認します。
- アップグレード パスを決定します。

  PAN-OS 機能リリースバージョンから後の機能リリースにアップグレードする場合、ターゲット リリースへのパスに含まれる機能リリース 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 パス内のすべてのリリースのアップグレード/ダウングレードに関する考慮事項を確認します。
- (グローバルプロテクトに必要です。グローバルプロテクト™エージェントの最小バージョンを確認して、GlobalProtect ユーザーが VPN 接続を失うことを防ぎます。グローバルプロテクトは、最新バージョンに直接アップグレードすることができます。
- インストールしたプラグインのターゲットリリースバージョンで、プラグインのリリースバージョンの最小値を確認します。

- 管理インターフェイスから更新サーバーへの接続を確認します。
  - デバイス > トラブルシューティング を選択し、**Update** サーバー接続 をテストして、DNS がアドレスを解決できることを確認します。

    解決しない場合は、DNS を **8.8.8.8** に変更し (独自の DNS サーバーではなくパブリック DNS サーバーを使用する必要があります)、再度 ping を実行します。

    この問題が解決しない場合は、更新サーバーを **staticupdates.paloaltonetworks.com** と **Commit** に変更します。
- (SD-WAN のみ)PAN-OS 11.1 にアップグレードするハブおよびブランチ firewall を特定します。

  SD-WAN リンクの正確なステータスを維持するには、ブランチ firewall をアップグレードする前に、ハブ firewall を PAN-OS 11.1 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、監視データが正しくなくなる可能性があります（ **Panorama** > **SD-WAN** > **Monitoring** ）。 誤って `down` と表示されます。
- 現在インストールされているプラグインがある場合は、アップグレードする前に、Panorama(**[Panorama]** > **[Plugins (プラグイン)]**)またはファイアウォール(**[Device (デバイス)]** > **[Plugins (プラグイン)]**)に現在インストールされているすべてのプラグインについて、PAN-OS 11.1でサポートされているプラグインバージョンをダウンロードしてください。

  PAN-OS 11.1 でサポートされている Panorama プラグインのバージョンについては、Panorama プラグイン互換性マトリックス を参照してください。

  これは、Panorama および firewall を PAN-OS 11.1 から PAN-OS 11.1 に正常にアップグレードするために必要です。ダウンロードしたプラグインのバージョンは、PAN-OS 11.1 へのアップグレード中に自動的にインストールされます。サポートされているプラグインバージョンがダウンロードされていない場合、PAN-OS 11.1へのアップグレードはブロックされます。

アップグレード/ダウングレードに関する考慮事項

次の表に、アップグレードまたはダウングレードに影響する新機能を示します。PAN-OS 11.1 リリースにアップグレードまたはダウングレードする前に、アップグレード/ダウングレードに関するすべての考慮事項を理解していることを確認してください。PAN-OS 11.1 以降のリリースの詳細については、PAN-OS Release Notes (PAN-OS リリース ノート)を参照してください。

機能	アップグレードに関する考慮事項	ダウングレードに関する考慮事項
IPv6アドレスプレフィックスが動的に割り当てられたNPTv6	なし。	PAN-OS 11.1.5 より前のリリースにダウングレードする前に、動的に割り当てられた IPv6 アドレスを持つインターフェイスで NPTv6 を無効にするか、設定を削除します。(PAN-OS 11.1.5 と 11.1.0 の間ではダウングレード ブロックは利用できないため、イメージのダウングレードは成功しますが、自動コミットは失敗します。)
重複する IP アドレスのサポート	なし。	重複 IP アドレスのサポートが有効になっている場合、PAN-OS 11.1.4 より前のリリースへのダウングレードの試行はブロックされます。ダウングレードを試みるとエラーメッセージが表示されます。 ダウングレードに失敗しました。古いバージョンでは重複した IP アドレスはサポートされていません。ダウングレードを続行する前に、重複する IP アドレス設定をすべて削除し、重複する IP アドレスのサポートを無効にしてコミットしてください。
高度なルーティングエンジン (PAN-OS 11.2.0)	PAN-OS 11.2.0 では、高度なルーティングが有効になっている場合、IP マルチキャストはサポートされません。今	なし

機能	アップグレードに関する考慮事項	ダウングレードに関する考慮事項
	後のバージョンではこの機能がサポートされる予定です。マルチキャストが設定されている、またはマルチキャストルーティングを展開する予定のお客様は、11.2.0 にアップグレードしないでください。 さらに、PAN-OS 11.2.0 では、高度なルーティングが有効になっている場合、BGP ダンプニング構成はどのピアまたはピア グループにも適用されません。構成は保持されますが、BGP には影響しません。顧客は、特定のピアセットにダンプニング プロファイルを適用している場合でも BGP を使用できます。この問題は他の BGP 機能には影響しません。	
シリアルナンバーと IP アドレス方式で LSVPN サテライトを認証する (PAN-OS 11.1.3 以降のリリース)	PAN-OS は構成の変更をデータベースに内部的に保存します。したがって、この機能にアップグレードすると、最後に保存された構成が適用されます。 PAN-OS 10.0 以前のリリースから PAN-OS 10.1 以降のリリース (ユーザー名/パスワードとサテライト Cookie 認証方法が有効) にアップグレードした後、サテライト Cookie の 有効期限が切れると、ログインに失敗します。 この場合、認証を成功させるにはユーザー名とパスワードを入力する必要があります。	• PAN-OS 10.1 以降のリリースにダウングレードすると、ユーザー名/パスワードとサテライト Cookie 認証方式 のみがサポートされます。 • プラグインのマイナー バージョンをダウンロードしてインストールし、同じリリースの別のマイナー バージョンにダウングレードする場合、ダウングレード前のマイナー バージョンで行われた構成が、同じリリースのダウングレード後のマイナー バージョンで有効になります。 PAN-OS は構成の変更をデータベースに内部的に保存します。したがって、この機能からダウン

機能	アップグレードに関する考慮事項	ダウングレードに関する考慮事項
		グレードすると、最後に保存された構成が適用されます。 たとえば、構成 (構成 1) で SD-WAN プラグイン 11.1.5 をインストールし、その後、異なる構成 (構成 2) で同じリリースの別のマイナー バージョン 11.1.4 にダウングレードすることにしたとします。この場合、マイナー バージョン (ダウングレード前) の構成、つまり構成 1 が、ダウングレードされたマイナー バージョン 11.1.4 に有効になります。
	PAN-OS 10.0 以前のリリース/PAN-OS 10.1 以降のリリースから PAN-OS 11.1.3 にアップグレードした後は、次の点を考慮してください。 • シリアルナンバーと IP アドレスの認証方法を無効にし、サテライトcookieの有効期限が切れると、ログインに失敗します。この場合、管理者は認証を成功させるためにユーザー名とパスワードを入力する必要があります。 • シリアルナンバーと IP アドレスの認証方法を有効にし、サテライトのシリアルナンバーが GlobalProtect ポータルに登録され、IP アドレスが IP 許可リストに存在する場合は、ログインは成功します。	• PAN-OS リリース 10.1 より前にダウングレードする場合は、シリアルナンバー認証方法のみがサポートされます。 • PAN-OS リリース 10.1 以降および 10.2.8 以前にダウングレードする場合、ユーザー名/パスワードおよびサテライト Cookie 認証方式がサポートされます。 • PAN-OS 10.2.8 以降の 10.2 リリースにダウングレードすると、「ユーザー名/パスワードとサテライト Cookie 認証」と「シリアルナンバーと IP アドレス認証」の両方の方法がサポートされます。

機能	アップグレードに関する考慮事項	ダウングレードに関する考慮事項
	• シリアルナンバーと IP アドレスの認証方法を有効にしているが、サテライトのシリアルナンバーが GlobalProtect ポータルに登録されていないか、IP アドレスが IP 許可リストに存在しない場合は、ログインは失敗します。この場合、ファイアウォールは他の認証方法にフォールバックせず、認証は失敗します。認証に失敗した場合、サテライトは設定された再試行間隔が経過するまで待機してから、再度認証を試行します。認証が成功するには、サテライトのシリアルナンバーがポータルに正しく登録され、サテライトの IP アドレスが IP 許可リストに含まれていることを確認してください。	
ポリシーごとの永続的なDIPP	Panorama を使用してファイアウォールを PAN-OS 11.0.0 から 11.1.1 にアップグレードする場合、通常の DIPP NAT ルールを永続的な DIPP NAT ルールに変換する必要がありますが、その変換は失敗し、ルールは通常の DIPP NAT ルールのままになります。	Panorama を使用してファイアウォールを PAN-OS 11.1.1 から 11.0 0 にダウングレードすると、ポリシーごとに永続的な DIPP NAT ルールが通常の DIPP NAT ルールに変換されます。
GlobalProtect の TLSv1.3 サポート	SSL/TLS サービス プロファイルで **Max Version (**最大バージョン**)** が **[Max (**最大**)]** に設定されている以前の PAN-OS バージョンから PAN-OS 11.1 にアップグレードすると、アップグレード後に TLS	TLSv1.3 を搭載した PAN-OS 11.1 から以前の PAN-OS バージョンにダウングレードすると、ダウングレード後に TLSv1.3 は TLSv1.2 に置き換えられます。PAN-OS 11.1 で TLS v1.3**aes-chacha20-**

機能	アップグレードに関する考慮事項	ダウングレードに関する考慮事項
	バージョンが TLSv1.2 に置き換えられます。 PAN-OS 11.1からそれ以降のバージョンにアップグレードする場合、 **Max Version (最大バージョン)** は **<TLS Version>** SSL/TLSサービスプロファイルでは、**<TLS Version>** アップグレード後TLSバージョンは設定されたままになります。 バージョンは 11.1.x 自体にすでに設定されているため、バージョンの置き換えはありません。	**poly1305**暗号を選択した場合、ダウングレードは成功しますが、自動コミットは失敗します。これは、以前の PAN-OS バージョンではサポートされていません。ダウングレードしたバージョンに適切なサポートされている暗号を追加または置き換え、変更を手動でコミットする必要があります。
VM-50 および VM-50L のアップグレード	VM-50 または VM-50L ファイアウォールを PAN-OS 11.1 にアップグレードする前に、アップグレードを開始する前に、最小プラグインバージョンをインストールする必要があります。 • **PAN-OS 10.2** からのアップグレード- 必要なプラグインの最小バージョンは 3.0.6 です • **PAN-OS 11.0** からのアップグレード- 必要なプラグインの最小バージョンは 4.0.3-h1 です。	なし。
VM-Series ファイアウォール	VM-Series ファイアウォールを PAN-OS バージョン 10.1.x から 11.1.x にアップグレードする場合は、HA の問題を回避するために、アップグレードを実行する前に、すべての 10.1.x ファイアウォールで VM-Series プラグインのバージョンを 2.1.6	なし。

機能	アップグレードに関する考慮事項	ダウングレードに関する考慮事項
	以降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	PAN-OS 10.0 以前のリリースの実行中に生成されたすべてのログは、PAN-OS 11.1.1 にアップグレードすると削除されます。 PAN-OS 11.0 以前のリリースで生成されたログを回復するには、PAN-OS 11.1.2 以降のリリースにアップグレードする 必要があります。これにより、Palo Alto Networks が提供する CLI コマンドを使用して、影響を受けるすべてのログを手動で回復できるようになります。	ダウングレードは お勧めしません。11.1 からダウングレードすることを選択した場合、PAN-OS 11.1 で生成されたすべてのログは削除され、手動で回復する必要があります。11.1 で生成されたログを回復するには、次の手順を実行する必要があります。 1. PAN-OS 11.1.2 以降の 11.1 リリースにアップグレードします。 これは、影響を受けたログを正常に回復するために必要です。 2. ログ コレクター CLI にログインし 、すべての `esdata` ディレクトリを削除します。 `admin>` デバッグ **`elasticsearch`** データを消去する 3. 対象の PAN-OS バージョンにダウングレードします。 4. 変更をコミットして、コレクター グループとすべての管理対象デバイスにプッシュします。 5. ログ コレクター CLI にログインし 、影響を受けたログを回復します。 `admin> debug logdb migrate-lc start log-type all`

機能	アップグレードに関する考慮事項	ダウングレードに関する考慮事項
		*PAN-OS 11.1*からすでにダウングレードしていて、*ElasticSearch*が再起動ループに陥っている場合は、Palo Alto Networksサポートにお問い合わせください。
	コレクター グループ内のすべてのログ コレクターを同時にアップグレードする必要があります。アップグレード ウィンドウ中にコレクター グループ内の一部のログ コレクターのみをアップグレードすることはサポートされていません。	なし。
	PAN-OS 11.1 を実行しているログ コレクターは、ログ コレクター間の通信のためにデバイス登録認証を使用してオンボードする必要があります。 PAN-OS 11.1 へのアップグレード パスでは、PAN-OS 9.1 以前のリリースを実行しているときに Panorama 管理に追加されたログ コレクターを、まず PAN-OS 10.1 以降のリリースにアップグレードし、 デバイス登録認証キーを使用して Panorama 管理に再オンボードする必要があります。 デバイス登録認証キーなしで Panorama 管理にオンボードされたログ コレクターが検出されると、PAN-OS 11.1	なし。

機能	アップグレードに関する考慮事項	ダウングレードに関する考慮事項
	へのアップグレードはブロックされます。	
	コレクター グループを使用している場合、11.1.0 にアップグレードするには次の要件を満たす必要があります。 • 管理対象ログ コレクターをアップグレードするには、11.1 へのアップグレード後に手動でコレクター グループ プッシュを実行する必要があります。 *PAN-OS* では、コレクター グループ内のすべてのログ コレクターが同じバージョンである必要があります。 • デバイス登録認証キーを使用して、ログ コレクターを Panorama に登録する必要があります。 デバイス登録認証キーが正しく初期化されない場合、ピアノードへの接続を形成できません。	なし。
	ログ コレクターを PAN-OS 11.1 にアップグレードすると、ログ コレクター間の通	なし。

機能	アップグレードに関する考慮事項	ダウングレードに関する考慮事項
	信に次の TCP ポートが必要になるため、ネットワーク上で開く必要があります。 • TCP/9300 • TCP/9301 • TCP/9302	
PANサービスプロキシ	なし。	PAN サービス プロキシが有効になっている場合、次世代ファイアウォールを PAN-OS 11.1 からダウングレードすることはできません。ダウングレードを正常に行うには、ダウングレードする前に PAN サービス プロキシを無効にします。 次世代ファイアウォール:**[Network (ネットワーク)]** > **[Proxy (プロキシ)]**を選択し、[プロキシの有効化]の設定アイコンをクリックして、**[None (なし)]**を選択し、**[OK]**をクリックします。 Panorama：[テンプレート] > [ネットワーク] > [プロキシ]と順に進み 、プロキシ有効化の設定アイコンをクリックし、 なしを選択して、**OK** をクリックします。
認証シーケンス	PAN-OS 11.1.1 にアップグレードすると、「**Exit the sequence on failed authentication (**認証失敗時にシーケンスを終了する**)**」オプションは、「**Use domain to determine authentication profile (**ドメインを使用して認証プロファイルを決定する**)**」 オプションに依存しなくなります。	**[**認証失敗時にシーケンスを終了する**]** オプション を選択した場合、**[**認証失敗時にシーケンスを終了する**]** オプションが選択されていないか、**[**認証失敗時にシーケンスを終了する**]** オプションと **[**ドメインを使用して認証プロファイルを決定する**]** オプションの両方が選択されていない限り、PAN-OS 11.1.1 から以前のバージョンへのダ

機能	アップグレードに関する考慮事項	ダウングレードに関する考慮事項
		ウングレード は成功しません。
マルチ Vsys ファイアウォールの Panorama 管理 ソフトウェア バージョン アップグレードのスキップのみを使用して PAN-OS 10.1 から PAN-OS 11.1 にアップグレードします。	ソフトウェア バージョン アップグレードのスキップを使用して Panoramaマネージドマルチvsys ファイアウォールを PAN-OS 11.0 にアップグレードする前に: • **Panorama Shared** 構成内のオブジェクトと同じ名前を持つ、ローカルに構成されたファイアウォール **Shared (**共有**)** オブジェクトを削除するか、名前を変更します。そうしないと、アップグレード後にPanoramaからの設定プッシュが失敗し、エラーが表示されます。`<object-name>` 既に使用されています。 • Palo Alto Networks では、マルチvsysファイアウォールを Panorama で管理する場合は、すべての vsys設定をPanoramaで管理することを推奨しています。 これにより、マネージドマルチvsysファイアウォールでのコミット失敗を回避し、Panorama からの 最適化された共有オブジェクトのプッシュ を活用できるようになります。	なし。
	ソフトウェア バージョンのアップグレードをスキップを使用して、管理対象のマルチ vsys ファイアウォールを PAN-OS 10.2 に正常にアップグレードした後、ファイアウォールは Panorama 上で 同	

機能	アップグレードに関する考慮事項	ダウングレードに関する考慮事項
	期されなく なり、完全なコミットとプッシュが必要になります。 Panorama で、Panorama から構成の変更をコミットしてプッシュする前に、Panorama で管理される構成全体をマルチvsysファイアウォールに **[Commi (コミット)]** して **[Push to Devices (デバイスにプッシュする)]** を選択します。	
(PAN-OS 11.2) SSL インバウンドインスペクションによる HSM 統合の TLSv1.3 サポート	なし。	PAN-OS 11.2 から以前のバージョンにダウングレードすると、内部サーバーの秘密鍵が HSM に保存されている場合の TLSv1.3 セッションの確立と復号化のサポートが削除されます。クライアントとサーバーの両方が TLSv1.3 をサポートしている場合でも、アプライアンスは TLSv1.2 接続を確立します。

Firewall を PAN-OS 11.1 にアップグレードする

PAN-OS 11.1 にアップグレードする方法は、スタンドアロンの ファイアウォールまたはファイアウォールが高可用性(HA)設定にあるかどうか、およびどちらのシナリオでも panorama を使用してファイアウォールを管理するかどうかによって異なります。PAN-OS 11.1 リリース ノートを確認し、展開に固有の手順に従います。

- PAN-OS 11.1 へのアップグレード パスを決定する
- ファイアウォールを Panorama から PAN-OS 11.1 にアップグレードする
- スタンドアロン ファイアウォールのアップグレード
- HA ファイアウォール ペアのアップグレード

コンテンツを *WildFire* アプライアンスに転送するように構成されている *Panorama* またはファイアウォールで管理するファイアウォールをアップグレードする場合は、ファイアウォールをアップグレードする前に、まず Panorama とその Log Collectors をアップグレードしてから、で WildFire アプライアンス をアップグレードする必要があります。

また、*Panorama* より新しいメンテナンス リリースを実行しているファイアウォールを管理することはお勧めしません。機能が期待どおりに機能しない可能性があります。たとえば、*Panorama* が *PAN-OS 10.1.0* を実行している場合、*PAN-OS 10.1.1* 以降のメンテナンス リリースを実行しているファイアウォールを管理することはお勧めしません。

PAN-OS 11.1 へのアップグレード パスを決定する

PAN-OS 機能リリースバージョンから後の機能リリースにアップグレードする場合、ターゲット リリースへのパスに含まれる機能リリース 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。さらに、推奨されるアップグレード パスには、次の機能リリース バージョンの基本イメージをダウンロードする前に、各リリース バージョンに最新のメンテナンス リリースをインストールすることが含まれます。営業時間外にアップグレードを実行すれば、ユーザーのためにダウンタイムを最小限にできます。

手動アップグレードの場合、*Palo Alto Networks* では、アップグレード パスに沿って各 *PAN-OS* リリースの最新メンテナンス リリースをインストールしてアップグレードすることをお勧めします。機能リリースの *PAN-OS* ベース イメージは、アップグレード先のターゲット リリースでない限りインストールしないでください。

次のようにアップグレード パスを決定します。

STEP 1 | 現在インストールされているバージョンを特定します。

- Panorama から **Panorama** > 管理デバイス を選択し、アップグレードする予定のファイアウォールでソフトウェア バージョンを確認します。
- ファイアウォールから **Device** > **Software** を選択し、[現在インストールされている] 列にチェック マークが付いているバージョンを確認します。

STEP 2 | （PAN-OS 11.1.3以降）優先リリースを表示します。

- [Panorama]から**[Panorama]** > **[Software (ソフトウェア)]**をクリックし、**[Base Releases (基本リリース)]**チェックボックスを無効化(空白)にします。
- ファイアウォールから、**[Device (デバイス)]** > **[Software (ソフトウェア)]**をクリックし、**[Base Releases (基本リリース)]**チェックボックスを無効化(空白)にします。

STEP 3 | アップグレード パスを特定します。

アップグレードパスの一部として渡す各リリースのリリースノートとアップグレード/ダウングレードに関する考慮事項で、既知の問題とデフォルトの動作の変更点を確認します。

インストールされた **PAN-OS** バージョン	**PAN-OS 11.1** への推奨アップグレード パス
11.0.x	• PAN-OS 10.2 リリースをすでに実行している場合は、PAN-OS 11.1に直接 アップグレードきます
10.2.x	• PAN-OS 10.2 リリースをすでに実行している場合は、PAN-OS 11.1に直接 アップグレードきます
10.1.x	Skip Software Version Upgrade 機能を使用して、PAN-OS 10.1 以降のリリースからデバイスをアップグレードするときにソフトウェア バージョンをスキップできるようになりました。 • PAN-OS 10.1 リリースをすでに実行している場合は、PAN-OS 11.1に直接 アップグレードできます
10.0.x	• 最新の preferred PAN-OS 10.0 メンテナンス リリースをダウンロードしてインストールし、再起動します。 • PAN-OS 10.1.0をダウンロードしてください。

インストールされた PAN-OS バージョン	PAN-OS 11.1 への推奨アップグレード パス
	• 最新の 優先 PAN-OS 10.1 メンテナンス リリースをダウンロードしてインストールし、再起動します。 Skip Software Version Upgrade 機能を使用して、PAN-OS 10.1 以降のリリースからデバイスをアップグレードするときにソフトウェア バージョンをスキップできるようになりました。 • Firewall を PAN-OS 11.1 にアップグレードするに進みます。
9.1.x	• 最新の preferred PAN-OS 9.1 メンテナンス リリースをダウンロードしてインストールし、再起動します。 • PAN-OS 10.0.0をダウンロードしてください。 • 最新の preferred PAN-OS 10.0 メンテナンス リリースをダウンロードしてインストールし、再起動します。 • PAN-OS 10.1.0をダウンロードしてください。 • 最新の 優先 PAN-OS 10.1 メンテナンス リリースをダウンロードしてインストールし、再起動します。 Skip Software Version Upgrade 機能を使用して、PAN-OS 10.1 以降のリリースからデバイスをアップグレードするときにソフトウェア バージョンをスキップできるようになりました。 • Firewall を PAN-OS 11.1 にアップグレードするに進みます。
9.0.x	• 最新の preferred PAN-OS 9.0 メンテナンス リリースをダウンロードしてインストールし、再起動します。 ログ コレクタを最新の *PAN-OS 9.0* メンテナンス リリースにアップグレードする前に、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。 • PAN-OS 9.1.0をダウンロードしてください。

インストールされた PAN-OS バージョン	PAN-OS 11.1 への推奨アップグレード パス
	• 最新の preferred PAN-OS 9.1 メンテナンス リリースをダウンロードしてインストールし、再起動します。 • PAN-OS 10.0.0をダウンロードしてください。 • 最新の preferred PAN-OS 10.0 メンテナンス リリースをダウンロードしてインストールし、再起動します。 • PAN-OS 10.1.0をダウンロードしてください。 • 最新の 優先 PAN-OS 10.1 メンテナンス リリースをダウンロードしてインストールし、再起動します。 Skip Software Version Upgrade 機能を使用して、PAN-OS 10.1 以降のリリースからデバイスをアップグレードするときにソフトウェア バージョンをスキップできるようになりました。 • Firewall を PAN-OS 11.1 にアップグレードするに進みます。
8.1.x	• 最新の preferred PAN-OS 8.1 メンテナンス リリースをダウンロードしてインストールし、再起動します。 • PAN-OS 9.0.0をダウンロードしてください。 • 最新の preferred PAN-OS 9.0 メンテナンス リリースをダウンロードしてインストールし、再起動します。 ログ コレクタを最新の *PAN-OS 9.0* メンテナンス リリースにアップグレードする前に、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。 • PAN-OS 9.1.0をダウンロードしてください。 • 最新の preferred PAN-OS 9.1 メンテナンス リリースをダウンロードしてインストールし、再起動します。 • PAN-OS 10.0.0をダウンロードしてください。 • 最新の preferred PAN-OS 10.0 メンテナンス リリースをダウンロードしてインストールし、再起動します。

インストールされた PAN-OS バージョン	PAN-OS 11.1 への推奨アップグレード パス
	• PAN-OS 10.1.0をダウンロードしてください。 • 最新の 優先 PAN-OS 10.1 メンテナンス リリースをダウンロードしてインストールし、再起動します。 Skip Software Version Upgrade 機能を使用して、PAN-OS 10.1 以降のリリースからデバイスをアップグレードするときにソフトウェア バージョンをスキップできるようになりました。 • Firewall を PAN-OS 11.1 にアップグレードするに進みます。

スタンドアロン ファイアウォールのアップグレード

PAN-OS 11.1 リリース ノート を確認し、次の手順を使用して、HA 設定に含まれていないファイアウォールを PAN-OS 11.1 にアップグレードします。

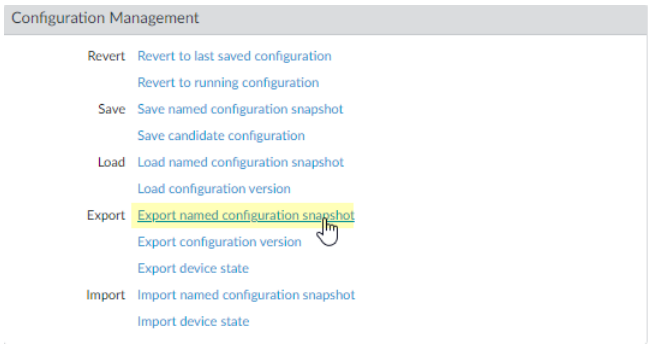
分析のためにサンプルを *WildFire* アプライアンスに転送するようにファイアウォールが構成されている場合、転送ファイアウォールをアップグレードする前に、WildFire アプライアンスを アップグレードする必要があります。

トラフィックへの影響を避けるために、稼働停止期間中にアップグレードすることを計画してください。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。

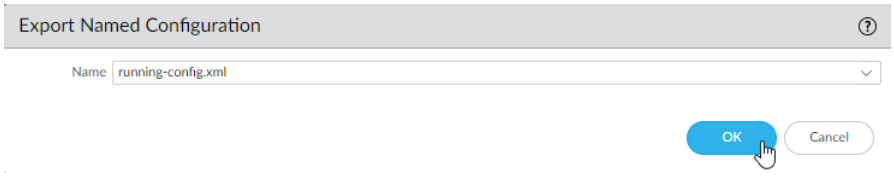
STEP 1 | 現在の構成ファイルのバックアップを保存します。

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. **Device**（デバイス） > **Setup**（セットアップ） > **Operations**（操作）を選択し、**Export named configuration snapshot**（名前付き設定スナップショットのエクスポート）をクリックします。



2. 実行中の設定を含む XML ファイル（**running-config.xml** など）を選択し、**OK** をクリックして設定ファイルをエクスポートします。



3. 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 | (オプション)User-ID を有効にした場合、アップグレード後にファイアウォールは現在の IP アドレスからユーザー名、およびグループマッピングをクリアして、User-ID ソースからの属性を再設定できるようにします。ご自分の環境でのマッピングの再取得に必要な時間を推定するには、ファイアウォール上で次の CLI コマンドを実行します。

- IPアドレス - ユーザー名間マッピングの場合:
  - **`show user user-id-agent state all`**
  - **`show user server-monitor state all`**
- For group mappings: **`show user group-mapping statistics`**

STEP 3 | ファイアウォールで、最新のコンテンツ リリース バージョンが動作していることを確認します。

PAN-OS 11.1 リリース用にインストールする必要がある最小コンテンツ リリース バージョンについては、リリース ノート を参照してください。必ずアプリケーションおよび脅威コンテンツ更新のベストプラクティスに従ってください。

1. **Device**（デバイス） > **Dynamic Updates**（ダイナミック アップデート）を選択して、どの **Applications**（アプリケーション）または**Applications and Threats**（アプリケー

ションと脅威）コンテンツ リリース バージョンが現在インストールされているのかを確認します。

VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLOA...	CURRENTLY INSTALLED	ACTION	DOCUMENTAT...
Applications and Threats	Last checked: 2020/07/08 01:02:02 PDT	Schedule: Every Wednesday at 01:02 (Download only)								
8287-6151	panupv2-all-contents-8287-6151	Apps, Threats	Full	56 MB	36315eff...	2020/06/26 17:34:56 PDT		✓		Release Notes
8287-6152	panupv2-all-contents-8287-6152	Apps, Threats	Full	56 MB	dced5c69...	2020/06/29 11:55:44 PDT	✓ previously		Revert Review Policies Review Apps	Release Notes
8287-6153	panupv2-all-contents-8287-6153	Apps, Threats	Full	56 MB	14af053b...	2020/06/29 17:15:33 PDT			Download	Release Notes
8287-6154	panupv2-all-contents-8287-6154	Apps, Threats	Full	56 MB	c872552f...	2020/06/30 16:14:19 PDT			Download	Release Notes
8287-6155	panupv2-all-contents-8287-6155	Apps, Threats	Full	56 MB	3f0fcb9a6...	2020/06/30 19:09:11 PDT			Download Review Policies Review Apps	Release Notes
8288-6157	panupv2-all-contents-8288-6157	Apps, Threats	Full	56 MB	54f355a1...	2020/07/01 17:00:41 PDT			Download	Release Notes
8288-6158	panupv2-all-contents-8288-6158	Apps, Threats	Full	56 MB	db9e5a8f...	2020/07/01 18:15:46 PDT			Download	Release Notes
8288-6159	panupv2-all-contents-8288-6159	Apps, Threats	Full	56 MB	b6863c96...	2020/07/02 11:55:30 PDT			Download	Release Notes

2. firewall が PAN-OS 11.1 に必要な最低限必要なコンテンツ リリース バージョンまたはそれ以降のバージョンを実行していない場合、**Check Now** は利用可能な更新のリストを取得します。
3. 目的のコンテンツ リリース バージョンを探して、**Download**（ダウンロード）します。

   コンテンツ アップデート ファイルを正常にダウンロードしたら、そのコンテンツ リリース バージョンの 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）に変化します。
4. アップデートをインストールします。

STEP 4 | PAN-OS 11.1 へのアップグレード パスを決定する

Release Notes のPAN-OS アップグレード チェックリスト、既知の問題、既定の動作の変更点を確認し、アップグレード パスの一部として渡す各リリースのアップグレード/ダウングレードに関する考慮事項を確認します。

STEP 5 | (ベスト プラクティス) Cortex データ レイク (CDL) を活用している場合は、デバイス証明書をインストールします。

firewall は、PAN-OS 11.1 へのアップグレード時に、CDL 取り込みおよびクエリ エンドポイントでの認証にデバイス証明書を使用するように自動的に切り替わります。

PAN-OS 11.1 にアップグレードする前にデバイス証明書をインストールしない場合、ファイアウォールは認証に既存のロギング サービス証明書を引き続き使用します。

STEP 6 | PAN-OS 11.1 にアップグレードします。

ファイアウォールで管理ポートからインターネットにアクセスできない場合は、Palo Alto Networks カスタマー サポート ポータル ポータルからソフトウェア イメージをダウンロードして、ファイアウォールに手動でアップロードできます。

1. **[Device**（デバイス） > **[Software**（ソフトウェア）**]**を選択して、**[Check Now**（今すぐ確認）**]**をクリックして最新の PAN-OS アップデートを表示します。

   次に利用可能な PAN-OS リリースのバージョンのみが表示されます。たとえば、PAN-OS 11.1 が firewall にインストールされている場合、PAN-OS 11.1 リリースのみが表示されます。

   （PAN-OS 11.1.3以降）デフォルトでは、優先リリースと対応する基本リリースが表示されます。優先リリースのみを表示するには、**[Base Releases (**基本リリース**)]**チェックボックスをオフ(選択解除)にします。
2. **[Panorama] > [Device Deployment (**デバイスデプロイメント**)] > [Software (**ソフトウェア**)] > [Action (**アクション**)] > [Validate (**検証**)]**

   [Panorama] > [Device Deployment (デバイスデプロイメント**)] > [Software (**ソフトウェア**)] > [Action (**アクション**)] > [Validate (**検証**)]** を使用して、11.1.0 にアップグレードするために必要なすべての中間ソフトウェアとコンテンツ イメージを表示します。
3. 中間ソフトウェアとコンテンツ イメージをダウンロードします。
4. イメージをダウンロードしたら（手動アップグレードの場合、イメージをアップロードしたら）、イメージを **Install**（インストール）します。
5. 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）**]**をクリックします。

   この時点で、ファイアウォールは ユーザー *ID* のマッピングをクリアした後、ユーザー *ID* のソースに接続して、マッピングを更新します。
6. ユーザー ID を有効にしている場合、次の CLI コマンドを使って、トラフィックを許可する前にファイアウォールが IP アドレス - ユーザー名およびグループのマッピングを更新していることを確認してください。
   - **`show user ip-user-mapping all`**
   - **`show user group list`**

STEP 7 | OpenSSL セキュリティー・レベル 2 に準拠するために、すべての証明書を再生成または再インポートします。

PAN-OS 11.1 へのアップグレードでは、すべての証明書が次の最小要件を満たしている必要があります。

- RSA 2048 ビット以上、または ECDSA 256 ビット以上
- Digest of SHA256 以上

証明書の再生成または再インポートの詳細については、PAN-OS Administrator's Guide を参照してください。

STEP 8 | ファイアウォールがトラフィックを渡していることを確認します。

Monitor（監視） > **Session Browser**（セッション ブラウザ）を選択して、新しいセッションが表示されていることを確認します。

START TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATI...	FROM PORT	TO PORT	PROTOC...	APPLICATI...	RULE	INGRESS I/F	EGRESS I/F	BYTES	VIRTUAL SYSTEM
07/08 11:29:02	z1	z2			56622	44060	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	558	vsys1
07/08 11:29:00	z1	z2			44823	42573	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	277874	vsys1
07/08 11:29:10	z1	z2			60162	47273	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	580	vsys1
07/08 11:29:10	z1	z2			45751	6013	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	560	vsys1
07/08 11:29:00	z1	z2			52923	42559	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	111119	vsys1
07/08 11:29:12	z1	z2			45772	8348	6	ftp-data	rules6-clone-with-group	ethernet1/3	ethernet1/4	785	vsys1
07/08 11:29:10	z1	z2			39762	61408	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	554	vsys1
07/08 11:29:06	z1	z2			53948	56596	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	792	vsys1
07/08 11:28:11	z1	z2			38185	42186	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	3243	vsys1

STEP 9 | ファイアウォールのソフトウェア アップグレード履歴を表示します。

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** > **Summary** > **Software** に移動し、[**Device History**] をクリックします。

HA ファイアウォール ペアのアップグレード

PAN-OS 11.1 リリース ノート を確認し、次の手順を使用して、高可用性(HA)構成の firewall のペアをアップグレードします。この手順は、アクティブ/パッシブ設定とアクティブ/アクティブ設定の両方に適用されます。

高可用性（HA）構成のファイアウォールをアップグレードする際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 firewall の場合、どのピアを最初にアップグレードするかは関係ありません(ただし、わかりやすくするために、この手順ではアクティブ/プライマリ ピアを最初にアップグレードする方法を示します)。アクティブ/パッシブ firewall の場合は、最初にアクティブ(プライマリ)ピアをサスペンド(フェールオーバー)してアップグレードする必要があります。プライマリ ピアをアップグレードした後、プライマリ ピアをサスペンド解除して、機能状態(パッシブ)に戻す必要があります。次に、パッシブ(セカンダリ)ピアを一時停止して、プライマリ ピアを再びアクティブにする必要があります。プライマリ ピアがアクティブになり、セカンダリ ピアが中断されたら、アップグレードを続行できます。HA ピアのアップグレード中のフェイルオーバーを防止するために、アップグレード作業に進む前にプリエンプションが無効になっていることを確認する必要があります。ペア内の 1 つのピアでのみ、プリエンプションを無効にする必要があります。

複数の機能 PAN-OS リリース間で HA firewall をアップグレードする場合は、続行する前に、アップグレード パスで各 HA ピアを同じ機能 PAN-OS リリースにアップグレードする必要があります。たとえば、HA ピアを PAN-OS 10.2 から PAN-OS 11.1 にアップグレードするとします。ターゲットの PAN-OS 11.0 リリースへのアップグレードを続行する前に、両方の HA ピアを PAN-OS 11.1 にアップグレードする必要があります。HA ピアが 2 つ以上の機能リリース離れている場合、古いリリースがインストールされている firewall は `suspended` 状態になり、`Peer version too long` というメッセージが表示されます。

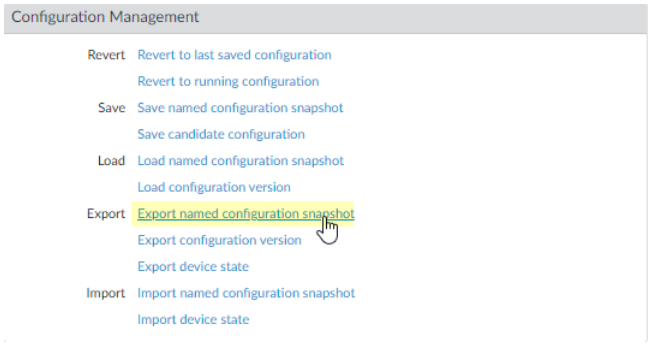
トラフィックへの影響を避けるために、稼働停止期間中にアップグレードすることを計画してください。ファイアウォールが信頼できる電源に接続されていることを確認してください。アップグレード中に電力が失われると、ファイアウォールを使用できなくなる可能性があります。

STEP 1 | 現在の構成ファイルのバックアップを保存します。

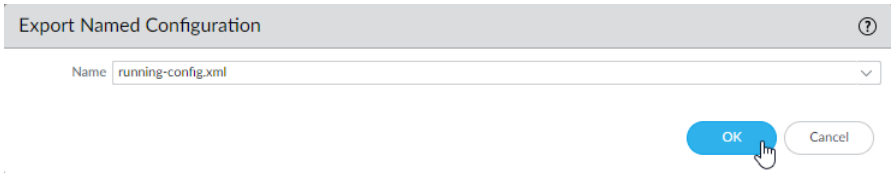
ファイアウォールは自動的に設定のバックアップを作成しますが、アップグレード前にバックアップを作成して外部に保存しておくことをお勧めします。

ペア内の各ファイアウォールで、これらの手順を実行します。

1. **Device**（デバイス） > **Setup**（セットアップ） > **Operations**（操作）を選択し、**Export named configuration snapshot**（名前付き設定スナップショットのエクスポート）をクリックします。



2. 実行中の設定を含む XML ファイル（**running-config.xml** など）を選択し、**OK** をクリックして設定ファイルをエクスポートします。



3. 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。

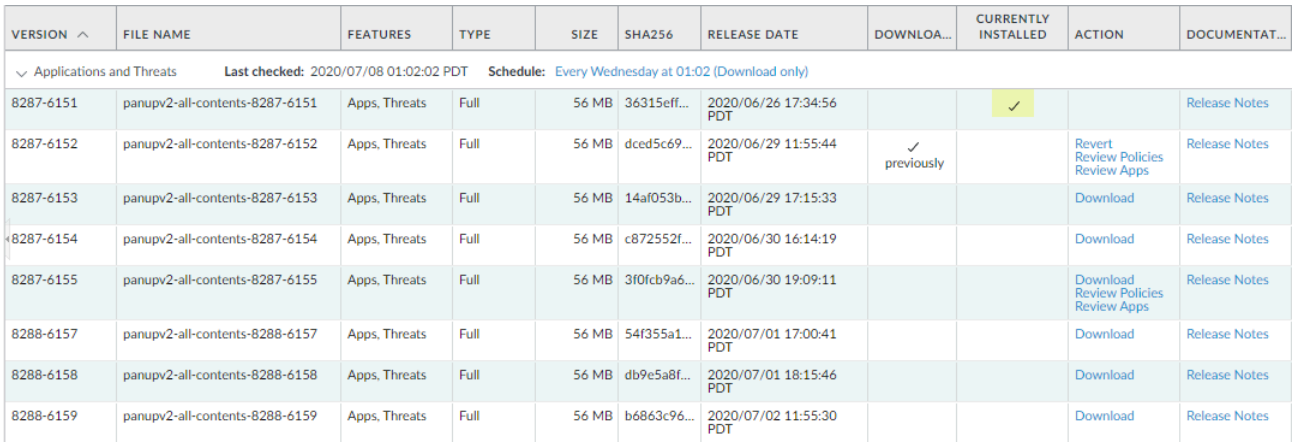
STEP 2 | 選ぶ **Device** > **Support** and **Generate Tech Support File**.

テクニカル サポート ファイルを生成するように求められたら、**Yes** をクリックします。

STEP 3 | HA ペア内の各ファイアウォールで、最新のコンテンツ リリース バージョンが動作していることを確認します。

PAN-OS 11.1 リリース用にインストールする必要がある最小コンテンツ リリース バージョンについては、リリース ノート を参照してください。必ずアプリケーションおよび脅威コンテンツ更新のベストプラクティスに従ってください。

1. 現在インストールされているアップデートを判断するには、**Device**（デバイス） > **Dynamic Updates**（ダイナミック アップデート）を選択して、どの **Applications**（アプリケーション）または**Applications and Threats**（アプリケーションと脅威）をチェックして、現在インストールされているアップデートを判断してください。



VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLOA...	CURRENTLY INSTALLED	ACTION	DOCUMENTAT...
Applications and Threats	**Last checked:** 2020/07/08 01:02:02 PDT	**Schedule:** Every Wednesday at 01:02 (Download only)								
8287-6151	panupv2-all-contents-8287-6151	Apps, Threats	Full	56 MB	36315eff...	2020/06/26 17:34:56 PDT		✓		Release Notes
8287-6152	panupv2-all-contents-8287-6152	Apps, Threats	Full	56 MB	dced5c69...	2020/06/29 11:55:44 PDT	✓ previously		Revert Review Policies Review Apps	Release Notes
8287-6153	panupv2-all-contents-8287-6153	Apps, Threats	Full	56 MB	14af053b...	2020/06/29 17:15:33 PDT			Download	Release Notes
8287-6154	panupv2-all-contents-8287-6154	Apps, Threats	Full	56 MB	c872552f...	2020/06/30 16:14:19 PDT			Download	Release Notes
8287-6155	panupv2-all-contents-8287-6155	Apps, Threats	Full	56 MB	3f0fcb9a6...	2020/06/30 19:09:11 PDT			Download Review Policies Review Apps	Release Notes
8288-6157	panupv2-all-contents-8288-6157	Apps, Threats	Full	56 MB	54f355a1...	2020/07/01 17:00:41 PDT			Download	Release Notes
8288-6158	panupv2-all-contents-8288-6158	Apps, Threats	Full	56 MB	db9e5a8f...	2020/07/01 18:15:46 PDT			Download	Release Notes
8288-6159	panupv2-all-contents-8288-6159	Apps, Threats	Full	56 MB	b6863c96...	2020/07/02 11:55:30 PDT			Download	Release Notes

2. firewalls が PAN-OS 11.1 に必要な最低限必要なコンテンツ リリース バージョンまたはそれ以降のバージョンを実行していない場合、今すぐチェック を使用して、利用可能な更新プログラムの一覧を取得します。
3. 目的のコンテンツ リリース バージョンを探して、**Download**（ダウンロード）します。

   コンテンツ アップデート ファイルを正常にダウンロードしたら、そのコンテンツ リリース バージョンの 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）に変化します。
4. アップデートをインストールします。アップデートは両方のピアにインストールする必要があります。

STEP 4 | PAN-OS 11.1 へのアップグレード パスを決定する

現在実行中の PAN-OS バージョンから PAN-OS 11.1 へのパスにある機能リリース 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。

Release Notes のPAN-OS アップグレード チェックリスト、既知の問題、既定の動作の変更点を確認し、アップグレード パスの一部として渡す各リリースアップグレード/ダウングレードに関する考慮事項を確認します。

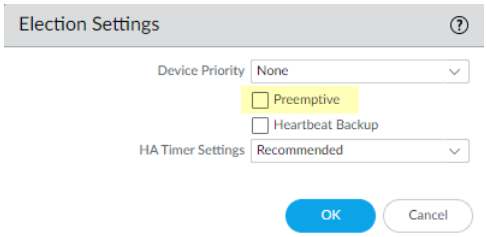
STEP 5 | (ベスト プラクティス) Cortex データ レイク (CDL) を活用している場合は、各 HA ピアにデバイス証明書 をインストールします。

firewall は、PAN-OS 11.1 へのアップグレード時に、CDL 取り込みおよびクエリ エンドポイントでの認証にデバイス証明書を使用するように自動的に切り替わります。

PAN-OS 11.1 にアップグレードする前にデバイス証明書をインストールしない場合、ファイアウォールは認証に既存のロギング サービス証明書を引き続き使用します。

STEP 6 | 各ペアの最初のピアのプリエンプションを無効にします。この設定は、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、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。

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。

STEP 7 | プライマリ HA ピアを一時停止して、フェールオーバーを強制します。

(Active/passive firewalls)アクティブ/パッシブ HA 構成の firewall の場合は、最初にアクティブ HA ピアを一時停止してアップグレードします。

(Active/active firewalls)アクティブ/アクティブ HA 構成の firewalls の場合は、最初にアクティブ/プライマリ HA ピアを一時停止してアップグレードします。

1. **Device** > **High Availability** > **Operational Commands** および **Suspend local device for high availability** を選択します。
2. 右下隅で、状態が `suspended` であることを確認します。

   結果として生じるフェイルオーバーにより、セカンダリ HA ピアは `active` 状態に移行します。

   結果のフェイルオーバーは、アップグレードする前に *HA* フェイルオーバーが正常に機能していることを確認します。

STEP 8 | 中断された HA ピアに PAN-OS 11.1 をインストールします。

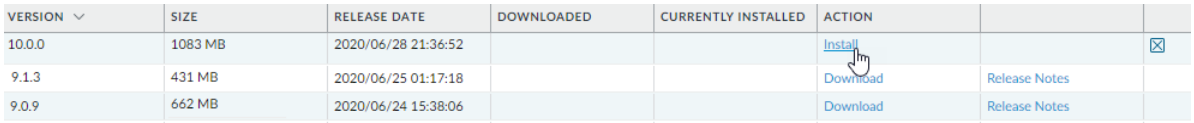
1. プライマリ HA ピアで、**[Device (デバイス)]** > **[Software (ソフトウェア)]** を選択し、**[Check Now (今すぐチェック)]** をクリックして最新のアップデートを表示します。

   次に利用可能な PAN-OS リリースのバージョンのみが表示されます。たとえば、PAN-OS 11.1 が firewall にインストールされている場合、PAN-OS 11.1 リリースのみが表示されます。

   （PAN-OS 11.1.3以降）デフォルトでは、優先リリースと対応する基本リリースが表示されます。優先リリースのみを表示するには、**[Base Releases (基本リリース)]**チェックボックスをオフ(選択解除)にします。
2. 検索し、ダウンロード PAN-OS 11.1.0.

   ファイアウォールで管理ポートからインターネットにアクセスできない場合は、Palo Alto Networks サポート ポータル ポータルからソフトウェアイメージをダウンロードして、ファイアウォールに手動でアップロードできます。

   ファイアウォールにインターネットアクセスが含まれ、ファイルダウンロードエラーが発生した場合は、チェック をもう一度クリックして *PAN-OS* イメージの一覧を更新します。
3. イメージをダウンロードしたら（手動アップグレードの場合、イメージをアップロードしたら）、イメージを **Install**（インストール）します。



4. 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。
5. デバイスの再起動が完了したら、**Dashboard** で高可用性ウィジェットを表示し、アップグレードしたデバイスがピアと同期していることを確認します。

STEP 9 | HA 機能をプライマリ HA ピアに復元します。

1. **Device** > **High Availability** > **Operational Commands** および **Make local device function for high availability**.
2. 右下隅で、状態が パッシブ であることを確認します。アクティブ/アクティブ構成の firewall の場合は、状態が `Active` であることを確認します。
3. HA ピア実行コンフィギュレーションが同期するのを待ちます。

   Dashboard で、高可用性ウィジェットで実行構成の状態を監視します。

STEP 10 | セカンダリ HA ピアで、HA ピアを一時停止します。

1. **Device** > **High Availability** > **Operational Commands** および **Suspend local device for high availability** を選択します。
2. 右下隅で、状態が `suspended` であることを確認します。

   結果として生じるフェールオーバーにより、プライマリ HA ピアは `Active` 状態に移行します。

STEP 11 | セカンダリ HA ピアに PAN-OS 11.1 をインストールします。

1. セカンダリ ピアで、**Device** > **Software** を選択し、最新の更新については **Check Now** をクリックします。
2. 検索し、ダウンロード PAN-OS 11.1.0.
3. イメージをダウンロードしたら、それを**Install**（インストール）します。
4. 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。

STEP 12 | HA 機能をセカンダリ HA ピアに復元します。

1. **Device** > **High Availability** > **Operational Commands** および **Make local device function for high availability**.
2. 右下隅で、状態が パッシブ であることを確認します。アクティブ/アクティブ構成の firewall の場合は、状態が `Active` であることを確認します。
3. HA ピア実行コンフィギュレーションが同期するのを待ちます。

   Dasbhoard で、実行構成の状態の高可用性ウィジェットを監視します。

STEP 13 | 前の手順で無効にした HA ピアでプリエンプションを再度有効にします。

1. **Device** > **High Availability** を選択し、**Election Settings** を編集します。
2. プリエンプティブ 設定を有効 (チェック) し、**OK** をクリックします。
3. 変更を **Commit**（コミット）します。

STEP 14 | OpenSSL セキュリティー・レベル 2 に準拠するために、すべての証明書を再生成または再インポートします。

PAN-OS 11.1 へのアップグレードでは、すべての証明書が次の最小要件を満たしている必要があります。

- RSA 2048 ビット以上、または ECDSA 256 ビット以上
- Digest of SHA256 以上

証明書の再生成または再インポートの詳細については、PAN-OS Administrator's Guide または Panorama Administrator's Guide を参照してください。

STEP 15 | 両方のピアが予定通りにトラフィックを渡していることを確認します。

アクティブ/パッシブ構成では、アクティブなピアのみがトラフィックを渡す必要があります。アクティブ/アクティブ構成では、両方のピアがトラフィックを渡す必要があります。

アップグレードが成功したことを確認するには、次の CLI コマンドを実行します:

- （アクティブなピアのみ）アクティブ ピアがトラフィックを渡していることを確認するには、**show session all** コマンドを実行します。
- セッションの同期を確認するには、**show high-availability interface ha2** コマンドを実行し、CPU テーブルのハードウェア インターフェースのカウンタが以下のように増加していることを確認します。
  - アクティブ/パッシブ設定では、アクティブピアだけが送信パケットを示します。パッシブピアは受信パケットだけを表示します。

    HA2 キープアライブを有効にした場合、パッシブピアのハードウェアインターフェイスカウンタには送信パケットと受信パケットの両方が表示されます。これは、*HA2* キープアライブが双方向で、両方のピアで *HA2* キープアライブ パケットが送信されるためです。
  - アクティブ/アクティブ設定では、両方のピアで受信パケットと送信パケットが表示されます。

ファイアウォールを Panorama から PAN-OS 11.1 にアップグレードする

Panorama™管理サーバーから、コンテンツの更新を展開し、管理対象ファイアウォール用のPAN-OS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 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 11.1 リリース ノート を確認し、次の手順を使用して、Panorama で管理する firewall 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。

複数の機能 PAN-OS リリース間で HA firewall をアップグレードする場合は、続行する前に、アップグレード パスで各 HA ピアを同じ機能 PAN-OS リリースにアップグレードする必要があります。たとえば、HA ピアを PAN-OS 10.2 から PAN-OS 11.1 にアップグレードするとします。ターゲットの PAN-OS 11.0 リリースへのアップグレードを続行する前に、両方の HA ピアを PAN-OS 11.1 にアップグレードする必要があります。HA ピアが 2 つ以上の機能リリース離れている場合、古いリリースがインストールされている firewall は `suspended` 状態になり、`Peer version too long` というメッセージが表示されます。

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。

新しい Skip Software Version Upgrade 機能を使用すると、PAN-OS 11.0 上の Panorama アプライアンスから PAN-OS 11.1 以降のバージョンのファイアウォールへのアップグレードを展開するときに、最大 3 つのリリースをスキップできます。

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。管理対象の firewall をこのバージョンにアップグレードする前に、Panoramaのアップグレード とその Log Collectors を 11.1 に アップグレードする必要があります。さらに、Log Collector を 11.1 にアップグレードする場合は、ロギング インフラストラクチャの変更により、すべての Log Collector を同時にアップグレードする必要があります。
- 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。

- Panorama 仮想アプライアンスが PAN-OS 11.1 へのアップグレード時にレガシー モードである場合は、レガシー モードのままにするかどうかを決定します。レガシ モードは、PAN-OS 9.1 以降のリリースを実行する新しい Panorama 仮想アプライアンスの展開ではサポートされません。Panorama 仮想アプライアンスを PAN-OS 9.0 以前のリリースから PAN-OS 11.1 にアップグレードする場合、Palo Alto Networks では、Panorama仮想アプライアンスの Setup 前提条件 を確認し、必要に応じて Panorama mode または 管理専用モード に変更することをお勧めします。

  Panorama 仮想アプライアンスをレガシー モードのままにする場合は、Panorama 仮想アプライアンスに割り当てられた CPU とメモリの増加 を最小 16 CPU と 32 GB メモリに割り当てて、PAN-OS 11.1 に正常にアップグレードします。詳細については、「セットアップの前提条件 Panorama 仮想アプライアンス を参照してください。
- （マルチvsysマネージドファイアウォール推奨）マルチvsysマネージドファイアウォールのすべてのvsysをPanoramaに移行します。

  これは、マルチvsysマネージドファイアウォールでのコミットの問題を回避するために推奨され、Panoramaから最適化された共有オブジェクトプッシュを利用できます。

  これは、Skip Software Version Upgradeのみを使用してPAN-OS 10.1からPAN-OS 11.1にアップグレードしたマルチvsysファイアウォールに適用されます。
- (マルチvsysマネージド ファイアウォール) ローカルで構成されたものを削除または名前変更シェアード パノラマ内のオブジェクトと同じ名前のオブジェクト シェアード 構成。それ以外の場合、Panoramaからの設定プッシュはアップグレード後に失敗し、エラー`<object-name>`がすでに使用されています。

  これは、Skip Software Version Upgradeのみを使用してPAN-OS 10.1からPAN-OS 11.1にアップグレードしたマルチvsysファイアウォールに適用されます。

STEP 1 | Panorama Web インターフェースにログインします。

STEP 2 | `ssl`アプリケーショントラフィックを許可するようにセキュリティポリシールールを変更しました。

> これは、スキップソフトウェアバージョンのアップグレードのみを使用してPAN-OS 10.1からPAN-OS 11.1にアップグレードしたファイアウォールに適用されます。
>
> これは、*`Panorama`App-ID*を使用して*Panorama*と管理対象デバイス間のトラフィックを制御している場合、*PAN-OS 11.1*へのアップグレード後に管理対象デバイスが*Panorama*から切断されるのを防ぐために必要です。アップグレード前に*`ssl`*アプリケーションが許可されていない場合、管理対象デバイスは*Panorama*から切断されます。

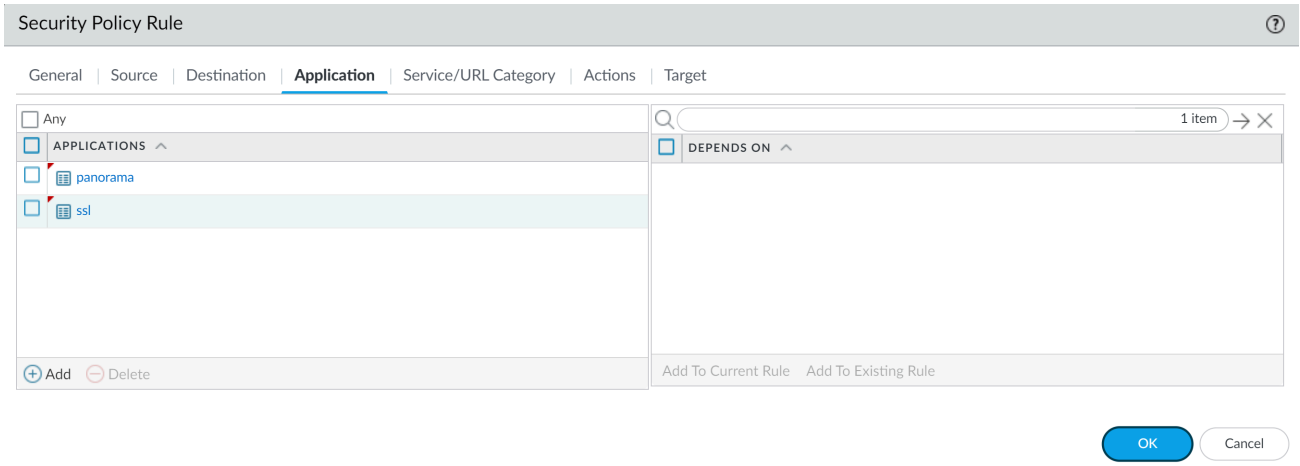
PAN-OS 11.1はTLSバージョン1.3を使用して、Panoramaとマネージドファイアウォール間のサービス証明書とハンドシェイクメッセージを暗号化します。これにより、マネージドファイアウォールからPanoramaへのトラフィックのApp-IDが`Panorama`から`ssl`に再分類されます。Panoramaと管理対象デバイス間の通信を継続するには、Panoramaと管理対象デバイス

間のトラフィックを制御するセキュリティポリシールールを変更して、sslアプリケーションも許可する必要があります。

Panoramaと管理対象デバイス間のトラフィックを制御するセキュリティポリシールールで任意のアプリケーションを許可している場合、またはPanoramaと管理対象デバイス間のトラフィックを制御するセキュリティポリシールールをすでに変更している場合は、この手順をスキップします。

1. **[Policies**（ポリシー）**] > [Security**（セキュリティ）**] > [Pre Rules**（プレルール）**]**を順に選択します。
2. Panoramaと管理対象ファイアウォール間のトラフィックを制御するセキュリティポリシールールを含む**[Device Group (**デバイスグループ**)]**を選択します。
3. セキュリティポリシー規則を選択します。
4. **[Application (**アプリケーション**)]**を選択し、sslを**[Add (**追加**)]**します。

   *Panorama*アプリケーションを削除しないでください。これにより、変更をプッシュした後、すべての管理対象ファイアウォールが*Panorama*から切断されます。

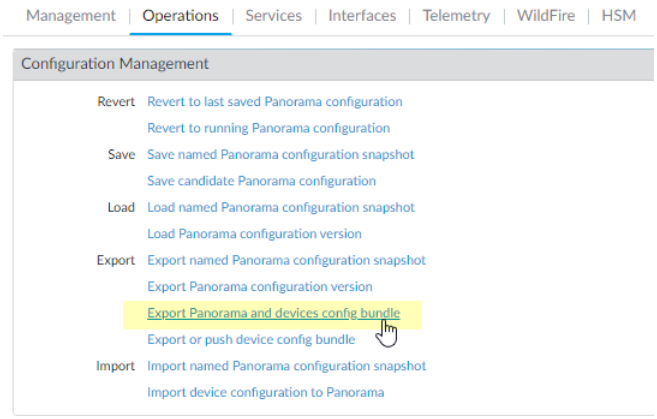


5. **OK** をクリックします。
6. **[Commit**（コミット）**] > [Commit and Push**（コミットおよびプッシュ配信）**]**を順に選択して、設定内容を**[Commit and Push**（コミットしてプッシュ配信）**]**します。

STEP 3 | 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. **Panorama > Setup > Operations** を選択し、**Export Panorama and Devices config bundle** をクリックして、Panorama および各管理対象アプライアンスの最新の構成バックアップを生成してエクスポートします。



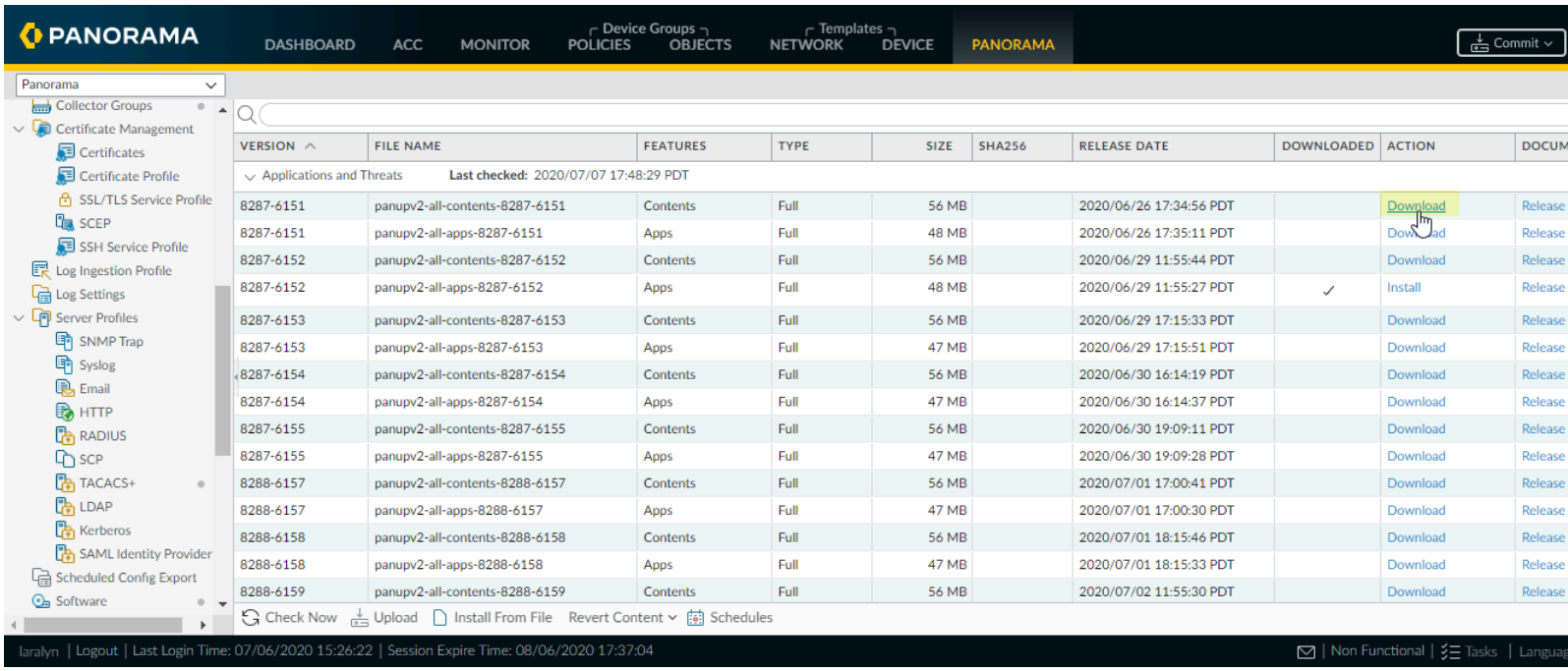
2. エクスポート ファイルをファイアウォールの外部に保存します。アップグレードで問題が発生した場合は、このバックアップを使用して設定を復元することができます。

STEP 4 | 最新のコンテンツ更新プログラムをインストールします。

PAN-OS 11.1 に必要な最小コンテンツ リリース バージョンについては、リリース ノート を参照してください。Panorama と管理された firewall にコンテンツの更新をデプロイするとき

は、必ずアプリケーションおよび脅威コンテンツ更新のベストプラクティスに従ってください。

1. 最新の更新プログラムについては、パノラマ > **Device Deployment** > **Dynamic Updates** および **Check Now** を選択します。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. インストール をクリックし、更新プログラムをインストールする firewall を選択します。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。
3. **[OK]** をクリックします。

STEP 5 | 「PAN-OS 11.1 へのアップグレード パスを決定する」を行います。

PAN-OS アップグレード チェックリスト、アップグレード パスの一部として渡す各リリースの リリース ノート および アップグレード/ダウングレードに関する考慮事項 の既知の問題と既定の動作の変更点を確認します。

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。

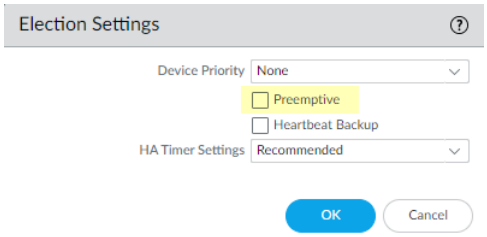
STEP 6 | (ベスト プラクティス) Cortex データ レイク (CDL) を活用している場合は、デバイス証明書をインストールします。

firewall は、PAN-OS 11.1 へのアップグレード時に、CDL 取り込みおよびクエリ エンドポイントでの認証にデバイス証明書を使用するように自動的に切り替わります。

PAN-OS 11.1 にアップグレードする前にデバイス証明書をインストールしない場合、ファイアウォールは認証に既存のロギング サービス証明書を引き続き使用します。

STEP 7 | （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。



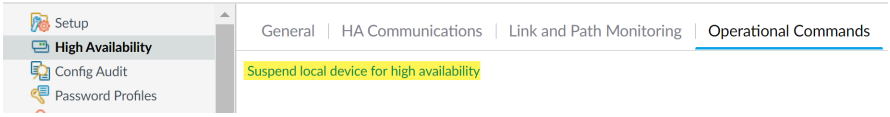
3. 変更を **Commit**（コミット）します。アップグレードを続行する前に、コミットが成功していることを確認してください。

STEP 8 | (HA firewall upgrades only)プライマリ HA ピアを一時停止して、フェールオーバーを強制します。

(Active/passive firewalls)アクティブ/パッシブ HA 構成の firewall の場合は、最初にアクティブ HA ピアを一時停止してアップグレードします。

(Active/active firewalls)アクティブ/アクティブ HA 構成の firewalls の場合は、最初にアクティブ/プライマリ HA ピアを一時停止してアップグレードします。

1. アクティブなプライマリ firewall HA ピアの firewall web interface にログインします。
2. 選ぶ **Device** > **High Availability** > **Operational Commands** and **Suspend local device for high availability**.



3. 右下隅で、状態が `suspended` であることを確認します。

   結果として生じるフェイルオーバーにより、セカンダリ・パッシブ HA ピアは `active` 状態に移行します。

   結果のフェイルオーバーは、アップグレードする前に *HA* フェイルオーバーが正常に機能していることを確認します。

STEP 9 | (Optional) Upgrade your managed firewalls to PAN-OS 10.1.

ソフトウェア バージョンのスキップ アップグレード機能は、PAN-OS 10.1 以降のリリースを実行している管理対象 firewall をサポートします。管理対象の firewall が PAN-OS 10.0 以前のリリースにある場合は、まず PAN-OS 10.1 以降のリリースにアップグレードします。

STEP 10 | (Optional) **Export** ファイルを構成済みの SCP サーバーに保存します。

PAN-OS 11.1 では、管理対象 firewall へのアップグレードを展開するときに、SCP サーバをダウンロード ソースとして使用できます。次の手順でソフトウェアとコンテンツイメージをダウンロードする前に、ファイルをエクスポートします。

STEP 11 | ターゲット リリースに必要なソフトウェアとコンテンツ バージョンを検証してダウンロードします。

この手順では、PAN-OS 11.1 へのアップグレードに必要な中間ソフトウェアとコンテンツ イメージの表示とダウンロードの両方を行うことができます。

マルチイメージダウンロードを使用したソフトウェアおよびコンテンツイメージのダウンロードはオプションです。画像を 1 つずつダウンロードできます。

1. クリック **panorama** > **Device Deployment** > **Software** > **Action** > **Validate**.
2. ダウンロードする必要がある中間ソフトウェアとコンテンツのバージョンを表示します。
3. アップグレードする firewall を選択し、デプロイ をクリックします。
4. ダウンロード元を選択し、ダウンロードをクリックします。

STEP 12 | PAN-OS 11.1.0 を firewalls にインストールします。

> *(SD-WAN のみ)SD-WAN リンクの正確なステータスを維持するには、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 firewall を PAN-OS 11.1 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、誤った監視データ **([Panorama] > [SD-WAN] > [Monitoring (モニタリング)]*** が発生し、*SD-WAN リンクが誤って down（ダウン）*と表示されることがあります。

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。たとえば、PA-440ファイアウォールをアップグレードする場合は、PanOS_440-11.1.0 に対応する行で **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。

   (HA firewall upgrades only)ダウンタイムを短縮するには、各 HA ペアでピアを 1 つだけ選択します。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. firewalls のリブートが完了したら、**[Panorama] > [Managed Devices (管理対象外デバイス)]** 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 11.1.0 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 13 | (HA firewall upgrades only)HA 機能をプライマリ HA ピアに復元します。

1. 中断されたプライマリ firewall HA ピアの firewall web インターフェイス にログインします。
2. 選択します。 **Device > High Availability > Operational Commands** and **Make local device function for high availability**.
3. 右下隅で、状態が パッシブ であることを確認します。アクティブ/アクティブ構成の firewall の場合は、状態が `Active` であることを確認します。
4. HA ピア実行コンフィギュレーションが同期するのを待ちます。

   Dashboard で、高可用性ウィジェットで実行構成の状態を監視します。

STEP 14 | (HA firewall upgrades only)セカンダリ HA ピアを一時停止して、プライマリ HA ピアへのフェイルオーバーを強制します。

1. アクティブなセカンダリ firewall HA ピアの firewall web interface にログインします。
2. 選ぶ **Device** > **High Availability** > **Operational Commands** and **Suspend local device for high availability**.
3. 右下隅で、状態が `suspended` であることを確認します。

   結果として生じるフェイルオーバーにより、プライマリ・パッシブ HA ピアは `active` 状態に移行します。

   結果のフェイルオーバーは、アップグレードする前に *HA* フェイルオーバーが正常に機能していることを確認します。

STEP 15 | （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. Panorama web interface で、**Panorama** > **Device Deployment** > **Software**を選択します。
2. 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。
3. 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。
4. **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。
5. **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。
6. アップグレードを開始するには、**OK** をクリックします。
7. 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。

STEP 16 | (HA firewall upgrades only)HA 機能をセカンダリ HA ピアに復元します。

1. 中断されたセカンダリ firewall HA ピアの firewall web interface にログインします。
2. 選択します。 **Device** > **High Availability** > **Operational Commands** and **Make local device function for high availability**.
3. 右下隅で、状態が パッシブ であることを確認します。アクティブ/アクティブ構成の firewall の場合は、状態が `Active` であることを確認します。
4. HA ピア実行コンフィギュレーションが同期するのを待ちます。

   Dashboard で、高可用性ウィジェットで実行構成の状態を監視します。

STEP 17 | (FIPS-CC モードのみ)FIPS-CC モードでの Panorama デバイスと管理対象デバイスのアップグレード.

管理対象 firewall が PAN-OS 11.1 リリースを実行しているときに専用 Log Collector を Panorama 管理に追加した場合、FIPS-CC モードで管理対象 firewall をアップグレードするには、セキュア接続ステータスをリセットする必要があります。

管理対象 firewall が PAN-OS 10.0 以前のリリースを実行している間は、Panorama 管理に追加された管理対象 firewall を再オンボードする必要はありません。

STEP 18 | 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。

	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 19 | （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。

STEP 20 | Panorama ウェブインターフェイス で、Panorama 管理対象構成全体を管理対象の firewall にプッシュします。

この手順は、デバイス グループとテンプレート スタックの構成変更を Panorama から管理対象の firewall に選択的にコミットしてプッシュできるようにするために必要です。

これは、PAN-OS 10.1 以前のリリースから PAN-OS 11.1 へのアップグレードが正常に行われた後、Panorama によって管理されるマルチvsysファイアウォールに設定変更を正常にプッシュするために必要です。詳細については、Panorama によって管理されるマルチ vsys firewall の 共有構成オブジェクトの既定の動作の変更を参照してください。

1. **Commit** > **Push to Devices**を選択します。
2. **Push**.

STEP 21 | OpenSSL セキュリティー・レベル 2 に準拠するために、すべての証明書を再生成または再インポートします。

PAN-OS 11.1 以降のリリースにアップグレードする場合は、すべての証明書が次の最小要件を満たしている必要があります。PAN-OS 10.2 からアップグレードしていて、証明書をすでに再生成または再インポートしている場合は、この手順をスキップします。

- RSA 2048 ビット以上、または ECDSA 256 ビット以上
- Digest of SHA256 以上

証明書の再生成または再インポートの詳細については、PAN-OS Administrator's Guide または Panorama Administrator's Guide を参照してください。

STEP 22 | ファイアウォールのソフトウェア アップグレード履歴を表示します。

1. Panorama インターフェイスにログインします。
2. パノラマ > **Managed Devices** > **Summary** に移動し、[**Device History**] をクリックします。

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。

新しい Skip Software Version Upgrade 機能を使用すると、PAN-OS 11.0 上の Panorama アプライアンスから PAN-OS 11.1 以降のバージョンのファイアウォールへのアップグレードを展開するときに、最大 3 つのリリースをスキップできます。

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。管理対象の firewall をこのバージョンにアップグレードする前に、Panoramaのアップグレード とその Log Collectors を 11.1 に アップグレードする必要があります。さらに、Log Collector を 11.1 にアップグレードする場合は、ロギング インフラストラクチャの変更により、すべての Log Collector を同時にアップグレードする必要があります。
- 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。
- Panorama 仮想アプライアンスが PAN-OS 11.1 へのアップグレード時にレガシー モードである場合は、レガシー モードのままにするかどうかを決定します。レガシ モードは、PAN-OS 9.1 以降のリリースを実行する新しい Panorama 仮想アプライアンスの展開ではサポートされません。Panorama 仮想アプライアンスを PAN-OS 9.0 以前のリリースから PAN-OS 11.1 にアップグレードする場合、Palo Alto Networks では、Panorama仮想アプライアンスの Setup 前提条件 を確認し、必要に応じて Panorama mode または 管理専用モード に変更することをお勧めします。

  Panorama 仮想アプライアンスをレガシー モードのままにする場合は、Panorama 仮想アプライアンスに割り当てられた CPU とメモリの増加 を最小 16 CPU と 32 GB メモリに割り当て

て、PAN-OS 11.1 に正常にアップグレードします。詳細については、「セットアップの前提条件 Panorama 仮想アプライアンス を参照してください。

- （マルチvsysマネージドファイアウォール推奨）マルチvsysマネージドファイアウォールのすべてのvsysをPanoramaに移行します。

  これは、マルチvsysマネージドファイアウォールでのコミットの問題を回避するために推奨され、Panoramaから最適化された共有オブジェクトプッシュを利用できます。

  これは、Skip Software Version Upgradeのみを使用してPAN-OS 10.1からPAN-OS 11.1にアップグレードしたマルチvsysファイアウォールに適用されます。

- （マルチvsysマネージドファイアウォール）ローカルに設定された共有オブジェクトのうち、Panorama共有設定のオブジェクトと同じ名前を持つものを削除するか、名前を変更します。それ以外の場合、Panoramaからの設定プッシュはアップグレード後に失敗し、エラー`<object-name>`がすでに使用されています。

  これは、Skip Software Version Upgradeのみを使用してPAN-OS 10.1からPAN-OS 11.1にアップグレードしたマルチvsysファイアウォールに適用されます。

STEP 1 | Panorama Web インターフェースにログインします。

STEP 2 | `ssl`アプリケーショントラフィックを許可するようにセキュリティポリシールールを変更しました。

これは、スキップソフトウェアバージョンのアップグレードのみを使用してPAN-OS 10.1からPAN-OS 11.1にアップグレードしたファイアウォールに適用されます。

これは、*PanoramaApp-ID*を使用して*Panorama*と管理対象デバイス間のトラフィックを制御している場合、*PAN-OS 11.1*へのアップグレード後に管理対象デバイスが*Panorama*から切断されるのを防ぐために必要です。アップグレード前に`ssl`アプリケーションが許可されていない場合、管理対象デバイスは*Panorama*から切断されます。

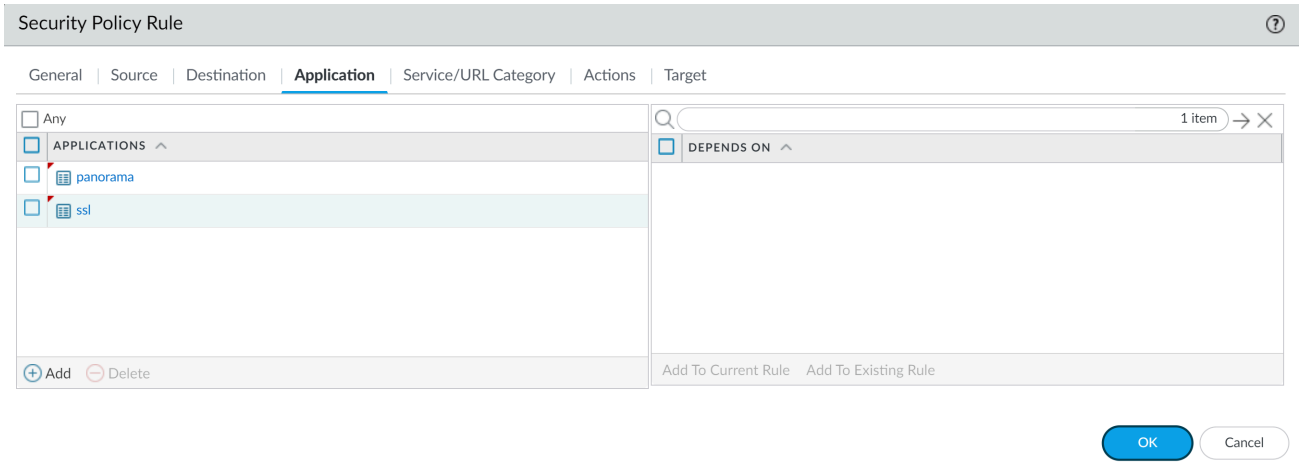
PAN-OS 11.1はTLSバージョン1.3を使用して、Panoramaとマネージドファイアウォール間のサービス証明書とハンドシェイクメッセージを暗号化します。これにより、マネージドファイアウォールからPanoramaへのトラフィックのApp-IDが`Panorama`から`ssl`に再分類されます。Panoramaと管理対象デバイス間の通信を継続するには、Panoramaと管理対象デバイス間のトラフィックを制御するセキュリティポリシールールを変更して、`ssl`アプリケーションも許可する必要があります。

Panoramaと管理対象デバイス間のトラフィックを制御するセキュリティポリシールールで任意のアプリケーションを許可している場合、またはPanoramaと管理対象デバイス間のトラフィックを制御するセキュリティポリシールールをすでに変更している場合は、この手順をスキップします。

1. **[Policies**（ポリシー）**]** > **[Security**（セキュリティ）**]** > **[Pre Rules**（プレルール）**]**を順に選択します。

2. Panoramaと管理対象ファイアウォール間のトラフィックを制御するセキュリティポリシールールを含む**[Device Group (デバイスグループ)]**を選択します。
3. セキュリティポリシー規則を選択します。
4. **[Application (アプリケーション)]**を選択し、`ssl`を**[Add (追加)]**します。

   *`Panorama`*アプリケーションを削除しないでください。これにより、変更をプッシュした後、すべての管理対象ファイアウォールが*Panorama*から切断されます。



5. **OK** をクリックします。
6. **[Commit（コミット）] > [Commit and Push（コミットおよびプッシュ配信）]**を順に選択して、設定内容を**[Commit and Push（コミットしてプッシュ配信）]**します。

STEP 3 | 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 4 | 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。

コンテンツアップデートごとに、更新が必要かどうかを判断し、次の手順でダウンロードする必要があるコンテンツアップデートをメモします。

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。

STEP 5 | Panorama 11.1 に更新する予定の firewalls のソフトウェア アップグレード パスを決定します。

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。

Release Notes のPAN-OS アップグレード チェックリスト、既知の問題、既定の動作の変更点を確認し、アップグレード パスの一部として渡す各リリースアップグレード/ダウングレードに関する考慮事項を確認します。

STEP 6 | (Optional) Upgrade your managed firewalls to PAN-OS 10.1.

ソフトウェア バージョンのスキップ アップグレード機能は、PAN-OS 10.1 以降のリリースを実行している管理対象 firewall をサポートします。管理対象の firewall が PAN-OS 10.0 以前のリリース上にある場合は、まず PAN-OS 10.1 以降のリリースにアップグレードします。

STEP 7 | リリースの検証チェックを行います。

この手順では、11.1 へのアップグレードに必要な中間ソフトウェアとコンテンツ イメージを表示できます。

1. **Panorama > Device Deployment > Software > Action > Validate**を選択。
2. ダウンロードする必要があるソフトウェアとコンテンツのバージョンを表示します。

STEP 8 | コンテンツとソフトウェアの更新を、SCP または HTTPS 経由で Panorama または設定された SCP サーバーに接続してファイルをアップロードできるホストに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。2 つ以上のソフトウェア更新プログラムまたは 1 つのタイプのコンテンツ更新プログラムをアップロード

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。

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-440 および PA-5430ファイアウォールを PAN-OS 11.1.0 にアップグレードするには、`PanOS_440-11.1.0` および `PanOS_5430-11.1.0` イメージをダウンロードします。

      PAN-OS*用の*PA-<series/model> を選択するには、***Filter By*** ドロップダウンから特定の *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 9 | 中間ソフトウェア バージョンと最新のコンテンツ バージョンをダウンロードします。

PAN-OS 11.0 では、マルチイメージ ダウンロード機能を使用して複数の中間リリースをダウンロードできます。

1. アップグレードする firewalls (**Required Deployment** > **Deploy**) を選択します。
2. ダウンロード元を選択し、**Download**をクリックします。

STEP 10 | 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 11 | （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。
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 12 | PAN-OS 11.1 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。

(SD-WAN のみ)SD-WAN リンクの正確なステータスを維持するには、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 *firewall* を *PAN-OS 11.1* 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、誤った監視データ *([Panorama] > [SD-WAN] > [Monitoring (*モニタリング*)]* が発生し、*SD-WAN* リンクが誤って *down (*ダウン*)* と表示されることがあります。

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。各 HA ペアの 1 つの firewall でこの設定を無効にするだけで済みますが、続行する前にコミットが成功したことを確認してください。
  2. 該当する更新プログラムの [Action (アクション)] 列の **[Install (インストール)]** をクリックし、**Group HA Peers** を無効化 (クリア) し、fw2を選択し、**[Reboot device after install (インストール後にデバイスを再起動)]**し 、**OK** をクリックします。続行する前に、fw2 の再起動が完了するのを待ちます。
  3. fw2 の再起動が完了したら、fw1 (**[Dashboard (ダッシュボード)]** >高可用性) で、fw2 がまだパッシブ 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状態は `[active (アクティブ)]` で、ピア (fw2) は `[passive (パッシブ)]`)。
  4. fw1 にアクセスし ローカルデバイスをサスペンドします(**[Device (デバイス)]** > **[High Availability (高可用性)]** > **[Operational Commands (オペレーショナルコマンド)]**)。
  5. fw2 にアクセスし (**[Dashboard (ダッシュボード)]** > [High Availability (高可用性)]) をクリックし、ローカルファイアウォールの状態が `[アクティブ (active)]` であり、ピアが `[suspended (サスペンド)]` であることを確認します。
  6. Panoramaにアクセスし、**[Panorama]** > **[Device Deployment (デバイスの開発)]** > **[Software (ソフトウェア)]** を選択し、該当するリリースの[アクション]列で**[Install (インストール)]**をクリックし、**Group HA Peers**を無効化(クリア)し、fw1を選択し、インストール後にデバイスを再起動して、[OK]をクリックします。続行する前に、fw1 の再起動が完了するのを待ちます。
  7. fw1 にアクセスし (**[Device (デバイス)]** > **[High Availability (高可用性)]** > **[Operational Commands (オペレーショナルコマンド)]**)をクリックし、**[Make local device functional (ローカル デバイスを機能させる)]**をクリックし、2 分間待ってから続行します。
  8. fw1の (**[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 (パッシブ)]` であり、ピア (fw2) が `[active (アクティブ)]` であることを確認します。

STEP 13 | (FIPS-CC モードのみ)FIPS-CC モードでの Panorama デバイスと管理対象デバイスのアップグレード.

管理対象 firewall が PAN-OS 11.1 リリースを実行しているときに専用 Log Collector を Panorama 管理に追加した場合、FIPS-CC モードで管理対象 firewall をアップグレードするには、セキュア接続ステータスをリセットする必要があります。

管理対象 firewall が PAN-OS 10.0 以前のリリースを実行している間は、Panorama 管理に追加された管理対象 firewall を再オンボードする必要はありません。

STEP 14 | 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 15 | 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。

STEP 16 | Panorama ウェブ インターフェイス で、Panorama 管理対象構成全体を管理対象の firewall にプッシュします。

この手順は、デバイス グループとテンプレート スタックの構成変更を Panorama から管理対象の firewall に選択的にコミットしてプッシュできるようにするために必要です。

これは、PAN-OS 11.1 へのアップグレードが成功した後、Panorama によって管理されるマルチ vsys firewall に設定変更を正常にプッシュするために必要です。詳細については、Panorama によって管理されるマルチ vsys firewall の 共有構成オブジェクトの既定の動作の変更を参照してください。

1. **Commit** > **Push to Devices**を選択します。
2. **Push**.

STEP 17 | OpenSSL セキュリティー・レベル 2 に準拠するために、すべての証明書を再生成または再インポートします。

PAN-OS 11.1 へのアップグレードでは、すべての証明書が次の最小要件を満たしている必要があります。

- RSA 2048 ビット以上、または ECDSA 256 ビット以上
- Digest of SHA256 以上

証明書の再生成または再インポートの詳細については、PAN-OS Administrator's Guide または Panorama Administrator's Guide を参照してください。

STEP 18 | ファイアウォールのソフトウェア アップグレード履歴を表示します。

1. Panorama インターフェイスにログインします。
2. パノラマ > **Managed Devices** > **Summary** に移動し、[**Device History**] をクリックします。

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 Webインターフェイスに管理者ユーザとしてログインします。

STEP 2 | Panorama に ZTP ファイアウォールを追加します。

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。

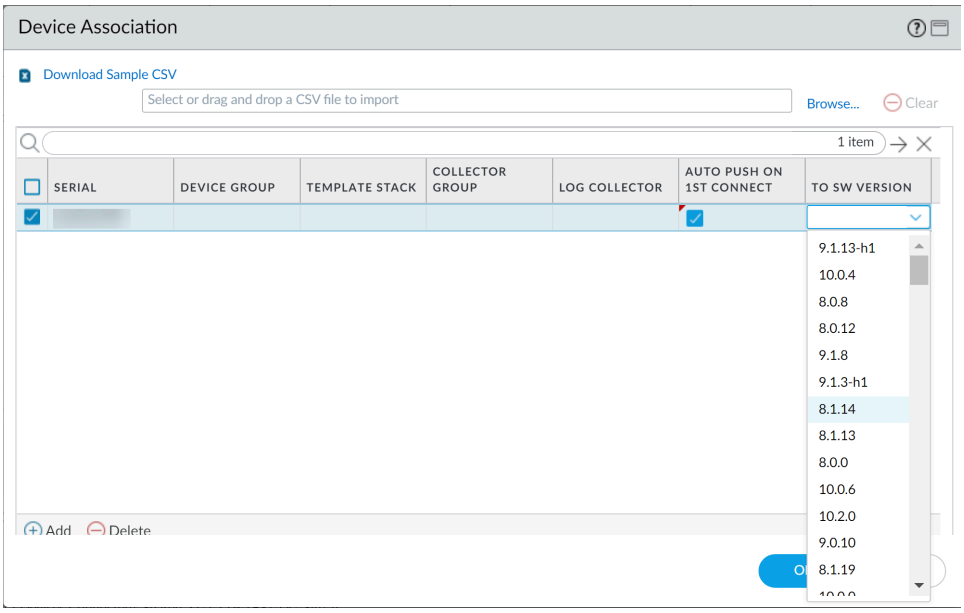
STEP 4 | **Panorama**（**Panorama**） > **Managed Devices**（管理対象デバイス） > **Summary**（概要）の順に選択して、次に 1 つ以上の ZTP ファイアウォールを選択します。

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 | Check (enable) **Auto Push on 1st Connect**.

STEP 7 | **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 8 | **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)** および **Commit to Panorama (Panorama** へのコミット**)** をクリックします。

STEP 10 | ZTP ファイアウォールの電源を入れます。

ZTP firewall が初めて Panorama に接続すると、選択した PAN-OS バージョンに自動的にアップグレードされます。

- **Panorama** が **PAN-OS 11.1.0** を実行している場合:PAN-OS メジャー リリースまたはメンテナンス リリース間で管理対象の firewall をアップグレードする場合、ターゲットの PAN-OS リリースがインストールされる前に、アップグレード パス上の中間 PAN-OS リリースが最初にインストールされます。

  たとえば、管理対象 firewall のターゲット **To SW** バージョンを PAN-OS 11.1.0 として設定し、ファイアウォールが PAN-OS 10.2 を実行しているとします。Panorama への最初の接続時に、PAN-OS 11.0.0 が最初に管理対象のファイアウォールにインストールされます。PAN-OS 11.0.0 が正常にインストールされると、ファイアウォールは自動的にターゲットの PAN-OS 11.1.0 リリースにアップグレードされます。

- **Panorama** が **PAN-OS 11.0.1** 以降のリリースを実行している:PAN-OS メジャー リリースまたはメンテナンス リリース間で管理対象 firewall をアップグレードする場合、アップグレード パス上の中間の PAN-OS メジャー リリースがインストールされ、ターゲットの PAN-OS メンテナンス リリースがインストールされる前にベース PAN-OS メジャー リリースがダウンロードされます。

  たとえば、管理対象の firewall のターゲット **To SW** バージョン を PAN-OS 11.0.1 として設定し、firewall が PAN-OS 10.0 で動作しているとします。Panorama への最初の接続時に、PAN-OS 10.1.0 および PAN-OS 10.2.0 が管理対象の firewall にインストールされます。管理対象の firewall がリブートすると、PAN-OS 11.0.0 がダウンロードされ、firewall がターゲットの PAN-OS 11.0.1 リリースに自動的にインストールされます。

STEP 11 | 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 Web インターフェイスへのログイン。
2. **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。
3. **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。

STEP 12 | 今後のすべての PAN-OS アップグレードについては、ファイアウォールを Panorama から PAN-OS 11.1 にアップグレードするを参照してください。

PAN-OSソフトウェアパッチのインストール

どこで使用できますか?	何が必要ですか?
• 次世代 Firewall	❑ サポートライセンス ❑ PAN-OS 11.1.3 以降もしくは 11.1 リリース ❑ アウトバウンドインターネットアクセス

「PAN-OS 11.1リリースノート」を確認してから、次の手順に従ってPAN-OSソフトウェアパッチをインストールし、現在次世代ファイアウォールで実行されているPAN-OSリリースのバグと共通脆弱性および暴露（CVE）に対処します。PAN-OSソフトウェアパッチをインストールすると、長期間のメンテナンスをスケジュールしなくてもバグやCVEに対する修正が適用され、新しいPAN-OSリリースのインストールに伴う新たな既知の問題やデフォルト動作の変更をもたらすことなく、すぐにセキュリティ体制を強化できます。さらに、現在インストールされているソフトウェアパッチを元に戻して、ソフトウェアパッチをインストールしたときに適用されたバグやCVEの修正をアンインストールすることもできます。

PAN-OSのソフトウェアパッチをインストールまたは元に戻すと、システムログが生成されます（**[Monitor (モニター)]** > **[Logs (ログ)]** > **[System (システム)]**）。パロアPalo Alto Networks カスタマーサポートポータルからPAN-OSソフトウェアパッチをダウンロードするには、アウトバウンドインターネット接続が必要です。

- インストール
- 元に戻す

インストール

STEP 1 | ファイアウォール Web インターフェイス にログインします。

STEP 2 | **[Device (デバイス)** > **Software (ソフトウェア)]** を選択し、**[Check Now (今すぐチェック)]** を選択して、パロアルトネットワークスアップデートサーバーから最新のPAN-OSソフトウェアパッチを入手してください。

STEP 3 | **Include Patch (パッチを含める)** をチェック (有効化) すると、使用可能なすべての PAN-OS ソフトウェアパッチが表示されます。

STEP 4 | 現在お使いの次世代ファイアウォールにインストールされているPAN-OSリリースのソフトウェアパッチを探してください。

ソフトウェアパッチは、バージョン名の横にパッチラベルが表示されます。

STEP 5 | 「**More Info (詳細情報)**」を参照して、重大なバグや CVE の修正などのソフトウェアパッチの詳細、および修正を適用するために次世代ファイアウォールの再起動が必要かどうかを確認してください。

STEP 6 | ソフトウェアパッチをダウンロードします。

（HA のみ）PAN-OS ソフトウェアパッチをダウンロードするには、[HA ピアに同期] をチェック（有効化）して **[Continue Download (ダウンロードを続行)]** を選択します。

ソフトウェアパッチが正常にダウンロードされたら、**[Close (閉じる)]** をクリックします。

STEP 7 | ソフトウェアパッチをインストールする

ソフトウェアパッチが正常にインストールされたら、**[Close (閉じる)]** をクリックします。

STEP 8 | ソフトウェアパッチを適用します。

インストールされている PAN-OS ソフトウェアパッチを次世代ファイアウォールに適用するかどうかを確認するメッセージが表示されたら、**[Apply (適用)]** をクリックします。

ステータスバーに、PAN-OS ソフトウェアパッチアプリケーションの現在の進行状況が表示されます。パッチが正常に適用されたら、**[Close (閉じる)]** をクリックします。

この時点で、次世代ファイアウォールへのPAN-OSソフトウェアパッチの適用を完了するために再起動が必要な場合、ファイアウォールは自動的に再起動します。

STEP 9 | （HA のみ）ファイアウォール HA ピアに PAN-OS ソフトウェアパッチをインストールします。

1. HA ピアの 1 つのファイアウォールWeb インターフェイスにログインします。
2. **[Device (デバイス)]** > **[Software (ソフトウェア)][Check Now (今すぐ確認)]** を選択します。
3. ソフトウェアパッチをインストールする
4. 必要に応じてファイアウォールを再起動します。

元に戻す

STEP 1 | ファイアウォール Web インターフェイス にログインします。

STEP 2 | **[Device (デバイス)]** > **[Software (ソフトウェア)]**を選択し、元に戻すPAN-OSソフトウェアパッチを探します。

STEP 3 | ソフトウェアパッチを元に戻します。

次世代ファイアウォールにインストールされているPAN-OSソフトウェアパッチを元に戻すかどうかを確認するメッセージが表示されたら、**[Revert (元に戻す)]**をクリックします。

PAN-OSソフトウェアパッチ適用の現在の進捗状況を示すステータスバーが表示されます。パッチが正常に適用されたら、**[Close (閉じる)]** をクリックします。

この時点で、次世代ファイアウォールへのPAN-OSソフトウェアパッチの適用を完了するために再起動が必要な場合、ファイアウォールは自動的に再起動します。

PAN-OS のダウングレード

firewall を PAN-OS 11.1 からダウングレードする方法は、以前の機能リリース(PAN-OS バージョンの 1 桁目または 2 桁目が 9.1.2 から 9.0.8 または 9.0.3 から 8.1.14 に変更されるなど)にダウングレードするか、同じ機能リリース内のメンテナンス リリース バージョンにダウングレードするか(リリース バージョンの 3 桁目が変更されたか、 たとえば、8.1.2 から 8.1.0 まで)。ある機能リリースから以前の機能リリースにダウングレードする場合、新しい機能に対応するために、後のリリースから構成を移行できます。PAN-OS 11.1 設定を以前の PAN-OS リリースに移行するには、まずダウングレード先の機能リリースの設定を復元します。同じフィーチャー・リリース内で保守リリースを別のリリースにダウングレードする場合は、構成を復元する必要はありません。

- ファイアウォールを以前のメンテナンス リリースにダウングレードする
- ファイアウォールを以前の機能リリースにダウングレードする
- Windows エージェントのダウングレード

ソフトウェアバージョンに一致する構成に常にダウングレードします。ソフトウェアのバージョンと構成が一致しない場合、ダウングレードが失敗したり、システムがメンテナンス モードに移行したりする可能性があります。これは、ある機能リリースから別の機能リリース *(9.0.0* から *8.1.3* など*)* へのダウングレードにのみ適用され、同じ機能リリースバージョン内のメンテナンス リリースにダウングレードされません *(8.1.3 ~ 8.1.1* など*)*。

ダウングレードに問題がある場合は、メンテナンス モードに入り、デバイスを工場出荷時のデフォルトにリセットしてから、アップグレード前にエクスポートされた元の設定ファイルから設定を復元する必要があります

ファイアウォールを以前のメンテナンス リリースにダウングレードする

メンテナンス リリースでは新機能が導入されないため、以前の構成を復元することなく、同じ機能リリースで以前のメンテナンス リリースにダウングレードできます。メンテナンス リリースとは、リリース バージョンの 3 桁目が変更されるリリースです (たとえば、 10.1.6 から 10.1.4 へのダウングレードは、リリース バージョンの 3 桁目のみが異なるため、メンテナンス リリースのダウングレードと見なされます)。

同じフィーチャー・リリース内の以前の保守リリースにダウングレードするには、以下の手順を使用します。

STEP 1 | 現在の構成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構成のバックアップを自動的に作成しますが、ダウングレードして外部に保存する前にバックアップを作成することをお勧めします。

1. **Device (デバイス) > Setup (セットアップ) > Operations (操作) Export named configuration snapshot (名前付き 設定スナップショットのエクスポート)** を選択します。
2. 実行中の設定を含む XML ファイル（**running-config.xml** など）を選択し、**OK** をクリックして設定ファイルをエクスポートします。
3. 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。ダウン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 | 以前のメンテナンス リリース イメージをインストールします。

ファイアウォールが管理ポートからインターネットにアクセスできない場合は、ソフトウェア更新プログラムを Palo Alto Networks サポート ポータル からダウンロードできます。その後、手動で アップロード ファイアウォールにアップロードできます。

1. 利用可能な画像については、今すぐチェック（ **[Device (デバイス)] > [Software (ソフトウェア)]**）。

   （PAN-OS 11.1.3以降）デフォルトでは、優先リリースと対応する基本リリースが表示されます。優先リリースのみを表示するには、**[Base Releases (基本リリース)]**チェックボックスをオフ(選択解除)にします。
2. ダウングレードするバージョンを見つけます。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、イメージを **Install**（インストール）します。
4. 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。
   - 再起動を求めるメッセージが表示されない場合は、デバイス操作 (デバイス > セットアップ > オペレーション) および 再起動デバイス に移動します。

ファイアウォールを以前の機能リリースにダウングレードする

次のワークフローを使用して、別の機能リリースにアップグレードする前に実行されていた構成を復元します。アップグレード以降に加えられた変更はすべて失われます。したがって、新しい機能リリースに戻ったときに変更を復元できるように、現在の構成をバックアップすることが重要です。firewall を以前の機能リリースにダウングレードする前に、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

PAN-OS 11.1 から以前の *PAN-OS* リリースにダウングレードするには、ターゲットの *PAN-OS* リリースへのダウングレード パスを続行する前に、*PAN-OS 10.1* 以降の *PAN-OS 10.1.3* リリースをダウンロードしてインストールする必要があります。*PAN-OS 10.1.2* 以前の *PAN-OS 11.1* リリースにダウングレードしようとすると、*PAN-OS 11.1* からのダウングレードは失敗します。

次の手順に従って、以前の機能リリースにダウングレードします。

STEP 1 | 現在の構成ファイルのバックアップを保存します。

設定のバックアップはファイアウォールで自動的に作成されますが、アップグレードの前にバックアップを作成して、そのバックアップを外部に保存することをお勧めします。

1. **Device (デバイス) > Setup (セットアップ) > Operations (操作) Export named configuration snapshot (名前付き 設定スナップショットのエクスポート)** を選択します。
2. 実行中の設定を含む XML ファイル（**running-config.xml** など）を選択し、**OK** をクリックして設定ファイルをエクスポートします。
3. 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。ダウン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 | 以前の機能リリースイメージをインストールします。

自動保存バージョンは、新しいリリースにアップグレードすると作成されます。

1. 利用可能なイメージについては、**Check Now (今すぐチェック)**（デバイス > ソフトウェア）を確認してください。
2. PAN-OS 10.1 をインストールします。

   PAN-OS 11.1 から以前の機能リリースにダウングレードするには、最初に PAN-OS 10.1.3 以降の PAN-OS 11.1 リリースにダウングレードする必要があります。PAN-OS 10.1.3 以降の PAN-OS 10.1 リリースに正常にダウングレードした後、ターゲットの PAN-OS バージョンへのダウングレードを続行できます

   1. PAN-OS 11.1 イメージを見つけて ダウンロード します。
   2. **Install (インストール)** PAN-OS 11.1 イメージ。
3. ダウングレードするターゲット PAN-OS イメージを見つけます。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。
4. ダウンロードが完了したら、イメージを **Install**（インストール）します。
5. ダウングレード用の構成ファイルを選択します。これは、デバイスを再起動した後にファイアウォールによってロードされます。ほとんどの場合、現在ダウングレードしているリリースからアップグレードしたときに自動的に保存された構成を選択する必要が

あります。たとえば、PAN-OS 11.0 を実行していて、PAN-OS 10.2.2 にダウングレードする場合は、`autosave-10.2.2` を選択します。

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。

Windows エージェントのダウングレード

PAN-OS 11.1 Windows ベースの User-ID エージェントをアンインストールした後、以前のエージェント リリースをインストールする前に次の手順を実行します。

STEP 1 | Windows の [スタート] メニューを開き、[管理ツール] を選択します。

STEP 2 | コンピュータの管理 > サービスとアプリケーション > サービス を選択し、 ユーザー **ID** エージェント をダブルクリックします。

STEP 3 | [ログオン] を選択し、[このアカウント] を選択して、User-ID エージェント アカウントのユーザー名を指定します。

STEP 4 | [パスワード] と [パスワードの確認] を入力します。

STEP 5 | **OK** をクリックして変更内容を保存します。

PAN-OS アップグレードのトラブルシューティング

PAN-OS のアップグレードのトラブルシューティングを行うには、次の表を参照して、考えられる問題とその解決方法を確認してください。

症状	解決策
ソフトウェア保証ライセンスの期限が切れています。	CLI から、期限切れのライセンス キーを削除します。 1. ライセンス キーの削除 **<software license key>** を入力します。 2. ライセンス キーの削除 **Software_Warranty<expiredate>.key** を入力します。
最新の PAN-OS ソフトウェア バージョンは使用できませんでした。	現在インストールされているバージョンより 1 つ先の機能リリースのソフトウェア バージョンのみが表示されます。たとえば、9.1 リリースがインストールされている場合、10.0 リリースのみが使用できます。11.1 リリースを表示するには、最初に 10.1 にアップグレードする必要があります。
動的更新の確認に失敗しました。	この問題は、ネットワーク接続エラーが原因で発生します。「今すぐチェック]ボタンをクリックすると、サポート技術情報の記事dynamic更新の表示エラーが表示されるを参照してください。
有効なデバイス証明書が見つかりませんでした。	PAN-OS 9.1.3 以降のバージョンでは、Palo Alto Networks クラウド サービスを利用している場合は、デバイス証明書をインストールする必要があります。デバイス証明書をインストールするには: 1. カスタマー サポート ポータルにログインします。 2. 生成 **OTP** (資産 > デバイス証明書) を選択します。 3. デバイスの種類で、[次世代ファイアウォール用の**OTP**を生成を選択します。 4. PAN-OS デバイスのシリアル番号を選択します。

症状	解決策
	5. **OTP** を生成し、ワンタイム パスワードをコピーします。 6. 管理者ユーザーとしてファイアウォールにログインします。 7. デバイス証明書 (デバイス > 設定< > 管理 > デバイス > 証明書 と 証明書を取得 を選択します。 8. OTP を貼り付け、[**OK** をクリックします。
イメージ認証エラーのため、ソフトウェア イメージ ファイルをソフトウェア マネージャに読み込めませんでした。	ソフトウェア イメージの一覧を更新するには、[チェック をクリックします。これにより、更新サーバーへの新しい接続が確立されます。
VMware NSX プラグインのバージョンは、新しいソフトウェア バージョンと互換性がありません。	VMware NSX プラグインは、8.0 にアップグレードすると自動的にインストールされました。プラグインを使用していない場合は、アンインストールできます。
PAN-OS 9.1にアップグレードした後の再起動時間が予想よりも長かった。	アプリケーションと脅威コンテンツリリースバージョン 8221 以降にアップグレードします。ソフトウェアとコンテンツの最小バージョンの詳細については、「<xref to 11.1 Associated Software and Content Versions>」を参照してください。
ライセンスがアクティブな場合でも、デバイスはサポートされていません。	デバイス > ソフトウェア で、今すぐ確認 をクリックします。 これにより、更新サーバーへの新しい接続を確立することにより、ファイアウォールのライセンス情報が更新されます。 Web インターフェイスからこの方法が機能しない場合は、要求システム ソフトウェア チェック を使用してください。
ファイアウォールに DHCP サーバーによって割り当てられた DHCP アドレスが設定されていません。	ISP DHCP サーバーから内部ネットワークへのトラフィックを許可するセキュリティ ポリシールールを設定します。
firewall は継続的にメンテナンスモードで起動します。	CLI では、Access the Maintenance Recovery Tool (MRT).MRT ウィンドウで、**Continue** > **Disk Image** を選択します。再インストール

症状	解決策
	<current version> または **<previous version>** に戻す] を選択します。元に戻す操作または再インストール操作が完了したら、再起動 を選択します。
HA 設定では、ピア firewall をアップグレードした後、firewall が古すぎるというエラーで firewall が一時停止状態になります。	1 つの firewall を複数のメジャーリリース前のバージョンにアップグレードすると、ネットワークが停止します。次のメジャーリリースにアップグレードする前に、両方の firewall を 1 つだけ先にアップグレードする必要があります。 ピア firewall を、中断された firewall が停止したバージョンにダウングレードします。

VM-Series ファイアウォールのアップグレード

VM-Series PAN-OS ソフトウェア(スタンドアロン)をアップグレードする

VM-Series PAN-OS ソフトウェア(HA ペア)をアップグレードする

Panoramaを使用してVM-Series PAN-OSソフトウェアをアップグレードする

PAN-OS ソフトウェア バージョンのアップグレード（VM-Series for NSX）

デプロイ環境に最も適したアップグレード方法を選択します。

- メンテナンスウィンドウ中に NSX 用の VM-Series をアップグレードする - このオプションを使用して、サービス定義中のOVF URL を変更せずに、メンテナンスウィンドウ中に VM-Series ファイアウォールをアップグレードします。
- トラフィックを中断せずに VM-Series for NSX をアップグレードする - このオプションを使用して、ゲスト VM へのサービスを中断したり、サービス定義の OVF URL を変更したりせずに、VM-Series ファイアウォールをアップグレードします。

次の画像は、現在サポートされているPanoramaとPanorama plugin for VMware NSXの組み合わせ、および正常にアップグレードを行うために必要なアップグレードパスを表しています。

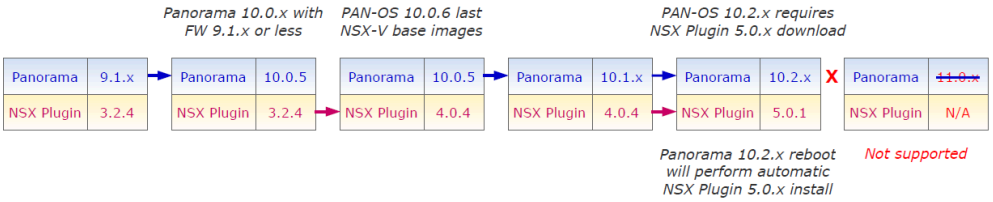
- 下の各ボックスが、サポートされている組み合わせを表しています。
- HAペア内のPanorama plugin for NSXまたはPanoramaをアップグレードする場合、まずパッシブPanoramaピアをアップグレードしてから、次にアクティブHAピアをアップグレードしてください。

VM-Series for VMware NSXデプロイメントをアップグレードする前に、以下の図に示されているアップグレードパスを参照して、ご利用の環境に適したプラグインとPAN-OSの組み合わせに至るまでのアップグレード手順を理解してください。

Panorama and PAN NSX Plugin Upgrade Paths

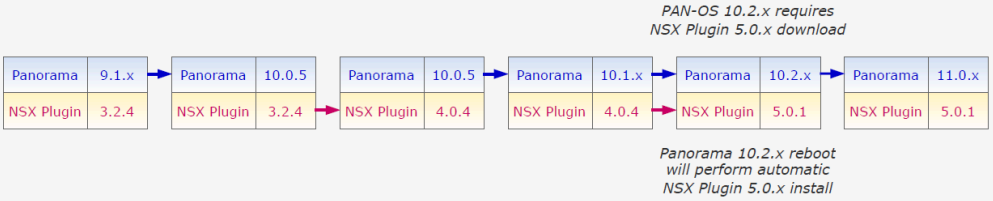
- For Panorama upgrades, first upgrade Panorama HA Passive, then Panorama HA Active
- For NSX Plugin upgrades, first upgrade Panorama HA Passive, then Panorama HA Active
- Best practice is always upgrade one at a time (either Panorama or NSX Plugin)

VM-Series for NSX-V



IMPORTANT! PAN-OS 10.0.6 are the last available base images for VM-Series for NSX-V.

VM-Series for NSX (formerly NSX-T)



IMPORTANT! VMware NSX-T has been renamed to VMware NSX as of version 4.0.x.

保守期間中に NSX 用 VM-Series をアップグレード

トラフィックを中断せずに NSX 用 VM-Series をアップグレード

VM-Series モデルのアップグレード

VM-Series ファイアウォールのライセンス プロセスでは、UUID と CPU ID を使用して VM-Series ファイアウォールの一意のシリアル番号を生成します。そのため、ライセンスを生成するときに、ライセンスは VM-Series ファイアウォールの特定のインスタンスにマッピングされ、変更することはできません。

以下の場合、このセクションの手順を実行します。

- 評価版ライセンスから製品ライセンスに移行する。
- キャパシティの大きいモデルにアップグレードする。VM-100 から VM-300 モデルへのアップグレードなど。

- キャパシティをアップグレードする。これで、ファイアウォール上の重要なプロセスを再起動します。サービスの中断を最小限に抑えるには、*HA* 設定をお勧めします。*HA* ペアでキャパシティをアップグレードするには、「HA ペアでの VM-Series モデルのアップグレード」を参照してください。
- プライベートクラウドまたはパブリッククラウドのデプロイメントでは、*BYOL* オプションを使用してファイアウォールのライセンスを付与されている場合、インスタンスタイプまたは *VM* タイプを変更する前に VM を非アクティブ化する必要があります。モデルまたはインスタンスをアップグレードすると *UUID* と *CPU ID* が変更されるため、 そのときにライセンスを適用する必要があります。

STEP 1 | 追加のハードウェア リソースを VM-Series ファイアウォールに割り当てます。

キャパシティのアップグレードを開始する前に、新しいキャパシティをサポートできるだけの十分なハードウェア リソースを VM-Series ファイアウォールで使用できることを確認してください。追加のハードウェア リソースを割り当てる手順は、ハイパーバイザごとに異なります。

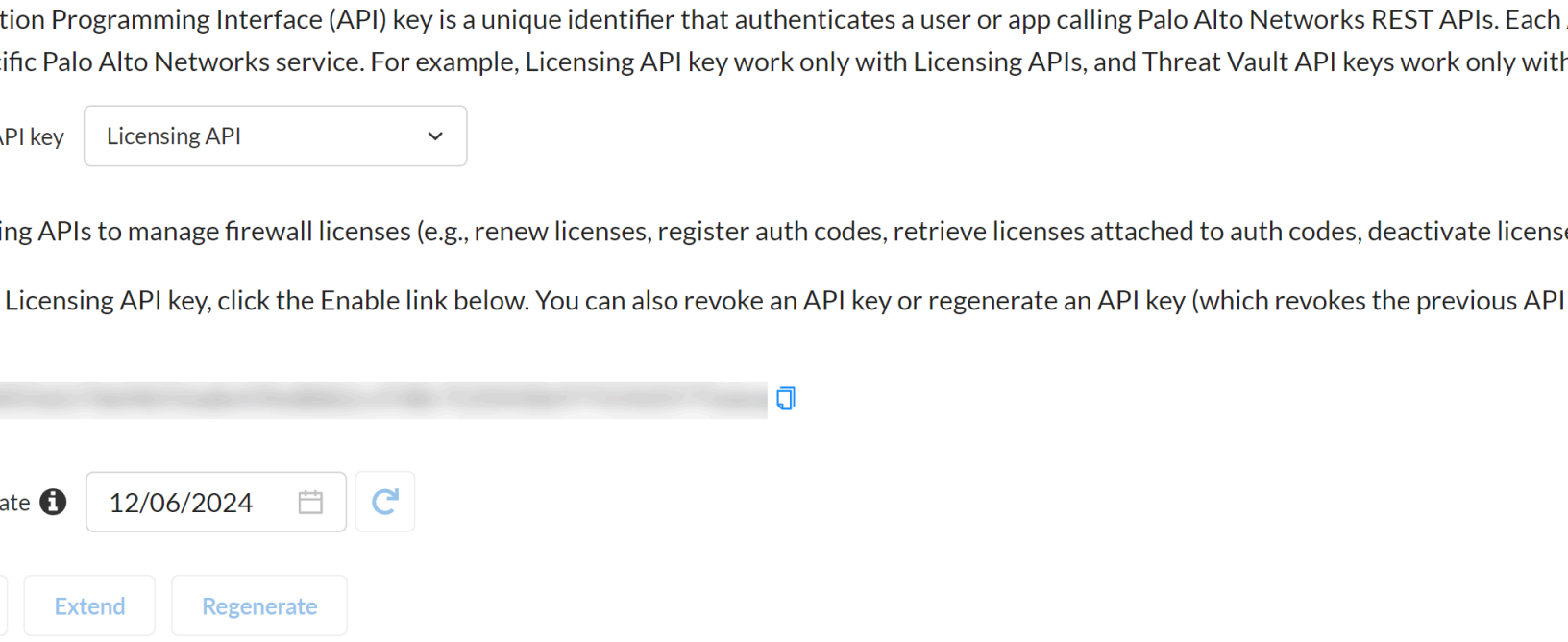
新しい VM-Series モデルのハードウェア要件を確認するには、「VM-Series モデル」を参照してください。

キャパシティのアップグレードでは VM-Series ファイアウォールを再起動する必要はありませんが、ハードウェアの割り当てを変更するために仮想マシンをパワーオフする必要があります。

STEP 2 | ライセンスの API キーをカスタマーサポートポータルから取得します。

1. カスタマー サポート ポータルにログインします。

   必ず、最初のライセンスを登録するために使用したのと同じアカウントを使用してください。
2. 左側のメニューから、アセット > **API** キー管理 を選択します。
3. API キーをコピーします。



STEP 3 | ファイアウォールで CLI を使用し、前の手順でコピーした API キーをインストールします。

```
request license api-key set key <key>
```

STEP 4 | (インターネットにアクセスできる場合) ファイアウォールを有効にして、 デバイス > セットアップ > サービスで 更新サーバー の **ID** の確認を行います。

STEP 5 | 変更を **Commit** (コミット) します。ファイアウォール上に、ローカルに設定したユーザーが存在していることを確認してください。設定がライセンスのない PA-VM オブジェクトの制限を超えている場合、非アクティブ化した後に、Panorama がプッシュしたユーザーは利用できなくなる可能性があります。

STEP 6 | キャパシティをアップグレードします。

Device（デバイス） > **Licenses**（ライセンス） > **Upgrade VM Capacity**（**VM** キャパシティのアップグレード）を選択し、次のいずれかの方法でライセンスおよびサブスクリプションをアクティベートします。

- (インターネット) ライセンスサーバーからライセンス キーを取得 - カスタマー サポートポータルでライセンスをアクティベートした場合は、このオプションを使用します。
- (インターネット) 認証コードを使用 - サポート ポータルで以前にアクティベートされていないライセンスの認証コードを使用して VM-Series キャパシティをアップグレードする場合は、このオプションを使用します。**Authorization Code**（認証コード）の入力を促されたら、認証コードを入力して **OK** をクリックします。
- (インターネットなし) ライセンスキーの手動アップロード - ファイアウォールとカスタマーサポートポータルとのネットワーク接続が確立されていない場合は、このオプションを使用します。インターネットにアクセスできるコンピュータから CSP にログインし、ライセンスキー ファイルをダウンロードし、ファイアウォールと同じネットワーク内のコンピュータに転送して、ファイアウォールにアップロードします。

STEP 7 | ファイアウォールが正常にライセンス登録されていることを確認します。

Device（デバイス） > **Licenses**（ライセンス）ページで、ライセンスが正常にアクティベートされたことを確認します。

HA ペアの VM-Series モデルのアップグレード

VM-Series ファイアウォールの以前のリリースへのダウングレード

Panorama プラグインのアップグレード

Panorama プラグインのアップグレード/ダウングレードに関する考慮事項

次の表に、アップグレードまたはダウングレードに影響する新機能を示します。PAN-OS 11.1 リリースにアップグレードまたはダウングレードする前に、秋のアップグレード/ダウングレードに関する考慮事項を理解していることを確認してください。PAN-OS 11.1 リリースの詳細については、PAN-OS 11.1 リリース ノート を参照してください。

表 **1 : Panorama** プラグインのアップグレード**/**ダウングレードに関する考慮事項

機能	アップグレードに関する考慮事項	ダウングレードに関する考慮事項
Panorama プラグイン • AWS プラグイン • Azure プラグイン • Kubernetes プラグイン • ソフトウェアFirewallライセンスプラグイン • SD-WAN プラグイン • IPS署名コンバータプラグイン • ZTP プラグイン • エンタープライズ DLP プラグイン • Openconfig プラグイン • GCP プラグイン • Cisco ACI プラグイン • Nutanix プラグイン • vCenter プラグイン	PAN-OS 11.1 にアップグレードする前に、Panorama にインストールされているすべてのプラグインについて、PAN-OS 11.1 でサポートされている Panoramaプラグインバージョンをダウンロードする必要があります。これは、PAN-OS 11.1 に正常にアップグレードするために必要です。詳細については、互換性マトリックスを参照してください。	PAN-OS 11.0 からダウングレードするには、Panorama にインストールされているすべてのプラグインについて、PAN-OS 10.2 以前のリリースでサポートされている Panoramaプラグインバージョンをダウンロードする必要があります。詳細については、Panorama プラグイン互換性マトリックス を参照してください。
	(Enterprise DLP) パノラマを PAN-OS 10.2 にアップグレードした後、PAN-OS 11.1 以前のリリースを実行しているすべての管理対象 firewall に、アプリケーションと脅威のコンテンツ リリース バージョン 8520 をインストールする必要があります。これは、PAN-OS 10.2 にアップグレードしていないエンタープライズ DLP を活用して、管理対象の firewall に設定変更を正常にプッシュするために必要です。	
	(Enterprise DLP) 共有エンタープライズ DLP 構成を含む Panorama 構成バックアップの読み込み は、ファイルベース以	

機能	アップグレードに関する考慮事項	ダウングレードに関する考慮事項
	外のトラフィックをスキャンするために必要な共有アプリ除外フィルターを削除します。	
	(SD-WAN)SD-WAN 2.2 以前のリリース用の Panorama プラグインは、PAN-OS 11.0 ではサポートされていません。 SD-WAN 2.2 以前のリリースの Panorama プラグインがインストールされている場合に Panorama 管理サーバを PAN-OS 11.1 にアップグレードすると、SD-WAN プラグインが Panorama Web インターフェイスで非表示になるか、SD-WAN 設定が削除されます。どちらの場合も、新しい SD-WAN プラグインバージョンをインストールしたり、SD-WAN プラグインをアンインストールしたりすることはできません。	
SD-WAN	Panorama を PAN-OS 11.1 に、および Panorama プラグインを SD-WAN バージョン 2.0.0 から SD-WAN バージョン 3.0 に正常にアップグレードしたら、既存の SD-WAN 展開に対してのみ、Panorama の SD-WAN キャッシュをクリアする必要があります。 SD-WAN キャッシュをクリアしても、既存の SD-WAN 設定は削除されませんが、SD-WAN バージョン 3.0 の Panorama プラグインで導入された新しい形式の IP アドレス、トンネル、およびゲートウェイの命名規則が削除されます。 SD-WAN の新規展開では、PAN-OS 11.0 にアップグレードした後に SD-WAN バー	なし。

機能	アップグレードに関する考慮事項	ダウングレードに関する考慮事項
	ジョン 3.0 用の Panorama プラグインを Panorama にインストールする場合、Panorama の SD-WAN キャッシュをクリアする必要はありません。 1. Panorama CLI へのログインを行います。 2. Panorama の SD-WAN キャッシュをクリアします。 `admin> プラグイン`**`sd_wan drop-config-cache all`**	

Panoramaプラグインをアップグレードする

Panorama管理サーバーにインストールされているほとんどのプラグインのバージョンをアップグレードするには、次の手順に従います。以下のいずれかのプラグインをアップグレードする場合は、表示されるリンクの手順を使用してください。最新のVMシリーズプラグインにアップグレードするには、

- エンタープライズ DLP プラグインのアップグレード
- Panorama Interconnect プラグインのアップグレード
- Panorama plugin for VMware NSXをアップグレードする場合は、[VM-Series for VMware NSX documentation (VMware用VM-SeriesNSXのマニュアル)] を参照してください。

STEP 1 | 各 Panorama プラグインでサポートされる最小の PAN-OS バージョンについては、Compatibility Matrixを参照してください。

STEP 2 | Panorama Plugin Release Notes (Panoramaプラグインリリースノート)を参照して、対象となるプラグインのバージョンを特定します。

STEP 3 | Panorama プラグインのアップグレード/ダウングレードに関する考慮事項をレビューします。

STEP 4 | 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。

STEP 5 | プラグインをインストールします。

前の手順でダウンロードしたプラグインのバージョンを選択し、[Action (アクション)]列の**[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。

Panorama HA ペアにプラグインを初めてインストールする場合は、アクティブピアの前にパッシブピアにプラグインをインストールしてください。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 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。

STEP 6 | (任意)次のCLIコマンドを使用して、プラグインのアップグレードログを確認できます。

```
tail plugins-log...tail mp-log plugin_install.log
```

エンタープライズ DLP プラグインのアップグレード

Panorama™ 管理サーバーにインストールされているエンタープライズデータ損失防止 (DLP) プラグインのバージョンをアップグレードします。

Palo Alto Networks パノラマ プラグイン互換性マトリックス を参照し、ターゲットのエンタープライズ DLP プラグイン バージョンに必要な最小 PAN-OS バージョンを確認してください。

STEP 1 | Panorama Web インターフェースにログインします。

STEP 2 | Panorama のエンタープライズ DLP プラグインのバージョンをアップグレードします。

Panorama が高可用性 (HA) 設定の場合、Panorama HA ピアでこのステップを繰り返します。

1. 選ぶ **Panorama** > **Plugins** and **Check Now** for the latest **`dlp`** plugin verison.
2. **Download** および **Install** は、Enterprise DLP プラグインの最新バージョンです。
3. 新しいプラグインバージョンが正常にインストールされたら、Panorama **Dashboard** を表示し、一般情報ウィジェットで、`Plugin DLP` バージョンにアップグレードしたエンタープライズ DLP プラグインのバージョンが表示されていることを確認します。

STEP 3 | (4.0.0 のみにアップグレード) エンタープライズ DLP データ フィルタリング設定を編集 を使用して、**Max** ファイル サイズ を 20 MB 以下に縮小します。

これは、エンタープライズ DLP 3.0.3 以降のリリース用の Panorama プラグインからエンタープライズ DLP 4.0.0 にアップグレードする場合、このプラグインバージョンは ラージ ファイル サイズ検査 をサポートしていないために必要です。

Panorama Interconnect プラグインのアップグレード

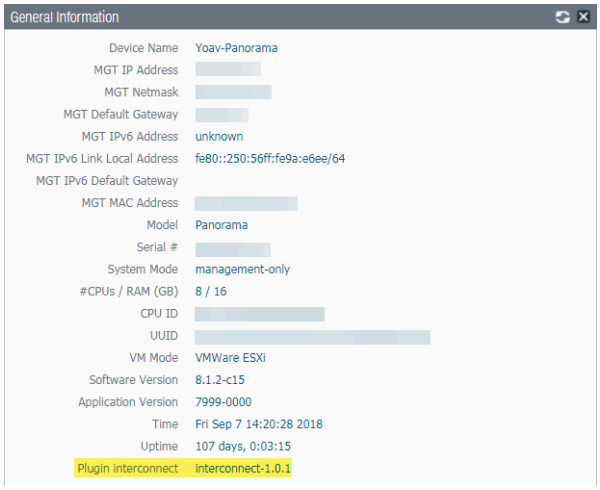
次の各作業を行い、Panorama Controller および Panorama ノード上の Panorama™ Interconnect プラグインをアップグレードします。Panorama Interconnect プラグインをアップグレードする際、Panorama ノードを Controllerと同じプラグイン バージョンにアップグレードする前に、Panorama Controller をアップグレードする必要があります。Panorama Controller および選択した Panorama ノードのプラグインのバージョンを必ず同じに保つために、ダウンロードして Panorama ノー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。

プラグインを初めてインストールする場合は、Panorama 相互接続プラグイン のセットアップを参照してください。

STEP 1 | Panorama コントローラの Panorama Web インターフェイス にログインします。

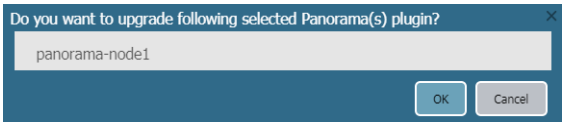
STEP 2 | Panorama Controller 上の Panorama Interconnect プラグインをアップグレードします。

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。

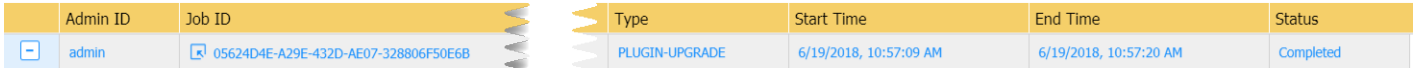


STEP 3 | Panorama ノード上の Panorama Interconnect プラグインをアップグレードします。

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。

互換性のある PAN-OS リリースによる SD-WAN プラグインのインストール/アップグレード

どこで使用できますか?	何が必要ですか?
• PAN-OS • SD-WAN	❑ SD-WAN plugin license

既存のネットワークインフラストラクチャを最新の状態に保ち、機能をアップグレードして新しい機能を引き出すことができるようにすることが不可欠です。SD-WANアップグレードガイドは、ネットワーク管理者がSD-WANプラグインリリースと互換性のあるPanorama管理サーバーとPalo Alto Networksファイアウォールをアップグレードするのに役立ちます。

実際のアップグレードまたはダウングレード手順を開始する前に、適切なアップグレードまたはダウングレード計画を立てることが重要です。現在インストールされている SD-WAN プラグインバージョンの有効なアップグレードおよびダウングレードパスを参照してください。

アップグレードプロセスを進める前に、次の点を確認してください。

- 各デバイスのすべての構成のバックアップを取ります。
- SD-WAN 用 Panorama プラグインの各バージョンで導入された機能を確認するには、Panoramaプラグイン互換性マトリックスを参照してください。
- Palo Alto Networksのデバイスへの管理者アクセス権があります。

前提条件

Panorama HA ペアをアップグレードする前に、設定ファイルを保存し、テクニカルサポートファイルを作成し、お使いのデバイスと互換性のあるコンテンツリリースバージョンを確認することが重要です。

設定ファイルをバックアップする

現在の設定ファイルのバックアップを作成します。現在のPanoramaとファイアウォールの設定をバックアップすることをお勧めします。

- デバイスをアップグレードする前に、Panoramaとファイアウォールの設定をバックアップしてください。
- 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、そのバックアップを復元します。
- ファイアウォールの設定を保存してエクスポートし、そのバックアップに戻します。

アップグレードに問題がある場合は、Panorama管理サーバーで管理されているファイアウォールに設定バックアップを読み込むことで、これらのバックアップを使用して構成を復元できます。

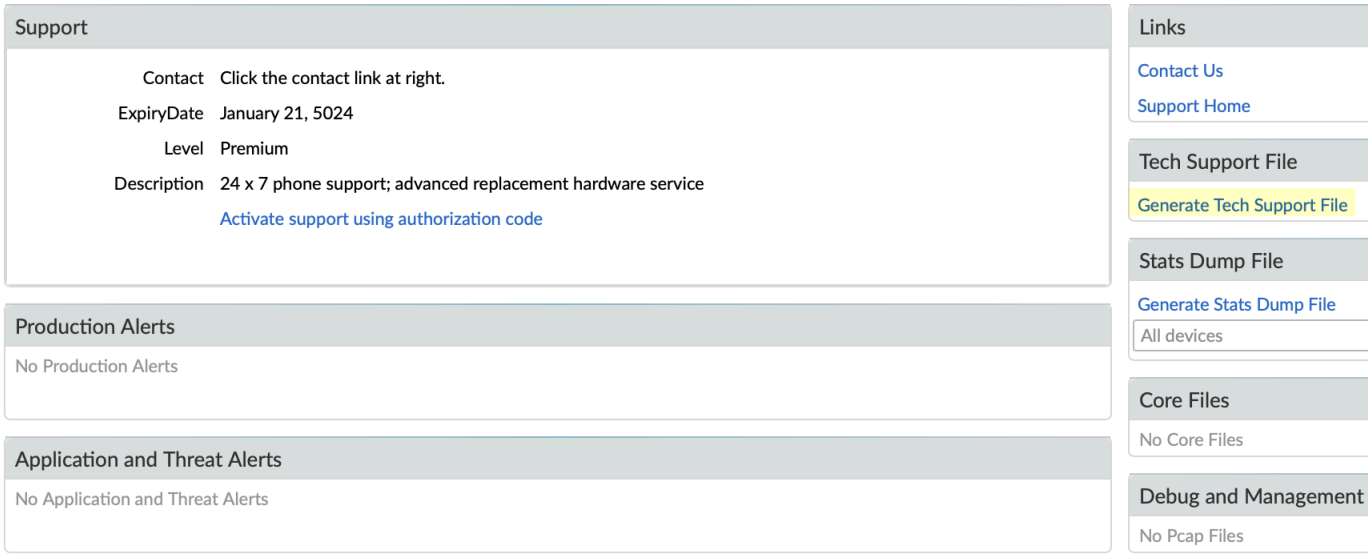
テクニカルサポートファイルの生成

デバッグ用にテクニカルサポートファイルを生成することが重要です。

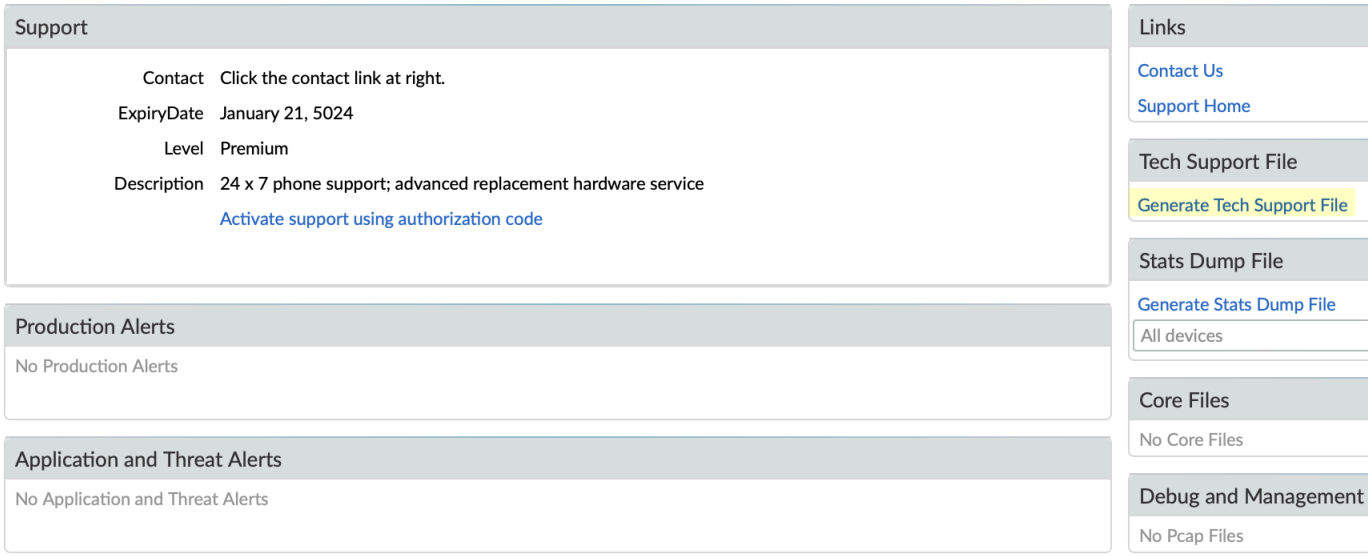
1. **[Device (デバイス)]** > **[Support (サポート)]** および **[Generate Tech Support File (テクニカル サポート ファイルの生成)]**を順に選択します。

   デバッグのためには、テクニカルサポートファイルを両方の HA ペアで生成する必要があります。

   テクニカルサポートファイルの生成には数分かかる場合があり、生成にかかる時間は異なります。



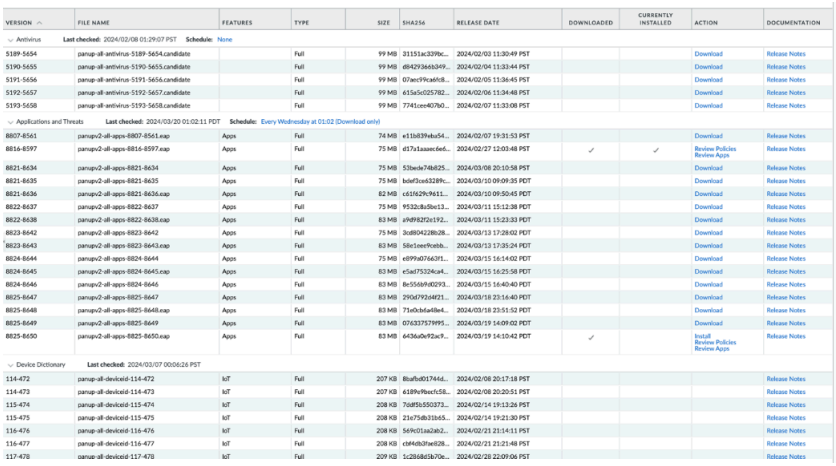
2. テクニカル サポート ファイルを生成するように求められたら、**Yes** をクリックします。
3. **[Download Tech Support File (テクニカルサポートファイルをダウンロード)]**をクリックして、ファイアウォールまたはPanoramaに保存します。



互換性のあるコンテンツリリース版をインストール

各ファイアウォールと Panorama HA ペアが最新のコンテンツリリース (**Applications and Threats (**アプリケーションと脅威**)**) バージョンを実行していることを確認します。

アップグレードを正常に実行するには、すべてのファイアウォールと***Panorama***に同じバージョンのアプリケーションと脅威をダウンロードしてインストールする必要があります。



対応する PAN-OS リリースにインストールする必要がある最小コンテンツリリース (アプリケーションや脅威など) バージョンについては、対応するリリースノートを参照してください。アプリケーションと脅威コンテンツの更新に関するベストプラクティスに必ず従ってください。

特定のPAN-OSバージョンを実行しているファイアウォールとPanoramaには、PAN-OSバージョンと互換性のある最低限のコンテンツリリース（**Applications and Threats (**アプリケーションと脅威**)**）バージョンが含まれている必要があります。

次のワークフローを使用して、PAN-OS バージョンと互換性のあるコンテンツリリースバージョンをダウンロードしてインストールします。

1. ファイアウォールの場合は **[Device (**デバイス**)]** > **[**ダイナミック更新**]**を順に選択し、Panoramaでは **[Panorama]** > **[**ダイナミック更新**]**を順に選択して、**Applications and Threats (**アプリケーションと脅威**)**のバージョン情報を確認します。
2. **Check Now**（今すぐチェック）を行い、利用可能な更新のリストを取得します。
3. 適切なコンテンツリリースバージョンを探してダウンロードしてください。コンテンツ アップデート ファイルを正常にダウンロードしたら、そのコンテンツ リリース バージョンの 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）に変化します。
4. Palo Alto Networksのデバイスにアップデートをインストールします。

Panoramaのアップグレードに関する重要な考慮事項

Panorama 管理サーバーの SD-WAN プラグインバージョンをアップグレードする際の重要な考慮事項は次のとおりです。

- (HA デプロイメントのみ) アクティブPanoramaとパッシブPanoramaの両方に、同じPanoramaソフトウェアと SD-WAN プラグインのバージョンが必要です。
- (HA 導入のみ) アップグレード後、およびすべてをコミットまたはコミットする前に、Panorama と Palo Alto Networks の次世代ファイアウォールで同じ HA 状態を維持して、構成の変更を最小限に抑えます。
- Panorama ソフトウェアのバージョンが PAN-OS バージョンよりも高いことを常に確認してください。
- SD-WAN プラグインバージョンの MongoDB 同期ステータスについては、を参照してください。SD-WANデータベースコレクションによるMongoDBの同期状況

- *(HA 展開のみ) アクティブとパッシブ Panorama HA* ペアの両方を同時にアップグレードする必要があります。
- *SD-WAN*プラグインのアップグレードが完了したら、*Palo Alto Networks*デバイスで（構成モードで）*CLI*コマンドを使用してコミットフォースを実行する必要があります。*commit force* の代わりにすべてコミットを実行すると、そのデバイスのすべての *SD-WAN* 設定が失われます。

アップグレードが完了したら、アップグレード後の変更点に注意してください。

SD-WANプラグインのアップグレードとダウングレードのパス

どこで使用できますか?	何が必要ですか?
• PAN-OS • SD-WAN	❑ SD-WAN plugin license

SD-WANプラグインをアップグレードまたはダウングレードする前に、ファイアウォールに現在インストールされているSD-WANプラグインのバージョンからアップグレードまたはダウングレードできる適切なプラグインのバージョンを知っておく必要があります。

アップグレードおよびダウングレードに関する考慮事項

- ***SD-WAN***プラグインをアップグレードする必要がある場合は、現在インストールされているバージョンよりも前にリリースされたリリースにアップグレードしないでください。

  例えば、*SD-WAN*プラグインバージョン*3.0.7*より前に*SD-WAN*プラグインバージョン*3.2.0*をリリースしているため、*SD-WAN*プラグインバージョン*3.0.7*から*3.2.0*へのアップグレードには対応しておりません。

  ただし、同じメジャーまたはマイナーリリースバージョン内で、任意のメンテナンスリリースから別のメンテナンスリリースにアップグレードすることはできます。たとえば、任意の*SD-WAN 2.2*から他の*SD-WAN 2.2*プラグインリリースにアップグレードできます。

- ***SD-WAN***プラグインをダウングレードする必要がある場合は、現在インストールされているバージョン以降にリリースされたリリースにダウングレードしないでください。

  例えば、*SD-WAN*プラグインバージョン*3.2.0*から*SD-WAN*プラグインバージョン*3.0.7*へのダウングレードは、*SD-WAN*プラグインバージョン*3.2.0*以降をリリースしているためサポートしておりません。

したがって、移行計画の最初のステップとして、現在インストールされている*SD-WAN*プラグインバージョンの有効なアップグレードパスとダウングレードパスを必ず参照してください。

SD-WANプラグインのアップグレードパス

アップグレード表の情報を次のように解釈します。

- アップグレード元–アップグレード前の現在のSD-WANプラグインのバージョン。
- **SD-WAN**プラグインバージョンへ–現在のSD-WANプラグインバージョンからアップグレードできるSD-WANプラグインバージョンの一覧です。
- **SD-WAN**プラグインバージョンへ（推奨） –現在のSD-WANプラグインバージョンからアップグレードすることを推奨するSD-WANプラグインバージョン。

たとえば、SD-WANプラグインバージョン2.2.1からSD-WANプラグインバージョン2.2.2、2.2.3、2.2.4、2.2.5、2.2.6、およびそれ以降の2.2リリースにアップグレードできます。ただし、すべての有効なSD-WANプラグインバージョン（2.2.2、2.2.3、2.2.4、2.2.5、2.2.6、およびそれ以降の2.2リリース）のうち、推奨バージョンは2.2.6です。なお、SD-WAN 2.2.1から3.0.7にアップグレードする場合は、直接アップグレードすることはできません。まずSD-WANプラグインを2.2.1から2.2.6（推奨バージョン）にアップグレードしてから、3.0.7にアップグレードする必要があります。

以下はSD-WANプラグイン版のアップグレードパスです。SD-WANアップグレードを実行すると、対象プラグインのバージョンが移行処理を実行します。

からのアップグレード（現在インストールされているバージョン）	許可されたSD-WANプラグインのバージョンへ	推奨SD-WANプラグインバージョンへ
SD-WANプラグイン2.2バージョン		
2.2.1	2.2.2、2.2.3、2.2.4、2.2.5、2.2.6、およびそれ以降の2.2リリース	2.2.6
2.2.2	2.2.3、2.2.4、2.2.5、2.2.6、およびそれ以降の2.2リリース	2.2.6
2.2.3	2.2.4、2.2.5、2.2.6、およびそれ以降の2.2リリース	2.2.6
2.2.4	2.2.5、2.2.6、およびそれ以降の2.2リリース	2.2.6
2.2.5	2.2.6以降の2.2リリース	2.2.6
2.2.6	• 3.0.7以降の3.0リリース • 3.1.3以降の3.1リリース • 3.2.1以降の3.2リリース • 3.3.0以降の3.3リリース	2.2.6
SD-WANプラグイン3.0バージョン		
3.0.0	3.0.5	—
3.0.1	3.0.5	—
3.0.2	3.0.5	—
3.0.3	3.0.5	—
3.0.4	3.0.5	—
3.0.5	• 3.0.6 • 3.0.7以降の3.0リリース • 3.1.0-hf • 3.1.1、3.1.3、およびそれ以降の3.1リリース • 3.2.0	3.0.7-h2、3.1.3、3.2.1、3.3.0

からのアップグレード（現在インストールされているバージョン）	許可されたSD-WANプラグインのバージョンへ	推奨SD-WANプラグインバージョンへ
	• 3.2.1、およびそれ以降の3.2リリース • 3.3.0以降の3.3リリース	
3.0.6	• 3.0.7以降の3.0リリース • 3.1.3、およびそれ以降の3.1リリース • 3.2.0 • 3.2.1以降の3.2リリース • 3.3.0以降の3.3リリース	3.0.7-h2、3.1.3、3.2.1、3.3.0
3.0.7	• 3.1.3、およびそれ以降の3.1リリース • 3.2.1以降の3.2リリース • 3.3.0以降の3.3リリース	3.1.3、3.2.1、3.3.0
SD-WANプラグイン3.1バージョン		
3.1.0	• 3.1.1 • 3.1.3以降の3.1リリース • 3.2.0 • 3.2.1以降の3.2リリース • 3.3.0以降の3.3リリース	3.1.3、3.2.1、3.3.0
3.1.1	• 3.1.3以降の3.1リリース • 3.2.0 • 3.2.1以降の3.2リリース • 3.3.0以降の3.3リリース	3.1.3、3.2.1、3.3.0
3.1.2	• 3.1.3以降の3.1リリース • 3.2.0 • 3.2.1以降の3.2リリース • 3.3.0以降の3.3リリース	3.1.3、3.2.1、3.3.0
3.1.3	• 3.2.1以降の3.2リリース • 3.3.0以降の3.3リリース	3.2.1 および 3.3.0

からのアップグレード（現在インストールされているバージョン）	許可されたSD-WANプラグインのバージョンへ	推奨SD-WANプラグインバージョンへ
SD-WANプラグイン**3.2**バージョン		
3.2.0	• 3.2.1以降の3.2リリース • 3.3.0以降の3.3リリース	3.2.1 および 3.3.0
2.1.1	3.3.0以降の3.3リリース	3.3.0

SD-WANプラグインのダウングレードパス

ダウングレード表の情報を次のように解釈します。

- **Downgrade From**–ダウングレード前の現在のSD-WANプラグインのバージョンです。
- **SD-WAN**プラグインバージョンへ–現在のSD-WANプラグインバージョンからダウングレードできるSD-WANプラグインバージョンの一覧です。
- **SD-WAN**プラグイン版へ（推奨）–現在のSD-WANプラグイン版からダウングレードすることを推奨するSD-WANプラグイン版です

。

以下はSD-WANプラグイン版のダウングレードパスです。SD-WANダウングレードを実行すると、現在のプラグインバージョンで移行処理が実行されます。

ダウングレード元（現在のインストールバージョン）	許可されたSD-WANプラグインのバージョンへ
2.2.2、2.2.3、2.2.4、2.2.5、および 2.2.6	2.2.1
2.2.3、2.2.4、2.2.5、および 2.2.6	2.2.2
2.2.4、2.2.5、および 2.2.6	2.2.3
2.2.5および2.2.6	2.2.4
2.2.6	2.2.5
3.0.7、3.1.3、3.2.1、および 3.3.0	2.2.6
3.0.5	3.0.0、3.0.1、3.0.2、3.0.3、および 3.0.4
3.0.6、3.0.7、3.1.0-hf、3.1.1、3.1.3、3.2.0、3.2.1、および 3.3.0	3.0.5
3.0.7、3.1.3、3.2.0、3.2.1、および 3.3.0	3.0.6

ダウングレード元（現在のインストールバージョン）	許可されたSD-WANプラグインのバージョンへ
3.1.3、3.2.1、および 3.3.0	3.0.7
3.1.1、3.1.3、3.2.0、3.2.1、および 3.3.0	3.1.0
3.1.3、3.2.0、3.2.1、および 3.3.0	3.1.1
3.1.3、3.2.0、3.2.1、および 3.3.0	3.1.2
3.2.1 および 3.3.0	3.1.3 および 3.2.0

SD-WAN プラグインのインストール

ご利用のPanorama™管理サーバーとSD-WANを利用するファイアウォールにSD-WANプラグインバージョンをインストールします。

Palo Alto Networks Panorama プラグイン互換性マトリックス を参照し、ターゲット SD-WAN プラグインバージョンに必要な最小 PAN-OS バージョンを確認してください。

STEP 1 | Panorama Web インターフェースにログインします。

STEP 2 | PanoramaにSD-WANプラグインのバージョンをインストールします。

Panorama が高可用性 (HA) 設定の場合、Panorama HA ピアでこのステップを繰り返します。

1. 最新の **Panorama** > **Plugins** および **Check Now** を選択して、最新の **sd_wan** プラグイン バージョンを入手してください。
2. 最新バージョンの SD-WAN 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。

STEP 3 | 新しいプラグインバージョンが正常にインストールされたら、Panorama **Dashboard** (ダッシュボード) を表示し、一般情報ウィジェットで SD-WAN プラグイン にインストールした SD-WAN プラグインのバージョンが表示されていることを確認します。

SD-WANプラグインを活用したアップグレードPanorama高可用性ペア（アクティブ/パッシブ）

どこで使用できますか?	何が必要ですか?
• PAN-OS • SD-WAN	❑ SD-WAN plugin license

Panorama管理サーバーが動作しているSD-WANプラグインのバージョンに基づいたアップグレードパスに従ってください。

SD-WANプラグイン版を実行するPanorama	以下の手順に従ってください
1.0.x	PanoramaHAペア:SD-WANプラグイン1.0.4から2.2.6リリースへのアップグレード
2.1.x	PanoramaHAペア:SD-WANプラグイン2.1.xを2.2.6リリースにアップグレード
2.2.6	PanoramaHAペア:SD-WANプラグイン2.2.6を3.0.7リリースにアップグレード

PanoramaHAペア:SD-WANプラグイン1.0.4から2.2.6リリースへのアップグレード

Panoramaが1.0.x～2.2.xのいずれかのSD-WANプラグインバージョンでインストールされており、SD-WANプラグインバージョンをアップグレードする場合は、まずSD-WANプラグインバージョン2.2.6にアップグレードする必要があります（中間バージョンではありません）。SD-WAN 2.2.6バージョンには、新機能、バグ修正、パフォーマンス改善、機能強化が含まれているからです。

Panoramaソフトウェアのバージョンが PAN-OSのバージョンよりも常に高いことを保証することをお勧めします。たとえば、Panoramaのバージョンが10.1.9の場合、PAN-OSのバージョンは以前のPAN-OS 10.1.9リリースのいずれかになります。

アップグレードプロセスを開始する前に、アップグレードの重要な考慮事項をお読みください。

SD-WAN 2.2.6プラグインバージョンでPanorama HAペアをアップグレードする場合は、以下のワークフローを同じ順序で使用します。

STEP 1 | Panorama管理サーバーのバージョンをアップグレードします。

1. Panorama 9.1.xからPanorama 10.0.7-h3をアクティブとパッシブの両方のPanoramaにダウンロードしてインストールします。
2. Panorama 10.0.7-h3から、アクティブとパッシブの両方のPanoramaに最新のPanorama 10.1リリースをダウンロードしてインストールします。
3. Panoramaを最新リリースの10.1にアップグレードした後、アクティブなPanoramaがアクティブのまま、パッシブなPanoramaがパッシブのままになっているか確認してください。HA ステートに変更がなければ、アップグレードは成功です。そうでない場合は、

アップグレード前の HA ペアの状態を維持するために強制切り替えを実行する必要があります。

強制切り替えを実行するには、現在のアクティブなHAピアから次のCLIコマンドを同じ順序で実行します。

```
admin> 高可用性状態の要求 suspendadmin
```

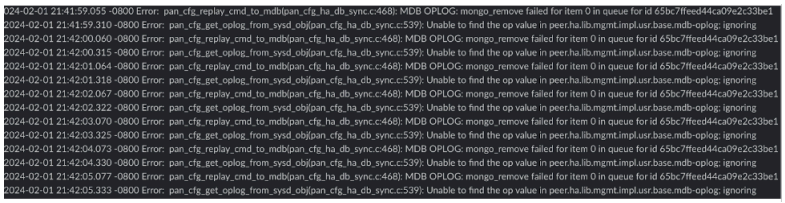
```
admin> 高可用性状態の要求 functional
```

STEP 2 | 設定済みのログを監視します。

（管理者モード）SD-WANプラグインを2.2.6にアップグレードする前に、Panorama HAペアの両方で設定済みのログの監視を開始します。

```
admin> tail follow yes mp-log configd.log
```

tail follow yes mp-log configd.log コマンドを実行したときに次のエラーメッセージが表示される場合、アクティブおよびパッシブPanoramaの Mongo DB が同期しなくなっている。



この問題の解決方法

1. （管理者モード）アクティブな Panorama とパッシブな Panorama の両方で、*pan_oplog* データベース全体を削除します。

   ```
   admin > debug mongo drop database pan_oplog instance mdb
   ```

2. （管理者モード）再起動パッシブPanoramaに設定されている。

   ```
   admin > debug software restart process configd
   ```

*configd*を再起動したら、それぞれのWebインターフェイスとコマンドラインインターフェイスを更新します。再起動後、どのコミットプロセスでも *mongo pan_oplog* エラーは表示されなくなります。

アップグレードプロセス全体を通じて、設定されたログを監視することをお勧めします。

STEP 3 | アクティブPanoramaとパッシブPanoramaの両方にSD-WANプラグインバージョン2.2.6をダウンロードしてインストールします。

STEP 4 | （管理者モード）SD-WANコレクションをアクティブPanoramaとパッシブPanoramaの両方でドロップします。

```
admin> debug mongo drop database pl_sd_wan instance mdb
```

```
admin@sdwan-hw-panorama(secondary-passive)> debug mongo drop database pl_sd_wan instance mdb

No collection given, drop the whole database pl_sd_wan instead
MongoDB shell version v3.6.19
connecting to: mongodb://127.0.0.1:27017/pl_sd_wan?gssapiServiceName=mongodb
Implicit session: session { "id" : UUID("c6dcb502-4582-4a0f-90d7-19a0becf8773") }
MongoDB server version: 3.6.19
{ "dropped" : "pl_sd_wan", "ok" : 1 }
```

この手順は、SD-WAN Mongo DBコレクションを同期させるために必要です。

STEP 5 | （設定モード時）アクティブなPanoramaからの変更を強制的にコミットします。

```
Number of failed attempts since last successful login: 0


admin@sdwan2_panorama(primary-active)> configure
Entering configuration mode
[edit]
admin@sdwan2_panorama(primary-active)# commit force


Commit job 5307 is in progress. Use Ctrl+C to return to command prompt
...11%.77%.80%....91%.....100%
sd_wan plugin validation: Config valid
Configuration committed successfully
Disk 'A' on log collector 0007AQA994 in group lc-group1 has a size of zero bytes

[edit]
admin@sdwan2_panorama(primary-active)#
```

SD-WANプラグインのアップグレードが完了したら、Palo Alto NetworksデバイスのCLIコマンド（コンフィギュレーションモード）からコミットフォースを実行する必要があります。commit forceではなくcommit allを実行すると、そのデバイスのSD-WAN設定がすべて失われます。

STEP 6 | Panorama HAアップグレード後に以下を確認。

1. 最初にブランチデバイスに選択プッシュを実行し、次にアクティブPanoramaからハブデバイスを実行します。
2. ［**Panorama**］> **[Managed Devices (管理対象外デバイス)]** > **[Summary (概要)]**を選択し、デバイス概要ページの［Active Panorama］と［Passive Panorama］の両方でデバイスグループとテンプレートが同期していることを確認します。
3. Tunnel、BGP、Key ID、トラフィックなどの SD-WAN 設定が期待通りかどうかを確認する。

> *Panorama HA* ペアのアップグレードが成功すると、キー *ID*、*PSK*、*IP* キャッシュ、*IPSec* トンネル キャッシュ、サブネット キャッシュがリフレッシュされ、*SD-WAN* の機能には影響しません。

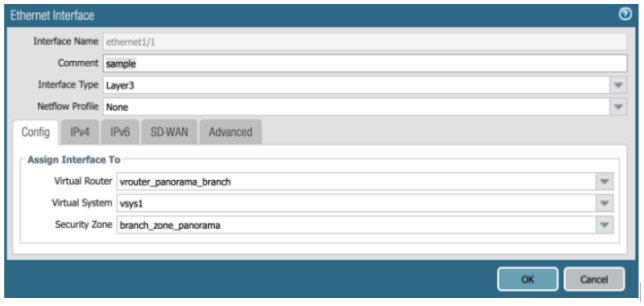
STEP 7 | （推奨）接続されているファイアウォールをアップグレードします。

Panorama HAペアのアップグレードに成功すると、接続されたハブとブランチのデバイスは、ブランチファイアウォールから順に1つずつアップグレードできます（ブランチファイア

ウォールとハブファイアウォールは、スタンドアロンファイアウォールまたはHAペアにできます）。

各ファイアウォールのバージョンアップ後に*SD-WAN*の構成や機能を確認することをおすすめします。

1. テンプレートのインターフェイスのコメントを変更または追加し、その後に**[Commit (コミット)]**と**[Push to Devices (デバイスにプッシュ)]**することで、すべてのテンプレートに小さな変更を加えます。これは、設定に問題がないか、アップグレードが機能しているかを確認するための検証作業に過ぎません。



2. SD-WANの構成や機能を確認する。
3. すべてのブランチがアップグレードされるまで、ブランチファイアウォールを1つずつアップグレードします。
4. ブランチファイアウォールの場合は、まず次の手順に従ってください。
    1. ブランチHAまたはスタンドアロンデバイスのペアをPanoramaバージョン9.1.xから10.0.7-h3にアップグレードしてから、Panorama10.1の最新リリースにアップグレードします。
    2. アップグレードが実行されたアクティブなPanorama、**Commit (コミット)**、および**[Push to Devices (デバイスにプッシュ)]**から、特定のファイアウォールテンプレートからインターフェイスのコメントに小さな変更を導入します。**Commit All (すべてコミット)**が完了したら、SD-WANの構成と機能を確認します。これは、ファイアウォールのアップグレード後に構成が正常で、アップグレードが機能していることを確認するための検証作業に過ぎません。
5. ハブファイアウォールについては、次の手順に従ってください。ブランチファイアウォールのアップグレードを完了してから、ハブファイアウォールのアップグレードを開始することが重要です。
    1. ハブHAまたはスタンドアロンデバイスのペアをPanoramaバージョン9.1.xから10.0.7-h3にアップグレードしてから、Panorama10.1の最新リリースにアップグレードします。
    2. アップグレードが実行されたアクティブなPanorama、**Commit (コミット)**、および**[Push to Devices (デバイスにプッシュ)]**から、特定のファイアウォールテンプレー

トからインターフェイスのコメントに小さな変更を導入します。**Commit All** (すべてコミット)が完了したら、SD-WANの構成と機能を確認します。

これは、ファイアウォールのアップグレード後に構成が正常で、アップグレードが機能していることを確認するための検証作業に過ぎません。

6. ［**Panorama**] > [**Managed Devices** (管理対象外デバイス)] > [**Summary** (概要)]を選択し、デバイス概要ページの［Active Panorama］と［Passive Panorama］の両方でデバイスグループとテンプレートが同期していることを確認します。
7. アップグレードが完了したら、アップグレード後の変更点に注意してください。

PanoramaHAペア:SD-WANプラグイン2.1.xを2.2.6リリースにアップグレード

PanoramaがSD-WANプラグインバージョン2.1.xでインストールされており、SD-WANプラグインのバージョンをアップグレードする場合は、まずSD-WANプラグインバージョン2.2.6にアップグレードする必要があります（中間バージョンではありません）。SD-WAN 2.2.6バージョンには、新機能、バグ修正、パフォーマンス改善、機能強化が含まれているからです。

Panoramaソフトウェアのバージョンが PAN-OSのバージョンよりも常に高いことを保証することをお勧めします。たとえば、Panoramaのバージョンが10.1.9の場合、PAN-OSのバージョンは以前のPAN-OS 10.1.9リリースのいずれかになります。

アップグレードプロセスを開始する前に、アップグレードの重要な考慮事項をお読みください。

以下のワークフローを同じ順序で使用して、SD-WAN 2.2.6プラグインバージョンでPanoramaHAペアをアップグレードします。

STEP 1 | Panorama管理サーバーのバージョンをアップグレードします。

1. Panorama 10.1から、アクティブとパッシブの両方のPanoramaに最新のPanorama 10.1リリースをダウンロードしてインストールします。
2. Panoramaを最新リリースの10.1にアップグレードした後、アクティブなPanoramaがアクティブのまま、パッシブなPanoramaがパッシブのままになっているか確認してください。HA ステートに変更がなければ、アップグレードは成功です。そうでない場合は、アップグレード前の HA ペアの状態を維持するために強制切り替えを実行する必要があります。

   強制切り替えを実行するには、現在のアクティブなHAピアから次のCLIコマンドを同じ順序で実行します。

   ```
   admin> 高可用性状態の要求 suspendadmin
   ```

   ```
   admin> 高可用性状態の要求 functional
   ```

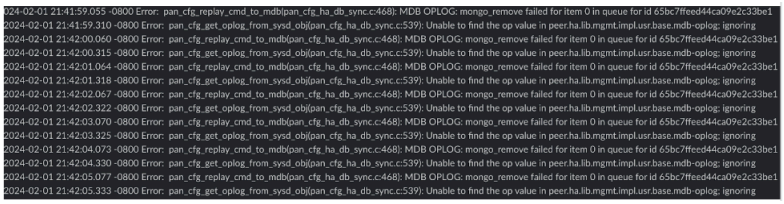
   ```
   admin@sdwan2-panorama-2(secondary-active)> request high-availability state suspend

   Successfully changed HA state to suspended
   admin@sdwan2-panorama-2(secondary-suspended)> request high-availability state functional

   Successfully changed HA state to functional
   admin@sdwan2-panorama-2(secondary-initial)>
   admin@sdwan2-panorama-2(secondary-passive)>
   admin@sdwan2-panorama-2(secondary-passive)>
   admin@sdwan2-panorama-2(secondary-passive)>
   ```

STEP 2 | 設定済みのログを監視します。

（管理者モード）SD-WANプラグインを2.2.6にアップグレードする前に、Panorama HAペアの両方で設定済みのログの監視を開始します。

```
admin> tail follow yes mp-log configd.log
```

`admin > tail follow yes mp-log configd.log` コマンドを実行したときに以下のエラーメッセージが表示された場合は、アクティブPanoramaとパッシブPanoramaのmongo DBが同期しなくなっています。



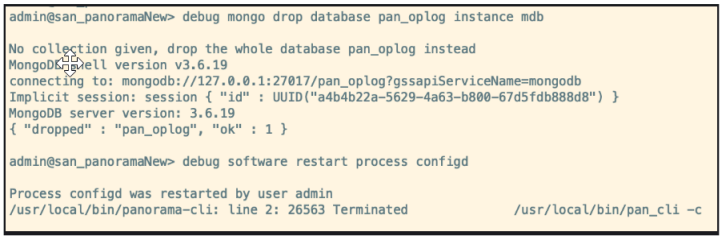
この問題の解決方法

1. （管理者モード）アクティブな Panorama とパッシブな Panorama の両方で、*pan_oplog* データベース全体を削除します。

   ```
   admin > debug mongo drop database pan_oplog instance mdb
   ```

2. （管理者モード）再起動パッシブPanoramaに設定されている。

   ```
   admin > debug software restart process configd
   ```



*configd*を再起動したら、それぞれのWebインターフェイスとコマンドラインインターフェイスを更新します。再起動後、どのコミットプロセスでも *mongo pan_oplog* エラーは表示されなくなります。

アップグレードプロセス全体を通じて、設定されたログを監視することをお勧めします。

STEP 3 | アクティブPanoramaとパッシブPanoramaの両方にSD-WANプラグインバージョン2.2.6をダウンロードしてインストールします。

STEP 4 | （管理者モード）SD-WANコレクションをアクティブPanoramaとパッシブPanoramaの両方でドロップします。

```
admin> debug mongo drop database pl_sd_wan instance mdb
```

```
admin@sdwan-hw-panorama(secondary-passive)> debug mongo drop database pl_sd_wan instance mdb

No collection given, drop the whole database pl_sd_wan instead
MongoDB shell version v3.6.19
connecting to: mongodb://127.0.0.1:27017/pl_sd_wan?gssapiServiceName=mongodb
Implicit session: session { "id" : UUID("c6dcb502-4582-4a0f-90d7-19a0becf8773") }
MongoDB server version: 3.6.19
{ "dropped" : "pl_sd_wan", "ok" : 1 }
```

この手順は、SD-WAN Mongo DBコレクションを同期させるために必要です。

STEP 5 | （設定モード時）アクティブなPanoramaからの変更を強制的にコミットします。

```
Number of failed attempts since last successful login: 0


admin@sdwan2_panorama(primary-active)> configure
Entering configuration mode
[edit]
admin@sdwan2_panorama(primary-active)# commit force


Commit job 5307 is in progress. Use Ctrl+C to return to command prompt
...11%.77%.80%....91%.....100%
sd_wan plugin validation: Config valid
Configuration committed successfully
Disk 'A' on log collector 0007AQA994 in group lc-group1 has a size of zero bytes

[edit]
admin@sdwan2_panorama(primary-active)#
```

SD-WANプラグインのアップグレードが完了したら、Palo Alto NetworksデバイスのCLIコマンド（コンフィギュレーションモード）からコミットフォースを実行する必要があります。commit forceではなくcommit allを実行すると、そのデバイスのSD-WAN設定がすべて失われます。

STEP 6 | Panorama HAアップグレード後に以下を確認。

1. 最初にブランチデバイスに選択プッシュを実行し、次にアクティブPanoramaからハブデバイスを実行します。
2. ［**Panorama**］> **[Managed Devices (管理対象外デバイス)]** > **[Summary (概要)]**を選択し、デバイス概要ページの［Active Panorama］と［Passive Panorama］の両方でデバイスグループとテンプレートが同期していることを確認します。
3. Tunnel、BGP、Key ID、トラフィックなどの SD-WAN 設定が期待通りかどうかを確認する。

> *Panorama HA* ペアのアップグレードが成功すると、キー *ID*、*PSK*、*IP* キャッシュ、*IPSec* トンネル キャッシュ、サブネット キャッシュがリフレッシュされ、*SD-WAN* の機能には影響しません。

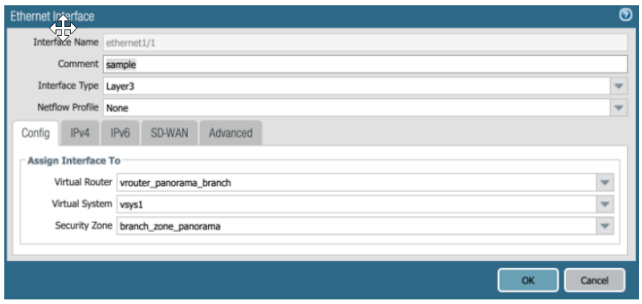
STEP 7 | （推奨）接続されているファイアウォールをアップグレードします。

Panorama HAペアのアップグレードに成功すると、接続されたハブとブランチのデバイスは、ブランチファイアウォールから順に1つずつアップグレードできます（ブランチファイア

ウォールとハブファイアウォールは、スタンドアロンファイアウォールまたはHAペアにできます）。

各ファイアウォールのバージョンアップ後に*SD-WAN*の構成や機能を確認することをおすすめします。

1. テンプレートのインターフェイスのコメントを変更または追加し、その後に**[Commit (コミット)]**と**[Push to Devices (デバイスにプッシュ)]**することで、すべてのテンプレートに小さな変更を加えます。これは、設定に問題がないか、アップグレードが機能しているかを確認するための検証作業に過ぎません。



2. SD-WANの構成や機能を確認する。
3. すべてのブランチがアップグレードされるまで、ブランチファイアウォールを1つずつアップグレードします。
4. ブランチファイアウォールの場合は、まず次の手順に従ってください。
    1. ブランチHAまたはスタンドアロンデバイスのペアをPanoramaバージョン9.1.xから10.0.7-h3にアップグレードしてから、Panorama10.1の最新リリースにアップグレードします。
    2. アップグレードが実行されたアクティブなPanorama、**Commit (コミット)**、および**[Push to Devices (デバイスにプッシュ)]**から、特定のファイアウォールテンプレートからインターフェイスのコメントに小さな変更を導入します。**Commit All (すべてコミット)**が完了したら、SD-WANの構成と機能を確認します。これは、ファイアウォールのアップグレード後に構成が正常で、アップグレードが機能していることを確認するための検証作業に過ぎません。
5. ハブファイアウォールについては、次の手順に従ってください。ブランチファイアウォールのアップグレードを完了してから、ハブファイアウォールのアップグレードを開始することが重要です。
    1. ハブHAまたはスタンドアロンデバイスのペアをPanoramaバージョン9.1.xから10.0.7-h3にアップグレードしてから、Panorama10.1の最新リリースにアップグレードします。
    2. アップグレードが実行されたアクティブなPanorama、**Commit (コミット)**、および**[Push to Devices (デバイスにプッシュ)]**から、特定のファイアウォールテンプレー

トからインターフェイスのコメントに小さな変更を導入します。**Commit All (**すべてコミット**)**が完了したら、SD-WANの構成と機能を確認します。

これは、ファイアウォールのアップグレード後に構成が正常で、アップグレードが機能していることを確認するための検証作業に過ぎません。

6. ［**Panorama**］> ［**Managed Devices (**管理対象外デバイス**)**］> ［**Summary (**概要**)**］を選択し、デバイス概要ページの［Active Panorama］と［Passive Panorama］の両方でデバイスグループとテンプレートが同期していることを確認します。
7. アップグレードが完了したら、アップグレード後の変更点に注意してください。

PanoramaHAペア:SD-WANプラグイン2.2.6から3.0.7リリースへのアップグレード

Panoramaソフトウェアのバージョンが PAN-OSのバージョンよりも常に高いことを保証することをお勧めします。たとえば、Panoramaのバージョンが10.1.9の場合、PAN-OSのバージョンは以前のPAN-OS 10.1.9リリースのいずれかになります。

アップグレードプロセスを開始する前に、アップグレードの重要な考慮事項をお読みください。

STEP 1 | SD-WANプラグイン3.0.7をダウンロードし、SD-WANプラグインバージョン3.0.7以外のPanorama HAペアの両方でダウンロードした3.0.xプラグインをすべて削除します。

STEP 2 | Panoramaソフトウェアのバージョンを最新の10.1バージョンから最新の10.2バージョンにアップグレードします。最新版の10.2へのアップグレードに成功すると、SD-WANプラグイン3.0.7が自動的にインストールされます。

SD-WANプラグイン3.0.7バージョンがPanoramaにインストールされているかどうかを確認するには、Panorama**[Dashboard (**ダッシュボード**)]**の**General Information (**一般情報**)**を確認してください。

STEP 3 | アップグレードが完了したら、SD-WANの構成や機能が期待通りかチェックしよう。

STEP 4 | パロアルトネットワークスデバイスのCLIコマンド（コンフィギュレーションモード）でコミットフォースを実行します。commit forceではなくcommit allを実行すると、そのデバイスのSD-WAN設定がすべて失われます。

STEP 5 | （推奨）接続されているデバイスを、ブランチペアから順に1つずつアップグレードし、次にハブペアをアップグレードします。

STEP 6 | デバイスをアップグレードしたら、SD-WANの構成とその機能を確認します。

STEP 7 | アップグレードが完了したら、アップグレード後の変更点に注意してください。

SD-WAN プラグインを活用したスタンドアロン型Panoramaのアップグレード

どこで使用できますか?	何が必要ですか?
• PAN-OS	☐ SD-WAN plugin license

どこで使用できますか?	何が必要ですか?
• SD-WAN	

アップグレード手順に進む前に、前提条件を満たしてください。

Panorama 管理サーバーが実行している SD-WAN プラグインのバージョンに基づいてアップグレードパスをたどってください。

SD-WANプラグイン版を実行するPanorama	以下の手順に従ってください
1.0.x	スタンドアロン型Panorama:SD-WANプラグイン1.0.4から2.2.6リリースへのアップグレード
2.1.x	スタンドアロン型Panorama:SD-WANプラグイン2.1.xを2.2.6リリースにアップグレード
2.2.6	スタンドアロン型Panorama:SD-WAN プラグイン 2.2.6 から 3.0.7 リリースへのアップグレード

スタンドアロン型Panorama:SD-WANプラグイン1.0.4から2.2.6リリースへのアップグレード

Panoramaソフトウェアのバージョンが PAN-OSのバージョンよりも常に高いことを保証することをお勧めします。たとえば、Panoramaのバージョンが10.1.9の場合、PAN-OSのバージョンは以前のPAN-OS 10.1.9リリースのいずれかになります。

アップグレードプロセスを開始する前に、アップグレードの重要な考慮事項をお読みください。

STEP 1 | Panorama ソフトウェアバージョン 10.0.7-h3 をダウンロードしてインストールします。

STEP 2 | Panorama 10.0.7-h3 から、最新の Panorama 10.1 リリースをダウンロードしてインストールします。

STEP 3 | SD-WAN プラグインバージョン 2.2.6 を Panorama にダウンロードしてインストールします。

STEP 4 | （設定モード時）アクティブなPanoramaからの変更を強制的にコミットします。

SD-WANプラグインのアップグレードが完了したら、Palo Alto NetworksデバイスでCLI（構成モード）を使用してコミットフォースを実行する必要があります。commit force の代わりにすべてコミットを実行すると、そのデバイスのすべての SD-WAN 設定が失われます。

```
Number of failed attempts since last successful login: 0


admin@sdwan2_panorama(primary-active)> configure
Entering configuration mode
[edit]
admin@sdwan2_panorama(primary-active)# commit force


Commit job 5307 is in progress. Use Ctrl+C to return to command prompt
...11%.77%.80%....91%.....100%
sd_wan plugin validation: Config valid
Configuration committed successfully
Disk 'A' on log collector 0007AQA994 in group lc-group1 has a size of zero bytes

[edit]
admin@sdwan2_panorama(primary-active)#
```

STEP 5 | スタンドアロンの Panorama をアップグレードしたら、次の点を確認してください。

1. Panorama からデバイスにプッシュします。
2. ［**Panorama**］> ［**Managed Devices** (管理対象外デバイス)］> ［**Summary** (概要)］を選択し、デバイス概要ページの［Active Panorama］と［Passive Panorama］の両方でデバイスグループとテンプレートが同期していることを確認します。

3. Tunnel、BGP、Key ID、トラフィックなどの SD-WAN 設定が期待通りかどうかを確認する。

Panorama HA ペアのアップグレードが成功すると、キー *ID*、*PSK*、*IP* キャッシュ、*IPSec* トンネル キャッシュ、サブネット キャッシュがリフレッシュされ、*SD-WAN* の機能には影響しません。

STEP 6 | Panorama のアップグレードが成功すると、必要に応じて、接続されているすべてのデバイスを 1 つずつアップグレードできます。まず、ブランチペア/スタンドアロンから始め、次にハブペア/スタンドアロンの順にアップグレードできます。アップグレードするたびに、SD-WAN の構成と機能を確認することをお勧めします。

STEP 7 | アップグレードが完了したら、アップグレード後の変更点に注意してください。

スタンドアロン型Panorama:SD-WANプラグイン2.1.xを2.2.6リリースにアップグレード

Panoramaソフトウェアのバージョンが PAN-OSのバージョンよりも常に高いことを保証することをお勧めします。たとえば、Panoramaのバージョンが10.1.9の場合、PAN-OSのバージョンは以前のPAN-OS 10.1.9リリースのいずれかになります。

アップグレードプロセスを開始する前に、アップグレードの重要な考慮事項をお読みください。

STEP 1 | 最新の Panorama 10.1 リリースをダウンロードしてインストールします。

STEP 2 | SD-WAN プラグインバージョン 2.2.6 を Panorama にダウンロードしてインストールします。

STEP 3 | （設定モード時）アクティブなPanoramaからの変更を強制的にコミットします。

SD-WANプラグインのアップグレードが完了したら、Palo Alto NetworksデバイスでCLI（構成モード）を使用してコミットフォースを実行する必要があります。commit force の代わりにすべてコミットを実行すると、そのデバイスのすべての SD-WAN 設定が失われます。

```
Number of failed attempts since last successful login: 0


admin@sdwan2_panorama(primary-active)> configure
Entering configuration mode
[edit]
admin@sdwan2_panorama(primary-active)# commit force


Commit job 5307 is in progress. Use Ctrl+C to return to command prompt
...11%.77%.80%....91%.....100%
sd_wan plugin validation: Config valid
Configuration committed successfully
Disk 'A' on log collector 0007AQA994 in group lc-group1 has a size of zero bytes

[edit]
admin@sdwan2_panorama(primary-active)#
```

STEP 4 | スタンドアロンの Panorama をアップグレードしたら、次の点を確認してください。

1. Panorama からデバイスにプッシュします。
2. ［**Panorama**］> **[Managed Devices (管理対象外デバイス)]** > **[Summary (概要)]**を選択し、デバイス概要ページの［Active Panorama］と［Passive Panorama］の両方でデバイスグループとテンプレートが同期していることを確認します。

3. Tunnel、BGP、Key ID、トラフィックなどの SD-WAN 設定が期待通りかどうかを確認する。

> *Panorama HA* ペアのアップグレードが成功すると、キー *ID*、*PSK*、*IP* キャッシュ、*IPSec* トンネル キャッシュ、サブネット キャッシュがリフレッシュされ、*SD-WAN* の機能には影響しません。

STEP 5 | Panorama のアップグレードが成功すると、必要に応じて、接続されているすべてのデバイスを 1 つずつアップグレードできます。まず、ブランチペア/スタンドアロンから始め、次にハブペア/スタンドアロンの順にアップグレードできます。アップグレードするたびに、SD-WAN の構成と機能を確認することをお勧めします。

STEP 6 | アップグレードが完了したら、アップグレード後の変更点に注意してください。

スタンドアロン型Panorama:SD-WANプラグイン2.2.6から3.0.7リリースへのアップグレード

Panoramaソフトウェアのバージョンが PAN-OSのバージョンよりも常に高いことを保証することをお勧めします。たとえば、Panoramaのバージョンが10.1.9の場合、PAN-OSのバージョンは以前のPAN-OS 10.1.9リリースのいずれかになります。

アップグレードプロセスを開始する前に、アップグレードの重要な考慮事項をお読みください。

STEP 1 | 最新の Panorama 10.1 リリースをダウンロードしてインストールします。

STEP 2 | SD-WAN プラグインバージョン 2.2.6 を Panorama にダウンロードしてインストールします。

STEP 3 | （設定モード時）アクティブなPanoramaからの変更を強制的にコミットします。

SD-WANプラグインのアップグレードが完了したら、Palo Alto NetworksデバイスでCLI（構成モード）を使用してコミットフォースを実行する必要があります。commit force の代わりにすべてコミットを実行すると、そのデバイスのすべての SD-WAN 設定が失われます。

```
Number of failed attempts since last successful login: 0


admin@sdwan2_panorama(primary-active)> configure
Entering configuration mode
[edit]
admin@sdwan2_panorama(primary-active)# commit force


Commit job 5307 is in progress. Use Ctrl+C to return to command prompt
...11%.77%.80%....91%.....100%
sd_wan plugin validation: Config valid
Configuration committed successfully
Disk 'A' on log collector 0007AQA994 in group lc-group1 has a size of zero bytes

[edit]
admin@sdwan2_panorama(primary-active)#
```

STEP 4 | スタンドアロンの Panorama をアップグレードしたら、次の点を確認してください。

1. Panorama からデバイスにプッシュします。
2. ［**Panorama**］ > ［**Managed Devices** (管理対象外デバイス)］ > ［**Summary** (概要)］を選択し、デバイス概要ページの［Active Panorama］と［Passive Panorama］の両方でデバイスグループとテンプレートが同期していることを確認します。

3. Tunnel、BGP、Key ID、トラフィックなどの SD-WAN 設定が期待通りかどうかを確認する。

Panorama HA ペアのアップグレードが成功すると、キー *ID*、*PSK*、*IP* キャッシュ、*IPSec* トンネル キャッシュ、サブネット キャッシュがリフレッシュされ、*SD-WAN* の機能には影響しません。

STEP 5 | Panorama のアップグレードが成功すると、必要に応じて、接続されているすべてのデバイスを 1 つずつアップグレードできます。まず、ブランチペア/スタンドアロンから始め、次にハブペア/スタンドアロンの順にアップグレードできます。アップグレードするたびに、SD-WAN の構成と機能を確認することをお勧めします。

STEP 6 | アップグレードが完了したら、アップグレード後の変更点に注意してください。

アップグレード後のメモの変更

どこで使用できますか?	何が必要ですか?
• PAN-OS • SD-WAN	❑ SD-WAN plugin license

アップグレード後、*Panorama*に変更をコミットする前に以下のチェックを行う必要があります。

- *VPN*クラスタ内の*SD-WAN*デバイスごとに［***Router Name (***ルーター名*)***］ が設定されていることを確認します（***[Panorama] > [SD-WAN] > [Devices (***デバイス*)]***）。***[Router Name (***ルータ名*)]***の設定は、*SD-WAN*プラグイン*3.1.0*以降のリリースからサポートされています。
- *VPN*クラスタ内の*SD-WAN*デバイスごとに ***BGP*** （***[Panorama] > [SD-WAN] > [Devices (***デバイス*)]***）が有効になっていることを確認します。アップグレード前に設定されていたのと同じ *BGP* アドレス ファミリ（***IPv4 BGP*** または ***IPv6 BGP***）がイネーブルになっていることを確認します。*IPv6*は*SD-WAN*プラグイン*3.1.1*以降のリリースから対応しています。したがって、アップグレードされたプラグインには、*SD-WAN 3.1.1*以降のリリースからアップグレードする場合にのみ*IPv6*オプションが含まれます。
- アップグレード前に設定したのと同じ*VPN*認証タイプ（事前共有鍵 または 証明書）が有効になっているか（***[Panorama] > [SD-WAN] > [Devices (***デバイス*)] > [VPN Tunnel (VPN*** トンネル*)]***）を確認します。証明書認証タイプは、*SD-WAN*プラグイン*3.2.0*以降のリリースからサポートされています。したがって、*SD-WAN*プラグイン*3.2.0*以降のリリースからアップグレードする場合にのみ、アップグレードされたプラグインには*VPN*認証タイプ（事前共有鍵または証明書）が含まれます。

アップグレード後(Panorama HAペアまたはスタンドアロンPanoramaの場合)、以下の変更を確認できます。

- 追加したSD-WANデバイスの［**Panorama] > [SD-WAN] > [Devices (**デバイス*)]***にゾーンタブが表示されなくなります。したがって、既存のゾーンと事前定義されたゾーン（ゾーンから

ブランチ、ゾーンからハブ、ゾーンからインターネット、およびゾーンから内部）の間にセキュリティポリシー規則を作成する必要があります。

- フルメッシュ VPN クラスタでは、シリアル番号が小さいブランチが IKE 発信側として使用されます。アップストリーム NAT の場合、着信 NAT と発信 NAT の両方が NAT デバイスに存在する必要があります。着信 NAT が存在しない場合、PLUG-15276 が表示されます。

SD-WANデータベースコレクションによるMongoDBの同期状況

一部のSD-WANプラグインのバージョンでは、MongoDBのSD-WANデータベースコレクションが同期しなくなる可能性があり、これは既知の問題です。そのため、それ以前のリリースからSD-WANプラグインバージョン2.2.6にアップグレードする場合は、アップグレード手順に追加の手順が必要になる場合があります。

次の表は、SD-WANプラグインのバージョン（テスト済み）について、SD-WAN MongoDBコレクションが同期するかどうかを示しています。

S.No	対応PAN-OSソフトウェアバージョンとSD-WANプラグインバージョン	SD-WANプラグイン版	Mongoポート	Mongo on Panorama HA配下のSD-WANコレクション
1	10.1.6	2.1.2	31377	同期していない
2	10.1.x	2.1.2	31377	同期していない
3	10.1.x	2.2.6	27017	同期中
4	10.2.7-h3	3.0.7	27017	同期中

アップグレードのための CLI コマンド

- アップグレード タスクに CLI コマンドを使用する

アップグレード タスクに CLI コマンドを使用する

アップグレード タスクを実行するには、次の CLI コマンドを使用します。

あなたがしたい場合.	使う。。。
ファイアウォールの現在のバージョンを確認する	
• ファイアウォールソフトウェアとコンテンツの最新バージョンを確認します。	**show system info**
利用可能な動的更新にアクセスし、ファイアウォールのコンテンツバージョンをアップグレードする	
• Palo Alto Networks サーバーから直接動的更新の利用可能なコンテンツ バージョンを確認します。	コンテンツアップグレードチェックの要求
• 動的更新の使用可能なコンテンツバージョンをファイアウォールから直接確認します。	コンテンツのアップグレード情報をリクエストする
• コンテンツのバージョンを直接ファイアウォールにダウンロードします。	コンテンツアップグレードのダウンロード**<content version>**をリクエストする
• コンテンツバージョンをインストールします。	

あなたがしたい場合.	使う。。。
	コンテンツアップグレードのインストール**<content version>**の要求
利用可能なソフトウェアバージョンにアクセスし、ファイアウォールをアップグレードする	
• ダウンロード可能なソフトウェアバージョンを確認してください。	システム ソフトウェア情報の要求
• ソフトウェアの優先リリースを確認してください。 (PAN-OS 11.1.3 以降のリリース)	システムソフトウェア情報のリクエストを推奨
• ソフトウェアのベースリリースを確認してください。 (PAN-OS 11.1.3 以降のリリース)	システムソフトウェア情報ベースをリクエスト
• ソフトウェアの優先リリースとベースリリースの両方を確認してください。 (PAN-OS 11.1.3 以降のリリース)	システムソフトウェア情報推奨ベースをリクエスト
• ダウンロードしたソフトウェアをインストールします。	システムソフトウェアインストールバージョン**10.1.0**の要求

あなたがしたい場合.	使う。。。
• ファイアウォールを再起動します。	**request restart system**

firewallで利用可能なソフトウェアパッチにアクセスします。

パッチ機能は現在プレビュー モードで提供されています。この機能では、完全なサポートは利用できません。

あなたがしたい場合.	使う。。。
• ダウンロード可能なソフトウェアパッチを確認してください。	システムパッチチェックの要求
• 現在インストールされている firewall バージョンで利用可能なパッチを確認してください。	システムパッチ情報の要求
• 特定のパッチバージョンをダウンロードします。	システムパッチのダウンロードをリクエストするバージョン**<version>**
• 特定のパッチ バージョンの詳細情報を確認します。	システムパッチ情報バージョン**<version>**のリクエスト

あなたがしたい場合.	使う。。。
• ダウンロードしたパッチをインストールします。	システムパッチのインストールをリクエストする バージョン **<version>**
• インストールしたパッチを適用します。	システムパッチの適用を要求する

アップグレード用の API

- アップグレード タスクに API を使用する

アップグレード タスクに API を使用する

アップグレード タスクを実行するには、次の CLI コマンドを使用します。

あなたがしたい場合.	使う。。。
ファイアウォールの現在のバージョンを確認する	
• ファイアウォールソフトウェアとコンテンツの最新バージョンを確認します。	**https://firewall/api/?type=op&cmd=<request><system><software><check></check></software></system>**
利用可能な動的更新にアクセスし、ファイアウォールのコンテンツバージョンをアップグレードする	
• Palo Alto Networks サーバーから直接動的更新の利用可能なコンテンツ バージョンを確認します。	**https://firewall/api/?type=op&cmd=<request><content><upgrade><check></check></upgrade></content></request>**
• 動的更新の使用可能なコンテンツバージョンをファイアウォールから直接確認します。	**https://firewall/api/?type=op&cmd=<request><content><upgrade><info></info></upgrade></content></request>**
• 最新のコンテンツバージョンをファイアウォールに直接ダウンロードします。	**https://firewall/api/?type=op&cmd=<request><content><upgrade><download><latest></download></upgrade></content></request>**
• 特定のコンテンツバージョンを直接ファイアウォールにダウンロードします。	**https://firewall/api/?type=op&cmd=<request><content><upgrade><download><file>**ここに特定のファイル名を入力してください**<file></download></upgrade></content></request>**
• コンテンツバージョンをインストールします。	**https://firewall/api/?type=op&cmd=<request><content><upgrade><install><version><content version></version></install></upgrade></content></request>**
利用可能なソフトウェアバージョンにアクセスし、ファイアウォールをアップグレードする	
• ダウンロード可能なソフトウェアバージョンを確認してください。	**https://firewall/api/?type=op&cmd=<request><system><software><info></**

あなたがしたい場合.	使う。。。
	info></software></system></request>
• ファイアウォールにロードされている利用可能なバージョンを確認します。	**https://firewall/api/?type=op&cmd=<request><system><software><check></check></software></system></request>**
• ソフトウェアの特定のバージョンをダウンロードします。	**https://firewall/api/?type=op&cmd=request><system><software><downl version></download></software></system></request>**
• 特定のダウンロード ジョブの状態を確認します。	**https://firewall/api/?type=op&cmd=<show><jobs></jobs></show>**
• ダウンロードしたソフトウェアをインストールします。	**https://firewall/api/?type=op&cmd=<request><system><software><install><versio 10.1.0</version></install></software></system></request>**
• ファイアウォールを再起動します。	**https://firewall/api/?type=op&cmd=<request><restart><system></system></restart></request>**

