paloalto TECHDOCS

WildFireアプライアンス管理

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

April 8, 2025

Table of Contents

WildFireアプライアンスの概要

WildFire™は、動的分析と静的分析を組み合わせて脅威を検出し、マルウェアをブロックするための保護を作成することで、ゼロデイマルウェアの検出と防止を実現します。WildFire は、Palo Alto Networks の次世代ファイアウォールの能力を拡張し、標的型攻撃および未知のマルウェアを特定し、ブロックします。

WildFire アプライアンスについて

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

WildFireアプライアンスは、オンプレミスのWildFireプライベートクラウドを提供し、ファイアウォールがネットワークからファイルを送信することなく、サンドボックス環境の疑わしいファイルの分析を可能にします。WildFireアプライアンスを使用してWildFireプライベートクラウドをホストするには、ファイアウォールの分析のためにWildFireアプライアンスにサンプルを送信するように設定してください。WildFireアプライアンスは、すべてのファイルをローカルのサンドボックスに格納し、WildFireパブリッククラウドで使用されているものと同じエンジンを使用して、有害な動作がないか分析します。分析結果はプライベートクラウドからファイアウォールの**WildFire Submission**（**WildFire**への送信） ログへ、数分のうちに返送されてきます。

*WildFire*アプライアンス管理は、*WildFire*アプライアンスのセットアップと構成をカバーしていますが、運用設計と機能の多くを*WildFire*パブリッククラウドと共有しています。*WildFire* 分析機能の詳細については、*Advanced WildFire Administration* を参照してください。

次に、WildFireアプライアンスを有効化します。

- ❑ 検出されたマルウェア用にアンチウイルスおよびDNSシグネチャをローカルで生成し、またURL categoryを有害なリンクに割り当てます。そして、接続されたファイアウォールで最新のシグネチャおよびURLカテゴリを５分毎に取得することのできます。
- ❑ Submit Malware to the WildFire Public Cloudマルウェアを WildFireパブリック クラウドへ送信する）。WildFireパブリッククラウドは、サンプルの再分析を行い、マルウェアを検出するシグネチャを生成します。このシグネチャは数分で世界中のユーザーが利用でき、当該マルウェアを防御します。
- ❑ ローカルで生成されたマルウェアレポート（実サンプルを送信することなく）をWildFireパブリッククラウドに送信し、マルウェア統計情報と脅威インテリジェンスの品質向上に役立てることができます。

有効なWildFireサブスクリプションが組み込まれた最大100個のPalo Alto Networksファイアウォールを、1つのWildFireアプライアンスへ送信するよう設定できます。ファイアウォールのWildFireサブスクリプションのみでWildFireプライベートクラウドを構成することができ、それ以上のWildFireサブスクリプションは必要ありません。

ローカルアプライアンスのCLIを使用してWildFireアプライアンスを管理することも、PanoramaでWildFireアプライアンスを集中管理することもできます。PAN-OS 8.0.1から、WildFireアプライアンスをWildFireアプライアンスクラスタにグループ化し、ローカルまたはPanoramaからクラスタを管理することもできます。

WildFire プライベート クラウド

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

Palo Alto Networksプライベートクラウドの導入環境では、Palo Alto Networksファイアウォールは、お客様の企業ネットワーク上でプライベートクラウド分析を提供しているWildFireアプライアンスへファイルを転送します。WildFireプライベートクラウドは、100の Palo Alto Networks ファイアウォールから分析用ファイルを受信できます。

WildFireプライベートクラウドはローカルサンドボックスなので、分析される良質な、グレーウェア、フィッシングサンプルはお使いのネットワークに常駐します。プライベートクラウドは、初期状態ではネットワーク外に発見したマルウェアを送らないように設定されていますが、WildFireパブリッククラウドへ自動的にマルウェアを転送してシグネチャを生成し配信するように設定することも可能です。この場合、WildFireパブリッククラウドはサンプルの再分析を行ってシグネチャを生成してサンプルを同定し、シグネチャを脅威防御やWildFireのライセンスを行っている世界中のPalo Alto Networksファイアウォールへ配信します。

WildFireプライベートクラウドに悪意のあるサンプルであってもお使いのネットワークの外に出したくない場合は、そのようにすることが可能です。

- WildFireアプライアンスを有効化することで、マルウェアレポート（サンプル自体ではなく）をWildFireパブリッククラウドに転送可能です。WildFireレポートには、Palo Alto Networksがマルウェアの蔓延の度合いを査定する際に役立つ統計情報が含まれています。詳細については、「WildFireアプライアンスからマルウェアやレポートを送信する」を参照してください。
- すべてのマルウェアを自動的に転送するのではなく、WildFireポータルにファイルを手動でアップロードするか、WildFire APIを使用して WildFire public cloud にファイルを送信します。

WildFireアプライアンスでローカルシグネチャおよびURLカテゴリ生成を有効にするすることもできます。同様のマルウェアが再度検出されたときに効果的にブロックできるよう、WildFireアプライアンスが生成したシグネチャは接続されたファイアウォールへ配信されます。

Android Application Package（APK）およびMAC OSXファイルは、WildFireプライベートクラウド分析ではサポートされていません。

WildFireハイブリッドクラウド

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

WildFire ハイブリッド クラウド展開のファイアウォールは、特定のサンプルをパロアルトネットワークスのホスト型 WildFire パブリック クラウドの 1 つに転送し、その他のサンプルを WildFire アプライアンスによってホストされる WildFire プライベート クラウドに転送できます。WildFireハイブリッドクラウドデプロメントでは、プライベートなドキュメントをローカルおよび内部ネットワーク内で分析し、また一方でインターネットからのファイルをWildFireパブリッククラウドで分析するといった柔軟な環境を構築することが可能です。例えば、クレジットカード業界（PCI）のデータや保護すべき健康状態に関する情報（PHI）のデータのみをWildFireプライベートクラウドに転送し、Portable Executables （PE）ファイルはWildFireパブリッククラウドへ転送して分析を行うことができます。WildFireハイブリッドクラウドの導入環境では、ファイルをパブリッククラウド上で分析することで、過去にWildFireパブリッククラウドで処理されたファイルに関して素早く判定結果を得ることができるだけでなく、他の機密度の高いコンテンツを処理できるようWildFireアプライアンスの負荷を軽減することが可能です。更に、WildFire アプライアンスでの分析がサポートされていないAndroidアプリケーション パッケージ（APK）ファイルなど、特定のファイルタイプをWildFireパブリッククラウドへ転送することも可能です。

WildFireハイブリッドクラウドデプロイメントでは、パブリッククラウド分析とプライベートクラウド分析の両方の基準に一致するファイルが1つの場合もあります。 このような場合、ファイルは警告としてプライベートクラウドにのみ送信れます。

ハイブリッド クラウド転送をセットアップするには、WildFireアプライアンス分析用のファイルの転送を参照してください。

WildFire アプライアンス インターフェース

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

WF-500アプライアンスには、アプライアンスの背面にある4つのRJ-45イーサネットポートが装備されています。これらのポートは**MGT**, **1**, **2**、および**3**とラベル付けされ、特定のインターフェイスに対応します。

WildFireアプライアンスには、次の3つのインターフェイスがあります。

- **MGT** — ファイアウォールから転送されたすべてのファイルを受信し、詳細な結果を含むログをファイアウォールに返します。WildFire アプライアンスの構成を参照してください。
- **Virtual Machine Interface (VM interface)**[仮想マシン インターフェイス（VM インターフェイス）] — WildFire サンドボックス システムがネットワーク アクセスを行えるようにし、サンプル ファイルがインターネットと通信できるようにすることで、WildFire のサンプル動作分析能力が向上します。VM インターフェイスを設定すると、WildFire は、ネットワーク アクセスがあるとマルウェアが実行するような有害な動作（phone-home アクティビティなど）を監視できるようになります。ただし、マルウェアがサンドボックスからユーザーのネットワークに侵入するのを防ぐために、VMインターフェイスはインターネット接続が可能な分離されたネットワーク上に設定します。また、Torオプションを有効にすることで、サンプルがアクセスする有害なサイトから企業のパブリックIPアドレスを隠すこともできます。VM インターフェースについて詳しくは、WildFire アプライアンスVMインターフェイスを設定 を参照してください。
- クラスタ管理インターフェイス — WildFireアプライアンスクラスタのメンバーであるWildFireアプライアンスノード間のクラスタ全体の通信を提供します。これはファイアウォール操作のためのMGTインターフェイスとは異なるインターフェイスです。Ethernet2インターフェイスまたはEthernet3インターフェイス（それぞれ**2**と**3**のラベルが付いています）をクラスタ管理インターフェイスとして構成できます。

ネットワーク管理者（IPアドレス、サブネットマスク、ゲートウェイ、ホスト名、DNSサーバ）から、MGTポート、VMインターフェイス、およびクラスタ管理インターフェイス（WildFireアプライアンスクラスタのみ）のネットワーク接続を設定するために必要な情報を取得します。ファイル送信、WildFire ログの配信、アプライアンス管理など、ファイアウォールとアプライアンス間のすべての通信は、管理ポートを介して行われます。したがって、ファイアウォールからアプライアンスの 管理ポートへの接続が必要です。さらに、アプライアンスが updates.paloaltonetworks.com に接続してオペレーティング システムのソフトウェア更新を取得できるようにする必要があります。

WildFireアプライアンス ファイルタイプのサポート

次の表に、WildFireアプライアンスプライベートクラウドおよびWildFireポータルの直接アップロードによる分析でサポートされているファイルタイプを示します。

File Types Supported for Analysis（分析用にサポートされているファイルの種類）	**WildFire Private Cloud**（**WildFire** プライベートクラウド）**(WildFire**アプライアンス**)**	**WildFire Portal |API (**直接アップロード、すべてのリージョン**)**
電子メール内のリンク	✓	✓
Androidアプリケーションパッケージ（APK）ファイル	✗	✓
Adobe Flashファイル	✓	✓
Java アーカイブ（JAR）ファイル	✓	✓
Microsoft Office ファイル (SLK ファイルと IQY ファイルを含む)	✓	✓
ポータブル実行可能ファイル (MSI ファイルを含む)	✓	✓
ポータブルドキュメントフォーマット（PDF）ファイル	✓	✓
Mac OS X ファイル	✗	✓
Linux (ELF ファイルおよびシェルスクリプト) ファイル	✗	✓
アーカイブ (RAR, 7-Zip, ZIP*) ファイル	✓	✓

File Types Supported for Analysis（分析用にサポートされているファイルの種類）	WildFire Private Cloud（WildFire プライベートクラウド）(WildFireアプライアンス)	WildFire Portal |API (直接アップロード、すべてのリージョン)
スクリプト (BAT、JS、VBS、PS1、および HTA) ファイル	✓	✓
スクリプト (Perl および Python) スクリプト	✗	✓
アーカイブ (ZIP [直接アップロード] および ISO) ファイル*	✗	✓

* ZIPファイルは、分析のためにWildfire cloudに直接転送されません。代わりに、最初に firewall によってデコードされ、WildFire 分析プロファイル基準に一致するファイルは、分析のために個別に転送されます。

** WildFireアプライアンスは、MSI、IQY、および SLK ファイル分析をサポートしていません。

WildFire アプライアンスの更新と管理

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

WildFire™アプライアンスは、ローカルにホストされるWildFireプライベートクラウドとして設定できます。次のトピックでは、分析のためにファイルを受信するためのWildFireアプライアンスの準備、アプライアンスの管理方法、アプライアンスで脅威の署名とURLカテゴリをローカルに生成する方法について説明します。

- WildFire アプライアンスについて
- WildFire アプライアンスの構成
- スタンドアロン WildFire アプライアンスでカスタム証明書を使用する認証のセットアップ
- WildFire アプライアンスVMインターフェイスを設定
- WildFire アプライアンス分析機能の開始
- インターネット接続による WildFireアプライアンスデバイス証明書のインストール

WildFire アプライアンスの構成

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

このセクションでは、ネットワーク上に WildFireアプライアンスを組み込み、基本セットアップを実行するために必要な手順について説明します。

STEP 1 | WildFireアプライアンスをラックマウントしてケーブル接続します。

方法については、WildFire Appliance Hardware Reference Guide（WildFireアプライアンスのハードウェア リファレンス ガイド）を参照してください。

STEP 2 | コンピュータを MGT ポートまたはコンソール ポートを使用してアプライアンスに接続し、アプライアンスに電源を入れます。

1. 管理ポートまたはコンソール ポートに接続します。どちらもアプライアンスの背面にあります。
   - **Console Port**（コンソール ポート）—9 ピン オスのシリアル コネクタです。コンソール アプリケーションで、以下の設定を使用します。9600-8-N-1準備したケーブルを管理コンピュータのシリアル ポートか、USB-シリアル コンバータに接続します。
   - **MGT Port**（MGTポート）—Ethernet RJ-45 ポートです。デフォルトでは、管理 ポートの IP アドレスは 192.168.1.1 です。管理コンピュータのインターフェイスのサブネットは、管理ポートと同じにする必要があります。たとえば、管理コンピュータの IP アドレスを 192.168.1.5 に設定します。
2. アプライアンスの電源を入れます。

   アプライアンスは第一電源に接続するとすぐに電源が入りますが、第二電源が供給されるまで警告ビープ音が鳴り続けます。アプライアンスがすでに接続され、シャットダウン状態にある場合は、アプライアンスの前面にある電源ボタンを使用して電源を入れます。

STEP 3 | WildFire アプライアンスを登録します。

1. アプライアンスの S/N タグに表示されているシリアル番号を確認するか、以下のコマンドを実行して、`serial`（シリアル）フィールドを参照します。

   ```
   admin@WF-500> show system info
   ```

2. ブラウザで、Palo Alto Networks Support Portal（Palo Alto Networks サポートポータル）に移動し、ログインします。
3. デバイスを以下のように登録します。

   - これが初めて登録する Palo Alto Networks デバイスであり、ログイン情報がない場合は、ページの下部にある **Register**（登録）をクリックします。

     登録するには、電子メール アドレスと、デバイスのシリアル番号を指定します。メッセージが表示されたら、Palo Alto Networks サポート コミュニティへのアクセス用に、ユーザー名とパスワードを設定します。
   - すでにアカウントがある場合は、ログインしてから **My Devices**（マイデバイス）をクリックします。画面下部の **Register Device**（デバイス登録）セクションまでスクロールし、デバイスのシリアル番号、市区町村、および郵便番号を入力して、**Register Device**（デバイス登録）をクリックします。
4. WildFireアプライアンスのWildFire登録を確認するには、SSHクライアントを使用するか、コンソールポートを使用してアプライアンスにログインします。管理ユーザーのユーザーネームおよびパスワードを入力し、アプライアンス上で以下のコマンドを実行してください。

   ```
   admin@WF-500> test wildfire registration
   ```

   以下の出力は、アプライアンスが Palo Alto Networks WildFire クラウド サーバーの 1 つに登録されていることを示しています。

   ```
   WildFireの登録をテストする:成功したダウンロードサーバーリスト:最適なサーバーを選択します:cs-s1.wildfire.paloaltonetworks.com
   ```

STEP 4 | 管理者パスワードをリセットします。

1. 以下のコマンドを実行して新しいパスワードを設定します。

```
admin@WF-500> set password
```

2. 現在のパスワードを入力して Enter（エンター） キーを押してから、新しいパスワードを入力して確認します。再起動時に新しいパスワードが確実に保存されるよう、設定にコミットします。

   PAN-OS 9.0.4 からは、事前定義済みのデフォルトの管理者パスワード *(admin/admin)* はデバイス初回ログイン時に変更されるようになっています。新しいパスワードは*8*文字以上で、*1*文字以上の小文字と*1*文字以上の大文字、および*1*つの数字または特殊文字を含める必要があります。

   パスワードの強度を高めるために、必ずパスワード強度のベストプラクティスに従ってください。

3. **exit**と入力してログアウトし、再度ログインして新しいパスワードが設定されたことを確認します。

STEP 5 | 管理インターフェイスを設定します。

この例では以下の IPv4 値が使用されていますが、アプライアンスは IPv6 アドレスもサポートしています。

- IPv4 アドレス - 10.10.0.5/22
- サブネット マスク - 255.255.252.0
- デフォルト ゲートウェイ - 10.10.0.1
- ホスト名 - wildfire-corp1
- DNS サーバー - 10.0.0.246

1. SSH クライアントかコンソール ポートを使用してアプライアンスにログインし、設定モードに切り替えます。

```
admin@WF-500> configure
```

2. IP 情報の設定

```
admin@WF-500# set deviceconfig system ip-address 10.10.0.5
 netmask 255.255.252.0 default-gateway 10.10.0.1 dns-setting
 servers primary 10.0.0.246
```

セカンダリ *DNS* サーバーを設定します。上記のコマンドの「*primary*」を「*secondary*」に置き換え、他の *IP* 情報を除外します。以下に例を示します。

```
admin@WF-500# set deviceconfig system dns-setting servers
 secondary 10.0.0.247
```

3. ホスト名を設定します（この例では「wildfire-corp1」）。

```
admin@WF-500# set deviceconfig system hostname wildfire-corp1
```

4. 設定をコミットして、新しい管理（MGT）ポート設定をアクティベートします。

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

5. 管理インターフェイス ポートをネットワーク スイッチに接続します。
6. 管理 PC を会社のネットワークに戻します。管理ネットワーク上のアプライアンスにアクセスするためにネットワークが必要になります。
7. 管理コンピュータから、SSH クライアントを使用してアプライアンスの 管理ポートに割り当てられた新しい IP アドレスまたはホスト名でアプライアンスに接続します。この例では、IP アドレスは「10.10.0.5」です。

STEP 6 | Palo Alto Networks から受信した WildFire 認証コードでアプライアンスをアクティベーションします。

*WildFire*アプライアンスは認証コードなしでも機能しますが、ソフトウェア更新を入手するには有効な認証コードが必要です。

1. 操作モードに変更します。

```
admin @ WF-500# exit
```

2. WildFire ライセンスを取得してインストールします。

```
admin@WF-500> request license fetch auth-code <auth-code>
```

3. ライセンスを確認します。

```
admin@WF-500> request support check
```

サポート サイトとサポート契約日付に関する情報が表示されます。表示された日付が有効であることを確認します。

STEP 7 | WildFireアプライアンスのクロックを設定します。

これには 2 つの方法があります。日付、時刻、タイムゾーンを手動で設定することも、ローカルクロックをNetwork Time Protocol（NTP）サーバと同期させるようにWildFireアプライアンスを設定することもできます。

- クロックを手動で設定するには、次のコマンドを入力します。

```
admin@WF-500> set clock date <YYYY/MM/DD> time <hh:mm:ss>
 admin@WF-500> configure admin@WF-500# set deviceconfig system
 timezone <timezone>
```

*WildFire*詳細レポートに表示されるタイムスタンプは、アプライアンスで設定されたタイムゾーンを使用します。さまざまな地域の管理者がレポートを表示する場合は、タイム ゾーンを *UTC* に設定することを検討してください。

- NTP サーバーと同期するように WildFire アプライアンスを構成するには、次のコマンドを入力します。

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

```
servers secondary-ntp-server ntp-server-address <NTP secondary
 server IP address>
```

WildFire アプライアンスはプライマリまたはセカンダリ *NTP* サーバーに優先順位を付けず、どちらのサーバーとも同期します。

STEP 8 | （NTP設定の場合はオプション）NTP認証を設定します。

- NTP 認証を無効にする:

```
admin@WF-500# set deviceconfig system ntp-servers primary-ntp-
server authentication-type none
```

- 対称鍵交換 (共有シークレット) を有効にして NTP サーバー時刻の更新を認証します:

```
admin@WF-500# set deviceconfig system ntp-servers プライマリー ntp-
server 認証タイプ対称鍵
```

key-ID (1 から 65534) を引き続き入力し、NTP 認証で使用する <アルゴリズム (**MD5** または **SHA1**) を入力して確認し、認証アルゴリズム 認証キー**8}3}** を入力して確認します

- 自動キー (公開キー暗号化) を使用して NTP サーバーの時刻更新を認証します:

```
admin@WF-500# set deviceconfig system ntp-servers primary-ntp-
server authentication-type autokey
```

STEP 9 | アプライアンスがファイルの分析に使用する仮想マシンイメージを選択します。

エンド ユーザーのコンピュータにインストールされているソフトウェアと同じまたは最も近いイメージを選択する必要があります。各仮想イメージに含まれるオペレーティング システムやソフトウェアのバージョンは異なります（Windows XP、Windows 7 32 ビットまたは 64 ビット、Adobe Reader や Flash の特定のバージョンなど）。アプライアンスの設定には 1 つの仮想マシン イメージを使用しますが、稼働時のアプライアンスは仮想マシン イメージの複数のインスタンスを使用してパフォーマンスを向上します。

- 使用可能な仮想マシンのリストを表示して、環境を最もよく表している仮想マシンを特定するには:

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

- 次のコマンドを実行して現在の仮想マシン イメージを表示し、選択された VM フィールドを参照してください:

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

- アプライアンスが分析に使用するイメージを選択します。

```
admin@WF-500# set deviceconfig setting wildfire active-vm <vm-image-number>
```

たとえば、vm-5:

```
admin@WF-500# set deviceconfig setting wildfire active-vm vm-5
```

STEP 10 | 分析対象のファイルがネットワークアクセスを試みた際に、有害な動作がないかWildFireアプライアンスが監視できるようにします。

Set Up the WildFire Appliance VM Interface（WildFire アプライアンスVMインターフェイスを設定）。

STEP 11 | #unique_16

STEP 12 | (オプション)ワイルドファイアアプライアンスがクイック評決ルックアップを実行し、WildFire パブリッククラウドと評決を同期できるようにします。

次の CLI コマンドを使用すると、WildFire アプライアンスは判定ルックアップを実行し、WildFire パブリック クラウドと評決を同期できます。この機能はデフォルトで無効になっています。 コマンドを**yes**（はい）に設定して機能を有効にします。

```
admin@WF-500# set deviceconfig setting wildfire cloud-intelligence
 cloud-query yes | no
```

STEP 13 | （任意）WildFireアプライアンスを有効化してPalo Alto Networksコンテンツの日次更新を取得しマルウェア分析の向上と改善します。

WildFire アプライアンス分析機能の開始

STEP 14 | （任意）WildFireアプライアンスを有効化してDNSとアンチウイルスのシグネチャ、URLカテゴリを生成し、新しいシグネチャとURLカテゴリを、接続したファイヤーウォールに配布します。

ローカルシグネチャおよびURLカテゴリ生成を有効にする

STEP 15 | （任意）WildFireプライベートクラウドが検出したマルウェアをWildFireパブリッククラウドに自動的に送信し、世界中のユーザーをマルウェアから保護する支援をします。

Submit Malware to the WildFire Public Cloud.（マルウェアをWildFireパブリック クラウドへ送信する）。

STEP 16 | （任意）マルウェアのサンプルをWildFireプライベートクラウドから外部へ送りたくない場合は、サンプルの代わりにWildFire分析レポートをWildFireパブリッククラウドへ送信することもできます。

ローカルで検出したマルウェアを*WildFire*パブリッククラウドに送信したくない場合、*WildFire*脅威インテリジェンスの向上に役立てるため、マルウェア分析レポートの送信を有効化することを強く推奨します。

Submit Analysis Reports to the WildFire Public Cloud（分析レポートをWildFireパブリック クラウドへ送信する）。

STEP 17 | （任意）追加のユーザーにWildFireアプライアンスの管理を許可します。

スーパーユーザーとスーパーリーダーの 2 つのロールを割り当てることができます。スーパーユーザーは管理者アカウントに相当し、スーパーリーダーには読み取り専用アクセス権のみ与えられます。

この例では、ユーザー bsimpson にスーパーリーダー アカウントを作成します。

1. 設定モードに切り替えます。

```
admin@WF-500> configure
```

2. ユーザー アカウントを作成します。

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

3. 新しいパスワードを入力して確認します。
4. スーパーリーダー ロールを割り当てます。

```
admin@WF-500# set mgt-config users bsimpson パーミッション ロールベースのスーパーリーダー yes
```

STEP 18 | 管理者アクセス用のRADIUS認証を設定します。

1. 以下のオプションを使用して RADIUS プロファイルを作成します。

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

   （RADIUS サーバーおよびその他の属性を設定します。）
2. 認証プロファイルを作成します。

   ```
   admin@WF-500# set shared authentication-profile <profile-name>
    method radius server-profile <server-profile-name>
   ```
3. プロファイルをローカル管理者アカウントに割り当てます。

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

WildFireアプライアンス分析用のファイルの転送

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

Palo Alto Networksファイアウォールを設定して、解析のために不明なファイルまたは電子メールリンクと、既存のアンチウィルスシグネチャと一致してブロックされたファイルを転送するようにします。**WildFire**分析プロファイルを使用して、WildFireクラウドに転送するファイルを定義し（ハイブリッドクラウド導入の場合はパブリッククラウドを使用）、プロファイルをセキュリティルールにアタッチして、ゼロデイ マルウェアの検査をトリガーします。

使用中のアプリケーション、検出されたファイルタイプ、電子メールメッセージに含まれるリンク、または検体の送信方向（アップロード、ダウンロード、またはその両方）に基づいて、解析のために転送されるトラフィックを指定します。たとえば、ファイアウォールをセットアップして、 ユーザーがWebブラウズセッション中にダウンロードしようとするPortable Executables(ポータブル実行可能ファイル-PE）またはファイルを転送できます。未知の検体に加えて、ファイアウォールは既存のアンチウイルスシグネチャと一致するブロックされたファイルを転送します。これにより、Palo Alto Networksは、シグネチャが正常に防止できたが、WildFireもファイアウォールもこれまでに見たことのないマルウェアの亜種に基づく脅威インテリジェンスの貴重な送信元を提供します。

WildFire分析リソースをWildFireハイブリッドクラウドに拡張できます。実行するには、機密ファイルは引き続き WildFire プライベート クラウドに転送してローカルで解析し、機密性の低いファイルやサポートされていないファイルタイプを WildFireパブリック クラウドに転送するようにファイアウォールを構成します。

さらに、専用のWildFireアプライアンスのリソースを使用して、ドキュメント（Microsoft OfficeファイルとPDF）またはPEの特定のファイルの種類を解析できます。たとえば、WildFireハイブリッドクラウドを展開してドキュメントをローカルに分析し、WildFireパブリック クラウドの 1 つに含まれる PE を分析する場合、すべての解析環境をドキュメント専用にできます。これにより、PEの解析をパブリッククラウドにオフロードでき、機密ドキュメントを処理するために追加のWildFireアプライアンスリソースを割り当てることができます。

開始する前に：

- ❑ ファイルを転送するように構成しているファイアウォールとWildFireクラウドまたはWildFireアプライアンスの間に別のファイアウォールが存在する場合は、そのファイアウォールで次のポートが許可されていることを確認してください:

ポート	使用率
443	• 登録 • PCAP ダウンロード

ポート	使用率
	• 検体ダウンロード • HIP レポートの取得 • ファイル送信 • PDFレポートのダウンロード
10443	ダイナミック更新

STEP 1 | (PA-7000シリーズ ファイアウォールのみ)PA-7000 シリーズ ファイアウォールで WildFire 解析用のサンプルを転送できるようにするには、まず をログ カード インターフェイス として NPC のデータ ポートを設定する必要があります。LFC(ログ転送カード)を装備したPA-7000シリーズアプライアンスを使用している場合は、LFC で使用されるポートをに設定する必要があります。設定すると、WildFire サンプルを転送する際に、ログ カード ポートまたは LFC インターフェイスが管理ポートよりも優先されます。

STEP 2 | サンプルの転送先となる WildFire プライベート クラウドまたはハイブリッド クラウドを指定します。

デバイス > セットアップ > **WildFire**を選択して、ご利用のWildFireクラウドデプロイメント（プライベートまたはハイブリッド）に基づき一般設定を編集します。

WildFire Private Cloud（**WildFire** プライベート クラウド）

1. **WildFire Private Cloud**（**WildFire**プライベートクラウド）フィールドで、WildFireアプライアンスのIPアドレスとFQDNを入力します。

WildFireハイブリッドクラウド

1. **WildFire**パブリック クラウド URL を入力します:
   - 米国: **wildfire.paloaltonetworks.com**
   - ヨーロッパ: **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**
   - 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: **kr.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**
2. **WildFire Private Cloud**（**WildFire**プライベートクラウド）フィールドで、WildFireアプライアンスのIPアドレスとFQDNを入力します。

STEP 3 | ファイアウォールが転送するファイルのサイズ制限を定義し、WildFireのログとレポートの設定を構成します。

WildFire一般設定の編集を続行します (デバイス > セットアップ > **WildFire**)。

- ファイアウォールから転送されるファイルの ファイル サイズ制限 を確認します。

  PE の ファイル サイズ を最大サイズ制限の *10 MB* に設定し、他のすべての ファイル タイプについては <ファイル サイズ> を既定値に設定したままにすることは、 推奨される WildFireのベスト プラクティスです です。

- **Report Benign Files**（安全なファイルのレポート）を選択して、安全であるとWildFire判定を受けるファイルのロギングを許可します。
- **Report Grayware Files**（レポートのグレイウェア ファイル）を選択して、グレイウェアであるとWildFire判定を受けるファイルのロギングを許可します。
- セッション情報設定を編集して、WildFire分析レポートに記録するセッション情報を定義します。デフォルトでは、すべてのセッション情報がWildFire分析レポートに表示されます。チェックボックスをオフにして対応するフィールドをWildFire分析レポートから削除し、 **OK** をクリックして設定を保存します。

STEP 4 | （Panorama専用） PAN-OS 7.0より前のPAN-OSバージョンを実行しているファイアウォールから収集された検体に関する追加情報を収集するようにPanoramaを設定します。

PAN-OS 7.0で導入された一部のWildFire送信ログフィールドは、以前のソフトウェアバージョンを実行しているファイアウォールによって送信された検体では入力されません。Panoramaを使用してPAN-OS 7.0より前のソフトウェアバージョンを実行しているファイアウォールを管理している場合、PanoramaはWildFireと通信して、定義された**WildFire**サーバー（デフォルトではWildFireグローバルクラウド）からこれらのファイアウォールによって送信されたサンプルの完全な解析情報を収集でき、ログの詳細を完了します。

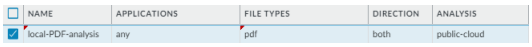
デフォルト設定を変更して、代わりにPanoramaが指定のWildFireクラウドまたはWildFireアプライアンスから詳細情報を収集することを許可するには、**Panorama** > **Setup**（セットアップ） > **WildFire**を選択し、**WildFire Server**（**WildFire**サーバー）を入力します。

STEP 5 | WildFireに転送し分析するトラフィックを定義します。

*WildFire*アプライアンをセットアップする場合は、ハイブリッドクラウドの導入において、プライベートクラウドとパブリッククラウドの両方を使用することができます。機密ファイルをネットワーク上でローカルに分析し、他のすべての不明なファイルを*WildFire*パブリッククラウドに送信して、包括的な解析と迅速な判定を行います。

1. **Objects**（オブジェクト）> **Security Profiles**（セキュリティプロファイル）> **WildFire Analysis**（**WildFire**分析）を選択して、新しいWWildFire分析プロファイルを追加するとともに、そのプロファイルに説明用の名称を記入します。
2. 解析用に転送されるトラフィックを定義するためにプロファイルのルールを追加し、そのルールに名前を付けます（例：local-PDF-analysis）。
3. 不明なトラフィックと一致させ、以下の解析ベース用に検体を転送するために、プロファイルのルールを定義します。
   - アプリケーション—使用中のアプリケーションを基準にした解析用にファイルを転送します。
   - ファイルの種類—電子メール内に含まれるリンクを含む、ファイルの種類を基準にした解析用にファイルを転送します。例えば、解析用ファイアウォールで検出された不明なPDFを転送するには、**PDF**を選択します。
   - 方向—ファイルの送信方向（アップロード、ダウンロード、またはその両方）に基づいて解析のためにファイルを転送します。例えば、送信方向に関係なく、すべての不明なPDFを解析のために転送するには、両方を選択します。
4. ファイアウォールがルールに一致するファイルを転送する解析ロケーションを設定します。
   - 一致する検体を解析のためにWildFireパブリッククラウドに転送するには、パブリッククラウドを選択します。
   - 一致する検体を解析のためにWildFireプライベートクラウドに転送するには、プライベートクラウドを選択します。

     たとえば、ネットワークからこれらのドキュメントを送信せずに機密情報や専有情報を含む可能性のあるPDFを解析するには、ルール「local-PDF-analysis」の解析ロケーションをプライベートクラウドに設定します。



ニーズに応じて、異なるルールが一致した検体を異なる解析ロケーションに転送できます。上記の例は、*WildFire*プライベートクラウドでローカル解析のために機密ファイルタイプを転送するルールを示しています。*PE*などの機密性の低いファイルの種類を*WildFire*パブリッククラウドに転送する別のルールを作成できます。この柔軟性は、WildFireハイブリッドクラウドの導入でサポートされます。

ハイブリッドクラウドの導入では、プライベートクラウドとパブリッククラウドの両方のルールに一致するファイルは、予備手段としてプライベートクラウドにのみ転送されます。

5. （オプション）必要に応じて、引き続きWildFire分析プロファイルにルールを追加します。たとえば、プロファイルに2つ目のルールを追加して、Androidアプリケーションパッケージ（APK）、Portable Executable(ポータブル実行可能（PE）)ファイル、およびFlashファイルを解析のためにWildFireパブリッククラウドに転送できます。
6. **OK**をクリックすると、WildFire分析プロファイルを保存します。
7. （オプション）必要に応じて、引き続きWildFire分析プロファイルにルールを追加します。たとえば、プロファイルに2つ目のルールを追加して、Androidアプリケーションパッケージ（APK）、Portable Executable(ポータブル実行可能（PE）)ファイル、およびFlashファイルを解析のためにWildFireパブリッククラウドに転送できます。
8. **OK**をクリックすると、WildFire分析プロファイルを保存します。

STEP 6 | （オプション）WildFireアプライアンスのリソースを割り当てて、ドキュメントまたは実行可能ファイルのいずれかを解析します。

ハイブリッド クラウドを展開して、特定のファイルの種類をローカルおよび *WildFire* パブリック クラウドで分析する場合は、解析環境を専用にしてファイルタイプを処理できます。これにより、解析環境の構成に応じてリソースを適切に割り当てることができます。リソースを解析環境専用にしない場合、リソースはデフォルト設定を使用して割り当てられます。

以下の CLI コマンドを実行します。

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

次に、以下のいずれかのオプションを選択します:

- ドキュメント — 25のドキュメント、1つのPE、2つの電子メールリンクを同時に解析する専用解析リソース。
- 実行可能—25のPE、1つのドキュメント、2つの電子メールリンクを同時に解析する専用解析リソース。
- default（デフォルト）のオプションでは、16個のドキュメント、10個の実行可能ファイル（PE）、2個の電子メールリンクを同時に分析します。

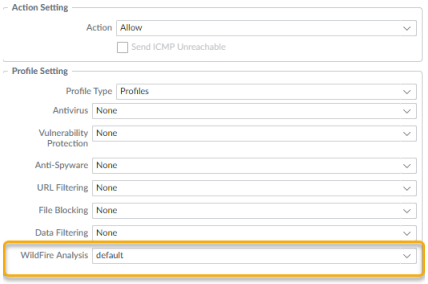
すべてのWildFireアプライアンスのプロセスが、次のコマンドで実行中であることを確認します:

```
admin@WF-500> show system software status
```

STEP 7 | WildFire 分析プロファイルをセキュリティ ポリシー ルールにアタッチします。

セキュリティ ポリシー ルールによって許可されるトラフィックは、添付のWildFire分析プロファイルに対して評価されます。ファイアウォールは、WildFire分析用プロファイルに一致するトラフィックを転送します。

1. **[Policies]** > > **[**セキュリティ**]** の順に選択して、セキュリティ ポリシー ルールを **[**追加**]** または変更します。
2. セキュリティ ポリシー内の **[**アクション**]** タブをクリックします。
3. Profile Settings（プロファイル設定）セクションで、**Profiles**（プロファイル）を**Profile Type**（プロファイルの種類）として選択し、**WildFire Analysis**（**WildFire**分析）プロファイルを選択して、ポリシールールを添付します



STEP 8 | ファイアウォールがWildFire分析のために 復号されたSSLトラフィックを転送できるようにします。

これはrecommended WildFire best practice（WildFire推奨のベストプラクティス）です。

STEP 9 | WildFire Best Practices（WildFireのベストプラクティス）を確認して実装します。

STEP 10 | **Commit**（コミット）をクリックしてWildFire設定を適用します。

STEP 11 | (オプション)WildFire の送信を確認します。

STEP 12 | 次の操作を選択します...

- ファイアウォールがファイルをWildFire分析用に正常に転送することを確認するために、WildFireの送信を検証します。
- WildFireアプライアンスからマルウェアやレポートを送信します。この機能を有効にして、WildFireプライベートクラウドで識別されたマルウェアを自動的にWildFireパブリッククラウドに転送します。WildFireパブリッククラウドは検体を再分析し、検体がマルウェアの場合はシグネチャを生成します。このシグネチャは、WildFireシグネチャ更新を通じてグローバルユーザーに配布されます。
- WildFire アプライアンスのアクティビティを監視する マルウェアに関して報告されたアラートと詳細を評価します。

WildFireアプライアンスからマルウェアやレポートを送信する

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

WildFireアプライアンスのクラウド インテリジェンス機能を有効化し、WildFireプライベート クラウド内で検出されたマルウェアのサンプルを自動的に送信するように設定します。WildFireパブリック クラウドはサンプルを更に分析し、今後サンプルを特定できるようにシグネチャを生成します。このシグネチャはWildFireシグネチャに追加され、世界中に配信されてユーザーをマルウェアから保護します。自分のネットワーク上で発見されたマルウェアのサンプルをネットワーク外へ転送したくない場合は、マルウェアに関するWildFireレポートのみを送信することでWildFireの統計情報と脅威インテリジェンスの拡充に役立てることができます。

マルウェアをWildFireパブリック クラウドへ送信する

WildFireアプライアンスからWildFireパブリック クラウドへマルウェアサンプルを自動送信する場合は、WildFireアプライアンスで以下のCLIコマンドを実行します。

```
admin@WF-500admin@WF-500# set deviceconfig setting wildfire cloud-intelligence submit-sample yes
```

*WildFire*プライベート クラウドへサンプルを最初に送信したファイアウォール上でパケットキャプチャ（*PCAP*）が有効になっている場合、そのマルウェアに対する*PCAP*も同じく*WildFire*パブリック クラウドへ転送されます。

マルウェアレポートをWildFireパブリック クラウドへ送信する

*WildFire*アプライアンスがSubmit Malware to the WildFire Public Cloud（WildFireパブリッククラウドにマルウェアを送信）するように設定されている場合、アプライアンスがパブリッククラウドにマルウェアレポートを送信するようにする必要もありません。マルウェアが*WildFire*パブリック クラウドへ送信されると、パブリック クラウドはそのサンプルに対して新規のマルウェアレポートを生成します。

WildFireアプライアンスからWildFireパブリック クラウドへ（マルウェア サンプルではなく）マルウェアレポートを自動的に送信できるようにするには、WildFireアプライアンスで以下のCLIコマンドを実行してください。

```
admin@WF-500# set deviceconfig setting wildfire cloud-intelligence
 submit-report yes
```

クラウド インテリジェンスの設定を検証する

以下のコマンドを実行して、クラウド インテリジェンスが有効化され、WildFireパブリック クラウドに向けたマルウェアの送信またはマルウェアレポートの送信が実行されていることを確認します。

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

`Submit sample`（サンプル送信）と`Submit report`（レポート送信）のフィールドを参照してください。

スタンドアロン WildFire アプライアンスでカスタム証明書を使用する認証のセットアップ

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

デフォルトでは、WildFire アプライアンスは管理アクセスおよびデバイス間通信に使用される SSL 接続を確立するための相互認証に事前定義済みの証明書を使用します。ただし、代わりにカスタム証明書を使用して認証を設定することもできます。カスタム証明書を使用すれば、WildFire アプライアンスおよびファイアウォールまたは Panorama 間の相互認証を確認する固有の信頼チェーンを確立できます。Panorama またはファイアウォールでこれらの証明書をローカルに生成したり、信頼できるサードパーティ認証局（CA）から取得したり、エンタープライズ秘密鍵インフラストラクチャ（PKI）から証明書を取得することができます。

次のトピックでは、Panorama で管理されていないスタンドアロン WildFire アプライアンスを設定する方法について説明します。WildFire アプライアンスと Panorama で管理する WildFire クラスタのカスタム証明書を設定する場合は、Panorama 管理者ガイドを参照してください。

- WildFire アプライアンスの SSL 相互認証
- WildFire アプライアンス上のカスタム証明書で認証を設定する

WildFire アプライアンスの SSL 相互認証

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

ファイアウォールまたは Panorama が分析のために WildFire アプライアンスにサンプルを送信すると、ファイアウォールはクライアントとして機能し、WildFire アプライアンスはサーバーとして機能します。相互に認証するために、各デバイスは、デバイス自体を他のデバイスに識別させるための証明書を提示します。

デプロイ環境で相互認証のカスタム証明書をデプロイするには、次のものが必要となります。

- **SSL/TLS** サービス プロファイル — SSL/TLS サービス プロファイルでは、カスタム証明書を参照し、サーバー デバイスがクライアント デバイスと通信するために使用する SSL/TLS プロトコル バージョンを確立することによって、接続のセキュリティを定義します。
- サーバー証明書およびプロファイル—WildFire アプライアンスには、ファイアウォールを識別するための証明書と証明書プロファイルが必要です。この証明書は、会社の公開鍵基盤（PKI）からデプロイするか、信頼できるサードパーティ CA から購入するか、自己署名証

明書をローカルで生成することができます。サーバー証明書の証明書共通名（CN）またはサブジェクト代替名には、WildFire アプライアンスの管理インターフェイスの IP アドレスか FQDN を含める必要があります。ファイアウォールまたは、サーバーが提示する証明書の CN またはサブジェクト代替名を WildFire アプライアンスの IP アドレスまたは FQDN と照合し、WildFire アプライアンス のアイデンティティを確認します。

証明書の失効状態（OCSP/CRL）および失効状態に基づいて取るアクションを定義するには、証明書プロファイルを使用します。

- クライアントの証明書とプロファイル — 各ファイアウォールには、クライアント証明書と証明書プロファイルが必要です。クライアント デバイスは、その証明書を使用して、サーバー デバイスに対して自身を識別します。証明書は、SCEP（Simple Certificate Enrollment Protocol）を使用して会社の PKI からデプロイするか、信頼できるサードパーティ CA から購入するか、自己署名証明書をローカルで生成することができます。

  カスタム証明書は、各クライアント デバイスで固有にするか、すべてのデバイスで共通にすることができます。固有のデバイス証明書では、管理対象デバイスのシリアル番号と CN のハッシュが使用されます。サーバーは、CN またはサブジェクト代替名を管理対象デバイスで設定されているシリアル番号と照合します。クライアント証明書を CN に基づいて検証するには、ユーザー名をサブジェクト共通名に設定する必要があります。

WildFire アプライアンス上のカスタム証明書で認証を設定する

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

次のワークフローを使用して、事前定義された証明書を WildFire デプロイメントのカスタム証明書に置き換えます。ファイアウォールまたは Panorama が分析のために WildFire アプライアンスにサンプルを送信すると、ファイアウォールはクライアントとして機能し、WildFire アプライアンスはサーバーとして機能します。

STEP 1 | WildFire アプライアンス、ファイアウォール、または Panorama のキーペアと認証局（CA）証明書を取得します。

STEP 2 | ファイアウォールの証明書を検証するために CA 証明書をインポートします。

1. WildFire アプライアンスで CLI にログインし、設定モードを開始します。

   ```
   admin@WF-500> configure
   ```

2. TFTP または SCP を使用して証明書をインポートします。

   ```
   admin@WF-500#{tftp | scp} import certificate from <value>
    file <value> remote-port <1-65535> source-ip <ip/netmask>
   ```

```
certificate-name <value> passphrase <value> format {pkcs12 |
pem}
```

STEP 3 | TFTP または SCP を使用して、WildFire アプライアンスのサーバー証明書と秘密鍵を含むキーペアをインポートします。

```
admin@WF-500# {tftp | scp} import keypair from<value> file <value>
 remote-port <1-65535> source-ip <ip/netmask> certificate-
name <value> passphrase <value> format {pkcs12 | pem}
```

STEP 4 | ルート CA および中間 CA が含まれる証明書プロファイルを設定します。この証明書プロファイルは、WildFire アプライアンスとファイアウォールの相互認証方法を定義します。

1. WildFire アプライアンスの CLI にログインし、設定モードを開始します。

   ```
   admin@WF-500> configure
   ```

2. 証明書プロファイルに名前を付けます。

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

3. CA を設定します。

   コマンド *default-ocsp-url* および *ocsp-verify-cert* はオプションです。

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

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

   ```
   admin@WF-500# set shared certificate-profile <name> CA <name>
    [ocsp-verify-cert <value>]
   ```

STEP 5 | WildFire アプライアンスの SSL/TLS プロファイルを設定します。このプロファイルは、WildFire アプライアンスとファイアウォールが SSL/TLS サービスに使用する証明書と SSL/TLSプロトコルの範囲を定義します。

1. SSL/TLS プロファイルを識別します。

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

2. 証明書を選択します。

```
admin@WF-500# set shared ssl-tls-service-profile <name>
 certificate <value>
```

3. SSL/TLS 範囲を定義します。

> *PAN-OS 8.0* 以降のリリースでは、*TLS 1.2* 以降の *TLS* バージョンのみがサポートされています。最大バージョンを *TLS 1.2* または最大に設定する必要があります。

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

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

STEP 6 | WildFire アプライアンスでセキュア サーバー通信を設定します。

1. SSL/TLS プロファイルを設定します。この SSL/TLS サービス プロファイルは、WildFire とクライアント デバイス間のすべての SSL 接続に適用されます。

```
admin@WF-500# set deviceconfig setting management secure-conn-
server ssl-tls-service-profile <ssltls-profile>
```

2. 証明書プロファイルを設定します。

```
admin@WF-500# set deviceconfig setting management secure-conn-
server certificate-profile <certificate-profile>
```

WildFire アプライアンスVMインターフェイスを設定

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

仮想マシン インターフェイス（VM インターフェイス）を使用すると、WildFire アプライアンス上のサンドボックス仮想マシンから外部ネットワークへの接続を確立して、分析対象のファイルがネットワークへのアクセス経路を探索するような有害な動作をしていないか監視できます。以下の各セクションでは、VM インターフェイスと、その設定に必要な手順について説明します。VM インターフェイスでは、Tor 機能を有効にして、VM インターフェイス経由でWildFireアプライアンスから送信される有害なトラフィックをマスキングできます（任意）。これにより、トラフィックの送信先となる可能性のあるマルウェア サイトによって、パブリック空間に接するユーザー側の IP アドレスが検出されるのを防ぐことができます。

このセクションでは、VM インターフェイスを Palo Alto Networks ファイアウォールの専用ポートに接続して、インターネット接続を可能にするために必要な手順についても説明します。

- 仮想マシン インターフェイスの概要
- WildFire アプライアンスの VM インターフェイスの設定
- ファイアウォールをWildFire のVMインターフェイスに接続する

仮想マシン インターフェイスの概要

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

VM インターフェイス（アプライアンス背面の **1** というラベルの付いたインターフェイス）は、マルウェア検出機能を強化するために WildFire で使用されます。このインターフェイスにより、WildFire 仮想マシンで実行するファイル サンプルがインターネットと通信できるため、WildFireアプライアンスはサンプル ファイルの動作をより的確に分析して、マルウェアの特性を示すかどうかを判別できます。

- *VM* インターフェイスは有効にすることをお勧めしますが、自社環境のサーバーやホストにアクセス可能なネットワークにこのインターフェイスを決して接続しないでください。*WildFire* 仮想マシンで動作しているマルウェアがこのインターフェイスを使用してサーバーやホストに感染するおそれがあります。
- *VM* インターフェイスには、専用の *DSL* 線を接続するか、*VM* インターフェイスからインターネットへの直接アクセスのみを許可して、内部のサーバー/クライアント ホストへのアクセスをすべて制限するネットワークを接続します。
- *FIPS/CC*モードで運用中の*WildFire*アプライアンスでは、*VM*インターフェースは無効です。

以下の図は、VM インターフェイスからネットワークに接続するための 2 つのオプションを示しています。

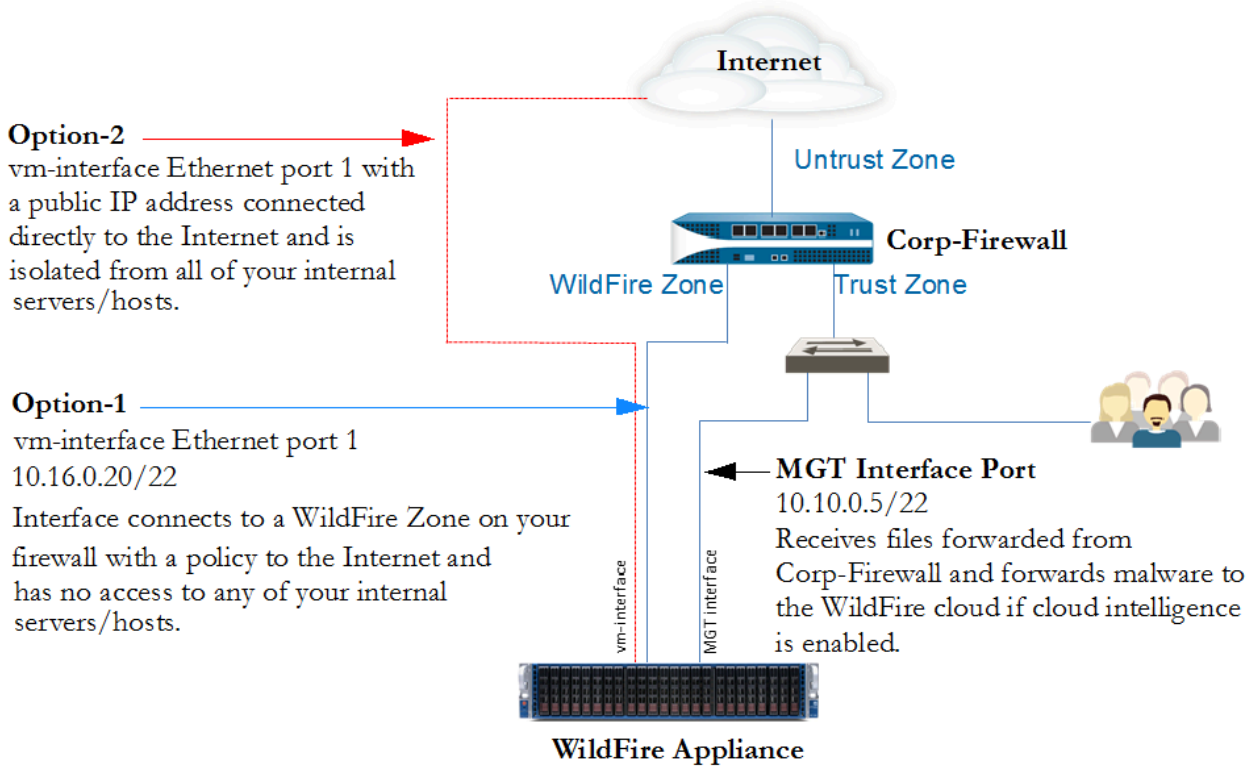


図 **1 :** 仮想マシン インターフェイスの例

- オプション **1**（推奨） — VM インターフェイスを、インターネットへのアクセスのみを許可するポリシーが定義されたファイアウォール上の専用ゾーンのインターフェイスに接続します。WildFire 仮想マシンで実行されるマルウェアが、このインターフェイスを使用して感染するおそれがあるため、これは重要です。VM インターフェイスによって生成されたすべてのトラフィックをファイアウォールのログで確認できるため、このオプションをお勧めします。
- オプション **2** — DSL 接続などの専用インターネット プロバイダー接続を使用し、VM インターフェイスをインターネットに接続します。この接続から内部のサーバー/ホストにアクセスすることがないようにします。これは簡易な方法ですが、マルウェアによって生成され VM インターフェイスから送出されるトラフィックをログに記録するには、WildFire アプライアンスと DSL 接続の間にファイアウォールまたはトラフィック モニタリング ツールを設置する必要があります。

WildFire アプライアンスの VM インターフェイスの設定

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

このセクションでは、Virtual Machine Interface Example（バーチャルマシーンインターフェースの例）で説明したオプション1の設定を使用して、WildFireアプライアンスでVMインターフェイスを設定するために必要な手順について説明します。このオプションを使用してVMインタフェースを設定した後、Palo Alto Networksファイアウォールのインタフェースを設定して、Connect the Firewall to the WildFire Appliance VM Interface（ファイアウォールをWildFireアプライアンスVMインタフェースに接続する）の説明に従って、VMインタフェースからのトラフィックをルーティングする必要があります。

VM インターフェイスのデフォルトの設定値は以下のとおりです。

- IPアドレス:192.168.2.1
- ネットマスク：255.255.255.0
- デフォルトゲートウェイ:192.168.2.254
- DNS：192.168.2.254

このインターフェイスを有効にする予定がある場合は、ネットワークに適した設定値を使用して設定します。このインターフェイスを使用する予定がない場合は、デフォルト設定値のままにします。このインターフェイスには、ネットワーク値を設定しておく必要があります。ネットワーク値がないとコミット エラーが発生します。

STEP 1 | WildFire アプライアンスの VM インターフェイスの IP 情報を設定します。この例では以下の IPv4 値が使用されていますが、アプライアンスは IPv6 アドレスもサポートしています。

- IP Address (IP アドレス) - 10.16.0.20/22
- サブネット マスク - 255.255.252.0
- デフォルト ゲートウェイ - 10.16.0.1
- DNS サーバー - 10.0.0.246

VM インターフェイスを管理インターフェイス（*MGT*）と同一ネットワーク上に置くことはできません。

1. 設定モードに切り替えます。

```
admin@WF-500> configure
```

2. VM インターフェイスの IP 情報を設定します。

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

VM インターフェイスに設定できる *DNS* サーバーは *1* つだけです。ベスト プラクティスとして、お使いの *ISP* の *DNS* サーバーか、オープン *DNS* サービスを使用します。

STEP 2 | VM インターフェイスを有効にします。

1. VM インターフェイスを有効にします。

```
admin @ WF-500#set deviceconfig settings wildfire vm-network-
enable yes
```

2. 設定をコミットします：

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

STEP 3 | VM インターフェイスの接続をテストします。

システムに Ping を送信し、VM インターフェイスを送信元として指定します。たとえば、VM インターフェイスの IP アドレスが 10.16.0.20 の場合は、以下のコマンドを実行しま

す。ここで、*ip-or-hostname* は、Ping が有効になっているサーバー/ネットワークの IP またはホスト名です。

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

以下に例を示します。

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

STEP 4 | （オプション）マルウェアが生成した悪意あるトラフィックの全てをインターネットに送信します。Torネットワークはパブリックipアドレスをマスクしているため、悪質なサイトの所有者はトラフィックの送信元を特定できません。

1. Tor ネットワークを有効にします。

   ```
   admin @ WF-500#set deviceconfig settings wildfire vm-network-use-tor
   ```

2. 設定をコミットします：

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

STEP 5 | (オプション) Tor ネットワーク接続が有効であり正常であることを確認します。

1. アプライアンスのログ内の Tor イベント ID を検索するには、次の CLI コマンドを発行します。適切に設定された運用 WildFire アプライアンスは、イベント ID を生成しないようになっています:

   - **admin@WF-500(active-controller)>showlog system direction equal backward | match anonymous-network-unhealthy**—Tor サービスが停止しているか、運用休止状態です。Tor サービスを再起動して、適切に稼働していることを確認することを検討してください。
   - **admin@WF-500(active-controller)>show log systemdirection equal backward | match anonymous-network-unavailable**—Tor サービスは正常に動作していますが、WildFire アプライアンス VM インターフェースは接続を確立できません。ネットワークの接続状態と設定を確認してから、再試行してください。

STEP 6 | Connect the Firewall to the WildFire Appliance VM Interface（ファイアウォールをWildFireのVMインターフェイスに接続する]。

ファイアウォールをWildFire のVMインターフェイスに接続する

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

以下のワークフロー例では、VM インターフェイスを Palo Alto Networks ファイアウォール上のポートに接続する方法について説明します。VM インターフェイスをファイアウォールに接続する前に、ファイアウォール側で Untrust ゾーンをインターネットに接続しておく必要があります。この例では、アプライアンス上の VM インターフェイスをファイアウォールに接続するために使用するインターフェイスを含む、「wf-vm-zone」という名前の新しいゾーンを設定しています。wf-vm-zone に関連付けられたポリシーでは、VM インターフェイスから Untrust ゾーンへの通信のみが許可されます。

STEP 1 | ファイアウォール上に VM インターフェイスの接続先となるインターフェイスを設定し、仮想ルーターを設定します。

wf-vm-zone には、アプライアンス上の *VM* インターフェイスをファイアウォールに接続するために使用するインターフェイス（この例では *ethernet1/3*）だけを含める必要があります。これは、マルウェアによって生成されたトラフィックが他のネットワークに到達するのを防ぐための措置です。

1. ファイアウォールのWebインターフェイスから**Network**（ネットワーク） > **Interfaces**（インターフェース）を選択し、**Ethernet1/3**（イーサネット**1/3**）などのインターフェイスを選択します。
2. **Interface Type**（インターフェイス タイプ） ドロップダウン リストで、**Layer3**（レイヤー **3**） を選択します。
3. **Config**（設定）タブの**Security Zone** （セキュリティゾーン）ドロップダウンボックスから **New Zone**（新規ゾーン）を選択します。
4. Zone （ゾーン） ダイアログの **Name**（名前）フィールドに「wf-vm-zone」と入力し、**OK** をクリックします。
5. **Virtual Router**（仮想ルーター）ドロップダウンリストから**default** （デフォルト） を選択します。
6. インターフェイスに IP アドレスを割り当てるには、 **IPv4** または **IPv6** タブを選択し、[IP] セクションで**Add**（追加） をクリックし、インターフェイスに割り当てる IP アドレスとネットワーク マスク（例：10.16.0.0/22 (IPv4) または 2001:db8:123:1::1/64 (IPv6)）を入力します。
7. インターフェイス設定を保存するには、**OK** をクリックします。

STEP 2 | ファイアウォール上に、VM インターフェイスからインターネットへのアクセスを許可し、すべての受信トラフィックをブロックするセキュリティ ポリシーを作成します。この例で

のポリシー名は「WildFire VM Interface」です。ここでは Untrust ゾーンから wf-vm-interface ゾーンへのセキュリティ ポリシーは作成しないため、すべての受信トラフィックはデフォルトでブロックされます。

1. **[Policies]** > **[**セキュリティ**]** の順に選択し、**[**追加**]** をクリックします。
2. **General**（全般）タブの **Name**（名前）フィールドに名前を入力します。
3. **Source**（送信元）タブで **Source Zone**（送信元ゾーン）を**wf-vm-zone**に設定します。
4. **Destination** （宛先）タブで **Destination Zone**（宛先ゾーン） を**Untrust**（アントラスト）に設定します。
5. **Application**（アプリケーション） タブおよび **Service/URL Category** （サービス/**URL** カテゴリ） タブでは、デフォルトの **Any** （いずれか） のままにします。
6. **Actions** （アクション）タブで、**Action Setting**（アクション設定）を**Allow**（許可）に設定します。
7. **Log Setting** （ログ設定） の中から、**Log at Session End**（セッション終了時にログ） のチェックボックスを選択します。

   他のユーザーが不注意から別のインターフェイスを *wf-vm-zone* に追加する可能性がある場合は、*WildFire VM Interface* のセキュリティ ポリシーをコピーし、コピーしたルールの ***Action***（アクション）タブで ***Deny***（拒否）を選択します。この新しいセキュリティ ポリシーが、*WildFire VM Interface* ポリシーの下に表示されることを確認します。これにより、同じゾーン内にあるインターフェイス間の通信を許可する暗黙的なゾーン内許可ルールがオーバーライドされ、すべてのゾーン内通信が拒否/ブロックされます。

STEP 3 | ケーブルを接続します。

ストレート スルー RJ-45 ケーブルを使用して、WildFire アプライアンス上の VM インターフェイスを、ファイアウォール上に設定したポート（この例では Ethernet 1/3）に物理的に接続します。VM インターフェイスはアプライアンスの背面にあり、**1**とラベルが付けられています。

WildFire アプライアンス分析機能の開始

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

- WildFire アプライアンスコンテンツ更新の設定
- ローカルシグネチャおよびURLカテゴリ生成を有効にする
- ローカルで検出されたマルウェアまたはレポートをパブリッククラウドに提出する

WildFire アプライアンスコンテンツ更新の設定

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

WildFire アプライアンスで毎日のコンテンツ更新を設定します。WildFire のコンテンツ更新によりマルウェアを正確に検出できるようになり、安全なサンプルと有害なサンプルを区別するアプライアンスの機能が向上するとともに、シグネチャ生成に必要な最新情報をアプライアンスに提供することができます。

- 更新サーバーから直接WildFireの更新コンテンツをインストールする
- SCP対応サーバーからWildFire の更新コンテンツをインストールする

更新サーバーから直接**WildFire**の更新コンテンツをインストールする

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

STEP 1 | アプライアンスから更新サーバーへの接続を確認して、インストールするコンテンツ更新を特定します。

1. WildFire アプライアンスにログインし、以下のコマンドを実行して現在のコンテンツのバージョンを表示します。

```
admin@WF-500> show system info | match wf-content-version
```

2. アプライアンスが Palo Alto Networks 更新サーバーと通信して、利用可能な更新を表示できることを確認します。

```
admin@WF-500> request wf-content upgrade check
```

このコマンドは、Palo Alto Networks 更新サーバーにクエリを発行して利用可能な更新に関する情報を提供し、アプライアンスに現在インストールされているバージョンを識別します。

```
Version Size  Released on      Downloaded Installed
 ---------------------------------------------------
 2-253   57MB 2014/09/20 20:00:08 PDT no         no 2-39
 44MB 2014/02/12 14:04:27 PST yes     current
```

アプライアンスが更新サーバーに接続できない場合は、アプライアンスからPalo Alto Networks 更新サーバー(updates.paloaltonetworks.com)への接続を許可するか、SCP対応サーバーからのWildFireコンテンツ更新のインストールの説明に従って、SCP を使用して更新をダウンロードおよびインストールする必要があります。

STEP 2 | 最新のコンテンツ更新をダウンロードおよびインストールします。

1. 最新のコンテンツ更新をダウンロードします。

```
admin@WF-500> request wf-content upgrade download latest
```

2. ダウンロードの状態を確認します。

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

show jobs pending（待機中のジョブを表示） を実行すると、保留中のジョブが表示されます。以下の出力は、ダウンロード（ジョブ ID: 5）によってダウンロード処理が完了した（Status（状態）: FIN（終了））ことを示しています。

```
Enqueued           ID  Type Status Result Completed
 ---------------------------------------------------
 2014/04/22 03:42:20  5  Downld  FIN   OK   03:42:23
```

3. ダウンロードが完了したら、更新をインストールします。

```
admin@WF-500> request wf-content upgrade install version
 latest
```

show jobs all（すべてのジョブを表示） コマンドを再度実行して、インストールの状態をモニターします。

STEP 3 | コンテンツ更新を確認します。

以下のコマンドを実行し、wf-content-version フィールドを参照します。

```
admin@WF-500> show system info
```

以下の出力例は、コンテンツ更新バージョン 2-253 がインストールされたことを示しています。

```
admin@WF-500> システム情報を表示 ホスト名:WildFire ip-
address:10.5.164.245 netmask:255.255.255.0 default-
gateway:10.5.164.1 mac-address:00:25:90:c3:ed:56 vm-interface-
ip-address:192.168.2.2 vm-interface-netmask:255.255.255.0
 vm-interface-default-gateway：192.168.2.1 vm-interface-dns-
server：192.168.2.1 time:Mon Apr 21 09:59:07 2014 uptime:17
 days, 23:19:16 family: m model:WildFire serial: abcd3333 sw-
version:6.1.0 wf-content-version:2-253 wfm-release-date:2014/08/20
 20:00:08 logdb-version:6.1.2 platform-family: m
```

STEP 4 | （オプション）更新コンテンツを毎日、あるいは毎週インストールするよう設定します。

1. アプライアンスに対してコンテンツ更新をダウンロードおよびインストールするようにスケジュールします。

```
admin@WF-500# set deviceconfig system update-schedule wf-
content recurring [daily | weekly] action [download-and-
install | download-only]
```

たとえば、更新を毎日午前 8:00 にダウンロードおよびインストールするには、以下のコマンドを入力します。

```
admin@WF-500# set deviceconfig system update-schedule wf-
content recurring daily action download-and-install at 08:00
```

2. 設定をコミットします。

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

SCP対応サーバーからWildFire の更新コンテンツをインストールする

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

以下の手順では、Palo Alto Networks 更新サーバーに直接接続されていないWildFire アプライアンスにコンテンツ更新をインストールする方法について説明します。コンテンツ更新を一時的に格納するためのSCP（セキュアコピー）対応サーバーが必要です。

STEP 1 | 更新サーバーからコンテンツ更新ファイルを取得します。

1. Palo Alto Networks Support Portalにログインし、**Dynamic Updates (**動的更新**)**をクリックします。
2. WildFire Appliance（WildFire アプライアンス）セクションで、最新の WildFire アプライアンス コンテンツ更新を探して、ダウンロードします。
3. コンテンツ更新ファイルを SCP 対応サーバーにコピーして、ファイル名とディレクトリ パスをメモします。

STEP 2 | WildFire アプライアンスのコンテンツ更新をインストールします。

1. WildFire アプライアンスにログインし、SCP サーバーからコンテンツ更新ファイルをダウンロードします。

   ```
   admin @ WF-500>scp import wf-content from username @ host：path
   ```

   以下に例を示します。

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

   SCP サーバーが標準以外のポートで実行されている場合、または送信元*IP*を指定する必要がある場合は、それらのオプションを ***scp import*** コマンドで定義することもできます。

2. 更新をインストールします。

   ```
   admin@WF-500> request wf-content upgrade install file panup-
   all-wfmeta-2-253.tgz
   ```

3. インストールの状態を表示します。

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

STEP 3 | コンテンツ更新を確認します。

コンテンツ バージョンを確認します。

```
admin@WF-500> show system info | match wf-content-version
```

以下の出力ではバージョン 2～253 が示されています。

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

ローカルシグネチャおよびURLカテゴリ生成を有効にする

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

WildFireアプライアンスは、マルウェアをパブリッククラウドに送信してシグネチャを生成する代わりに、接続されたファイアウォールやWildFire APIから受信したサンプルに基づいてローカルでシグネチャを生成できます。アプライアンスは以下のタイプのシグネチャを生成し、ファイ

アウォールがマルウェアやそれに関連したコマンドをブロックしてトラフィックを制御できるようにします。

- **Antivirus signatures**（アンチウイルス シグネチャ）— 有害なファイルを検出してブロックします。WildFire はこれらのシグネチャを WildFire およびアンチウイルス コンテンツ更新に追加します。
- **DNS signatures**（DNS シグネチャ）— マルウェアに関連付けられたコマンド アンド コントロール トラフィックのコールバック ドメインを検出およびブロックします。WildFire はこれらのシグネチャを WildFire およびアンチウイルス コンテンツ更新に追加します。
- **URL categories**（URL カテゴリ）— コールバック ドメインをマルウェアとして分類し、PAN-DBのURLカテゴリを更新します。

Wildfireアプライアンスで生成されたシグネチャを5分ごとに取得するようにファイアウォールを設定します。マルウェアのサンプルをWildFireパブリッククラウドに送信し、生成されたシグネチャをPalo Alto Networksのコンテンツリリースに乗せて世界中に配信されるように設定することも可能です。

*WildFire*アプライアンスでローカルファイルを分析する場合でも、enable connected firewalls to receive the latestsignatures distributed by the WildFire public cloud（WildFire パブリッククラウドが配信する最新のシグネチャを、接続したファイヤーウォールで受信する）こともできます。

STEP 1 | Set Up WildFire Appliance Content Updates（WildFire アプライアンスコンテンツ更新の設定）。

これにより、WildFireアプライアンスはPalo Alto Networksから最新の脅威情報を受け取ることができます。

STEP 2 | シグネチャおよびURLカテゴリ生成を有効にします。

1. アプライアンスにログインし、**configure**（設定）と入力して設定モードに入ります。
2. すべての脅威防御オプションを有効にします。

```
admin@WF-500# set deviceconfig setting wildfire signature-
generation av yes dns yes url yes
```

3. 設定をコミットします：

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

*WildFire 8.0.1*以降の環境で生成されたシグネチャのシグネチャのステータスは、次のコマンドを使用して表示できます。

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

WildFireアプライアンスは、WildFire 8.0.1にアップグレードする前に生成されたシグネチャのステータスを表示できません。

STEP 3 | WildFireアプライアンスが生成するシグネチャとURLカテゴリを取得するために、接続されたファイアウォールのスケジュールを設定します。

*WildFire*パブリッククラウドと*WildFire*アプライアンスの両方からコンテンツ更新を取得するようにファイアウォールを設定することをお勧めします。これによりファイアウォールは、ローカルのアプライアンスで生成されたシグネチャに加え、世界中で検出された脅威をベースに生成されたシグネチャを受信するようになります。

- Panorama によって管理される複数のファイアウォールの場合:

  Panoramaを起動し**Panorama** > **Device Deployment** > 動的更新を選択し、**Schedules**、**Add** をクリックして、管理対象デバイスに対してスケジュールされたコンテンツ更新を行います。

  Panorama を使用して管理対象ファイアウォールを設定し、WildFire アプライアンスから署名と URL カテゴリを受信する方法の詳細については、「Panorama を使用してデバイスにコンテンツ更新をスケジュールする」を参照してください。

- 単一のファイアウォールの場合

  1. ファイアウォールWebインターフェイスにログインして、**Device (デバイス)** > **Dynamic Updates (動的更新)**の順に選択します。

     ファイルをWildFireアプライアンスに転送するように設定されたファイアウォール（WildFireプライベートクラウドまたはハイブリッドクラウドデプロイメントのいずれか）では、WF-Privateセクションが表示されます。

  2. ファイアウォールがアプライアンスから更新コンテンツの**Schedule**（スケジュール）を設定しdownload and install content updates（ダウンロードとインストール）を行います。

ローカルで検出されたマルウェアまたはレポートをパブリッククラウドに提出する

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

WildFireアプライアンスからWildFireパブリッククラウドへのマルウェアサンプルの自動送信を有効化するWildFireパブリック クラウドはサンプルを更に分析し、今後サンプルを特定できるようにシグネチャを生成します。このシグネチャはWildFireシグネチャに追加され、世界中に配信されてユーザーをマルウェアから保護します。自分のネットワーク上で発見されたマルウェアのサンプルをネットワーク外へ転送したくない場合は、マルウェアに関するWildFireレポートのみを送信することでWildFireの統計情報と脅威インテリジェンスの向上と拡充に役立てることができます。

マルウェアをWildFireパブリック クラウドへ送信する。

1. WildFireアプライアンスからWildFireパブリック クラウドへマルウェアサンプルを自動送信する場合は、WildFireアプライアンスで以下のCLIコマンドを実行します。

   ```
   admin@WF-500# set deviceconfig setting wildfire cloud-intelligence submit-sample yes
   ```

   *WildFire*プライベート クラウドへサンプルを最初に送信したファイアウォール上でパケットキャプチャ（*PCAP*）が有効になっている場合、そのマルウェアに対する*PCAP*も同じく*WildFire*パブリック クラウドへ転送されます。

2. WildFire portal（WildFire ポータル）にアクセスし、WildFireパブリッククラウドに自動送信されたマルウェアの分析レポートを確認してください。マルウェアがWildFireパブリック クラウドへ送信されると、パブリック クラウドはそのサンプルに対して新規の分析レポートを生成します。

分析レポートをWildFireパブリック クラウドへ送信する

WildFireパブリッククラウドへ（マルウェアサンプルではなく）マルウェアレポートを自動的に送信したい場合は、WildFireアプライアンスで以下のCLIコマンドを実行してください。

```
admin@WF-500# set deviceconfig setting wildfire cloud-intelligence
 submit-report yes
```

*WildFire*アプライアンスから*WildFire*パブリッククラウドへのマルウェアの自動送信が有効になっている場合、このオプションを有効化する必要はありません。*WildFire*パブリッククラウドはサンプル用の新しい分析レポートを生成します。

WildFireパブリッククラウドに送信されたレポートはWildFire　Portal（WildFireポータル）上で閲覧できません。WildFireポータルはWildFireパブリッククラウドレポートのみを表示します。

マルウェアとレポート送信設定を検証します。

以下のコマンドを実行して、クラウド インテリジェンスが有効化され、WildFireパブリッククラウドに向けたマルウェアの送信またはレポートの送信が実行されていることを確認します。

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

`Submit sample`（サンプル送信）と`Submit report`（レポート送信）のフィールドを参照してください。

WildFire アプライアンスのアップグレード

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

次のワークフローを使用して、WildFireアプライアンスのオペレーティングシステムをアップグレードします。WildFireクラスタの一部であるアプライアンスをアップグレードする場合は、Upgrade WildFire Appliances in a Cluster（クラスタ内のWildFireアプライアンスのアップグレード）を参照してください。アプライアンスでは同時に複数の環境を使用してサンプルを分析できないため、アプライアンスをアップグレードした後で利用可能な VM イメージのリストを確認し、お使いの環境に最適なイメージを選択してください。Windows 7 をお使いの場合で、Windows 7 の 32 ビット版と 64 ビット版が混在している環境では、Windows 7 64 ビット イメージを選択することをお勧めします。これにより、32 ビットと 64 ビットの両方の PE ファイルが分析されるようになります。アプライアンスの設定には 1 つの仮想マシン イメージを使用しますが、稼働時のアプライアンスは仮想マシン イメージの複数のインスタンスを使用してファイル分析を実行します。

WildFireアプライアンスが分析して保存したサンプルの数に応じて、アプライアンスソフトウェアのアップグレードに必要な時間は異なります。 アップグレードするには、すべてのマルウェアサンプルの移行と14日間の良性サンプルが必要です。製造環境で使用したWildFireアプライアンスのアップグレードには、30～60分かかります。

次の手順では、PAN-OS 10.2.2 リリースのファイル名の例を使用します。WildFireアプライアンスにインストールするリリースの正確なファイル名は、特定のリリースによって異なる場合があります。

STEP 1 | WildFireアプライアンスを初めて設定する場合は、まずconfiguring the WildFire appliance（WildFireアプライアンスを設定）します。

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。

```
admin@WF-500> show wildfire latest samples
```

*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。

古いアプライアンスでは、このプロセスに最大 6 時間以上かかる場合があります。

1. WildFireアプライアンスで最新のコンテンツ更新を実行していることを確認します。

```
admin@WF-500> request wf-content upgrade check
```

2. 最新の WildFire コンテンツ更新パッケージをダウンロードします。

```
admin@WF-500> request wf-content upgrade download latest
```

Palo Alto Networks Update Serverに直接接続していない場合は、Install WildFire Content Updates from an SCP-Enabled Server（SCP対応サーバーからWildFireコンテンツ更新をダウンロードしてインストール）できます。

3. ダウンロードのステータスを表示します。

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

4. ダウンロードが完了したら、アップデートをインストールします。

```
admin@WF-500> request wf-content upgrade install version latest
```

STEP 4 | (PAN-OS 10.2.2 にアップグレードする場合に必要) WildFireアプライアンスの VM イメージをアップグレードします。

1. ログインして、 Palo Alto Networks カスタマー サポート ポータル ソフトウェア ダウンロード ページにアクセスします。サポート ホームページから **[アップデート]** > **[ソフトウェア アップデート]** に移動して、ソフトウェア ダウンロード ページに手動で移動することもできます。

2. ソフトウェア アップデート ページから、**WF-500** ゲスト **VM** イメージ を選択し、次の VM イメージ ファイルをダウンロードします。

   Palo Alto Networks は、*VM* イメージ ファイルを定期的に更新します。その結果、特定のファイル名は利用可能なバージョンに基づいて変更されます。必ず最新バージョンをダウンロードしてください。ファイル名の *mx.xx* はリリース番号を示します。さらに、最新バージョンを確認するために相互参照できるリリース日もあります。

   - WFWinXpAddon3_m-1.0.1.xpaddon3
   - WFWinXpGf_m-1.0.1.xpgf
   - WFWin7_64Addon1_m-1.0.1.7_64addon1
   - WFWin10Base_m-1.0.1.10base

3. VM イメージを WildFire アプライアンスにアップロードします。

   1. SCP サーバーから VM イメージをインポートします。

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

      以下に例を示します。

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

   2. ダウンロードの進行状況を確認する場合は、以下のCLIコマンドを使用します。

      ```
      admin@WF-500> ジョブをすべて表示
      ```

   3. 残りの VM イメージについてもこの手順を繰り返します。

4. VM イメージをインストールします。

   1. ```
      admin@WF-500> システム wildfire-vm-image アップグレードインストールファイルを要求しますか？
      ```

   2. 残りの VM イメージについてもこの手順を繰り返します。

5. VM イメージが WildFireアプライアンスに適切にインストールされ、有効になっていることを確認します。

   1. (オプション) 使用可能な仮想マシン イメージのリストを表示します:

      ```
      admin@WF-500>show wildfire vm-images (wildfire VM イメージ を表示)
      ```
      ```

出力には、使用可能な VM イメージが表示されます。

2. 設定をコミットします:

```
admin@WF-500#コミット
```

3. 次のコマンドを実行して、アクティブな VM イメージを表示します:

```
admin@WF-500>show wildfire status (wildfire ステータスを表示)
```

STEP 5 | PAN-OS 10.2.2 ソフトウェア バージョンを WildFireアプライアンスにダウンロードします。

WildFireアプライアンスをアップグレードするときにメジャーリリースのバージョンをスキップすることはできません。たとえば、PAN-OS 6.1からPAN-OS 7.1にアップグレードする場合は、まずPAN-OS 7.0をダウンロードしてインストールする必要があります。

この手順の例は、PAN-OS 10.2.2 にアップグレードする方法を示しています。10.2.2 をアップグレードに適したターゲット リリースに置き換えます。

10.2.2 ソフトウェアバージョンをダウンロードします。

- 直接インターネット接続：
  1. **admin@WF-500>** システム ソフトウェア ダウンロード バージョン **10.2.2** を要求
  2. ダウンロードの進行状況を確認する場合は、以下のCLIコマンドを使用します。

     ```
     admin@WF-500> show jobs all
     ```
- インターネット接続なし：
  1. Palo Alto Networks Support サイトに移動し、ログインして **Software Updates**（ソフトウェアの更新）をクリックします。
  2. インストールする WildFire アプライアンス ソフトウェア イメージ ファイルを SCP サーバー ソフトウェアを実行しているコンピュータにダウンロードします。
  3. SCP サーバーからソフトウェア イメージをインポートします。

     ```
     admin@WF-500> scp import software from <username@ip_address>/
     <folder_name>/<imagefile_name>
     ```

     以下に例を示します。

     ```
     admin@WF-500> scp import software from user1@10.0.3.4:/tmp/
     WildFire_m-10.2.2
     ```
  4. ダウンロードの進行状況を確認する場合は、以下のCLIコマンドを使用します。

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

STEP 6 | すべてのサービスが実行されていることを確認します。

```
admin@WF-500> show system software status
```

STEP 7 | ソフトウェア バージョン 10.2.2 をインストールします。

```
admin@WF-500> システム ソフトウェア インストール バージョン 10.2.2 を要求
```

STEP 8 | ソフトウェアのアップグレードを完了します。

1. 更新が完了したことを確認してください。以下のコマンドを実行して、ジョブのtype（タイプ）が Install（インストール）、status （状態）が FIN（終了）になっているエントリを探します。

```
admin@WF-500> show jobs all Enqueued
 Dequeued ID Type Status Result Completed
 ------------------------------------------------- 02:42:36
 02:42:36 5 Install FIN OK 02:43:02
```

2. アプライアンスを再起動します。

```
admin@WF-500> request restart system
```

*WildFire*アプライアンスに保存されているサンプル数に応じて、アップグレードプロセスには*10*分か*1*時間以上かかります。

STEP 9 | 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 10.2.2 が表示されていることを確認します。

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

STEP 10 | （オプション）WildFireアプライアンスが分析を実行するために使用するVMイメージを有効にします。使用可能な各VMイメージは、単一のオペレーティングシステムを表し、そのオペレーティングシステムに基づいて複数の異なる分析環境をサポートします。

- ネットワーク環境に*Windows 7 32*ビットシステムと*Windows 7 64*ビットシステムが混在している場合は、*Windows 7 64*ビットイメージを選択することをお勧めします。そのため、*WildFire*は*32*ビットと*64*ビットの両方の*PE*ファイルを分析します。
- 現在利用可能な分析環境は、*vm-3 (Windows XP)*、*vm-5 (Windows 7 64* ビット*)*、および *vm-7 (Windows 10 64* ビット*)* です。

- 次のコマンドを実行してアクティブな仮想マシン イメージを表示し、 以下`Selected VM`フィールドを参照してください。

```
admin@WF-500> wildfire ステータスを表示
```

- 使用可能な仮想マシン イメージの一覧を表示します。

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

次の出力は、`vm-5` が Windows 7 64 ビット イメージであることを示しています。

```
vm-5 Windows 7 64bit, Adobe Reader 11, Flash 11, Office
 2010.Support PE, PDF, Office 2010 and earlier
```

- 分析に使用するイメージを設定します。

```
admin@WF-500# set deviceconfig setting wildfire active-vm <vm-
image-number>
```

たとえば、vm-5を使用するには、次のコマンドを実行します。

```
admin@WF-500# set deviceconfig setting wildfire active-vm vm-5
```

および構成をコミットする:

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

STEP 11 | 次のステップ

- (オプション) ファイアウォールを PAN-OS 10.2.2 にアップグレードします。『PAN-OS 10.2 新機能ガイド』に収録されている firewall アップグレード手順 を参照してください。PAN-OS 10.2.2 より前のリリース バージョンを実行しているファイアウォールは、10.2.2 を実行している WildFireアプライアンスに引き続きサンプルを転送できます。

- （トラブルシューティング）データ移行の問題やアップグレード後のエラーが発生した場合は、WildFireアプライアンスを再起動してアップグレードプロセスを再開してください.WindFireアプライアンスを再起動してもデータが失われることはありません。

インターネット接続による WildFireアプライアンスデバイス証明書のインストール

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス ❑ 次のいずれかのユーザーロールを持つカスタマーサポートポータル（CSP）アカウント。 Super User、Standard User、Limited User、Threat Researcher、AutoFocus Trial Role、Group Super User、Group Standard User、Group Limited User、Group Threat Researcher、Authorized Support Center (ASC) User、ASC Full Service User。 ❑ WildFire アプライアンスへのスーパーユーザー アクセス

インターネット接続が利用可能なときに WF-500 アプライアンスでデバイス証明書を取得するには、Palo Alto Networks サポートポータルにログインして、証明書へのアクセスに使用されるワンタイムパスワードを生成する必要があります。次に、この OTP を使用して特定のアプライアンスのデバイス証明書を取得します。

WF-500B アプライアンスにはトラステッド・プラットフォーム・モジュール（*TPM*）が搭載されており、これを使用して安全に自身を識別し、デバイス証明書を自動的に取得します。*WF-500B* デバイス証明書を管理するためにユーザーの介入は必要ありません。

WildFire プライベート クラウドを操作していて、どの WildFire サービスにも接続していない場合は、WildFireアプライアンスデバイス証明書を更新する必要はありません。代わりに、WildFireアプライアンスは事前定義された証明書を使用して相互認証を行い、管理アクセスとデバイス間通信に使用される SSL 接続を確立します。ただし、代わりに設定することもできます。スタンドアロン WildFire アプライアンスでカスタム証明書を使用する認証のセットアップ

WF-500B アプライアンスがインターネットに接続されていない場合、アプライアンスがデバイス証明書を取得しようと繰り返し試みたためにジョブが失敗することがあります。

ファイアウォールにデバイス証明書を正常にインストールするには、ネットワーク上で次の FQDN とポートを許可する必要があります。

FQDN	ポート
• http://ocsp.paloaltonetworks.com • http://crl.paloaltonetworks.com • http://ocsp.godaddy.com	TCP 80
• https://api.paloaltonetworks.com • http://apitrusted.paloaltonetworks.com • certificatetrusted.paloaltonetworks.com • certificate .paloaltonetworks.com	TCP 443
• *.gpcloudservice.com	TCP 444 および TCP 443

STEP 1 | WildFireアプライアンスで以下の PAN-OS リリースのいずれかを実行していることを確認します。

- （PAN-OS 11.0.1 以降）
- （PAN-OS 10.2.4 以降）
- PAN-OS 10.1.10 およびそれ以降 (WF-500B アプライアンスではサポートされていません)
- PAN-OS 10.0.12 およびそれ以降 (WF-500B アプライアンスではサポートされていません)
- PAN-OS 9.1.17 およびそれ以降 (WF-500B アプライアンスではサポートされていません)

STEP 2 | ワンタイム パスワード（OTP）を生成します。

1. OTPを生成する権限を持つユーザーロールでカスタマーサポートポータルにログインします。
2. [**Products (**製品**)** > **Device Certificates (**デバイス証明書**)**] を選択し、[**Generate OTP (OTP** を生成**)**] を選択します。
3. **Device Type**（デバイス タイプ）で、**Generate OTP for WF-500 (WF-500** の **OTP** の生成**)** を選択します。
4. **WF-500** デバイスのシリアルナンバーを選択します。
5. **OTP** を生成して、OTP をコピーします。

STEP 3 | スーパーユーザー管理権限で WF-500 アプライアンス CLI にアクセスします。

STEP 4 | NTP サーバと同期するように WildFireアプライアンスを設定します。

```
管理者 @WF-500> 管理者 @WF -500# デバイス構成システムの設定 ntp-サーバー
プライマリ ntp-サーバー ntp-サーバー ntp-サーバーアドレス <NTP primary
 server IP address> admin @WF -500#  デバイス構成システム ntp-サーバーセ
カンダリ ntp-サーバー ntp-サーバーアドレスを設定 <NTP secondary server IP
 address>
```

STEP 5 | 以下の CLI コマンドを使用して WF-500 アプライアンスデバイス証明書をダウンロードしてインストールします (カスタマーサポートポータルで生成した正しいワンタイムパスワードを使用してください)。

```
管理者 @WF-500> 証明書の取得を要求 <otp_value>
```

STEP 6 | WF-500 アプライアンスはデバイス証明書を正常に取得してインストールします。

STEP 7 | （オプション）以下の CLI コマンドを使用して、デバイス証明書のダウンロードとインストールが正常に完了したことを確認します。

```
管理者 @WF-500> デバイス証明書のステータスを表示
```

デバイス証明書が正常にインストールされると、以下の応答が表示されます。

```
デバイス証明書情報:現在のデバイス証明書のステータス:発効日時:2022/11/30
 15:17:47 太平洋標準時 最終有効時間:2023/02/28 15:17:47 太平洋標準時 最後
に所得したタイムスタンプ:2022/11/30 15:29:42 太平洋標準時 最終所得ステータ
ス:成功最終所得情報:デバイス証明書が正常に取得されました
```

STEP 8 | 次の CLI コマンドを使用して WildFireアプライアンス設定を更新し、更新されたデバイス証明書で Advanced WildFireクラウドへの接続を確立します。

表 **1 :**

WildFireアプライアンスで動作する **PAN-OS** バージョン	**CLI**コマンド
• （PAN-OS 11.0.1 以降） • （PAN-OS 10.2.5 以降） • （PAN-OS 10.1.10 以降）	`admin@WF-500> test wildfire registration`
• PAN-OS 10 2.4 • （PAN-OS 10.0.12 以降） • （PAN-OS 9.1.17 以降）	`admin@WF-500> request restart system` この処理が完了するまでに最大 *20* 分かかることがあります。

WildFireアプライアンスで動作する PAN-OS バージョン	CLIコマンド
WildFire クラスタノードとして設定されたすべてのバージョン	`admin@WF-500(active-controller)> request cluster reboot-local-node` 次の *CLI* コマンドを使用して、*WildFire* コントローラーノードでの再起動タスクのステータスを表示できます。 *admin @WF-500 (アクティブコントローラー) > 保留中のクラスタタスクを表示* 保留中のタスクが残っていない場合は、次の *CLI* コマンドを使用して再起動が成功したことを確認します。 *admin @WF-500 (アクティブコントローラー) > クラスタタスク履歴を表示。その後、* *YYYY-MM-DD HH: MM: SS UTC* に *Finished: success* というステータスが表示され、再起動プロセスがいつ完了したかが示されます。

WildFire アプライアンスのアクティビティを監視する

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

WildFireアプライアンスに送信されたサンプルの分析結果を表示するには、サンプルを送信したファイアウォール (複数のファイアウォールを集中管理している場合は Panorama) にアクセスするか、WildFire API を使用します。

WildFireがサンプルを分析し、悪意のある、フィッシング、グレーウェア、または良性の判定を行った後、詳細な分析レポートがサンプル用に生成されます。サンプルを送信したファイアウォールから閲覧できるWildFire分析レポートには、サンプルが検出された際のセッションに関する詳細情報も含まれています。新たにマルウェアと判定されたサンプルについては、関連が疑われる既存のWildFireシグネチャ情報や、サンプルがマルウェアであることを示すファイル特性、挙動、アクティビティに関する情報もWildFire分析レポートに記載されています。

WildFireへのサンプル送信状況を監視する方法の詳細、サンプルの分析レポートを参照する方法、WildFire分析のサンプルレポートの送信・分析結果の内容によりアラートや通知を設定する方法については以下のトピックをご参照ください。

- WildFireログとレポートについて
- WildFire CLIを使用してWildFireアプライアンスを監視する
- ファイアウォールを使用して WildFireアプライアンスの送信を監視する

WildFireログとレポートについて

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

WildFireアプライアンスのログは、ファイアウォール、WildFire ポータル、または WildFire API を使用して監視できます。

WildFireは分析する各サンプルを安全、マルウェア、フィッシング、グレイウェアに分類し、そのサンプルの詳細と挙動を記載したWildFire分析レポートを生成します。WildFire 分析レポートは、サンプルを送信したファイアウォールと、サンプルを分析した WildFire クラウド (パブリックまたはプライベート) で見つけるか、WildFire API を使用して取得できます。

- ファイアウォール : WildFire 分析用のファイアウォールによって送信されたすべてのサンプルは、WildFire サブミッション エントリとして記録されます (モニタ > **WildFire** サブミッション)。WildFire SubmissionsログのAction［挙動］列には、ファイルがファイアウォールによって許可されたかブロックされたかが示されます。それぞれのWildFireへの送信エントリにつき、詳細ログビューを展開し、そのサンプルのWildFire分析レポートを閲覧したり、レポートをPDF形式でダウンロードしたりすることができます。
- WildFireポータル上で - 各サンプルのWildFire分析レポートを含めたWildFireアクティビティを監視することができます。また、レポートをPDF形式でダウンロードすることもできます。WildFireプライベートクラウドの導入環境では、ポータルへ手動でアップロードされたサンプル、およびクラウドインテリジェンスが有効化されたWildFire アプライアンスから送信されたサンプルの詳細をWildFireポータルから閲覧することができます。

  *WildFire*分析レポートをポータル上で見るオプションは、クラウドインテリジェンス 機能が有効化された*WildFire* アプライアンス のみに対応しています。
- WildFire APIでは：WildFire アプライアンスまたはWildFireパブリッククラウドからのWildFire分析レポートを取得します。

WildFireアプライアンスを使用して、検体解析ステータスを監視する

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

WildFireアプライアンスの解析関連の詳細を監視するには、WildFire CLI（コマンドラインインターフェース）を使用します。解析プラットフォームの使用状況情報、現在の検体キュー、および検体プロセスの詳細を表示できます。

WildFireアプライアンスを用いてWildFireアクティビティを監視する方法については以下のセクションをご覧ください:

- WildFire分析環境ユーティリゼイションを表示する
- WildFire検体解析処理の詳細を見る

WildFire分析環境ユーティリゼイションを表示する

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

WildFireアプライアンスは、さまざまな解析環境を使用して、検体内の悪意のある動作を検出します。使用されている解析環境、使用可能な数、解析のためにキューに入れられているファイルの数を表示できます。特定の分析環境の使用率が常に最大ワークロード容量である場合、機密性の低いファイルの分析を、WildFire パブリック クラウドでホストされる Palo Alto Networks にオフロードする、ファイル転送ポリシーを更新する、またはファイル転送制限の再定義を検討してください(パロアルトネットワークスでは、すべてのファイルタイプに対してデフォルトのファイル転送値を使用することをお勧めします)。

STEP 1 | 使用率統計を表示する解析環境に基づいて、CLIおよび以下のコマンドのいずれかにアクセスします。

- Portable Executable解析環境使用率—**show wildfire wf-vm-pe-utilization**
- ドキュメント解析環境使用率—**show wildfire wf-vm-doc-utilization**
- 電子メールリンク解析環境使用率—**show wildfire wf-vm-elinkda-utilization**
- アーカイブ解析環境使用率—**show wildfire wf-vm-archive-utilization**

特定の解析環境で、アプライアンスは使用中の数と使用可能な数を示します。

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

STEP 2 | 解析待ちのWildFireアプライアンス検体の数と内訳を表示します。解析環境が利用可能になると、検体が処理されます。

show wildfire wf-sample-queue-status

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

WildFire検体解析処理の詳細を見る

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

WildFireアプライアンスは、解析アクティビティの記録をイベントログ内に保持します。ネットワーク内の接続サービスまたはアプライアンスが特定の検体を解析した詳細、および特定の時間枠で解析された検体の数を表示できます。この情報を使用して、アクティビティを監視し、悪意のあるアクティビティに対するポリシーと対策を作成できます。異常に重いアクティビティは、不審なアクティビティを示している可能性があります。AutoFocusなどの脅威インテリジェンスツールを使用して、脅威の性質を調査および決定することも検討してください。

STEP 1 | 指定されたタイムスパン内でローカルに処理された検体の数、または検体の最大数を基準に示します。

show wildfire local サンプル処理済み **{time [last-12-hrs]|**最後の **15** 分間 **|**過去 **1** 時間 **|**過去 **24** 時間 **|**過去 **30** 日間 **|**過去**7**日間**|**最終カレンダー日 **|**最後のカレンダー月**] \ count <number_of_samples>}**.

```
最新のサンプル情報：+ ------------------------------------------------
 ------------------- + --------------------- + ------ ----- +
 ------------ + ----------- + ------------ + ------ -------------
 + | SHA256 |時間の作成|ファイル名|ファイルタイプ|ファイルサイズ|悪意のある|ステータス| + ------------------------------------------------
```

```
 ----------------- + -------------------- + ---------- -+
 ------------ + ----------- + ------------ + ---------- --------- +
 | ce752b7b76ac2012bdff2b76b6c6af18e132ae8113172028b9e02c6647ee19bb
 | 2018-12-09 16:55:53 | |メールリンク| 31,522 | |ダウンロード完了| |
 349e57e51e7407abcd6eccda81c8015298ff5d5ba4cedf09c7353c133ceaa74b
 | 2018-12-09 16:53:40 | |メールリンク| 39,679 | |ダウンロード
完了| + ------------------------------------------------
 ----------------- + -------------------- + ---------- -+
 ------------ + ----------- + ------------ + ---------- --------- +
```

STEP 2 | WildFire解析に指定の検体を送信したデバイスを指定します。

wildfire グローバル **sample-device-lookup sha256** を等しく表示します**<SHA_256>**.

```
 サンプル
 1024609813c57fe174722c53b3167dc3cf5583d5c7abaf4a95f561c686a2116e は、
次のデバイスで最後に確認されました:
 +----------------------------------------
 -------------------------+-----------+-----------+
 ----------------------+ | SHA256 |デバイス ID |デバイス IP |提出時間 |
 +-------------------------------------------------------------------
 ------+----------------------+-----------+-------- -------------+
 | 1024609813c57fe174722c53b3167dc3cf5583d5c7abaf4a95f561c686a2116e
 |マニュアル |マニュアル | 2019-08-05 19:24:39 |
 +-------------------------------------------------------------------
 ------+----------------------+-----------+-------- -------------
+
```

WildFire CLIを使用してWildFireアプライアンスを監視する

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

WildFire™ CLI（コマンドライン インターフェース）を使用して内部システム ログを閲覧します。ログイベントを確認して、クラスターノード、コアサービス、アナライザーサービスなどのWildFireコンポーネントの状態とステータスを監視したり、システム設定のトラブルシューティングや検証を行ったりできます。その他のPAN-OS コマンドの詳細は、PAN-OS CLI Quick Start（PAN-OS CLIクイックスタート）を参照してください。

- WildFireアプライアンスのシステム ログを表示する

WildFireアプライアンスのシステム ログを表示する

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

PuTTYなどのターミナルエミュレータを使用し、secure shell 接続(セキュアシェル-SSH) または管理コンピューターのシリアルインターフェースからデバイスのコンソールポートへの物理的な直接シリアル接続を使用してWildFireアプライアンスに接続します。

STEP 1 | ターミナル エミュレーションソフトウェアを起動し、接続のタイプ（シリアルまたはSSH）を選択します。

- SSH接続を確立するには、接続するデバイスのWildFireホスト名またはIPアドレスを入力し、ポートを **22** に設定します。
- シリアル接続を確立するには、管理コンピューターのシリアル インターフェースをデバイスのコンソール ポートに接続します。ターミナル エミュレーション ソフトウェアでシリアル接続を次のように設定します。
  - データ速度:**9600**
  - データ ビット:**8**
  - パリティ: なし
  - ストップ ビット:**1**
  - フロー制御: なし

STEP 2 | ログインを求められたら、管理アクセス認証情報を入力します。

STEP 3 | WildFireアプライアンスで、以下のコマンドを入力します:

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

このコマンドは、WildFireアプライアンス サブタイプとして分類されたすべてのWildFireログイベントを最も古いものから最新のものへと表示します。

- コマンド引数 `direction equal backward`を追加することにより、ログの表示を新しいものから最も古いものに逆にすることができます。
- WildFireアプライアンスのCLIによって返されるログメッセージには、多数のサブタイプが含まれる場合があります。ログは一般的なキーワードに基づいてフィルタリングできます。特定の文字列に基づいてフィルタリングするには、以下のコマンド引数を使用します: `match queue < keyword >`

  以下のWildFireアプライアンスログは、起動時のシステム初期化プロセスを示しています。

```
Time Severity Subtype Object EventID ID Description
 ================================================================================
 2017/03/29 12:04:33 medium general general 0 Hostname changed to
 WF-500 2017/03/29 12:04:40 info general general 0 VPN Disable mode
 = off 2017/03/29 12:04:41 info hw ps-inse 0 Power Supply #1 (top)
 inserted 2017/03/29 12:04:41 high general system- 1 The system
 is starting up.2017/03/29 12:04:41 info raid pair-de 0 New Disk
 Pair A detected.2017/03/29 12:04:41 info raid pair-de 0 New Disk
 Pair A detected.2017/03/29 12:04:41 info raid pair-de 0 New Disk
 Pair B detected.2017/03/29 12:04:41 info raid pair-de 0 New Disk
 Pair B detected.2017/03/29 12:04:41 info cluster cluster 0 Cluster
 daemon is initializing.2017/03/29 12:04:41 info port eth1 link-
ch 0 Port eth1:Up 1Gb/s Full duplex 2017/03/29 12:04:41 info port
 MGT link-ch 0 Port MGT:Up 1Gb/s Full duplex 2017/03/29 12:04:41
 info port eth3 link-ch 0 Port eth3:Up 1Gb/s Full duplex 2017/03/29
 12:04:41 info port eth2 link-ch 0 Port eth2:Up 1Gb/s Full duplex
 2017/03/29 12:04:41 info general general 0 Power Supply #1 (top)
 is not present on startup 2017/03/29 12:04:41 info general general
 0 Power Supply #2 (bottom) is not present on startup
```

ファイアウォールを使用して WildFireアプライアンスの送信を監視する

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

ファイアウォールによって (WildFire プライベートクラウドやパブリッククラウドに) 転送されたサンプルは、**WildFire**送信ログのエントリとして追加されます。WildFireへの送信エントリを展開すると、詳細なWildFire分析レポートを表示することができます。ファイアウォールを使用してマルウェアを監視する方法の詳細については、「WildFire アクティビティの監視」を参照してください。

WildFireアプライアンスのログと分析レポートを表示する

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

WildFire のログには、WildFire が分析したサンプル (ファイルやメールリンク) に関する情報が含まれています。これには、アプリケーションの種類や攻撃者のIPアドレスなど、ログに記録されたイベントに関連するプロパティ、アクティビティ、動作などのアーティファクトのほか、サンプルをマルウェア、フィッシング、グレイウェア、または良性に分類するなどの高レベルの分析結果や詳細なサンプル情報など、Wildfire固有の特性が含まれます。WildFire送信ログを確認することで、ネットワーク内のユーザーが疑わしいファイルをダウンロードしたかどうかもわかります。WildFire分析レポートには、詳細なサンプル情報のほか、対象ユーザーに関する情報、電子メールヘッダー情報 (有効な場合)、ファイルを配信したアプリケーション、およびファイルのコマンドと制御のアクティビティに関連するすべての URL が表示されます。これにより、ファイルが有害かどうか、レジストリ キーを変更したかどうか、ファイルの読み取り/書き込みを行ったかどうか、新しいファイルを作成したかどうか、ネットワーク接続チャネルを開いたのかどうか、アプリケーションのクラッシュを引き起こしたかどうか、プロセスを生成したかどうか、ファイルをダウンロードしたかどうか、他の有害な動作が示されているかどうかがわかります。

STEP 1 | 「WildFireアプライアンス分析用のファイルの転送」を行います。

STEP 2 | Configure WildFire Submissions Log Settings（WildFire提出ログの設定を設定する）。

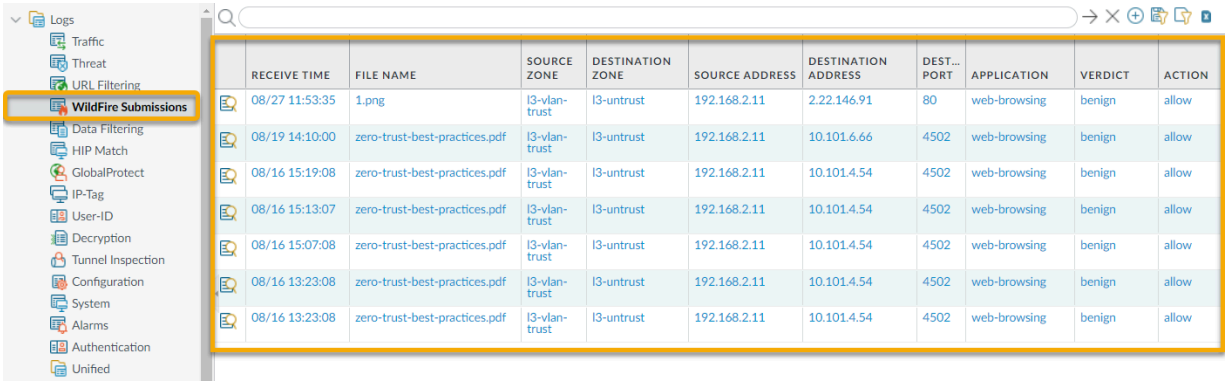
STEP 3 | ファイアウォールが WildFire パブリック、プライベート、もしくはハイブリッドクラウドに送信したサンプルを閲覧する場合は、 **Monitor (モニター)** > **Logs (ログ)** > **WildFire Submissions (WildFire** へ送信**)**を選択します。サンプルのWildFire分析が完了すると、サンプルを送信したファイアウォールへ結果が送り返され、WildFireへの送信ログから閲覧できるようになります。送信ログには次の情報のような、任意のサンプルについての詳細情報が含まれています：

- 判定の列にはサンプルが安全なファイル、グレイウェア、マルウェアのいずれにあたるかが表示されます。
- Action（アクション）列はファイアウォールが、サンプルを許可またはブロックしているかどうかを示します。

- Severity (重大度) 列は、対象のサンプルが組織に及ぼす脅威の大きさを critical (重要)、high (高)、medium (中)、low (低)、informational (通知) という値を使って示します。

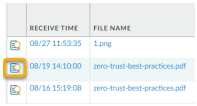
  次の重大度レベルの値は、判定およびアクションの値を組み合わせて決定されます。

  - 低—アクションが許可に設定されたグレイウェアのサンプルです。
  - 高—アクションが許可に設定された悪意のあるサンプルです。
  - 通知：
    - アクションが許可に設定された安全なサンプルです。
    - アクションがブロックに設定されたいずれかの判定を持つサンプルです。

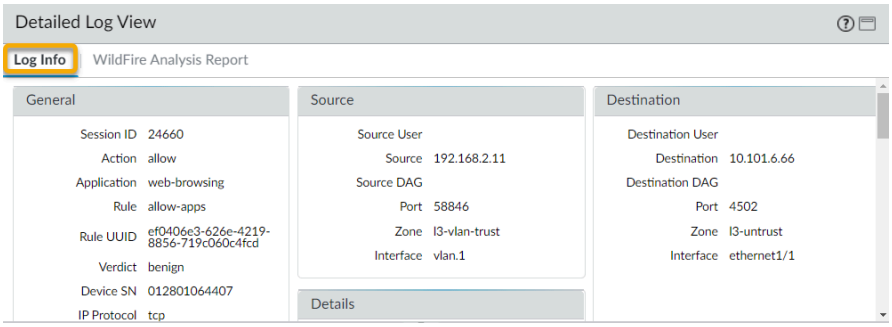


RECEIVE TIME	FILE NAME	SOURCE ZONE	DESTINATION ZONE	SOURCE ADDRESS	DESTINATION ADDRESS	DEST... PORT	APPLICATION	VERDICT	ACTION
08/27 11:53:35	1.png	l3-vlan-trust	l3-untrust	192.168.2.11	2.22.146.91	80	web-browsing	benign	allow
08/19 14:10:00	zero-trust-best-practices.pdf	l3-vlan-trust	l3-untrust	192.168.2.11	10.101.6.66	4502	web-browsing	benign	allow
08/16 15:19:08	zero-trust-best-practices.pdf	l3-vlan-trust	l3-untrust	192.168.2.11	10.101.4.54	4502	web-browsing	benign	allow
08/16 15:13:07	zero-trust-best-practices.pdf	l3-vlan-trust	l3-untrust	192.168.2.11	10.101.4.54	4502	web-browsing	benign	allow
08/16 15:07:08	zero-trust-best-practices.pdf	l3-vlan-trust	l3-untrust	192.168.2.11	10.101.4.54	4502	web-browsing	benign	allow
08/16 13:23:08	zero-trust-best-practices.pdf	l3-vlan-trust	l3-untrust	192.168.2.11	10.101.4.54	4502	web-browsing	benign	allow
08/16 13:23:08	zero-trust-best-practices.pdf	l3-vlan-trust	l3-untrust	192.168.2.11	10.101.4.54	4502	web-browsing	benign	allow

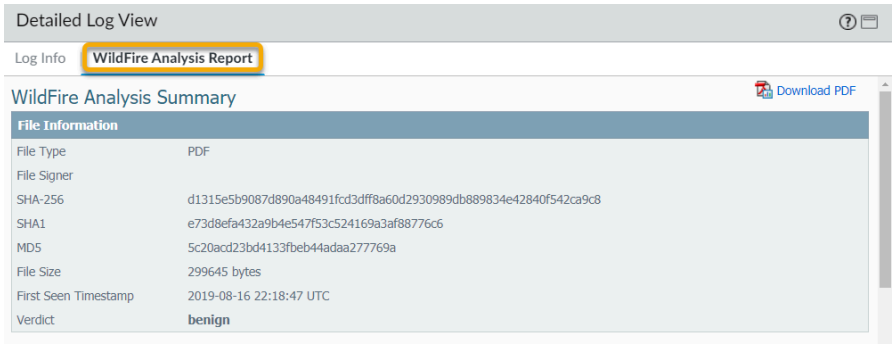
STEP 4 | 各エントリの詳細ログビューを開く際はLog Details （ログ詳細） のアイコンを選択してください。



詳細ログビューには、エントリ内のログ情報とWildFire分析レポートが表示されます。ファイアウォールのパケットキャプチャ（PCAP）が有効化されている場合、サンプルのPCAPもここに表示されます。



全てのサンプルに対し、WildFire分析レポートからファイルとセッションの詳細を表示させることができます。マルウェアのサンプルの場合はWildFire分析レポートの内容が拡張され、そのファイルに悪意があると判断される原因となった性質や挙動について詳細情報が表示されています。



STEP 5 | （オプション）WildFire分析レポートの**Download PDF**（**PDF**をダウンロード）を行います。

WildFire アプライアンス クラスタ

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire ライセンス

*WildFire*アプライアンスクラスタは、サンプル分析とストレージ容量を増やし、より大きなファイアウォールグループをサポートし、複数のWildFireアプライアンスの設定と管理を簡素化するためにリソースをプールする、WildFireアプライアンスの相互接続グループです。これは、WildFireパブリッククラウドへのアクセスが許可されていない環境で特に便利です。1つのネットワーク上に最大20台のWildFireアプライアンスをWildFireアプライアンスクラスタとして設定および管理できます。また、クラスタは、クラスタが接続されたすべてのファイアウォールに配布する単一のシグネチャパッケージ、フォールトトレランス用の高可用性（HA）アーキテクチャ、およびPanoramaを使用してクラスタを集中管理する機能も提供します。また、Panoramaを使用してstandalone WildFire appliances（スタンドアロンのWildFireアプライアンス）を管理することもできます。

WildFireアプライアンスクラスタを作成するには、クラスタに配置するすべてのWildFireアプライアンスがPAN-OS 8.0.1以降を実行する必要があります。Panoramaを使用してWildFireアプライアンスクラスタを管理する場合、PanoramaはPAN-OS 8.0.1以降を実行する必要があります。WildFireアプライアンスクラスタを作成および管理するために別途ライセンスは必要ありません。

- WildFire アプライアンスクラスターの弾力性とスケール
- WildFire アプライアンス クラスタ管理
- WildFireアプライアンスでローカルにクラスタを設定する
- WildFire アプライアンス間の暗号化を設定する
- WildFire クラスターのモニター
- クラスタ内のWildFireアプライアンスをアップグレードする
- WildFire クラスターのトラブルシューティング

WildFire アプライアンスクラスターの弾力性とスケール

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

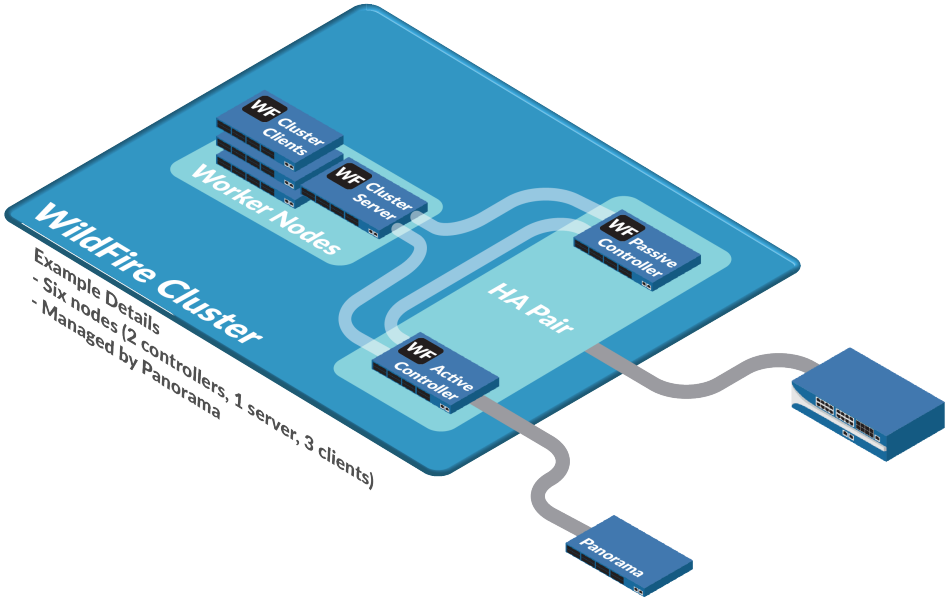
WildFireアプライアンスクラスタは、最大20台のWildFireアプライアンスのサンプル分析およびストレージ容量を集約し、単一のネットワーク上の大規模なファイアウォールの導入を実現します。CLIを使用してConfigure a Cluster Locally on WildFire Appliances（WildFireアプライアンス上でローカルにクラスタを管理および設定）したり、PanoramaMシリーズまたは仮想アプライアンスサーバ上でConfigure a Cluster Centrally on Panorama（クラスタを集中管理および設定）することができます。WildFireアプライアンスのクラスタ環境には、以下が含まれます。

- クラスタとしてグループ化して管理する2～20個のWildFireアプライアンス。クラスタには、最低2つのWildFireアプライアンスがハイアベイラビリティ（HA）ペアで設定。
- トラフィック分析とシグネチャ生成のためにサンプルをクラスタに転送するファイアウォール。
- （オプション）クラスタをローカルで管理しない場合は、クラスタ管理を集中管理するための1台または2台のPanoramaアプライアンス。HAを提供するには、HAペアとして設定された2台のPanoramaアプライアンスを使用します。

WildFireアプライアンスクラスタに追加される各WildFireアプライアンスは、スタンドアロンのWildFireアプライアンスではなく、そのクラスタ内のノードになります。Panoramaは、合計200個のWildFire*cluster nodes*（クラスタノード）（最大20個のノードを持つ10個のクラスタ）で最大10個のWildFireアプライアンスクラスタを管理できます。

*Panorama*は、*WildFire*アプライアンスクラスタだけでなく、standalone WildFire appliances（スタンドアロンのWildFireアプライアンス）も管理できます。*Panorama*が管理できるスタンドアロン*WildFire*アプライアンスと*WildFire*アプライアンスクラスタノードの合計は*200*個です。たとえば、*Panorama*が合計*15*の*WildFire*クラスタノードと*8*個のスタンドアロン*WildFire*アプライアンスを持つ*3*個のクラスタを管理する場合、*Panorama*は合計*23*個の*WildFire*アプライアンスを管理し、最大*177*の*WildFire*アプライアンスをさらに管理できます。

*Panorama*に接続された*WildFire*アプライアンスには登録制限がありません。Capacity License（容量ライセンス）に影響を与えずに、多数のデバイスに接続できます。*Panorama* ライセンスの詳細については、Register Panorama and Install Licenses（Panorama の登録とライセンスのインストール）を参照してください。



クラスタノードは、次の3つの役割のいずれかを実行します。

- コントローラノード—パノラマMシリーズまたは仮想アプライアンスでクラスタを管理していない場合は、2つのコントローラノードがキューイングサービスとデータベースを管理し、シグネチャを生成し、クラスタをローカルで管理します。各クラスタには最大2つのコントローラノードがあります。各WildFireアプライアンスクラスタには、フォールトトレランス用にプライマリコントローラノードとコントローラバックアップノードHAペアとして構成されたノードが2つ以上必要です。通常のメンテナンスまたは障害状態の場合を除き、各クラスタには2つのコントローラノードが必要です。
- ワーカーノード（クラスタクライアント）（— コントローラノードではないクラスタノードはワーカーノードです。ワーカーノードは、クラスタの分析能力、ストレージ容量、およびデータ回復力を向上させます。
- サーバノード（クラスタサーバ — Wildfireクラスタ内の3番目のノードは、標準のワーカノード機能に加えてデータベースおよびインフラストラクチャの冗長性機能を提供する特別なタイプのワーカノードであるサーバノードとして自動的に設定されます。

ファイアウォールがクラスタノードに登録されたとき、またはすでにファイアウォールを登録しているWildFireアプライアンスをクラスタに追加するときに、クラスタは登録リストを接続されたファイアウォールにプッシュします。登録リストには、クラスタ内のすべてのノードが含まれます。クラスタノードに障害が発生すると、そのノードに接続されているファイアウォールは別のクラスタノードに再登録されます。この種の復元力は、WildFireアプライアンスクラスタを作成する利点の1つです。

利点	説明
スケール	WildFireアプライアンスクラスタは、単一のネットワーク上で利用可能な分析スループットとストレージ容量を向上させるので、ネット

利点	説明
	ワークをセグメント化せずに、より大きなファイアウォールネットワークに対応できます。
高可用性	クラスタノードが停止した場合、HA構成はフォールトトレランス機能を提供し、重要なデータやサービスの損失を防ぎます。パノラマを使用してクラスタを集中管理する場合、パノラマHA構成では集中管理のフォールトトレランス機能が提供されます。
単一シグニチャーパッケージ配布	クラスタに接続されたすべてのファイアウォールは、データを受信または分析したクラスタノードに関係なく、同じシグネチャパッケージを受信します。シグネチャパッケージは、すべてのクラスタメンバのアクティビティと結果に基づいています。つまり、接続された各ファイアウォールは、クラスタの統合知識から利益を得ます。
集中管理(Panorama)	Panoramaを使用してWildFireアプライアンスクラスタを管理する場合は、時間を節約し、管理プロセスを簡素化できます。WildFireアプライアンスまたはクラスタを管理するためにCLIおよびスクリプトを使用する代わりに、Panoramaはネットワークデバイスの単一のペイントウィンドウビューを提供します。一般的な設定、設定の更新、ソフトウェアのアップグレードを複数のWildFireアプライアンスクラスタにプッシュすることもできます。また、WildFireアプライアンスのCLIではなく、PanoramaのWebインターフェイスを使用してこのすべてを実行できます。
ロード バランシング	クラスタに2つ以上のアクティブノードがある場合、クラスタはノード間で分析、レポート生成、シグネチャ作成、ストレージ、およびWildFireコンテンツの配布を自動的に分散および負荷分散します。

WildFire クラスターの高可用性

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

HAは重要なデータやサービスの損失を防止するため、WildFireアプライアンスクラスタの高可用性が非常に重要です。HAクラスタは、分析結果、レポート、シグネチャなどの重要なデータをノードにコピーして配布するため、ノードに障害が発生してもデータが失われることはありません。また、HAクラスタは、分析機能、WildFire API、シグネチャ生成などの冗長な重要なサービスを提供し、ノードの障害によってサービスが中断されないようにします。クラスタには、高可用性の利点をもたらすために少なくとも2つのノードが必要です。障害ノードに登録された

ファイアウォールはクラスタ登録リストを使用して別のクラスタノードに登録するため、クラスタノードの障害はファイアウォールに影響しません。

HAペア内の2つのデバイスのそれぞれは、プライマリおよびセカンダリアプライアンスとしてユーザによって設定されます。この初期優先順位値の設定に基づいて、WildFireは、アクティブな操作ステータスをプライマリアプライアンスに割り当て、受動ステータスをセカンダリデバイスに割り当てます。このステータスは、管理およびインフラストラクチャコントロールの接点として使用されるWildFireアプライアンスを決定します。パッシブデバイスは、常にアクティブなアプライアンスと同期され、システムまたはネットワークの障害が発生した場合にその役割を引き受ける準備ができています。たとえば、アクティブ状態（アクティブプライマリ）のプライマリアプライアンスに障害が発生すると、フェールオーバーイベントが発生し、セカンダリアプライアンスがアクティブセカンダリに移行する間にパッシブプライマリステートに移行します。最初に割り当てられたプライオリティ値は、アプライアンスのステータスに関係なく同じです。

フェールオーバーは、HAペアが互いに通信できなくなったり、応答がなくなったり、致命的なエラーが発生した場合に発生します。WildFire HAペアは軽微な中断を自動解決しようとしますが、主なイベントはユーザの介入が必要です。フェイルオーバーは、コントローラーがユーザーによって中断または廃止されたときにもトリガーされます。

*1*つのコントローラノードでクラスタを構成しないでください。各クラスタには、*HA*コントローラのペアが必要です。クラスタには、コントローラノードを交換する場合やコントローラノードに障害が発生した場合など、一時的な状況でのみ単一のコントローラノードが必要です。

2ノードクラスタHAペアでは、1つのコントローラノードに障害が発生すると、もう1つのコントローラノードがクラスタ操作を引き継ぎます。残りのクラスタノードで検体を処理するには、スタンドアロンのWildFireアプライアンスとして機能するように設定する必要があります。残りのクラスターノードのHAおよびクラスター設定を削除し、ノードを再起動します。ノードはスタンドアロンWildFireアプライアンスとして再起動されます。

3ノードクラスタは、サーバノードを追加してHAペアを運用し、冗長性を強化します。サーバーは、コントローラーと同じデータベースおよびサーバー・インフラストラクチャー・サービスを操作しますが、シグニチャーは生成しません。このデプロイメントにより、コントローラノードに障害が発生した場合にクラスタが機能するようになります。

WildFireクラスタに追加される追加ノードは、ワーカーノードまたはサーバノードとして機能します。3番目のノードは自動的にサーバーとして構成されますが、その後の各追加はワーカーとして追加されます。

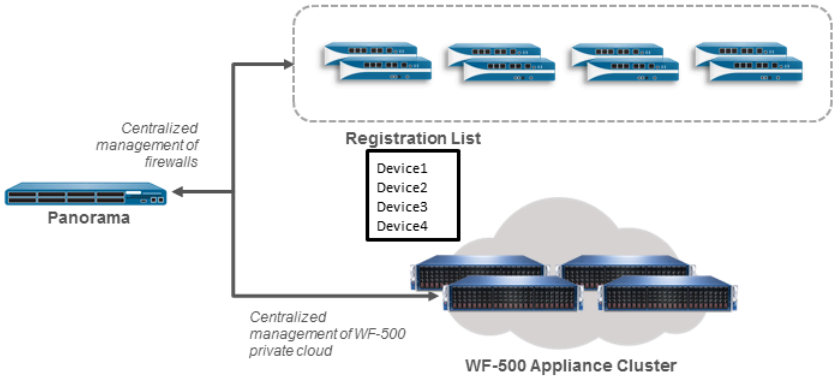
Panoramaを使用したWildFireクラスタの管理の利点

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

PanoramaでWildFireアプライアンスクラスタを管理する場合は、2つのPanorama Mシリーズまたは仮想アプライアンスをHAペアとして設定して、管理の冗長性を実現できます。冗長なPanoramaアプライアンスを設定していない状態でPanoramaが失敗した場合でも、コントローラーノードからローカルでクラスターを管理できます。

PanoramaHAペアを使用してクラスタを管理し、1つのPanoramaが失敗すると、もう1つのPanoramaアプライアンスがクラスタの管理を引き継ぎます。PanoramaHAピアに障害が発生した場合、失敗したPanoramaピアからサービスをできるだけ早く復元して、管理HAを復元します。

分析、ストレージ、および集中管理HAを提供するには、クラスタコントローラとコントローラのバックアップノードとして2つ以上のWildFireアプライアンス、および2つのPanoramaMシリーズまたは仮想アプライアンスが必要です。



ファイアウォールには、クラスタのメンバーであるすべてのWildFireアプライアンスを含む登録リストが送信されます。ファイアウォールはクラスタ内の任意のノードに登録することができ、クラスタはノード間で負荷のバランスを自動的に調整します。

WildFire アプライアンス クラスタ管理

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

WildFireアプライアンスクラスタを管理するには、クラスタの機能と管理の推奨事項を理解する必要があります。

カテゴリ	説明
クラスタの運用と設定	分析とアプライアンス間の一貫性を保証するために、すべてのクラスタノードを同じように構成します。 • すべてのクラスタノードは、同じバージョンのPAN-OS（PAN-OS 8.0.1以降）を実行する必要があります。Panoramaは、クラスタノードと同じソフトウェアバージョンまたは新しいバージョンを実行する必要があります。ファイアウォールは、サンプルをWildFireアプライアンスに提出できるようにする同じソフトウェアバージョンを実行できます。ファイアウォールでは、WildFireアプライアンスクラスタにサンプルを送信するための特定のソフトウェアバージョンは必要ありません。 • クラスターノードは、インターフェース構成を除いて、コントローラーノードから構成を継承します。クラスタノードは、コントローラノードの構成を監視し、コントローラノードが更新された構成をコミットするときに、独自の構成を更新します。ワーカーノードは、コンテンツ更新サーバー設定、WildFireクラウドサーバー設定、サンプル分析イメージ、サンプルデータ保持時間枠、分析環境設定、署名生成設定、ログ設定、認証設定、Panoramaサーバー、DNSサーバー、NTPサーバー設定などの設定を継承します 。 • Panoramaでクラスタを管理すると、Panoramaアプライアンスは一貫した構成をすべてのクラスタノードにプッシュします。WildFireアプライアンスノードでローカルに設定を変更することはできますが、次にPanoramaでアプライアンスが設定をプッシュしたときにノード上の実行コンフィギュレーションを置き換えるため、 Palo Alto Networksはこれを行うことはお勧めしません。Panorama で管理されているクラスタノードのローカル変更により、Out of Sync（同期していない）エラーが発生することがよくあります。

カテゴリ	説明
	• クラスタノードメンバシップリストが2つのコントローラノードで異なる場合、クラスタはOut of Sync（同期していない）警告を生成します。両方のコントローラー・ノードが他のノードの同期外メンバーシップ・リストを継続的に更新する状況を回避するには、クラスター・メンバーシップの強制は停止します。この場合、操作コマンド**request high-availability sync-to-remote running-configuration**（高可用性同期からリモート実行設定のリクエスト）を実行して、コントローラーおよびコントローラーのバックアップ・ノード上のローカルCLIからクラスター・メンバーシップ・リストを同期することができます。プライマリコントローラノードの設定とコントローラバックアップノードの設定が一致しない場合は、プライマリコントローラノードの設定がコントローラバックアップノードの設定を上書きします。各コントローラノードで**show cluster all-peers(**クラスタすべてのピアを表示 を実行し、メンバーシップリストを比較して修正します。 • クラスタにはコントローラノードが2つしかないんので（プライマリとバックアップ）、3番目のコントローラノードをクラスタにローカルに追加しようとすると失敗します。（Panorama のWebインターフェイスでは、自動的に3番目のコントローラノードを追加できなくなります）。クラスタに追加される3番目以降のノードは、ワーカーノードでなければなりません。 • HA構成の特徴は、クラスタノードに障害が発生した場合の冗長性を提供するために、クラスタがデータベース、キューイングサービス、およびサンプル送信の複数のコピーを分散して保持することです。HAに冗長性を持たせるために必要な追加サービスを実行することで、スループットに対する影響は最小限に抑えられます。 • クラスタは、分析環境ネットワークに使用される重複IPアドレスを自動的にチェックします。 • ノードがクラスタに属していて、それを別のクラスタに移動する場合は、最初にノードを現在のクラスタから削除する必要があります。 • クラスタ内で現在運用中のWildFireアプリケーションのIPアドレスを変更しないでください。変更すると、関連付けされたファイアウォールがノードから登録解除されます。
クラスタデータ保存ポリシー	データ保存ポリシーは、WildFireアプライアンスクラスタがさまざまなタイプのサンプルを保存する期間を決定します。

カテゴリ	説明
	• **Benign and grayware samples**（良性およびグレーウェアサンプル）— クラスタは良性およびグレーウェアサンプルを1～90日間保持します（デフォルトは14）。 • **Malicious samples**（悪意のあるサンプル）— クラスタは悪意のあるサンプルを最低1日間保持します（デフォルトは不定 - 決して削除されません）。悪質のあるサンプルデータには、phishing verdict samples（フィッシング判定サンプル）が含まれます。 クラスター全体で同じデータ保持ポリシーを構成します (4一般的なクラスター設定をローカルで構成する 、または 4 パノラマで一般的なクラスター設定を構成します)。
ネットワーク	WildFireアプライアンスクラスタ間の通信は許可されません。ノードは、所与のクラスタ内で互いに通信しますが、他のクラスタ内のノードとは通信できません。 すべてのクラスタメンバーは、以下を守ってください。 • クラスタ管理と通信に専用のクラスタ管理インターフェイスを使用する（パノラマで実施）。 • 同じサブネットに静的IPアドレスを所持する。 • クラスタノード間の接続を短時間で行う。接続の最大レイテンシは500ミリ秒以下にする。
専用クラスター管理インターフェース	専用のクラスタ管理インターフェイスにより、コントローラノードはクラスタを管理でき、標準管理インターフェイス（Ethernet0）とは異なるインターフェイスです。Panoramaは、専用のクラスタ管理インターフェイスの設定を強制します。

カテゴリ	説明
	*2*ノード構成の*2*つのコントローラノード間でクラスタ管理リンクがダウンすると、コントローラバックアップノードのサービスとサンプル分析は、プライマリコントローラノードとの管理通信がない場合でも実行され続けます。これは、クラスタ管理リンクがダウンすると、コントローラのバックアップノードは、プライマリコントローラノードがまだ機能しているかどうかを認識せず、split-brain（スプリットブレイン）状態になるためです。プライマリコントローラノードが機能していない場合、コントローラバックアップノードはクラスタサービスを提供し続ける必要があります。クラスタ管理リンクが復元されると、各コントローラノードからのデータがマージされます。
DNS	Wildfireアプライアンスクラスタのコントローラノードは、クラスタの信頼できるDNSサーバとして使用できます。（権限のあるDNSサーバーは、再帰的なDNSサーバーではなく、正式なDNSサーバーに照会し、要求された情報を最初の要求を行ったホストに渡す）とは対照的に、クラスターメンバーの実際のIPアドレスを提供します。 WildFireアプライアンスクラスタにサンプルを送信するファイアウォールは、社内の企業DNSサーバなどの通常のDNSサーバにDNSクエリを送信する必要があります。内部DNSサーバは、（クエリのドメインに基づいて）DNSクエリをWildFireアプライアンスクラスタコントローラに転送します。クラスタコントローラをDNSサーバーとして使用すると、以下のような多くの利点があります。 • **Automatic load balancing**（自動ロードバランシング） - クラスタコントローラがサービス通知ホスト名を解決すると、ホストクラスタノードはランダムな順序になり、ノードの負荷を有機的にバランスさせる効果があります。 • **Fault tolerance**（フォールトトレランス） - 1つのクラスタノードに障害が発生すると、クラスタコントローラはそれを自動的にDNS応答から削除し、ファイアウォールは起動しているノードに新しい要求を送信します。 • **Flexibility and ease of management**（柔軟性と管理の容易性 ）- コントローラがDNS応答を自動的に更新するため、クラスタにノードを追加すると、ファイアウォールを変更する必要はなく、要求は自動的に新しいノードと既存のノードに移動します。 DNSレコードはトラブルシューティングのためにキャッシュされるべきではありませんが、DNS検索が成功すると、TTLは0になりま

カテゴリ	説明
	す。ただし、DNS検索がNXDOMAINを返却する時は、TTLと「最小TTL」は両方とも0です。
管理	WildFireアプライアンスクラスタは、ローカルのWildFire CLIまたはPanoramaを使用して管理できます。WildFireクラスタノードには、ローカルで使用できる管理者ロールが2つあります。 • **Superreader**（スーパーリーダー） - 読み取り専用アクセス。 • **Superuser**（スーパーユーザー） - 読み取りと書き込みのアクセス権。
ファイアウォール登録	WildFireアプライアンスクラスタは、クラスタ内のすべてのノードを含む登録リストを、クラスタノードに接続されているすべてのファイアウォールにプッシュします。クラスタ内のアプライアンスにファイアウォールを登録すると、ファイアウォールは登録リストを受信します。すでにファイアウォールを接続しているスタンドアロンのWildFireアプライアンスをクラスタに追加してクラスタノードにすると、それらのファイアウォールは登録リストを受信します。 ノードに障害が発生した場合、接続されたファイアウォールは登録リストを使用してリストの次のノードに登録します。
データ移行	データの冗長性を実現するために、クラスタ内のWildFireアプライアンスノードはデータベース、キューイングサービス、およびサンプル提出コンテンツを共有しますが、このデータの正確な場所はクラスタトポロジによって異なります。その結果、クラスタ内のWildFireアプライアンスは、トポロジの変更が行われるたびにデータの移行やデータの再配置が行われます。トポロジの変更には、ノードの追加と削除、および既存のノードの役割の変更が含まれます。また、WildFire 7.1から8.0へのアップグレードのように、データベースが新しいバージョンに変換されると、データの移行が発生する可能性があります。 WildFire CLIからステータスコマンドを発行すると、データ移行ステータスを表示できます。この処理には、WildFireアプライアンス上のデータ量に応じて数時間かかることがあります。

WildFire クラスターのデプロイ

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

WildFireアプライアンスクラスタを展開するには、クラスタに登録するすべてのアプライアンスをアップグレードし、WildFireクラスタを作成してから、最後に必要に応じて設定を構成する必要があります。これらのタスクは、WildFireアプライアンスのCLIまたはPanoramaからローカルで実行できます。これにより、設定変更やアップグレードを接続したWildFireアプライアンスに迅速に適用できます。

次に、WildFire HA（高可用性）ペアを作成および設定し、アプライアンスノードをクラスタに追加する方法を示します。

STEP 1 | Upgrade your WildFire appliances locally（Wildfireアプライアンスをローカルで更新アップグレード）クラスタを動作させるためにサポートされている最小限のリリースであるPAN-OS 8.0.1以降にアップグレードします。

STEP 2 | WildFireアプライアンスクラスタにノードを作成、設定、追加します。

- Panoramaにクラスタを設定してノードをローカルに追加する
- Panoramaにクラスタを設定してノードを追加する

STEP 3 | WildFireアプライアンスクラスタが正常に動作していることを確認する。

- Panoramaの一般的なクラスタ設定をローカルで構成する
- Panoramaの一般的なクラスタ設定を構成する

STEP 4 | WildFire クラスタ アプライアンスからアプライアンス 通信の暗号化。

- CLI で事前定義済み証明書を使用するアプライアンス間暗号化の設定
- CLI でカスタム証明書を使用するアプライアンス間暗号化の設定
- Panorama 中枢で UsingPredefined 証明書を使用するアプライアンス間暗号化の設定
- Panorama 中枢で UsingCustom 証明書を使用するアプライアンス間暗号化の設定

STEP 5 | WildFireアプライアンスクラスタが正常に動作していることを確認する。

- CLIを使用したWildFireクラスタのステータスの表示
- Panoramaを使用したWildFireクラスタのステータスの表示

STEP 6 | （オプション）すでにクラスタに登録されているWildFireアプライアンスをアップグレードします。

- インターネット接続を使用してクラスタをローカルにアップグレードする
- インターネット接続なしでクラスタをローカルにアップグレードする
- インターネット接続を使用してクラスタをセンターでアップグレードする
- インターネット接続を使用してクラスタをセンターでアップグレードする

WildFireアプライアンスでローカルにクラスタを設定する

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

WildFireアプライアンスクラスタをローカルに設定する前に、高可用性コントローラノードのペアとして設定できる2つのWildFireアプライアンスと、クラスタの分析、ストレージ容量、および復元力を高めるワーカーノードとして機能するために必要な追加のWildFireアプライアンスを用意してください。

WildFireアプライアンスが新しい場合は、 WildFireで始動する をチェックして、WildFireライセンスの有効性の確認、ログの有効化、ファイアウォールのWildFireアプライアンスへの接続、基本的なWildFire機能の設定などの基本手順を完了させます。

Panorama を使用して WildFire アプライアンス クラスタを管理している場合は、WildFire クラスタを Panorama で一元的に設定することもできます。

WildFire アプライアンス クラスタを作成するには、クラスタに配置するすべてのWildFireアプライアンスをPAN-OS 8.0.1以降にアップグレードする必要があります。クラスタに追加する各*WildFire*アプライアンスで、システム情報の表示 | バージョンの一致を実行します。 *WildFire*アプライアンスの*CLI*でバージョンと一致し、アプライアンスが*PAN-OS 8.0.1*以降を実行していることを確認します。

WildFireアプライアンスが使用可能になったら、適切なタスクを実行します。

- Panoramaにクラスタを設定してノードをローカルに追加する
- Panoramaの一般的なクラスタ設定をローカルで構成する
- ローカルでクラスタからノードを削除する

Panoramaにクラスタを設定してノードをローカルに追加する

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

クラスタにノードを追加すると、クラスタはコントローラノード用に構成したインタフェースに基づいてノード間の通信を自動的にセットアップします。

STEP 1 | クラスタに追加する各WildFireアプライアンスがPAN-OS 8.0.1以降を実行していることを確認します。

各WildFireアプライアンスで、次を実行します。

```
admin@WF-500> show system info | match version
```

STEP 2 | WildFireアプライアンスがサンプルを分析しておらず、スタンドアロン状態（別のクラスタのメンバーではない）であることを確認します。

1. 各アプライアンスで、アプライアンスがサンプルを分析しているかどうかを表示します。

   ```
   admin@WF-500> show wildfire global sample-analysis
   ```

   pendingのサンプルは表示されません。すべてのサンプルは完成した状態でなければなりません。サンプルがpending（保留中）の場合、分析が完了するまで待ちます。Pending（保留中）のサンプルは、悪質なサンプルや悪意のあるサンプルとは別に表示されます。Finish Date（完了日）は、分析が終了した日時を表示します。
2. 各アプライアンスで、すべてのプロセスが実行中であることを確認します。

   ```
   admin@WF-500> show system software status
   ```
3. 各アプライアンスで、アプライアンスがスタンドアロン状態にあり、まだクラスタに属していないことを確認します。

   ```
   admin@WF-500> show cluster membership Service Summary:
    wfpc signature Cluster name:アドレス:10.10.10.100 Host
    name:WF-500 Node name: wfpc-000000000000-internal Serial
    number:000000000000 Node mode: stand_alone Server role:True
    HA priority:Last changed:Mon, 06 Mar 2017 16:34:25 -0800
    Services: wfcore signature wfpc infra Monitor status:Serf
    Health Status: passing Agent alive and reachable Application
    status: global-db-service:ReadyStandalone wildfire-
   apps-service:Ready global-queue-service:ReadyStandalone
    wildfire-management-service:Done siggen-db:ReadyMaster Diag
    report:10.10.10.100: reported leader '10.10.10.100', age 0.
    10.10.10.100: local node passed sanity check.
   ```

   強調表示された行は、ノードがスタンドアロンモードにあり、スタンドアロンアプライアンスからクラスタノードに変換する準備ができていることを示しています。

   これらの例(*000000000000*) の*12*桁のシリアル番号は一般的な例であり、実際のシリアル番号ではありません。ネットワーク内の*WildFire*アプライアンスには、一意の実際のシリアル番号があります。

STEP 3 | プライマリコントローラノードを設定します。

これには、ノードをHAペアのプライマリコントローラとして設定し、HAを有効にし、アプライアンスがHA制御リンクおよびクラスタ通信および管理に使用するインターフェイスを定義することが含まれます。

1. ハイアベイラビリティをイネーブルにし、コントローラのバックアップノードへの制御リンクインターフェイス接続を設定します（たとえば、eth3インターフェイス上）。

   ```
   admin@WF-500# set deviceconfig high-availability enabled yes
    interface ha1 port eth3 peer-ip-address <secondary-node-eth3-
   ip-address>
   ```

2. アプライアンスをプライマリコントローラノードとして設定します:

   ```
   admin@WF-500# set deviceconfig high-availability election-
   option priority primary
   ```

3. （オプション）コントローラーノードとコントローラーバックアップノード間のバックアップ高可用性インターフェースを、例えば管理インターフェース上で構成します。

   ```
   admin@WF-500# set deviceconfig high-availability interface
    ha1-backup port management peer-ip-address <secondary-node-
   management-ip-address>
   ```

4. クラスター内の通信と管理のための専用インターフェースを構成します。これには、クラスター名の指定、ノード・ロールのコントローラー・ノードへの設定などが含まれます。

   ```
   admin@WF-500# set deviceconfig cluster cluster-name <name>
    interface eth2 mode controller
   ```

   この例では、専用のクラスタ通信ポートとしてeth2を使用しています。

   クラスタ名は、最大長が63文字の有効なサブドメイン名である必要があります。小文字と数字のみが許可され、クラスタ名の先頭または末尾にない場合はハイフンとピリオドが使用されます。

STEP 4 | コントローラのバックアップノードを設定します。

これには、ノードをHAペアのバックアップコントローラとして設定し、HAを有効にし、アプライアンスがHA制御リンクおよびクラスタ通信および管理に使用するインターフェイスを定義することが含まれます。

1. ハイアベイラビリティをイネーブルにし、プライマリコントローラノード（この例ではeth3）で使用されているのと同じインターフェイス上のプライマリコントローラノードへの制御リンクインターフェイス接続を設定します。

```
admin@WF-500# set deviceconfig high-availability enabled yes
 interface ha1 port eth3 peer-ip-address <primary-node-eth3-
ip-address>
```

2. アプライアンスをコントローラのバックアップノードとして設定します。

```
admin@WF-500# set deviceconfig high-availability election-
option priority secondary
```

3. （推奨）コントローラーノードとコントローラーバックアップノード間のバックアップ高可用性インターフェースを、例えば管理インターフェース上で構成します。

```
admin@WF-500# set deviceconfig high-availability interface
 ha1-backup port management peer-ip-address <primary-node-
management-ip-address>
```

4. クラスター内の通信と管理のための専用インターフェースを構成します。これには、クラスター名の指定、ノード・ロールのコントローラー・ノードへの設定などが含まれます。

```
admin@WF-500# set deviceconfig cluster cluster-name <name>
 interface eth2 mode controller
```

STEP 5 | 両方のコントローラノードで設定を確定します。

各コントローラノードで：

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

両方のコントローラーノードで構成をコミットすると、2ノードのクラスターが形成されます。

STEP 6 | プライマリコントローラノードの設定を確認します。

プライマリコントローラノード：

```
admin@WF-500(active-controller)> show cluster membership
 Service Summary: wfpc signature Cluster name: mycluster
```

```
Address:10.10.10.100 Host name:WF-500 Node name:
wfpc-000000000000-internal Serial number:000000000000 Node mode:
controller Server role:True HA priority: primary Last changed:Sat,
04 Mar 2017 12:52:38 -0800 Services: wfcore signature wfpc
infra Monitor status:Serf Health Status: passing Agent alive and
reachable Application status:  global-db-service:oinedCluster
wildfire-apps-service:Ready  global-queue-service:JoinedCluster
wildfire-management-service:Done  siggen-db:ReadyMaster Diag
report:10.10.10.110: reported leader '10.10.10.100', age 0.
10.10.10.100: local node passed sanity check.
```

プロンプト (active-controller（アクティブ・コントローラー）) および強調表示されたApplication status（アプリケーション・ステータス）行は、ノードがコントローラー・モードであり、準備ができていて、プライマリ・コントローラー・ノードであることを示しています。

STEP 7 | セカンダリコントローラノードの設定を確認します。

セカンダリコントローラノード：

```
admin@WF-500(passive-controller)> show cluster membership
 Service Summary: wfpc signature Cluster name: mycluster
 Address:10.10.10.110 Host name:WF-500 Node name:
 wfpc-000000000000-internal Serial number:000000000000 Node
 mode: controller Server role:True HA priority: secondary Last
 changed:Fri, 02 Dec 2016 16:25:57 -0800 Services: wfcore signature
 wfpc infra Monitor status:Serf Health Status: passing Agent alive
 and reachable Application status:  global-db-service:oinedCluster
 wildfire-apps-service:Ready  global-queue-service:JoinedCluster
 wildfire-management-service:Done  siggen-db:ReadySlave Diag
 report:10.10.10.110: reported leader '10.10.10.100', age 0.
 10.10.10.110: local node passed sanity check.
```

プロンプト (passive-controller（パッシブ・コントローラー）) および強調表示されたApplication status（アプリケーション・ステータス）行は、ノードがコントローラー・モードであり、準備ができていて、バックアップコントローラー・ノードであることを示しています。

STEP 8 | ノード設定のテストを行います。

コントローラノードのAPIキーがグローバルに表示可能であることを確認します。

```
admin@WF-500(passive-controller)> show wildfire global api-keys
 allService Summary: wfpc signatureCluster name: mycluster
```

両方のアプライアンスのAPIキーを表示する必要があります。

STEP 9 | コントローラノード上の高可用性設定を手動で同期します。

コントローラーノードを同期させることで、設定が一致し、一度行うだけで済みます。構成が同期された後、コントローラー・ノードは設定を同期させたままにしておき、それらを再度同期させる必要はありません。

1. プライマリコントローラノードで、高可用性設定をリモートピアコントローラノードに同期させます。

```
admin@WF-500(active-controller)> request high-availability
 sync-to-remote running-config
```

プライマリコントローラノードの設定とコントローラバックアップノードの設定が一致しない場合は、プライマリコントローラノードの設定がコントローラバックアップノードの設定を上書きします。

2. 設定をコミットします：

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

STEP 10 | クラスタが正常に機能していることを確認します。

ファイアウォール関連の情報を確認するには、まず*DeviceSetupWildFire**Device (**デバイス**)** > ***Setup (**選択し**)** > ***WildFire**を、ノードを指すように**General Settings**（一般設定）を編集して、少なくとも*1*つのファイアウォールをクラスタノードに接続する必要があります。

1. 両方のコントローラがクラスタメンバーであることを確認するために、クラスタピアを表示します。

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

2. いずれかのコントローラノードから両方のノード(API keys（API キー）を作成した場合）からのAPIキーを表示します。

```
admin@WF-500(active-controller)> show wildfire global api-keys
 all
```

3. いずれかのコントローラノードから任意のサンプルにアクセスします。

```
admin@WF-500(active-controller)> show wildfire global sample-
status sha256 equal <value>
```

4. ファイアウォールはファイルを両方のノードに登録しアップロードすることができます。ファイヤーウォールがサンプルの転送に成功したことを確認します。
5. 両方のノードがファイルをダウンロードして分析できます。
6. クラスタの作成後に分析されたすべてのファイルには、各ノードに1つずつ、2つの格納場所が表示されます。

STEP 11 | （オプション）ワーカーノードを設定し、それをクラスタに追加します。

ワーカーノードはコントローラノードの設定を使用して、クラスタが一貫した設定になるようにします。クラスタに最大18のワーカーノードを追加できるので、クラスタ内に合計20ノードを追加できます。

1. プライマリコントローラノードで、コントローラノードのワーカーリストにワーカーを追加します。

   ```
   admin@WF-500(active-controller)> configure
    admin@WF-500(active-controller)# set deviceconfig cluster
    mode controller worker-list <ip>
   ```

   <*ip*> は、クラスターに追加するワーカー ノードの クラスター管理インターフェイス IP アドレスです。個別のコマンドを使用して、各ワーカー・ノードをクラスタに追加します。
2. コントローラー・ノードの設定をコミットします。

   ```
   admin@WF-500(active-controller)# commit
   ```
3. WildFireアプライアンスでクラスタワーカーノードに変換し、クラスタを参加するように設定し、クラスタ通信インターフェイスを設定して、アプライアンスをworker（ワーカー）モードにします。

   ```
   admin@WF-500> configure admin@WF-500# set deviceconfig cluster
    cluster-name <name> interface eth2 mode worker
   ```

   クラスター通信インターフェースは、コントローラー・ノード上のクラスター内通信に指定されたインターフェースと同じでなければなりません。この例では、eth2はクラスタ通信用にコントローラノードで設定されたインターフェイスです。
4. ワーカー・ノードの設定をコミットします。

   ```
   admin@WF-500# commit
   ```
5. すべてのサービスがワーカー・ノードで起動するのを待ちます。**show cluster membership**（クラスターメンバーシップを表示）を実行して、すべてのサービスが

表示されているApplicationstatus（アプリケーションステータス）と、すべてのサービスが起動している場合は Ready（準備完了） 状態のsiggen-dbを確認します。

6. いずれかのクラスタコントローラノードで、ワーカーノードが追加されたことを確認します。

```
admin@WF-500> show cluster all-peers
```

追加したワーカーノードがクラスタノードのリストに表示されます。間違ってWildFireアプライアンスをクラスタに誤って追加した場合は、Remove a Node from a Cluster Locally（ノードをクラスタからローカルに削除）できます。

STEP 12 | ワーカー・ノードの設定を確認します。

1. ワーカー・ノードで、Node mode（ノード・モード）フィールドにノードがワーカー・モードであることが示されていることを確認します。

```
admin@WF-500> show cluster membership
```

2. ファイアウォールがワーカーノードに登録され、ワーカーノードがファイルをダウンロードして分析できることを確認します。

Panoramaの一般的なクラスタ設定をローカルで構成する

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	☐ WildFire アライセンス

一部の一般的な設定はオプションで、一部の一般的な設定はデフォルト値であらかじめ設定されています。少なくとも、これらの設定をチェックして、クラスタ構成がニーズに合っていることを確認することが最善です。一般的な設定は次のとおりです。

- WildFireパブリッククラウドに接続し、サンプルをパブリッククラウドに送信する。
- データ保持ポリシーの設定。
- ログの設定。
- ファイアウォールがWildFireに送信するサンプルのタイプに最も適した解析環境をカスタマイズし、解析環境を設定する（環境に最も適したVMイメージ）
- DNSサーバ、NTPサーバなどのIPアドレスを設定する。

クラスタのプライマリコントローラノードでConfigure WildFire settings using the CLI（CLIを使用してWildFire設定を設定）する。残りのクラスタノードは、クラスタコントローラで設定された設定を使用します。

STEP 1 | WildFireクラスタの一般設定を構成します。このプロセスは、Configuring the WildFire Appliance（WildFireアプライアンス設定） と似ています。

1. （推奨）Reset the admin password（管理者パスワードをリセット）。
2. 管理インターフェイスを設定します。WildFireアプライアンスクラスタノードのIPアドレスとデフォルトゲートウェイを設定します。各WildFireアプライアンスクラスタノードには、同じサブネット内に静的IPアドレスが必要です。また、DNSサーバーのIPアドレスを設定します。
3. WildFireアプライアンスのクロックを設定します。手動で、またはNTPサーバーを指定してクロックを設定し、NTPサーバー認証を設定します。
4. アプライアンスがファイルの分析に使用する仮想マシンイメージを選択します。
5. （オプション）追加のユーザーにWildFireアプライアンスの管理を許可します。管理者アカウントを追加し、役割を割り当ててクラスタを管理します。
6. 管理者アクセス用のRADIUS認証を設定します。

STEP 2 | （オプション）クラスタをWildFireパブリッククラウドに接続し、クラスタが使用するクラウドサービスを設定します。

ビジネス上の理由でWildFireアプライアンスクラスタをパブリックWildFireクラウドに接続できない場合、クラスタをクラウドに接続すると次のような利点があります。

- クラウドのリソースを使用して、さまざまな方法を使用して、複数の環境でサンプル分析を実行します。
- ローカル分析を実行してクラスタから作業をオフロードする前に、自動的にクラウドに判定を問い合わせます。（デフォルトで無効化されています。）
- グローバルなWildFireコミュニティの恩恵を受け、その知性に貢献します。

この表の行で説明されている機能はクラスタ固有ではありません。スタンドアロンの*WildFire*アプライアンスでこれらの機能を設定することもできます。

1. 接続されているすべてのWildFireアプライアンスから集められたインテリジェンスのメリット：

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

   WildFireパブリッククラウドサーバのホスト名のデフォルト値は、`wildfire-public-cloud`です。Forward Files for WildFire Analysis（WildFire 分析のためのファイル）を任意の公開WildFireクラウドに転送することができます。
2. クラスタをWildFireパブリッククラウドに接続する場合、ローカル分析を実行する前にパブリッククラウドに判定を自動的に照会するかどうかを設定します。パブリッククラウドをクエリすると、まずローカルのWildFireクラスタの負荷が軽減されます。

   ```
   admin@WF-500(active-controller)# set deviceconfig setting
    wildfire cloud-intelligence cloud-query (no | yes)
   ```
3. クラスタをWildFireパブリッククラウドに接続する場合は、Submit Locally-Discovered Malware or Reports to the WildFire Public Cloud（ローカルで検出されたマルウェアまたはレポートをWildFireパブリッククラウドに送信する）情報のタイプ（診断データ、マルウェア分析に関するXMLレポート、マルウェアサンプル）を設定します。マルウェアサンプルを送信すると、クラスタはレポートを送信しません。

   ```
   admin@WF-500(active-controller)# set deviceconfig setting
    wildfire cloud-intelligence submit-diagnostics (no | yes)
    submit-report (no | yes) submit-sample (no | yes)
   ```

STEP 3 | （オプション）DNSプロトコルを使用してサービスステータスを公開するようにコントローラノードを設定します。

```
admin@WF-500(active-controller)# set deviceconfig cluster mode
 controller service-advertising dns-service enabled yes
```

STEP 4 | （オプション）悪意のある、良質なサンプルやグレーウェアサンプルのデータ保持ポリシーを設定します。

1. さまざまな種類のデータを保持する時間を選択します。

   ```
   admin@WF-500(active-controller)# set deviceconfig setting
    wildfire file-retention malicious <indefinite | 1-2000> non-
   malicious <1-90>
   ```

   悪質なサンプルを保持するためのデフォルトは不定です（削除しないでください）。悪質でない（良性およびグレーウェア）サンプルを保持するためのデフォルトは14日間です。

STEP 5 | （オプション）優先分析環境を設定します。

1. 分析環境が主に実行可能なサンプルまたはほとんどのドキュメントサンプルを分析する場合は、大半のクラスタリソースをそのサンプルタイプの分析に割り当てることができます。

   ```
   admin@WF-500(active-controller)# set deviceconfig setting
    wildfire preferred-analysis-environment (Documents |
    Executables | default)
   ```

   クラスタ内の各WildFireアプライアンスの場合：

   - `default`（デフォルト）のオプションでは、16個のドキュメント、10個の実行可能ファイル（PE）、2個の電子メールリンクを同時に分析します。
   - Documents（ドキュメント）オプションは、25個のドキュメント、1個のPE、2個の電子メールリンクを同時に分析します。
   - Executables（実行可能）オプションは、25個のドキュメント、1個のPE、2個の電子メールリンクを同時に分析します。

   クラスタ内の各ノードに異なる優先分析環境を構成できます。（Panoramaからクラスタを管理する場合、Panoramaはクラスタ全体の分析環境を設定できます）。

STEP 6 | ノード分析設定を設定する。

1. （オプション）マルウェア分析を改善するためにSet Up Content Updates（コンテンツ更新を設定）します。
2. Set Up the VM Interface（VMインターフェイスを設定）して、分析対象のサンプルがネットワークアクセスを求める悪意のある動作をクラスタが観察できるようにします。
3. （オプション）DNSおよびウイルス対策シグネチャおよびURLカテゴリを生成するには、Enable Local Signature and URL Category Generation（ローカル署名およびURLカテゴリ生成を有効）にします。

STEP 7 | ログの設定。

1. Configure WildFire Submissions Log Settings（WildFire提出ログの設定を設定する）。

ローカルでクラスタからノードを削除する

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

ローカルCLIを使用して、クラスタからノードを削除できます。ノードを削除する手順は、2ノードのクラスタでは、3ノード以上のクラスタとは異なります。

ノードが3つ以上あるクラスタからワーカーノードを削除します。

1. ワーカーノードのCLIからワーカーノードを削除する：

```
admin@WF-500> request cluster decommission start
```

   decommission（廃止）コマンドは、*3*つ以上のノードを持つクラスタでのみ機能します。*2*ノードクラスタ内のノードを削除するために*decommission*（廃止）を使用しないでください。

2. ノードの廃止が成功したことを確認します。

```
admin@WF-500> show cluster membership
```

   このコマンドは、ワーカーノードがクラスタから削除された後の`decommission: success`（廃止：成功）を報告します。コマンドで正常停止が表示されない場合は、廃止が終了するまで数分待ってからコマンドを再実行してください。

3. ワーカーノードのCLIからクラスタ設定を削除する：

```
admin@WF-500># delete deviceconfig cluster
```

4. 設定をコミットします：

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

5. 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> show system software status
```

6. ワーカーノードのCLIからワーカーノードを削除する：

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

7. 設定をコミットします：

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

8. いずれかのコントローラノードで、ワーカーノードが追加されたことを確認します。

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

   削除したワーカーノードはクラスタノードのリストに表示されません。

2ノードクラスタからコントローラノードを削除します。

各クラスタには、通常の状態で高可用性構成で2つのコントローラノードが必要です。ただし、コントローラノードをメンテナンスまたはスワップするには、CLIを使用してコントローラノードをクラスタから削除する必要があります。

1. 削除するコントローラノードをサスペンドします。

```
admin@WF-500(passive-controller)> debug cluster suspend on
```

2. 削除するコントローラノードで、高可用性構成を削除します。次に、コントローラのバックアップノードを削除する例を示します：

```
admin@WF-500(passive-controller)> configure
 admin@WF-500(passive-controller)# delete deviceconfig high-availability
```

3. クラスタ構成を削除します。

```
admin@WF-500(passive-controller)# delete deviceconfig cluster
```

4. 設定をコミットします：

```
admin@WF-500(passive-controller)# commit
```

5. サービスが復旧するのを待ちます。**show cluster membership**（クラスターメンバーシップを表示）を実行して、すべてのサービスが表示されているApplication status（アプリケーションステータス）と、すべてのサービスが起動している場合はReady（準備完了） 状態のsiggen-dbを確認します。Node mode（ノードモード）はstand_aloneである必要があります。
6. 残りのクラスタノードで、ノードが削除されたことを確認します。

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

削除したワーカーノードはクラスタノードのリストに表示されません。

7. 別のWildFireアプライアンスを準備している場合は、できるだけ早くクラスタに追加して高可用性を復元します（Configure a Cluster and Add Nodes Locally（クラスタの設定とローカルでのノードの追加））。

削除されたクラスタノードを置き換える準備ができている別のWildFireアプライアンスがない場合は、1ノードクラスタが推奨されず高可用性を提供しないため、残りのクラスタノードから高可用性およびクラスタ設定を削除する必要があります。1つ

のWildFireアプライアンスを1ノードクラスタではなくスタンドアロンアプライアンスとして管理する方がよい場合があります。

残りのノード（この例では、プライマリコントローラノード）から高可用性とクラスタ構成を削除するには、次の手順を実行します。

```
admin@WF-500(active-controller)> configure
 admin@WF-500(active-controller)# delete deviceconfig
 high-availability admin@WF-500(active-controller)# delete
 deviceconfig cluster admin@WF-500(active-controller)# commit
```

サービスが復旧するのを待ちます。**show cluster membership**（クラスターメンバーシップを表示）を実行して、すべてのサービスが表示されているApplication status（アプリケーションステータス）と、すべてのサービスが起動している場合はReady（準備完了） 状態のsiggen-dbを確認します。Node mode（ノードモード）はstand_aloneである必要があります。

WildFire アプライアンス間の暗号化を設定する

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

クラスタにデプロイされたアプライアンス間の WildFire 通信を暗号化できます。WildFire アプライアンスは、デフォルトで、管理アプライアンスおよび WildFire クラスタ ピアと通信するときにクリアテキストを使用してデータを送信します。事前定義した証明書またはカスタム証明書を使用して、IKE/IPsec プロトコルを使用して WildFire アプライアンス ピア間の接続を認証することができます。定義済みの証明書は、現在のFIPS/CC/UCAPL で承認されている証明書および準拠要件を満たしています。代わりにカスタム証明書を使用する場合は、FIPS/CC/UCAPL 準拠の証明書を選択する必要があります。これを選択しないと、証明書をインポートできなくなります。

WildFire CLI を使用して、または Panorama を通じて集中的に WildFire アプライアンス間の暗号化を設定できます。特定のクラスタ内のすべての WildFire アプライアンスは、暗号化された通信をサポートするバージョンの PAN-OS を実行する必要があります。

クラスタ内の *WildFire* アプライアンスが *FIPS/CC* モードを使用する場合、暗号化は事前定義された証明書を使用して自動的に有効になります。

アプライアンスをアプライアンスの暗号化に展開する方法に応じて、次のいずれかのタスクを実行します：

- Panorama 中枢で UsingPredefined 証明書を使用するアプライアンス間暗号化の設定
- Panorama 中枢で UsingCustom 証明書を使用するアプライアンス間暗号化の設定
- CLI で事前定義済み証明書を使用するアプライアンス間暗号化の設定
- CLI でカスタム証明書を使用するアプライアンス間暗号化の設定

CLI で事前定義済み証明書を使用するアプライアンス間暗号化の設定

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

CLI を使用してアプライアンス間の暗号化を設定する場合は、アクティブ コントローラとして指定された WildFire アプライアンスからすべてのコマンドを発行する必要があります。構成の変更はパッシブ コントローラに自動的に配信されます。3 つ以上のノードを持つクラスタを運用す

る場合は、アクティブ ノードと同じ設定でサーバー ノードとして機能する WildFire クラスタ アプライアンスも設定する必要があります。

STEP 1 | 管理対象の各 WildFire アプライアンスを PAN-OS 9.0 にアップグレードします。

STEP 2 | WildFire アプライアンス クラスタが正しく設定され、正常な状態で動作していることを確認します。

STEP 3 | アクティブ コントローラとして指定された WildFire アプライアンスで、安全なクラスタ通信を有効にします。

```
set deviceconfig cluster encryption enabled yes
```

STEP 4 | （推奨）HA トラフィックの暗号化を **Enable**（有効）にします。このオプションの設定は、HA ペア間の HA トラフィックを暗号化し、Palo Alto Networks が推奨するベストプラクティスです。

HA トラフィック暗号化は、*FIPS/CC* モードで動作しているときは無効にできません。

```
set deviceconfig high availability encryption enabled yes
```

STEP 5 | （ノードが 3 つ以上のアプライアンス クラスタのみ）クラスタに登録されている3番目の WildFire アプライアンスサーバノードについて、ステップ 2～4 を繰り返します。

CLI でカスタム証明書を使用するアプライアンス間暗号化の設定

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

CLI を使用してアプライアンス間の暗号化を設定する場合は、アクティブ コントローラとして指定された WildFire アプライアンスからすべてのコマンドを発行する必要があります。構成の変更はパッシブ コントローラに自動的に配信されます。3 つ以上のノードを持つクラスタを運用する場合は、アクティブ ノードと同じ設定でサーバー ノードとして機能する WildFire クラスタ アプライアンスも設定する必要があります。

STEP 1 | 管理対象の各 WildFire アプライアンスを PAN-OS 9.0 にアップグレードします。

STEP 2 | WildFire アプライアンス クラスタが正しく設定され、正常な状態で動作していることを確認します。

STEP 3 | 秘密鍵とその CA 証明書を使用して証明書をインポート（またはオプションで生成）します。以前にカスタム証明書を使用して WildFire アプライアンスとファイアウォールを安全

な通信用に設定していた場合、そのカスタム証明書を WildFire アプライアンス間のセキュア通信に使用することもできます。

1. カスタム証明書をインポートするには、WildFireアプライアンスCLIから次のように入力します: **scp import certificate from<value> file <value> remote-port <1-65535> source-ip <ip/netmask> certificate-name <value> passphrase <value> format <value>**
2. カスタム証明書を生成するには、WildFire アプライアンス CLI で以下のように入力します: **request certificate generate certificate-name name digest country-code state locality organization email filename ca signed-by | ocsp-responder-url days-till-expiry hostname [...] request certificate generate certificate-name name digest country-code state locality organization email filename ca signed-by | ocsp-responder-url days-till-expiry ip [...] request certificate generate certificate-name name**

STEP 4 | サーバー証明書と秘密鍵を含む WildFire アプライアンス鍵ペアをインポートします。

```
scp import keypair from<value> file <value> remote-port <1-65535>
 source-ip <ip/netmask> certificate-name <value> passphrase <value>
 format <pkcs12|pem>
```

STEP 5 | WildFire アプライアンスが SSL/TLS サービスに使用する証明書とプロトコルを定義するために、SSL/TLS プロファイルを設定および指定します。

set deviceconfig setting management secure-conn-server ssl-tls-service-profile <profile name>

1. SSL/TLS プロファイルを作成します。

```
set shared ssl-tls-service-profile <name>
```

2. カスタム証明書を指定します。

```
set shared ssl-tls-service-profile<name>certificate<value>
```

3. SSL/TLS 範囲を定義します。

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

```
set shared ssl-tls-service-profile<name>protocol-settings max-
version <tls1-0|tls1-1|tls1-2|max>
```

4. SSL/TLS プロファイルを指定します。この SSL/TLS サービス プロファイルは、WildFire アプライアンスとファイアウォール、および WildFire アプライアンス ピア間のすべての接続に適用されます。

```
set deviceconfig setting management secure-conn-server ssl-
tls-service-profile <ssltls-profile>
```

STEP 6 | WildFire アプライアンスが SSL/TLS サービスに使用する証明書とプロトコルを定義するために、証明書プロファイルを設定および指定します。

1. 証明書プロファイルを作成します。

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

2. （任意）サブジェクト（共通名）またはサブジェクト代替名を設定します

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

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

3. （任意）ユーザー ドメインを設定します。

```
set shared certificate-profile <name> domain <value>
```

4. CA を設定します。

```
set shared certificate-profile <name> CA <name>
```

```
set shared certificate-profile <name> CA <name> default-ocsp-
url <value>
```

```
set shared certificate-profile <name> CA <name> ocsp-verify-
cert <value>
```

5. 証明書プロファイルを指定します。

```
set deviceconfig setting management secure-conn-server
 certificate-profile <certificate-profile>
```

STEP 7 | 証明書と秘密鍵ペアをインポートします。

STEP 8 | WildFire アプライアンス クラスタをファイアウォール カスタム証明書に関連付けるには、Panorama のファイアウォールのセキュア通信設定を構成します。これにより、ファイアウォールと WildFire アプライアンス クラスタ間の安全な通信チャネルが提供されます。ファイアウォールと WildFire アプライアンスクラスター間のセキュリティで保護された通信を既に構成していて、既存のカスタム証明書を使用している場合は、手順に進みます。 9

1. **Device (**デバイス**)** > **Certificate Management (**証明書管理**)** > **Certificate Profile (**証明書プロファイル**)** を選択します。
2. 証明書プロファイルの設定を行います。

3. **Device**（デバイス）> **Setup**（セットアップ）> **Management**（管理）> **Secure Communication Settings**（セキュア通信設定）を選択して、**Secure Communication Settings**（セキュア通信設定）の **Edit**（編集）アイコンをクリックすることで、 ファイアウォールのカスタム証明書設定を設定します。
4. ドロップダウンメニューから **Certificate Type**（証明書タイプ）、**Certificates**（証明書）、および **Certificate Profile**（証明書プロファイル）をそれぞれ選択して、ステップ 2 で作成したカスタム証明書を使用するように設定します。
5. カスタマイズ通信で、**WildFire Communication**（**WildFire** 通信）を設定します。
6. **OK** をクリックします。

STEP 9 | 事前定義の証明書の使用を無効にします。

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

STEP 10 | カスタム証明書に含まれる認証に使用される DNS 名（通常は SubjectName または SubjectAltName）を指定します。たとえば、デフォルトのドメイン名は **`wfpc.service.mycluster.paloaltonetworks.com`** です。

```
set deviceconfig setting wildfire custom-dns-name <custom_dns_name>.
```

STEP 11 | （ノードが 3 つ以上のアプライアンス クラスタのみ）クラスタに登録されている3番目の WildFire アプライアンスサーバノードについて、ステップ 2～10 を繰り返します。

WildFire クラスターのモニター

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

CLIまたはPanoramaを使用して、WildFireクラスタの動作ステータスを確認できます。これにより、特定のノード上で実行されているapplications（アプリケーション）およびservices（サービス）が正しく機能していることを確認できます。WildFireクラスタを正しく実行するには、適切なサービスとアプリケーションが各ノードでアクティブでなければならず、それぞれのステータスが正常な状態でなければなりません。これらのパラメータの外部で動作するクラスタは、最適な条件下では動作しないか、その他の問題と構成の問題を示す可能性があります。

*CLI*は、*Panorama*から入手できない情報を表示します。クラスタ関連の問題をトラブルシューティングする場合は、*WildFire CLI*を使用することを強くお勧めします。

WildFire CLIから一連のshow（表示）コマンドを実行することにより、WildFireコントローラノードの現在のステータスを表示できます。コマンドは、構成の詳細、アプライアンス上で実行されている現在のアプリケーションとサービス、およびステータス/エラーメッセージを表示します。これらの詳細を使用して、クラスターの状況を判別することができます。ステータスを表示してもWildFireサービスが中断されることはなく、いつでも実行できます。

WildFire アプライアンスの監視詳細については以下のセクションをご覧ください。

- CLIを使用したWildFireクラスタのステータスの表示
- Panoramaを使用したWildFireクラスタのステータスの表示
- WildFireアプリケーションの状態
- WildFireサービスの状態

CLIを使用したWildFireクラスタのステータスの表示

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

WildFireクラスタが通常の動作パラメータ内で動作していることを確認するには、次のshowコマンドを実行する必要があります。

- **`show cluster controller`**（クラスタコントローラーのっ表示）—アクティブ/パッシブのWildFireクラスタノードのステータスを表示します。

- **show cluster all-peers**（クラスタすべてのピアを表示） —特定のWildFireクラスタ内のすべてのメンバーに関する情報を表示します。
- **show cluster membership**（クラスタメンバーシップを表示）—クラスタノードとスタンドアロンノードのWildFireアプライアンス情報を表示します。
- **show cluster data-migration-status**—データ移行プロセスの最新のステータスを表示します。
- **show log system**—システムステータス詳細を含むWildFireイベントログを表示します。

STEP 1 | WildFireアプライアンスコントローラノードで次のコマンドを実行します。

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

正常なWildFireクラスタには、次の詳細が表示されます。

- アプライアンスが登録されているクラスターの名前とその構成済みの役割。
- 内部クラスタインターフェイスが正常に機能している場合、`K/V API online status`（K / V APIオンラインステータス）は`True`（真）を示します。ステータスが`False`（誤） の場合、ノードまたはネットワークの問題が正しく構成されていない可能性があります。
- `Task processing`（タスク処理）は、アクティブコントローラ（プライマリ）では`True`（真）を、パッシブコントローラ（バックアップ）では`False`（誤）を示します。
- クラスタ内のすべてのWildFireノードのIPアドレスは、`App Service Avail`（アプリサービスアヴェイル）の下に表示されます。
- 三大`Good Core Servers`（良好なコアサーバ）。`Good Core Servers`（良好なコアサーバ）の数は、クラスタ内で実行されているノードの数によって異なります。3つ目のノードがクラスタ内で動作している場合、クラスタの整合性を最大限にするために自動的にサーバーノードとして構成されます。
- `Suspended Nodes`（中断されたノード）はありません。
- `Current Task`（現在のタスク）は、再起動、廃止、タスクの中断など、クラスタレベルの操作に関する背景情報を提供します。

次の例は、健全な状態で動作している2ノードのWildFireクラスタで構成されたアクティブコントローラからの出力を示しています。

```
クラスター名:WildFire_Cluster K/V API オンライン:真のタスク処
理: アクティブ コントローラ上:True DNS Advertisement:App Service
 DNS Name:App Serviceの利用可能性：2.2.2.14、2.2.2.15 コア サー
バー:009701000026:2.2.2.15 009701000043:2.2.2.14 優れたコア サー
バー:注2 サスペンドノード:現在のタスク: * 完了した最新のタスクを表示 要
求: qa14 (009701000043/80025) から 2017-09-18 21:43:34 UTC に起動
 null 応答: 2017-09-18 21:45:15 UTC 1/2 コア サーバが利用可能で qa15 に
よる許可。終了: 2017-09-18 21:43:47 UTC での成功
```

STEP 2 | WildFireアプライアンスコントローラノードで次のコマンドを実行します。

```
admin@WF-500> クラスター全ピアを表示
```

正常なWildFireクラスタには、次の詳細が表示されます。

- クラスタ内のWildFireノードに関する一般的な情報は、`Address`（アドレス）、`Mode`（モード）、`Server`（サーバー）、`Node`（ノード）および`Name`（名前）の下に表示されます。
- すべてのWildFireクラスタノードは、内部ファイルサンプル分析サービスである`wfpc`サービスを実行しています。
- アクティブ、パッシブ、またはサーバーとして動作するノード`Server role applied`（適用されたサーバーの役割）は、`Status`（ステータス）の横に適用されます。ノードがサーバーとして構成されていても、サーバーとして動作していない場合は、`Server role assigned`（割り当てられたサーバーの役割）が`status`（ステータス）に表示されます。

  *3*ノードデプロイメントでは、*3*番目のサーバーノードがワーカーに分類されます。
- 最近削除されたノードが存在する可能性がありますが、`Disconnected`（接続切断）と表示されます。切断されたノードをクラスタノードリストから削除するには、数日かかることがあります。
- アクティブコントローラノードに`siggen-db:ReadyMaster`が表示されます。
- パッシブコントローラノードに`siggen-db:ReadySlave`が表示されます。

  一般的な*WildFire*アプリケーションとサービスステータスの詳細については、WildFire Application States（WildFireアプリケーション状態）およびWildFire Service States（WildFire サービス状態）を参照してください。
- `Diag report`（ダイアログレポート）には、クラスタシステムのイベントとエラーメッセージが表示されます。

エラー メッセージ	詳説
到達不能	クラスタコントローラはノードに到達できませんでした。
予期しないメンバー	ノードはクラスタ構成の一部ではありません。ノードが最近クラスタ構成または構成ミスの結果から削除された可能性があります。
左クラスタ	クラスタコントローラはもうノードに到達できません。

エラー メッセージ	詳説
正しくないクラスタ名	ノードのクラスタ名が正しく設定されていません。
接続が不安定	クラスタコントローラへのノードの接続は不安定です。
接続の損失	クラスタコントローラへのノードの接続が失われました。
予期しないサーバーのシリアル番号	予期せぬサーバーノードの存在が検出されました。

次の例は、正常な状態で動作している3ノードのWildFireクラスタを示しています。

```
アドレス モード サーバー ノード名 ------- ---- ------ --------- 2.2.2.15
 controller Self True qa15 Service: infra signature wfcore wfpc
 Status:接続済み、適用されたサーバーの役割 変更:月, 18 Sep 2017 15:37:40
 -0700 WF アプリ: グローバル db-service:JoinedCluster wildfire-apps-
service：global-queue-serviceを停止しました：JoinedCluster wildfire-
management-service：完了siggen-db：ReadySlave2.2.2.14コントロー
ラーPeerTrueqa14サービス：インフラ署名wfcore wfpcステータス：接続済み、
適用されたサーバーの役割 変更:2017年9月18日月曜日15:37:40-0700WFアプ
リ：global-db-service：commit-lock wildfire-apps-service：global-
queue-serviceを停止しました：ReadyStandaloneの山火事管理サービ
ス：完了siggen-db：ReadyMaster2.2.2.16ワーカーTruewf6240サービ
ス：インフラwfcore wfpcステータス：接続済み、適用されたサーバーの役
割 変更:2017年2月22日水曜日11:11:15-0800WFアプリ：wildfire-apps-
service：Ready global-db-service:JoinedCluster global-queue-
service:JoinedCluster local-db-service：DataMigrationFailed Diagレ
ポート：2.2.2.14: 報告されたリーダー「2.2.2.15」、0歳。2.2.2.15: ローカル
ノードがサニティチェックに合格しました。
```

STEP 3 | WildFireアプライアンスコントローラノードで次のコマンドを実行します。

```
admin@WF-500>クラスター メンバーシップを表示
```

正常なWildFireクラスタには、次の詳細が表示されます。

- クラスタ名、アプライアンスのIPアドレス、シリアル番号など、一般的なWildFireアプライアンスの設定の詳細
- `Server role`（サーバの役割）は、WildFireアプライアンスがクラスタサーバとして動作しているかどうかを示します。クラスタサーバーは、追加のインフラストラクチャアプリ

ケーションとサービスを運用します。クラスタごとに最大3つのサーバーを持つことができます。

- `Node mode`（ノードモード）は、WildFireアプライアンスの役割を示します。クラスタに登録されているWildFireアプライアンスは、コンフィグレーションと展開内のノード数に応じて、`controller`（コントローラ）ノードまたは`worker`（ワーカー）ノードのいずれかになります。クラスタの一部ではないアプライアンスは`stand_alone`を表示します。
- クラスタノードの役割に基づいて、次の`Services`（サービス）を操作します。

ノードタイプ	ノード上で動作するサービス
コントローラノード（アクティブまたはパッシブ）	• インフラ • `wfpc` • シグネチャ • `wfcore`
サーバーノード	• インフラ • `wfpc` • `wfcore`
ワーカーノード	• インフラ • `wfpc`

- `HA priority`（HAの優先順位）は、設定された役割によってプライマリまたはセカンダリを表示しますが、この設定はアプライアンスの現在のHA状態とは関係ありません。
- `Work queue status`（ワークキューステータス）には、サンプル分析バックログと現在分析中のサンプルが表示されます。これは、特定のWildFireアプライアンスが受信する負荷量も示します。

*WildFire*のアプリケーションとサービスのステータスの詳細については、WildFire Application States（WildFireのアプリケーションの状態）とWildFire Service States（WildFireのサービスの状態）を参照してください。

次の例は、正常な状態で動作しているWildFireクラスタを示しています。

```
サービス概要: wfpc 署名 クラスター名: qa-auto-0ut1 アドレ
ス:2.2.2.15 ホスト名: qa15 ノード名: wfpc-009701000026-内部シリアル番
号:009701000026 ノード モード: コントローラー サーバーの役割:真の HA 優
先度: セカンダリ 最終更新日:Fri, 22 Sep 2017 11:30:47 -0700 サービス:
 wfcore 署名 wfpc infra モニターの状態:Serf 正常性状態: エージェントが生
きていて到達可能なサービスに合格する 'infra' チェック: 合格 アプリケーショ
ン状態: global-db-service:ReadyLeader wildfire-apps-service:Ready
```

```
 global-queue-service:ReadyLeader wildfire-management-service:完了siggen-db：準備完了ワーク キューの状態: キューに入れられたサンプル分析:0サンプル分析の実行:0 sample copy queued:0 sample copy running:0 診断レポート:2.2.2.14: 報告されたリーダー「2.2.2.15」、0歳。2.2.2.15: ローカルノードがサニティチェックに合格しました。
```

STEP 4 | WildFireアプライアンスコントローラノードで次のコマンドを実行します。

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

WildFireアプライアンスには、以下のデータ移行の詳細が表示されます:

- データの移行中は、ファイルをWildFireアプライアンス クラスタに転送しないでください。データ移行が完了すると、完了タイムスタンプが表示されます。
- WildFireクラスターへのトポロジーの変更（ノードの追加または削除、ノードのロールの変更など）は、データ移行イベントをトリガーします。
- WildFireの新しいバージョンへのアップグレード時にデータの移行が発生する可能性があります。アップグレード後、WildFireクラスターの動作ステータスを確認して、適切な機能を確認してください

以下の例は、WildFireアプライアンスクラスタでのデータ移行の進行状況を示しています。

```
admin@WF-500(active-controller)>:9月9日(月)21:44:48 PDT 2019に完了したデータ移行ステータスを100%表示
```

STEP 5 | WildFireアプライアンスのアクティブ、パッシブ、およびサーバーノードで、次のコマンドを実行します。

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

このコマンドは、WildFireアプライアンス サブタイプとして分類されたすべてのWildFireログイベントを最も新しいものから古いものへと表示します。

- このコマンドは、クラスタ内のすべてのノードに発行する必要があります。たとえば、3ノード クラスタを運用している場合は、アクティブ コントローラ、パッシブ コントローラ、およびサーバー ノードのステータスを確認する必要があります。
- WildFireアプライアンスのCLIによって返されるログメッセージには、多数のサブタイプが含まれる場合があります。ログは一般的なサブタイプのキーワードに基づいてフィルタリングできます。特定の文字列に基づいてフィルタリングするには、以下のコマンド引数を使用します:
  - global-queue—**matchqueue**、例: **show log system directionequal backward | match queue**
  - global-database—**match global**、例: **show log system direction equal backward | matchglobal**

- signature-generation—**match signature**、例: **show log system direction equal backward| match signature**

- WildFireアプライアンスクラスターは、通常、2ノードクラスターの各ノードについて次のステータスの読み出しを返します。正常なWildFireクラスターノードは、アプライアンスのロールに基づいて異なるステータスの読み取り値を持っています。

  次のチェックリストを使用して、WildFire アプライアンスサービスがクラスター展開で正しく実行されていることを確認します。

  - **Active Controller**

Component	Active Controller Status
global-queue	❑ info ワイルドファイアクラスター 0 Global queue (rabbitmm) q) クラスターの形成は、ステータス ReadyLeader ❑ info general 0 グローバル キュー サービスのセットアップ ポリシー
global-database	❑ 情報一般 0 私はクラスタリーダーです、bootstrap for global-db service ❑ info general 0 Setup policy for global-queue service
signature-generation	❑ info wildfir cluster 0 Signature generation service status set to ReadyMaster ❑ info wildfir cluster 0 Signature generation service status set to ReadyMaster

*WildFire*アプライアンスから返されるログメッセージは、新しいものから古いものに表示されます。上記の手順に示すように、***direction equalbackward*** コマンド引数を使用しない場合、*WildFire* アプライアンス *CLI* はログメッセージを最も古いものから新しいものへ返します。

  - パッシブコントローラー

コンポーネント	PAssive コントローラーステータスの例
グローバルキュー	❑ infogeneral general 0 グローバル・キュー・サービスのポリシー設定 ❑ info wildfire cluster 0 グローバルキュー (rabbitmq)クラスタ形成が成功し、ステータスが JoinedCluster になった

コンポーネント	PAssive コントローラーステータスの例
	❑ info general general 0 Join cluster for global-queueservice - 成功 ❑ info general general 0 グローバル・キュー・サービスのポリシー設定
グローバルデータベース	❑ infogeneral general 0 グローバル・キュー・サービスのポリシー設定 ❑ info general general 0 アプリケーションをリストアする：global-dbのブートストラップとクラスタへの参加の完了 ❑ info general general 0 vm_mgrを起動ブートストラップとクラスタへの参加 ❑ info general general 0 uwsgiを開始ブートストラップとクラスタへの参加 ❑ info general general 0 wf_servicesを開始global-dbブートストラップとクラスタへの参加 ❑ info general general 0 アプリケーションを一時停止する：global-dbのブートストラップとクラスタへの参加は完了 ❑ info general general 0 vm_mgr を停止、global-db 用ブートストラップとクラスタへの参加 ❑ info general general 0 uwsgiを停止ブートストラップとクラスタへの参加 ❑ 0 wf_servicesを停止global-db ブートストラップとクラスタへの参加 ❑ info general general 0 ブートストラップとクラスタへの参加グローバルDBサービス用
署名生成	❑ infowildfir cluster 0 署名生成サービスのステータスをReadySlaveに設定 ❑ info wildfir cluster 0 署名生成サービスステータスをReadySlaveに設定

WildFire アプライアンスから返されるログ メッセージは、新しいものから古いものへと表示されます。上記の手順に示すように、***direction equalbackward*** コマンド引数を使用しない場合、*WildFire* アプライアンス *CLI* はログメッセージを最も古いものから新しいものへ返します。

- WildFireアプライアンスクラスターは、通常、3ノードクラスターの各ノードについて次のステータスの読み出しを返します。正常なWildFireクラスターノードは、アプライアンスのロールに基づいて異なるステータスの読み取り値を持っています。

  次のチェックリストを使用して、WildFireアプライアンスのサービスがクラスタ展開で正しく実行されていることを確認します。.

  - アクティブコントローラー

コンポーネント	アクティブ・コントローラーのステータス
グローバルキュー	☐ infowildfire cluster 0 グローバルキュー(rabbitmq)クラスタ形成成功 status JoinedCluster ☐ info general general 0 global-queueのクラスタに参加する。サービス - 成功 ☐ info general general 0 グローバル・キュー・サービスのポリシー設定
グローバルデータベース	☐ info0 アプリケーションのリストア：完了、グローバルDBブートストラップ用およびクラスター参加用 ☐ info general general 0 vm_mgrを起動する。ブートストラップとクラスタへの参加 ☐ info general general 0 uwsgiを開始するブートストラップとクラスタへの参加 ☐ info general general 0 wf_servicesを開始するglobal-db ブートストラップとクラスタへの参加 ☐ info general general 0 アプリケーションを一時停止する：global-dbのブートストラップとクラスタへの参加の完了 ☐ info general general 0 Stop vm_mgr, For global-dbブートストラップとクラスタへの参加 ☐ info general general 0 Stop uwsgi, For global-dbブートストラップとクラスタへの参加 ☐ info general general 0 Stop wf_services, Forglobal-db bootstrap and join cluster ☐ 2019/07/19 14:40:19 info general general 0global-dbサービスのブートストラップとクラスタへの参加
signature-generation	☐ infowildfire cluster 0 署名生成サービスのステータスをReadyMasterに設定

コンポーネント	アクティブ・コントローラーのステータス

WildFire アプライアンスから返されるログ メッセージは、新しいものから古いものへと表示されます。上記の手順に示すように、***direction equalbackward*** コマンド引数を使用しない場合、*WildFire* アプライアンス *CLI* はログメッセージを最も古いものから新しいものへ返します。

- パッシブコントローラ

Component	パッシブコントローラステータス
global-queue	❑ info general 0 グローバル キュー サービスのセットアップ ポリシー ❑ info general general 0 グローバル キュー サービスのセットアップ ポリシー ❑ info wildfireクラスター 0 グローバル キュー (rabbitmq) クラスターの形成は、ステータス ReadyLeader ❑ info 一般的な一般的な 0 グローバル キュー サービスのセットアップ ポリシー
global-database	❑ infogeneral 0 I'm cluster leader, bootstrap for global-db service ❑ info general general 0 Setup Policy for global-queue service
signature-generation	❑ info wildfireクラスター 0 署名生成サービスの状態がReadySlaveに設定 ❑ info wildfireクラスター 0 署名生成サービスのステータスが ReadySlaveに設定

*WildFire*アプライアンスから返されるログメッセージは、新しいものから古いものに表示されます。上記の手順に示すように、***direction equalbackward*** コマンド引数を使用しない場合、*WildFire* アプライアンス *CLI* はログメッセージを最も古いものから新しいものへ返します。

- サーバーノード

コンポーネント	サーバー・ノード・ステータス
global-queue	❑ infowildfire cluster 0 グローバルキュー(rabbitmq)クラスタ形成成功status JoinedCluster

コンポーネント	サーバー・ノード・ステータス
	❑ info general general 0 Join cluster for global-queueservice - succeeded ❑ info general general 0 グローバル・キュー・サービスのポリシー設定 ❑ info wildfire cluster 0 グローバルキュー(rabbitmq)クラスタ形成はStandbyAsWorkerステータスで成功
グローバルデータベース	❑ info0 アプリケーションのリストア：完了、グローバルDBのブートストラップとクラスタへの参加 ❑ info general general 0 vm_mgrを起動ブートストラップとクラスタへの参加 ❑ info general general 0 uwsgiを開始ブートストラップとクラスタへの参加 ❑ info general general 0 wf_servicesを開始global-dbブートストラップとクラスタへの参加 ❑ info general general 0 アプリケーションを一時停止する：global-dbのブートストラップとクラスタへの参加の完了 ❑ info general general 0 vm_mgrを停止ブートストラップとクラスタへの参加 ❑ info general general 0 uwsgiを停止ブートストラップとクラスタへの参加 ❑ 0 wf_servicesを停止global-db ブートストラップとクラスタへの参加 ❑ 2019/07/19 14:32:50 一般情報一般 0ワーカーノードをプロモートし、global-dbサービスのクラスタに参加
署名生成	❑ infowildfire cluster 0 署名生成サービスのステータスを停止に設定 ❑ critical wildfire cluster 0 Signature DataMigrationDone

WildFire アプライアンスから返されるログ メッセージは、新しいものから古いものへと表示されます。上記の手順に示すように、***direction equalbackward*** コマンド引数を使用しない場合、*WildFire* アプライアンス *CLI* はログメッセージを最も古いものから新しいものへ返します。

WildFireアプリケーションの状態

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

WildFireアプライアンスは、サンプルデータの処理を管理および調整するための一連の内部アプリケーションを実行します。これらのアプリケーションとその必要なステータスは、WildFireアプライアンスクラスタのステータスを表示するときに表示されます。

次のリストは、クラスタのコンポーネント、目的、および状態の条件を示しています。

名前	説明	可能なステータス条件	定義
global-db-service	このアプリケーションデータベースは、WildFire分析データを格納するために使用されます。	AcquiringSessionSpinLock	ロックまたはタイムアウトを取得するまで、セッションのスピンロックを待っている状態です。
		Bootstrapping	サンプル・データベース・アプリケーションは、現在、ブートストラップ状態です。
		BootstrappingNoMeet	ローカルのサンプルデータベースサービスは、他のWildFireアプライアンスとクラスタを形成することなく開始されました。
		FailedToBecomeWorker	ワーカーノードとしてクラスタに参加できませんでした。
		FailedToBootstrap	ブートストラップ処理が失敗しました。
		FailedToJoinCluster	クラスタに参加できませんでした。
		FailedToStartServices	内部データベースサービスの開始に失敗しました。

名前	説明	可能なステータス条件	定義
		MaintenanceDecommission	データベースサービスのデコミッションプロセスの開始。
		MaintenanceDecommissionDone	データベースサービスが廃止されました。
		MaintenanceFailover	ローカルサービスを降格させ、バックアップレプリカをフェールオーバーするプロセスを開始します。
		MaintenanceFailover	サービスフェールオーバーに失敗しました。
		MaintenanceFailoverDone	サービスのフェールオーバーが完了しました。
		MaintenanceRecoverFromSplitbrain	WildFireアプライアンスが現在スプリットブレインモードの場合、データベースサービスの状態はサービスの開始時に MaintenanceRecoverFromSplitbrainに設定されます。
		MaintenanceSuspend	ユーザーが[debug cluster suspend]または[request cluster deommission]のいずれかのコマンドを発行した結果、データベースサービスが中断中です。
		MaintenanceSuspendDone	データベースサービスが停止プロセスを完了しました。
		DataMigration	ローカル・データベースの内容がプライマリ・データベースとマージされています。これは、WildFireアプ

名前	説明	可能なステータス条件	定義
			ライアンスがクラスタに加わるときに発生します。
		DataMigrationDone	データ移行プロセスは完了しました。
		DataMigrationFailed	データ移行プロセスが失敗しました。
		JoinedCluster	ローカルデータベースサービスがクラスタに参加しました。
		Ready	データベースサービスは準備完了状態です。
		ReadyLeader	データベースサービスは準備完了状態にあり、アプライアンスはリーダーとして設定されています。
		ReadyStandalone	データベースサービスは準備完了状態にあり、アプライアンスはスタンドアロンアプライアンスとして動作しています。
		Splitbrain	スプリットブレイン状態が検出され、データベースサービスがスプリットブレインモードに入りました。サービスはすぐにReadyStandaloneに移行します。
		StandbyAsWorker	ワーカー・ノード・データベース・サービスはスタンバイ状態です。
		WaitingforLeaderReady	ローカルノードはリーダーノードへの参加を待機中です。

名前	説明	可能なステータス条件	定義
global-queue-service	WildFire分析のために送信されたサンプルの管理と優先順位付けを処理します。	Bootstrapping	キューイングサービスアプリケーションは、現在、ブートストラップ状態にあります。
		FailedToBecomeWorker	ワーカーノードとしてクラスタに参加できませんでした。
		FailedToBootstrap	ブートストラップ処理が失敗しました。
		FailedToJoinCluster	クラスタに参加できませんでした。
		FailedToStartServices	内部キューベースサービスの開始に失敗しました。
		MaintenanceDecommission	キューサービスのデコミッションプロセスの開始。
		MaintenanceDecommissionDone	キューベースサービスが廃止されました。
		MaintenanceFailover	ローカルサービスを降格させ、バックアップレプリカをフェールオーバーするプロセスを開始します。
		MaintenanceFailover	サービスフェールオーバーに失敗しました。
		MaintenanceFailoverDone	サービスのフェールオーバーが完了しました。
		MaintenanceRecoverFromSplitbrain	WildFireアプライアンスが現在split-brainモードになっている場合、キューイングサービスの状態は次のように設定されます。

名前	説明	可能なステータス条件	定義
		MaintenanceSuspend	ユーザーが[debug cluster suspend]または[request cluster deommission]のいずれかのコマンドを発行した結果、キューサービスが中断中です。
		MaintenanceSuspendDone	キューサービスが停止プロセスを完了しました。
		JoinedCluster	キューサービスがクラスタに参加しました。
		Ready	キューサービスは準備完了状態です。
		ReadyLeader	キューサービスは準備完了状態にあり、アプライアンスはリーダーとして設定されています。
		ReadyStandalone	キューサービスは準備完了状態にあり、アプライアンスはスタンドアロンアプライアンスとして動作しています。
		Splitbrain	スプリットブレイン状態が検出され、キューサービスがスプリットブレインモードに入りました。サービスはすぐにReadyStandaloneに移行します。
		StandbyAsWorker	ワーカー・ノード・キュー・サービスはスタンバイ状態です。

名前	説明	可能なステータス条件	定義
siggen-db	WildFireのプライベートシグネチャと分析サンプルを生成します。	DatabaseFailover	HAフェールオーバーが発生すると、パッシブコントローラがアクティブコントローラになります。パッシブコントローラのシグネチャサービスがプライマリになり、状態がDatabaseFailoverに設定されます。
		DatabaseFailoverFaild	シグネチャデータベースフェールオーバーに失敗しました。
		DataMigration	ローカルシグネチャデータベースの内容がプライマリ・データベースとマージされています。これは、WildFireアプライアンスがクラスタに加わるときに発生します。
		DataMigrationDone	データ移行プロセスは完了しました。
		DataMigrationFailed	データ移行プロセスが失敗しました。
		Deregistered	シグネチャデータベースサービスが登録抹消されました。
		MaintenanceDecommission	シグネチャデータベースサービスのデコミッションプロセスの開始。
		MaintenanceDecommissionDone	キューベースサービスが廃止されました。
		MaintenanceFailover	ローカルサービスを降格させ、バックアップレプリカ

名前	説明	可能なステータス条件	定義
			をフェールオーバーするプロセスを開始します。
		MaintenanceFailoverDone	サービスのフェールオーバーが完了しました。
		MaintenanceSuspend	ユーザーが[debug cluster suspend]または[request cluster deommission]のいずれかのコマンドを発行した結果、シグネチャデータベースサービスが中断中です。
		MaintenanceSuspendDone	シグネチャデータベースサービスが停止プロセスを完了しました。
		MigrateMalwareDatabase	PAN-OSをバージョン7.1から8.0にアップグレードすると、サンプルデータは別の形式に変換されます。これらの状態は、データ移行プロセスの進行状況を示します。
		MigrateSiggenDatabaseStage1	
		MigrateSiggenDatabaseStage2	
		MigrateSiggenDatabaseStage3	
		Ready	シグネチャデータベースサービスは準備完了状態です。
		ReadyMaster	シグネチャデータベースサービスはプライマリモードであり、アクティブコントローラ上で動作しています。
		ReadySlave	シグネチャデータベースサービスはバックアップモードにあり、パッシブコントローラで動作しています。

名前	説明	可能なステータス条件	定義
		ReadyStandalone	シグネチャデータベースサービスは準備完了状態にあり、アプライアンスはスタンドアロンアプライアンスとして動作しています。
		Splitbrain	スプリットブレイン状態が検出され、シグネチャデータベースサービスがスプリットブレインモードに入りました。サービスはすぐにReadyStandaloneに移行します。
		Stopped	シグネチャデータベースサービスがアプライアンスで停止しました。

名前	説明	可能なステータス条件	定義
wildfire-management-service	WildFire作業モード管理サービス。	実行中	WildFire管理サービスは操作可能状態です。
		完了	WildFire管理サービスの実行が終了しました。

名前	説明	可能なステータス条件	定義
wildfire-apps-service	WildFireインフラストラクチャアプリケーション。	Deregistered	WildFireアプリケーションサービスの登録が解除されました。
		Ready	WildFireアプリケーションサービスは準備完了状態です。キューサービスは準備完了状態です。
		リストア	WildFireアプリケーションサービスのメンテナンスが完了しました。

名前	説明	可能なステータス条件	定義
		Scheduling	WildFireアプリケーションサービスはスケジューリング状態にあります。
		SetupSampleStorage	このWildFireアプリケーションサービスは、WildFireが7.1から8.0にアップグレードされるときに動作します。
		Stopped	WildFireアプリケーションサービスがアプライアンスで停止しました。
		サスペンド	WildFireアプリケーションサービスは、メンテナンスのため停止されました。

WildFireサービスの状態

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

WildFireアプライアンスは、サンプルデータの処理を管理および調整するための一連の内部サービスを実行します。これらのサービスとその必要なステータスは、WildFireアプライアンスクラスタのステータスを表示するときに表示されます。

次のリストは、WildFireサービスのコンポーネント、説明、ステータス条件、およびその他の関連情報を示しています。

名前	目的	**Impacted Nodes**（影響を受けるノード）	ステータス
インフラ	指定されたノードでWildFireクラスタインフラストラクチャサービスが動作していることを示します。	すべてのノード	サービスが動作しているときにCLIステータス画面に表示されます。特定のノードに対してこれらのサービスが存

名前	目的	**Impacted Nodes**（影響を受けるノード）	ステータス
`wfpc`	ファイルサンプル分析サービス（WildFireプライベートクラウド）がファイルの分析とレポート作成が可能であることを示します。		在しない場合は、アプライアンスの構成を確認してください。
シグネチャ	WildFireのプライベートシグネチャと分析サンプルを生成します。	アクティブ（プライマリ）/パッシブ（バックアップ）コントローラ	
`wfcore`	ノードがWildFireクラスタインフラストラクチャサービスのサーバとして動作していることを示します。	サーバーノード	

クラスタ内のWildFireアプライアンスをアップグレードする

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

CLIを使用して、クラスタに登録されているWildFireアプライアンスを個別にアップグレードするか、またはPanoramaを使用してクラスタをグループとしてアップグレードすることができます。

WildFireアプライアンスが分析して保存したサンプルの数に応じて、アプライアンスソフトウェアのアップグレードに必要な時間は異なります。 アップグレードするには、すべてのマルウェアサンプルの移行と14日間の良性サンプルが必要です。製造環境で使用したWildFireアプライアンスには、それぞれ30～60分かかります。

- クラスタ内のすべてのノードは、同じバージョンのオペレーティングシステムを実行する必要があります。
- *Panorama*は、*PAN-OS*ソフトウェアバージョン*8.0.1*以降を実行している*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。
- デバイス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、デバイスを使用できなくなる可能性があります。

デプロイメントに応じて、次のいずれかのタスクを実行してWildFireクラスタをアップグレードします。

- インターネット接続を使用してクラスタをセンターでアップグレードする
- インターネット接続を使用してクラスタをセンターでアップグレードする
- インターネット接続を使用してクラスタをローカルにアップグレードする
- インターネット接続なしでクラスタをローカルにアップグレードする

インターネット接続を使用してクラスタをローカルにアップグレードする

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

クラスタをローカルにアップグレードするには、クラスタに登録されている各WildFireアプライアンスを個別にアップグレードする必要があります。アプライアンスがアップグレードを完了すると、アプライアンスは最初に割り当てられたクラスタに自動的に再登録されます。

STEP 1 | 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。

```
admin@WF-500(passive-controller)> show wildfire latest samples
```

*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 2 | 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。

古いアプライアンスでは、このプロセスに最大 6 時間以上かかる場合があります。

1. WildFireアプライアンスで最新のコンテンツ更新を実行していることを確認します。

```
admin@WF-500> request wf-content upgrade check
```

2. 最新の WildFire コンテンツ更新パッケージをダウンロードします。

```
admin@WF-500> request wf-content upgrade download latest
```

Palo Alto Networks Update Serverに直接接続していない場合は、Install WildFire Content Updates from an SCP-Enabled Server（SCP対応サーバーからWildFireコンテンツ更新をダウンロードしてインストール）できます。

3. ダウンロードのステータスを表示します。

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

4. ダウンロードが完了したら、アップデートをインストールします。

```
admin@WF-500> request wf-content upgrade install version latest
```

STEP 3 | (PAN-OS 10.2.2 にアップグレードする場合に必要) WildFireアプライアンスの VM イメージをアップグレードします。

1. ログインして、 Palo Alto Networks カスタマー サポート ポータル ソフトウェア ダウンロード ページにアクセスします。サポート ホームページから **[アップデート]** > **[ソフトウェア アップデート]** に移動して、ソフトウェア ダウンロード ページに手動で移動することもできます。

2. ソフトウェア アップデート ページから、**WF-500** ゲスト **VM** イメージ を選択し、次の VM イメージ ファイルをダウンロードします。

   Palo Alto Networks は、*VM* イメージ ファイルを定期的に更新します。その結果、特定のファイル名は利用可能なバージョンに基づいて変更されます。必ず最新バージョンをダウンロードしてください。ファイル名の *mx.xx* はリリース番号を示します。さらに、最新バージョンを確認するために相互参照できるリリース日もあります。

   - WFWinXpAddon3_m-1.0.1.xpaddon3
   - WFWinXpGf_m-1.0.1.xpgf
   - WFWin7_64Addon1_m-1.0.1.7_64addon1
   - WFWin10Base_m-1.0.1.10base

3. VM イメージを WildFire アプライアンスにアップロードします。

   1. SCP サーバーから VM イメージをインポートします。

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

      以下に例を示します。

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

   2. ダウンロードの進行状況を確認する場合は、以下のCLIコマンドを使用します。

      ```
      admin@WF-500> ジョブをすべて表示
      ```

   3. 残りの VM イメージについてもこの手順を繰り返します。

4. VM イメージをインストールします。

   1. ```
      admin@WF-500> システム wildfire-vm-image アップグレードインストールファイルを要求しますか？
      ```

   2. 残りの VM イメージについてもこの手順を繰り返します。

5. VM イメージが WildFireアプライアンスに適切にインストールされ、有効になっていることを確認します。

   1. (オプション) 使用可能な仮想マシン イメージのリストを表示します:

      ```
      admin@WF-500>show wildfire vm-images (wildfire VM イメージ を表示)
      ```
      ```

出力には、使用可能な VM イメージが表示されます。

2. 設定をコミットします:

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

3. 次のコマンドを実行して、アクティブな VM イメージを表示します:

```
admin@WF-500>show wildfire status (wildfire ステータスを表示)
```

STEP 4 | インストールするWildFireアプライアンスソフトウェアのバージョンが使用可能であることを確認します。

```
admin@WF-500(passive-controller)> request system software check
```

STEP 5 | PAN-OS 10.2.2 ソフトウェア バージョンを WildFireアプライアンスにダウンロードします。

WildFireアプライアンスをアップグレードするときにメジャーリリースのバージョンをスキップすることはできません。たとえば、PAN-OS 6.1からPAN-OS 7.1にアップグレードする場合は、まずPAN-OS 7.0をダウンロードしてインストールする必要があります。この手順の例は、PAN-OS 10.2.2 にアップグレードする方法を示しています。10.2.2 をアップグレードに適したターゲット リリースに置き換えます。

ソフトウェア バージョン 10.2.2 をダウンロードします。

```
admin@WF-500(passive-controller)> request system software download
 version 10.2.2 (システムソフトウェアダウンロードバージョン10.2.2 を要求)
```

ダウンロードの進行状況を確認する場合は、以下のCLIコマンドを使用します。

```
admin@WF-500(passive-controller)> show jobs all
```

STEP 6 | すべてのサービ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
```

STEP 7 | ソフトウェア バージョン 10.2.2 をインストールします。

```
admin@WF-500(passive-controller)> request system software install
 version 10.2 (システムソフトウェアダウンロードバージョン10.2 を要求)
```

STEP 8 | ソフトウェアのアップグレードを完了します。

1. 更新が完了したことを確認してください。以下のコマンドを実行して、ジョブのtype（タイプ）が **Install**（インストール）、status （状態）が **FIN**（終了）になっているエントリを探します。

```
admin@WF-500(passive-controller)> show jobs all
Enqueued Dequeued ID Type Status Result Completed
------------------------------------------------------
14:53:15 14:53:15 5 Install FIN OK 14:53:19
```

2. アプライアンスを正常に再起動します。

```
admin @ WF-500（passive-controller）>request clusterreboot-
local-node
```

*WildFire*アプライアンスに保存されているサンプル数に応じて、アップグレードプロセスには*10*分か*1*時間以上かかります。

STEP 9 | クラスタ内の各WildFireワーカーノードにおいて手順1-8を繰り返します。

STEP 10 | （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 11 | 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 フィールドにアップグレードされたリリース バージョン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
   ```

4. データ移行が正常に完了したことを確認します。データベース結合の進行状況を表示するには、`show cluster data-migration-status`を実行します。データ結合完了後は、完了のタイムスタンプが表示されます:

   ```
   100% completed on Mon Sep 9 21:44:48 PDT 2019
   ```

   データマージの期間は、*WildFire*アプライアンスに保存されているデータの量によって異なります。データのマージは時間のかかるプロセスであるため、少なくとも数時間はリカバリに割り当ててください。

インターネット接続なしでクラスタをローカルにアップグレードする

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

クラスタをローカルにアップグレードするには、クラスタに登録されている各WildFireアプライアンスを個別にアップグレードする必要があります。アプライアンスがアップグレードを完了すると、アプライアンスは最初に割り当てられたクラスタに自動的に再登録されます。

STEP 1 | 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。

```
admin@WF-500(passive-controller)> show wildfire latest samples
```

*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 2 | 更新サーバーからコンテンツ更新ファイルを取得します。

1. Palo Alto Networks Support Portalにログインし、**Dynamic Updates (**動的更新**)**をクリックします。
2. WildFire Appliance（WildFire アプライアンス）セクションで、最新の WildFire アプライアンス コンテンツ更新を探して、ダウンロードします。
3. コンテンツ更新ファイルを SCP 対応サーバーにコピーして、ファイル名とディレクトリ パスをメモします。

STEP 3 | WildFire アプライアンスのコンテンツ更新をインストールします。

1. WildFire アプライアンスにログインし、SCP サーバーからコンテンツ更新ファイルをダウンロードします。

   ```
   admin @ WF-500>scp import wf-content from username @ host：path
   ```

   以下に例を示します。

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

   SCP サーバーが標準以外のポートで実行されている場合、または送信元*IP*を指定する必要がある場合は、それらのオプションを ***scp import*** コマンドで定義することもできます。

2. 更新をインストールします。

   ```
   admin@WF-500> request wf-content upgrade install file panup-
   all-wfmeta-2-253.tgz
   ```

3. インストールの状態を表示します。

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

STEP 4 | コンテンツ更新を確認します。

コンテンツ バージョンを確認します。

```
admin@WF-500> show system info | match wf-content-version
```

以下の出力ではバージョン 2～253 が示されています。

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

STEP 5 | (PAN-OS 10.2.2 にアップグレードする場合に必要) WildFireアプライアンスの VM イメージをアップグレードします。

1. ログインして、 Palo Alto Networks カスタマー サポート ポータル ソフトウェア ダウンロード ページにアクセスします。サポート ホームページから **[**アップデート**]** > **[**ソフトウェア アップデート**]** に移動して、ソフトウェア ダウンロード ページに手動で移動することもできます。

2. ソフトウェア アップデート ページから、**WF-500** ゲスト **VM** イメージ を選択し、次の VM イメージ ファイルをダウンロードします。

   Palo Alto Networks は、*VM* イメージ ファイルを定期的に更新します。その結果、特定のファイル名は利用可能なバージョンに基づいて変更されます。必ず最新バージョンをダウンロードしてください。ファイル名の *mx.xx* はリリース番号を示します。さらに、最新バージョンを確認するために相互参照できるリリース日もあります。

   - WFWinXpAddon3_m-1.0.1.xpaddon3
   - WFWinXpGf_m-1.0.1.xpgf
   - WFWin7_64Addon1_m-1.0.1.7_64addon1
   - WFWin10Base_m-1.0.1.10base

3. VM イメージを WildFire アプライアンスにアップロードします。

   1. SCP サーバーから VM イメージをインポートします。

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

      以下に例を示します。

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

   2. ダウンロードの進行状況を確認する場合は、以下のCLIコマンドを使用します。

      ```
      admin@WF-500> ジョブをすべて表示
      ```

   3. 残りの VM イメージについてもこの手順を繰り返します。

4. VM イメージをインストールします。

   1. ```
      admin@WF-500> システム wildfire-vm-image アップグレードインストールファイルを要求しますか？
      ```

   2. 残りの VM イメージについてもこの手順を繰り返します。

5. VM イメージが WildFireアプライアンスに適切にインストールされ、有効になっていることを確認します。

   1. (オプション) 使用可能な仮想マシン イメージのリストを表示します:

      ```
      admin@WF-500>show wildfire vm-images (wildfire VM イメージ を表示)
      ```
      ```

出力には、使用可能な VM イメージが表示されます。

2. 設定をコミットします:

```
admin@WF-500#コミット
```

3. 次のコマンドを実行して、アクティブな VM イメージを表示します:

```
admin@WF-500>show wildfire status (wildfire ステータスを表示)
```

STEP 6 | インストールするWildFireアプライアンスソフトウェアのバージョンが使用可能であることを確認します。

```
admin@WF-500(passive-controller)> request system software check
```

STEP 7 | PAN-OS 10.2.2 ソフトウェア バージョンを WildFireアプライアンスにダウンロードします。

WildFireアプライアンスをアップグレードするときにメジャーリリースのバージョンをスキップすることはできません。たとえば、PAN-OS 6.1からPAN-OS 7.1にアップグレードする場合は、まずPAN-OS 7.0をダウンロードしてインストールする必要があります。この手順の例は、PAN-OS 10.2.2 にアップグレードする方法を示しています。10.2.2 をアップグレードに適したターゲット リリースに置き換えます。

10.2.2 ソフトウェアバージョンをダウンロードします。

1. Palo Alto Networks Support サイトに移動し、ログインして **Software Updates**（ソフトウェアの更新）をクリックします。
2. インストールする WildFire アプライアンス ソフトウェア イメージ ファイルを SCP サーバー ソフトウェアを実行しているコンピュータにダウンロードします。
3. SCP サーバーからソフトウェア イメージをインポートします。

```
admin@WF-500> scp import software from <username@ip_address>/
<folder_name>/<imagefile_name>
```

以下に例を示します。

```
admin@WF-500> scp import software from user1@10.0.3.4:/tmp/
WildFire_m-10.2.2
```

4. ダウンロードの進行状況を確認する場合は、以下のCLIコマンドを使用します。

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

STEP 8 | すべてのサービ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
```

STEP 9 | ソフトウェア バージョン 10.2.2 をインストールします。

```
admin@WF-500(passive-controller)> request system software install
 version 10.2.2 (システムソフトウェアダウンロードバージョン10.2.2 を要求)
```

STEP 10 | ソフトウェアのアップグレードを完了します。

1. 更新が完了したことを確認してください。以下のコマンドを実行して、ジョブのtype（タイプ）が **Install**（インストール）、status （状態）が **FIN**（終了）になっているエントリを探します。

   ```
   admin@WF-500(passive-controller)> show jobs all
   Enqueued Dequeued ID Type Status Result Completed
   ---------------------------------------------------
   14:53:15 14:53:15 5 Install FIN OK 14:53:19
   ```

2. アプライアンスを正常に再起動します。

   ```
   admin @ WF-500（passive-controller）>request clusterreboot-
   local-node
   ```

   *WildFire*アプライアンスに保存されているサンプル数に応じて、アップグレードプロセスには*10*分か*1*時間以上かかります。

STEP 11 | クラスタ内の各WildFireワーカーノードにおいて手順1-10を繰り返します。

STEP 12 | （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 13 | 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 フィールドにアップグレードされたリリース バージョン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
```

4. データ移行が正常に完了したことを確認します。データベース結合の進行状況を表示するには、`show cluster data-migration-status`を実行します。データ結合完了後は、完了時のタイムスタンプが表示されます:

```
100% completed on Mon Sep 9 21:44:48 PDT 2019
```

データマージの期間は、*WildFire*アプライアンスに保存されているデータの量によって異なります。データのマージは時間のかかるプロセスであるため、少なくとも数時間はリカバリに割り当ててください。

WildFire クラスターのトラブルシューティング

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

WildFireクラスタの問題を診断およびトラブルシューティングするには、次のトピックを参照してください。

- WildFireスプリットブレイン条件のトラブルシューティング

WildFireスプリットブレイン条件のトラブルシューティング

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

WildFire 2ノードHA（高可用性）クラスタは、ノード（または両方のHAピア）がもう一方のノードが動作しなくなったと考えたときにスプリットブレイン状態になります。これは、ネットワーク接続または構成の問題の結果としてHAおよびクラスタ接続の両方が失敗した場合に発生しますが、アプライアンスはサンプルの処理を続行できます。これが発生すると、両方のWildFireアプライアンスはバックアップなしでアクティブ（またはプライマリ）コントローラの役割を引き継ぎ、冗長性やロードバランシングなどのHAデプロイメントの利点が無効になります。さらに、これにより、WildFireアプライアンスは分析リソースを効率的に利用できなくなります。WildFireクラスタで軽微な障害が発生すると、スプリットブレイン状態から自動的に回復しようとします。より深刻なイベントは、手動介入が必要です。

スプリットブレインが発生すると、次の条件が適用されます。

- WildFireピアは、状態、HAの役割のどちらも認識しません。
- どちらのWildFireピアもプライマリサーバになり、ファイアウォールからサンプルを引き続き受信しますが、独立したアプライアンスとして動作します。
- クラスタ関連のタスクは、HAが使用できないときに中断されます。

*3*ノードの*Wildfire*アプライアンスクラスタは、*3*番目のサーバノードによって追加の冗長性が提供されるため、適切に構成されているとスプリットブレイン条件が発生しません。

スプリットブレイン状態を引き起こす要因は何か？

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

スプリットブレイン条件は、2ノードクラスタの単一ノード障害に対する修正応答です。この場合、WildFire高可用性ペアは、もはやお互いに通信することができなくなりますが、機能は限られています。高可用性とロードバランシング機能はもはや利用できませんが、解析のためにサンプルをWildFireに転送できます。スプリットブレインが発生すると、次のいずれかの原因が考えられます。

- ハードウェアの問題または停電。
- スイッチ/ルータの障害、ネットワークのフラップ、ネットワークパーティションなどのネットワーク接続の問題。
- WildFireアプライアンスの設定と接続に関する問題。

  *Palo Alto Networks*では、*HA1*とクラスタインターフェイスのリンクに直接ケーブル接続を使用することを推奨しています。
- 不健全なWildFireノード。

WildFireクラスタがスプリットブレイン状態にあるかどうかを判断する

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

WildFire 2ノードクラスタ内のアプライアンスがスプリットブレイン状態になると、サービス障害はWildFire CLIで警告を生成し、Panorama （使用可能な場合）を管理します。

STEP 1 | （WildFire アプライアンスCLIのみ）WildFireアプライアンスコントローラでは、次のコマンドを実行します。

```
admin@WF-500>show cluster membership
```

影響を受けるWildFireクラスタノードに、`Service Summary` （サービス概要）の横に`Cluster：splitbrain` （クラスター：スプリットブレイン）と表示されます。

次の例は、スプリットブレイン状態の2ノードのWildFireクラスタ内のノードを示しています。

```
Service Summary:Cluster:splitbrain Cluster name:WF_Cluster_1
 Address:2.2.2.114 Host name: wf1 Node name: wfpc-009707000380-
```

```
internal Serial number:009707000380 Node mode: controller Server
 role:True HA priority: secondary Last changed:Tue, 24 Oct 2017
 15:13:18 -0700 Services: wfcore signature wfpc infra Monitor
 status:Serf Health Status: passing Agent alive and reachable
 Service 'infra' check: passing Application status: global-db-
service:ReadyLeader wildfire-apps-service:Ready global-queue-
service:ReadyLeader wildfire-management-service:Done siggen-
db:ReadyMaster Work queue status: sample anaysis queued:0 sample
 anaysis running:0 sample copy queued:0 sample copy running:0 Diag
 report:2.2.2.114: reported leader '2.2.2.114', age 0. 2.2.2.114:
 local node passed sanity check.
```

STEP 2 | （Panorama のみ）WildFireクラスタを管理しているPanoramaアプライアンスの場合：

1. **Panorama > Managed WildFire Clusters**（管理**WildFire** クラスター）を選択。
2. **Cluster Status**（クラスタステータス）列で、**cluster**（**splitbrain**）クラスタ（スプリットブレイン）の存在を確認します。これは、アプライアンスがスプリットブレインモードであることを示します。

APPLIANCE	SOFTWARE VERSION	IP ADDRESS	CONNECTED	CLUSTER NAME	ANALYSIS ENVIRONM...	CONTENT	ROLE	CONFIG STATUS	CLUSTER STATUS	LAST COMMIT STATE	UTILIZATION	FIREWALLS CONNECTED
wfcluster1 (2/3 Nodes Connected)											View	View
qa19	10.0.2-c12		Connected	WF_Cluster1	vm-5	4033-4496	Controller		cluster [splitbrain]			
qa18			Connected		vm-5		Controller Backup					
qa17	10.0.2-c12		Connected		vm-5	4033-4496	Worker					

スプリットブレイン状態を修復

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

スプリットブレイン状態を解決するには、ネットワークの問題をデバッグし、WildFire HAペア間の接続を復元します。WildFireアプライアンスクラスタは、スプリットブレイン条件から自動的に回復を試みますが、これらの対策が失敗した場合は、手動で回復プロセスを開始する必要があります。

STEP 1 | ネットワークが正常に動作しており、WildFireアプライアンスがトラフィックを送受信していることを確認してください。

1. WildFireアプライアンスインターフェイスでpingを実行できるようにします。
   - 特定のアプライアンス インターフェイスで ping を有効にする—`setdeviceconfig システム <interface_number> サービス disable-icmp no`
   - すべてのアプライアンス インターフェイスで ping を有効にする:セット `deviceconfig システム サービス disable-icmp no`
2. WildFireインターフェースから外部デバイスへのpingトラフィックを生成します。受信カウンタと送信カウンタが増加することを確認します。

   送信元`<wildfire-interface-ip>`ホスト`<destination-ip-address>`に`ping`を実行し

STEP 2 | どのWildFireアプライアンスが不健全であるかを判断します。View WildFire Cluster Status Using the CLI（CLIを使用したWildFireクラスタステータスの表示）またはView WildFire Cluster Status Using Panorama（anoramaを使用したWildFireクラスタステータスの表示）を参照してください。

STEP 3 | 次のコマンドを使用して正常でないノードを正常に再起動します。

`request cluster reboot-local-node`（要求クラスタ再起動 **`-`** ローカルノード）

再起動されたWildFireアプライアンスは、設定されたWildFireクラスタに自動登録されます。

スプリットブレインモードにある残りのコントローラノードは正常な状態でなければなりません。

STEP 4 | Data Migration（データ移行）が完了するのを待ちます。データベース結合の進行状況を表示するには、`show cluster data-migration-status`を実行します。データ結合完了後は、完了のタイムスタンプが表示されます:

```
100% completed on Mon Sep 9 21:44:48 PDT 2019
```

データマージの期間は、*WildFire*アプライアンスに保存されているデータの量によって異なります。データのマージは時間のかかるプロセスであるため、少なくとも数時間はリカバリに割り当ててください。

STEP 5 | PanoramaまたはWildFireアプライアンスのCLIを使用して、Verify the status of the cluster（クラスタのステータスを確認）します。

WildFire アプライアンスのCLIを使用する

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

次のトピックでは、WildFire™アプライアンスソフトウェアに固有のCLIコマンドについて説明します。インターフェイスの設定、設定のコミット、システム情報の設定など、その他すべてのコマンドは PAN-OS と同一であり、階層内にも表示されます。PAN-OS コマンドの詳細は、PAN-OS CLI Quick Start（PAN-OS CLIクイックスタート）を参照してください。

- WildFire アプライアンス ソフトウェアの CLI の概念
- WildFire CLI コマンド モード
- WildFireアプライアンスCLIへのアクセス
- WildFire アプライアンスCLI操作
- WildFire アプライアンス設定モードのコマンド リファレンス
- WildFire アプライアンス設定モードのコマンド リファレンス

WildFire アプライアンス ソフトウェアの CLI の概念

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

このセクションでは、WildFire アプライアンス ソフトウェアのコマンド ライン インターフェイス (CLI) の概要と使用方法について説明します。

- WildFire アプライアンス ソフトウェアの CLI の構成
- WildFire アプライアンス ソフトウェア CLI コマンドの規則
- WildFire アプライアンスの CLI のコマンド メッセージ
- WildFire アプライアンスのコマンド オプションの記号
- WildFire アプライアンスの権限レベル

WildFire アプライアンス ソフトウェアの CLI の構成

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

WildFire アプライアンス ソフトウェア CLI は、アプライアンスの管理に使用します。CLI は、アプライアンスへの唯一のインターフェイスです。状態や設定情報を表示したり、アプライアンス設定を変更したりする場合に使用します。WildFire アプライアンス ソフトウェア CLI には、SSH 経由でアクセスするか、またはコンソール ポートを使用した直接コンソール アクセスを使用します。

WildFire アプライアンス ソフトウェア CLI の動作には2 つのモードがあります。

- 操作モード — システムの状態の表示、WildFire アプライアンス ソフトウェア CLI の操作、設定モードへの切り替えができます。
- 設定モード —設定階層の表示と変更ができます。

WildFire アプライアンス ソフトウェア CLI コマンドの規則

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

基本のコマンド プロンプトには、アプライアンスのユーザー名とホスト名が表示されます。

```
username @ hostname>
```

例:

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

設定モードに切り替えると、プロンプトは> から#に変わります。

```
username@hostname> (動作モード) username@hostname> 設定 コンフィギュレーション モードに入る [編集] username@hostname# (コンフィギュレーション モード)
```

設定モードでは、コマンドが発行されると、角括弧で囲まれた [edit...] バナーによって、現在の階層コンテキストが表示されます。

WildFire アプライアンスの CLI のコマンド メッセージ

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

コマンドを発行すると、メッセージが表示される場合があります。メッセージはコンテキスト情報を提供し、無効なコマンドを修正するのに役立ちます。以下の例では、メッセージが太字で表示されています。

例:不明なコマンド

```
username@hostname# アプリケーション グループ 不明なコマンド: アプリケーション グループ [ネットワークの編集] username@hostname#
```

例:モードの変更

```
username@hostname> configure Entering configuration mode [edit]
 username@hostname#
```

例:無効な構文

```
username@hostname> debug 17 Unrecognized command Invalid syntax.
 username@hostname>
```

CLI によって各コマンドの構文がチェックされます。構文が正しい場合、コマンドが実行されて候補階層が変更されます。構文が誤っている場合、以下の例の様に「Invalid syntax (無効な構文)」エラーが表示されます。

```
username@hostname# set deviceconfig setting wildfire cloud-
intelligence submit-sample yes Unrecognized command Invalid syntax.
 [edit] username@hostname#
```

WildFire アプライアンスのコマンド オプションの記号

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

オプションの前に表示される記号は、コマンド構文に関する追加情報を示します。

記号	詳説
*	このオプションは必須です。
>	このコマンドには、さらにネストされたオプションがあります。
+	このコマンドのこのレベルには、追加のコマンド オプションがあります。
|	「except (除外) する値」または「match (一致) する値」を指定してコマンドを制限するためのオプションがあります。
“ “	二重引用符は、コマンド オプション記号ではありませんが、CLI コマンドで複数の語からなる句を入力する場合に使用する必要があります。例えば、Test Group という名前のアドレス グループを作成し、user 1 という名前のユーザーをこのグループに追加するには、グループ名を以下の様に二重引用符で囲む必要があります。 set address-group “Test Group” user1. グループ名を二重引用符で囲まないと、CLI では Test をグループ名、Group をユーザー名として解釈し、以下のエラーが表示されます: `test is not a valid name`。 この例では、単一引用符も無効になります。

以下の例は、これらの記号の使用方法を示します。

例:以下のコマンドでは、キーワード `from` は必須です。

```
username@hostname> scp import configuration ? + remote-port SSH
 port number on remote host * from Source (username@host:path)
 username@hostname> scp import configuration例：このコマンド出力には、+お
よび>. username@hostname# set rulebase security rules rule1 ? +
 action action + application application + destination destination +
 disabled disabled + from from + log-end log-end + log-setting log-
setting + log-start log-start + negate-destination negate-destination
 + negate-source negate-source + schedule schedule + service service
 + source source + to to > profiles profiles <Enter> Finish input
 [edit] username@hostname# set rulebase security rules rule1
```

+でリストされた各オプションをコマンドに追加できます。

profilesキーワード（>付き）には、追加オプションがあります。

```
username@hostname# set rulebase security rules rule1 profiles ? +
 virus Help string for virus + spyware Help string for spyware +
 vulnerability Help string for vulnerability + group Help string for
 group <Enter> Finish input [edit] username@hostname# set rulebase
 security rules rule1 profiles
```

WildFire アプライアンスの権限レベル

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

権限レベルによって、ユーザーに実行が許可されるコマンドと、ユーザーに表示が許可される情報が決まります。

レベル	説明
スーパーリーダー	アプライアンスに対するすべての読み取り専用アクセス権があります。
スーパーユーザー	アプライアンスに対するすべての読み取り/書き込みアクセス権があります。

WildFire CLI コマンド モード

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

次のトピックでは、WildFireアプライアンスソフトウェアCLIとの対話に使用されるモードについて説明します。

- WildFire アプライアンスCLIの設定モード
- WildFire アプライアンスCLIのオプションモード

WildFire アプライアンスCLIの設定モード

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

設定モードでコマンドを入力すると、候補設定が変更されます。変更された候補設定は、アプライアンスのメモリに保存され、アプライアンスの動作中は維持されます。

各設定コマンドにはアクションが含まれ、さらにキーワード、オプション、値が含まれる場合もあります。

このセクションでは、設定モードと設定階層について説明します。

- 設定モード コマンドの使用
- 設定階層
- 階層パス
- 階層の移動

設定モード コマンドの使用

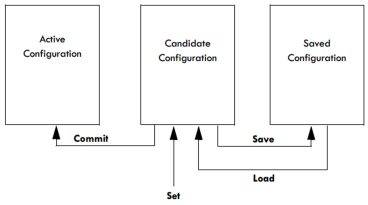
どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

設定の変更を保存して適用するには、以下のコマンドを使用します。

- `save`—アプライアンス上の不揮発性ストレージに候補設定を保存します。保存された設定は、次回保存コマンドで上書きされるまで維持されます。このコマンドによって、設定がアクティブになることはありません。

- `commit`—候補設定をアプライアンスに適用します。コミットされた設定は、デバイスのアクティブな設定になります。
- `set`—候補設定の値を変更します。
- `Load`—最後に保存された設定または指定された設定を、候補設定として割り当てます。

> ***save***または***commit***コマンドを発行せずに設定モードを終了すると、アプライアンスへの電源が切断された場合に設定変更が失われる可能性があります。



候補設定を維持し、save と commit ステップを分離する方法には、従来の CLI アーキテクチャと比べて重要な利点があります。

- save と commit の概念を区別することで、複数の変更を同時に行うことができ、システムの脆弱性が軽減されます。
- 類似の機能にコマンドを容易に適応できます。例えば、それぞれが異なる IP アドレス を持つ 2 つの Ethernet インターフェイスを設定するときに、1 つ目のインターフェイスの設定を編集し、コマンドをコピーし、インターフェイスと IP アドレスのみを変更してから、変更を 2 つ目のインターフェイスに適用できます。
- コマンド構造の整合性が常に保たれます。

候補設定は常に固有であるため、正当な権限で候補設定に加えられる変更すべてにおいて、相互の整合性が保たれます。

設定階層

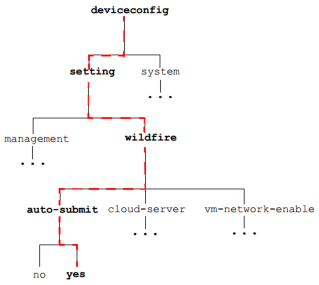
どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

アプライアンスの設定は、階層構造に編成されています。現在の階層レベルのセグメントを表示するには、`show`コマンドを使用します。「Show」（表示）と入力すると階層全体が表示されるのに対し、`show`にキーワードを指定して入力すると階層のセグメントが表示されます。たとえば、コンフィギュレーションモードの最上位レベルからコマンド`show`を実行すると、コンフィギュレーション全体が表示されます。コマンド`edit mgt-config`を実行しているときに`show`と入力するか、**`showmgt-config`**を実行すると、階層のmgt-config部分のみが表示されます。

階層パス

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

コマンドの入力時、パスは階層内で以下の様に追跡されます。

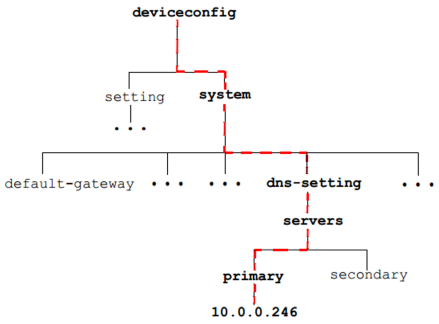


例えば、以下のコマンドは、プライマリ DNS サーバー 10.0.0.246 をアプライアンスに割り当てます。

```
[edit] username@hostname# set deviceconfig system dns-setting servers
 primary 10.0.0.246
```

このコマンドは、階層内と以下の show[表示] コマンドの出力内に、新しい要素を生成します。

```
[edit] username@hostname# show deviceconfig system dns-settings dns-
setting { servers { primary 10.0.0.246 } } [edit] username@hostname#
```



階層の移動

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

設定モードのコマンド プロンプト行の下に表示される [edit...] バナーは、現在の階層コンテキストを示します。

```
[edit]
```

は、相対コンテキストが階層の最上位レベルであることを示すのに対して、

```
[edit deviceconfig]
```

は、相対コンテキストが、deviceconfig レベルであることを示します。

設定階層内を移動するには、以下に挙げるコマンドを使用します。

レベル	説明
Edit（編集）	コマンド階層内の設定のコンテキストを設定します。
up（上）	コンテキストを階層内で次に高いレベルに変更します。
top（トップ）	コンテキストを階層内で最も高いレベルに変更します。

up（上） および ***top***（トップ） コマンドを使用した後に発行された ***set***（設定） コマンドは、新しいコンテキストから開始します。

WildFire アプライアンスCLIのオプションモード

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

デバイスに初めてログインすると、WildFire アプライアンス ソフトウェア CLI は操作モードで開きます。操作モード コマンドには、直ちに実行されるアクションが含まれます。設定への変更は含まれず、保存やコミットを行う必要はありません。

操作モード コマンドには、いくつかの種類があります。

- **Network access**[ネットワーク アクセス]—他のホストへのウィンドウを開きます。SSH がサポートされています。
- **Monitoring and troubleshooting**[モニタリングとトラブルシューティング] — 診断と分析を実行します。`debug` 、`ping` などのコマンドがあります。
- **Display commands**[表示コマンド] — 現在の情報を表示またはクリアします。`clear` 、`show`などのコマンドがあります。

- **WildFire** アプライアンス ソフトウェア　**CLI**　移動コマンド — 設定モードへの切り替えや WildFire アプライアンスソフトウェア CLI の終了を行います。`configure`、`exit`、`quit`などのコマンドがあります。
- **System commands**[システム コマンド]　—　システム レベルの要求や再起動を行います。`set`、`request`　などのコマンドがあります。

WildFireアプライアンスCLIへのアクセス

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

このセクションでは、WildFireアプライアンスソフトウェアCLIにアクセスする方法について説明します:

- コンソールへの直接接続の確立
- SSH 接続の確立

コンソールへの直接接続の確立

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

コンソール直接接続には、以下の設定を使用します。

- データ速度:9600
- データ ビット:8
- パリティ: なし
- ストップ ビット:1
- フロー制御:なし

SSH 接続の確立

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

WildFire アプライアンス ソフトウェア CLI にアクセスするには、以下の手順を実行します。

STEP 1 | 端末エミュレーションソフトウェアを使用して、WildFireアプライアンスとのSSHコンソール接続を確立します。

STEP 2 | 管理者のユーザー名を入力します。デフォルトは admin です。

STEP 3 | 管理者のパスワードを入力します。デフォルトは admin です。

WildFire アプライアンス ソフトウェア CLI が操作モードで開き、CLI プロンプトが表示されます。

```
username @ hostname>
```

WildFire アプライアンスCLI操作

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

- WildFireアプライアンス操作および設定モードへのアクセス
- WildFire アプライアンス ソフトウェア CLI コマンド オプションの表示
- WildFire アプライアンスのCLIのコマンド出力制限
- WildFire アプライアンス設定コマンドの出力フォーマットの設定

WildFireアプライアンス操作および設定モードへのアクセス

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

ログインすると、WildFire アプライアンス ソフトウェア CLI は操作モードで開きます。操作モードと設定モードは、いつでも切り替えることができます。

- 操作モードから設定モードに切り替えるには、**configure** コマンドを使用します。

```
username@hostname> configure Entering configuration mode [edit]
 username@hostname#
```

- 設定モードを終了して操作モードに戻るには、**quit** または **exit** コマンドを使用します。

```
username@hostname# quit Exiting configuration mode
 username@hostname>
```

設定モードのまま操作モードのコマンドを入力するには、**run** コマンドを使用します。例えば、設定モードからシステム リソースを表示するには、**run show system resources** を使用します。

WildFire アプライアンス ソフトウェア CLI コマンド オプションの表示

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

コマンド オプションのリストを表示するには、コンテキストに応じて以下のように **?**（またはMeta-H）を使用します。

- 操作コマンドのリストを表示するには、コマンド プロンプトに **?** と入力します。

```
username@hostname> ? クリア ランタイムパラメータのクリア 設定 ソフトウェア設定情報の操作 コマンドの作成 デバッグと診断 削除 ハードディスクからファイルを削除する 無効にするコマンドを無効にする 編集コマンドを終了する このセッションを終了する キーワード grep でCLIコマンドを検索 パターンマッチの少ない行を検索する デバッグファイルの内容を調べる ping ホストとネットワークを終了する このセッションを終了する 要求を終了する システムレベルの要求を行う scp scp を使用してインポートする / エクスポート ファイル セット 操作パラメータの設定 表示 操作パラメータの表示 ssh 別のホストへのセキュアシェルの開始 送信コマンドの送信 末尾 デバッグファイルの内容の最後の 10 行を印刷する telnet 別のホストへの telnet セッションを開始する テストテストケースでシステム設定を確認する tftp tftp を使用してファイルをインポート/エクスポートする traceroute パケットがネットワークホストに取るルートを印刷する username@hostname>
```

- 指定したコマンドで使用できるオプションを表示するには、コマンドに続けて **?** と入力します。

例:

```
username@hostname> ping ? + バイパスルーティング ルーティングテーブルをバイパス、指定されたインターフェイスを使用する + 送信する要求の数 (1..200000000000 パケット) + フラグメント化しない エコー要求パケットをフラグメント化しない (IPv4) + 間隔 要求間の遅延 (秒) + 解決なし アドレスをシンボル的に印刷しようとしない + パターン 16 進数の塗りつぶしパターン + サイズ 要求パケットのサイズ (0..65468 バイト) + エコー要求の送信元アドレス + tos IP サービスの種類の値 (0..255) + ttl IP 存続時間値 (IPv6 ホップ制限値) (0..255 ホップ) + 詳細 詳細出力の表示 * ホスト リモート・ホストのホスト名または IP アドレス
```

WildFire アプライアンスのCLIのコマンド出力制限

一部の操作コマンドには、表示される出力を制限するオプションがあります。出力を制限するには、パイプ記号を入力し、その後に **except**（以外） または **match(**一致**)**、および除外または含める値を続けます。

例:

以下は、show system info コマンドのサンプル出力です。

```
username@hostname>show system info hostname:WildFire
 ip-address:192.168.2.20 netmask:255.255.255.0 default-
gateway:192.168.2.1 mac-address:00:25:90:95:84:76 vm-interface-ip-
address:10.16.0.20 vm-interface-netmask:255.255.252.0 vm-interface-
default-gateway:10.16.0.1 vm-interface-dns-server:10.0.0.247 time:Mon
 Apr 15 13:31:39 2013 uptime:0 days, 0:02:35 family: m model:WF-500
 serial:009707000118 sw-version:8.0.1 wf-content-version:702-283 wf-
```

```
content-release-date: unknown logdb-version:8.0.15 プラットフォーム ファミリ: m 動作モード: 通常username@hostname> 次のサンプルでは、システム モデル情報のみを表示します: username@hostname> 一致するモデル|2} モデル<システム情報を表示します。WF-500 username @ hostname>
```

WildFire アプライアンス設定コマンドの出力フォーマットの設定

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

操作モードで **set cli config-output-format** コマンドを使用し、設定コマンドの出力フォーマットを変更します。オプションとして、デフォルトフォーマットのJSON（JavaScript Object Notation）、設定したフォーマット、XMLフォーマットがあります。デフォルト フォーマットは、階層フォーマットで、各設定セクションがインデントされ、波括弧で囲まれます。

WildFire アプライアンス設定モードのコマンド リファレンス

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

このセクションには、以下の WildFire アプライアンス ソフトウェア固有の設定モード コマンドに関するコマンド リファレンス情報が含まれます。WildFire アプライアンス software の一部である他のすべてのコマンドは、PAN-OS 11.0 CLI クイックスタートで説明されているように、PAN-OS と同じです。

- set deviceconfig cluster
- set deviceconfig high-availability
- set deviceconfig setting management
- set deviceconfig setting wildfire
- set deviceconfig system eth2
- set deviceconfig system eth3
- set deviceconfig system panorama local-panorama panorama-server
- set deviceconfig system panorama local-panorama panorama-server-2
- set deviceconfig system update-schedule
- set deviceconfig system vm-interface

set deviceconfig cluster

説明

WildFireアプライアンスのクラスタ設定をWildFireアプライアンスで設定します。クラスタ名、クラスタ通信に使用されるインターフェイス、およびクラスタコントローラまたはワーカーでのアプライアンスのモード（役割）を設定できます。クラスタコントローラとして設定したWildFireアプライアンスでは、クラスタにWildFireアプライアンスを追加し、コントローラが管理インターフェイスでDNSサービスを提供するかどうかを設定できます。

階層内の場所

```
set deviceconfig
```

構文

```
cluster { cluster-name <name>; interface {eth2 | eth3}; mode
 { controller { service-advertisement dns-service enabled {no | yes};
 worker-list {ip-address} } worker; } }
```

オプション

`+ cluster-name` — クラスタに名前を付けます。名前は有効なドメイン名セクションでなければなりません。

`+ interface` — クラスタ通信に使用するインターフェイスを設定します。クラスター通信インターフェースは、すべてのクラスター・メンバー上で同じでなければなりません。

`> mode` — WildFireアプライアンスがコントローラノードであるかワーカーノードであるかを設定します。コントローラーノードの場合、コントローラーが管理インターフェース（サービス通知）でDNSサービスを提供し、ワーカーノードをクラスター（ワーカーリスト）に追加するかどうかを構成します。各WildFireアプライアンスクラスタには、高可用性を提供するために2つのコントローラノードが必要です。２つのコントローラと最大18個のワーカーノードを1つのクラスタに追加して最大20個のノードを追加できます。

サンプル出力

```
admin@wf-500(active-controller)# show deviceconfig cluster cluster
 { cluster-name sid-6; interface eth2; mode { controller { worker-
list { 2.2.2.115; } } } }
```

必要な権限レベル

superuser, deviceadmin

set deviceconfig high-availability

説明

Wildfireアプライアンスクラスタの高可用性（HA）設定を設定します。

階層内の場所

```
set deviceconfig
```

構文

```
high-availability { enabled {no | yes}; election-option { preemptive
 {no | yes}; priority {primary | secondary}; timers { advanced
 {heartbeat interval <value> | hello-interval <value> | preemption-
hold-time <value> | promotion-hold-time <value>} aggressive;
```

```
recommended; } } interface { ha1 { peer-ip-address <ip-address>;
port {eth2 | eth3 | management}; encryption enabled {no | yes}; }
ha1-backup { peer-ip-address <ip-address>; port {eth2 | eth3 |
management}; } } }
```

オプション

`+ enabled` — 両方のコントローラノードでHAを有効にして、クラスタにフォールトトレランスを提供します。各WildFireアプライアンスクラスタには、高可用性を提供するために2つのコントローラノードが必要です。

`> election-option` —プリエンプティブ、プライオリティ、およびタイマーのHAオプション値を設定します。

`+ preemptive` — パッシブHAピア（コントローラバックアップノード）がHA`priority`の設定に基づいてアクティブHAピア（プライマリコントローラノード）をプリエンプトできるようにする選択オプション。たとえば、プライマリコントローラノードがダウンすると、セカンダリ（パッシブ）コントローラノードがクラスタ制御を引き継ぎます。プライマリコントローラノードが復旧すると、プリエンプションを設定しないと、セカンダリコントローラはクラスタを制御し続け、プライマリコントローラはコントローラバックアップノードとして機能します。ただし、両方のHAピアでプリエンプションを設定した場合、プライマリコントローラが復旧すると、クラスタの制御を取り戻すことでセカンダリコントローラをプリエンプトします。セカンダリコントローラはコントローラのバックアップノードとして以前の役割を再開します。プリエンプションを動作させるには、両方のHAピアでプリエンプティブ設定を設定する必要があります。

`+ priority` — HAペア内の各コントローラのプリエンプションプライオリティを設定する選択オプション。HAコントローラのペアの両方のメンバーにプリエンプションを設定します。

`> timers` — HA選択オプションのタイマーを設定します。WildFireアプライアンスには、あらかじめ設定された2つのタイマーオプション（積極的および推奨の設定）が用意されています。また、各タイマーを個別に設定することもできます。`Advanced`タイマーを使用すると、値を個別に設定できます。

- `Heartbeat-interval`は、ハートビートpingを送信する時間をミリ秒単位で設定します。値の範囲は1000-60,000ミリ秒で、デフォルト値は2000ミリ秒です。
- `hello-interval` は、Helloメッセージを送信する時間をミリ秒単位で設定します。値の範囲は8000-60,000ミリ秒で、デフォルト値は8000ミリ秒です。
- `preemption-hold-time`は、アクティブ（プライマリ）コントローラノードをプリエンプトする前にパッシブ（コントローラバックアップ）モードに留まる時間を分単位で設定します。値の範囲は1-60ミリ秒で、デフォルト値は1ミリ秒です。
- `promtion-hold-time`は、パッシブ（コントローラのバックアップ）状態からアクティブ（プライマリ）状態に状態を変更する時間をミリ秒単位で設定します。値の範囲は0-60,000ミリ秒で、デフォルト値は2000ミリ秒です。

> interfaceプライマリ（ha1）およびバックアップ（ha1-backup）コントロールリンクインターフェイスのHAインターフェイス設定を設定します。プライマリコントローラノードがダウンした場合に、制御リンクインターフェイスを使用すると、HAコントローラのペアを同期させたままにして、フェールオーバーを準備できます。ha1インターフェイスとha1-backupインターフェイスの両方を設定すると、リンクに障害が発生した場合にコントローラ間の冗長性が確保されます。設定：

- peer-ip-address。HAピアのIPアドレスを設定します。ha1インターフェイスピアは、HAペア内の他のコントローラノード上のha1インターフェイスIPアドレスです。ha1-backupインターフェイスピアは、HAペア内の他のコントローラノード上の ha1-backupインターフェイスIPアドレスです。
- port（ポート）。各コントローラノードで、ha1インターフェイスに使用するポートとha-backupインターフェイスに使用するポートを設定します。Ha制御リンクインターフェイスにeth2、eth3またはmanagementポート（eth0）を使用できます。Analysis Environment Network（分析環境ネットワーク）インターフェイス（eth1）をha1またはha1-backupコントロールリンクインターフェイスとして使用することはできません。両方のHAピアで同じインターフェイスをha1インターフェイスとして使用し、両方のHAピアで同じインターフェイス（ただしha1インターフェイスではない）をha1-backupインターフェイスとして使用します。たとえば、両方のコントローラノードでeth3をha1インターフェイスとして設定し、両方のコントローラノードでmanagementインターフェイスをha1-backupインターフェイスとして設定します。

サンプル出力

```
admin@wf-500(active-controller)# show deviceconfig high-availability
 high-availability { election-option { priority primary; } enabled
 no; interface { ha1 { peer-ip-address 10.10.10.150; port eth2 } ha1-
backup { peer-ip-address 10.10.10.160; port management } } }
```

必要な権限レベル

superuser, deviceadmin

set deviceconfig setting management

説明

WildFireアプライアンスの管理セッション設定を設定します。長すぎるアイドル状態で、管理者をロックアウトするのに必要なログイン再試行（ログイン試行の失敗回数）がある場合、管理セッションを終了するようにタイムアウトを設定できます。

階層内の場所

```
set deviceconfig setting
```

構文

```
management { idle-timeout {0 | <value>} admin-lockout { failed-
attempts <value> lockout-time <value> } }
```

オプション

`+ idle-timeout` —デフォルト管理セッション アイドル タイムアウト (分)アイドルタイムアウトを1-1440分に設定するか、タイムアウト値を0（ゼロ）に設定してセッションをタイムアウトさせないでください。

`> admin-lockout` — 管理者がシステムからロックアウトされる前にアプライアンスにログインする`failed-attempts`回数（0～10）、および管理者を`lockout-time`するロックアウト時間（0～60）を設定します。 管理者は`failed-attempts`試行しきい値を超えます。

サンプル出力

```
management { idle-timeout 0; admin-lockout { failed-attempts 3;
 lockout-time 5; } }
```

set deviceconfig setting wildfire

説明

WildFire アプライアンスで WildFire を設定します。有害なファイルの転送設定、マルウェアに感染したファイルを受信するクラウド サーバーの定義、および vm-interface の有効化または無効化を行うことができます。

階層内の場所

```
set deviceconfig setting
```

構文

```
wildfire { active-vm {vm-1 | vm-2 | vm-3 | vm-4 | vm-5 | <value>};
 cloud-server <value>; custom-dns-name <value>; preferred-analysis-
environment {Documents | Executables | default}; vm-network-
enable {no | yes}; vm-network-use-tor {enable | disable}; cloud-
intelligence { cloud-query {no | yes};submit-diagnostics {no |
 yes}; submit-report {no | yes}; submit-sample {no | yes}; } file-
retention { malicious {indefinite | <1-2000>}; non-malicious <1-90> }
 signature-generation { av {no | yes}; dns {no | yes}; url {no |
 yes}; } }
```

オプション

`+ active-vm` — サンプル解析にWildFireが使用する仮想マシン環境を選択します。Each vm has a different configuration, such as Windows XP, a specific versions of Flash, Adobe reader, etc.どのVMが選択されるかを表示するには、次のコマンド: **`show wildfire status`**(wildfireステータスを表示)を実行し、選択したVMフィールドを表示します。VM環境情報を表示するには、以下のコマンドを実行します。**`: show wildfire vm-images`**（**`wildfire vm`**イメージを表示）。

`+ cloud-server` — アプライアンスが再解析のために悪質なサンプル/レポートを転送するクラウドサーバのホスト名。デフォルトのクラウドサーバは、wildfire-public-cloudです。To configure forwarding, use the following command: **`set deviceconfig setting wildfire cloud-intelligence`**.

`+ custom-dns-name` — デフォルトの DNS 名 `wfpc.sevice.{` の代わりに、サーバー証明書と `WildFire` サーバーリストで使用するカスタム `DNS` 名を構成します。`<clustername>.<domain>`.

`+ preferred-analysis-environment` —顧客の環境で最も頻繁に分析されるサンプルのタイプに応じて、大部分のリソースをドキュメント分析または実行可能な分析に割り当てます。既定の割り当ては、ドキュメントと実行可能サンプルの間のリソースのバランスをとります。例えば、解析リソースの大部分をドキュメントに割り当てるには次を実行します: **`set deviceconfig setting wildfire preferred-analysis-environment Documents`**.

`+ vm-network-enable` — vmネットワークを有効または無効にします。有効にすると、仮想マシンサンドボックスで実行されているサンプルファイルがインターネットにアクセスできます。これにより、WildFireはマルウェアの動作をより詳細に分析し、電話のホームアクティビティなどを探すことができます。

`+ vm-network-use-tor` — vmインターフェイスのTorネットワークを有効または無効にします。このオプションを有効にすると、サンプル分析中にWildFireアプライアンスのサンドボックスシステムから送信された悪意のあるトラフィックがTorネットワーク経由で送信されます。Torネットワークはパブリックipアドレスを隠すので、悪質なサイトの所有者はトラフィックのソースを特定できません。

`> cloud-intelligence` — WildFireの診断、レポートまたはサンプルをパロアルトネットワークのWildFireクラウドに送信するようにアプライアンスを設定するか、ローカル分析を実行してWildFireアプライアンスのリソースを節約する前にパブリックのWildFireクラウドに自動的にクエリを送信します。レポート送信オプションは、統計収集のために悪質なサンプルのレポートをクラウドに送信します。サンプルを送信するオプションは、悪質なサンプルをクラウドに送信します。サンプル送信を有効にすると、クラウドがサンプルを再解析し、サンプルが悪意のある場合は新しいレポートとシグネチャが生成されるため、レポート送信を有効にする必要はありません。

`> file-retention` —マルウェア（マルウェアとフィッシング）のサンプルと悪意のない（グレーウェアと良性の）サンプルを保存する期間を設定します。悪質なサンプルを保持するためのデフォルトは不定です（削除しないでください）。悪質でないサンプルを保持するた

めのデフォルトは14日間です。たとえば、悪意のないサンプルを30日間保存するには： **set deviceconfig setting wildfire file-retention non-malicious 30**.

`+ signature-generation` — アプライアンスがローカルでシグネチャを生成できるようにし、悪質なコンテンツをブロックするためにパブリッククラウドにデータを送信する必要がなくなります。WildFireアプライアンスは、Palo Alto NetworksのファイアウォールまたはWildFire APIから転送されたファイルを分析し、悪意のあるファイルと関連するコマンドおよび制御トラフィックの両方をブロックするウイルス対策およびDNSシグネチャを生成します。When the appliance detects a malicious URL, it sends the URL to PAN-DB and PAN-DB assigns it the malware category.

サンプル出力

以下に、WildFire 設定の出力例を示します。

```
admin@WF-500# show deviceconfig setting wildfire wildfire
 { signature-generation { av yes; dns yes; url yes; } cloud-
intelligence { submit-report no; submit-sample yes; submit-
diagnostics yes; cloud-query yes; } file-retention { non-malicious
 30; malicious 1000; { active-vm vm-5; cloud-server wildfire-public-
cloud; vm-network-enable yes; }
```

set deviceconfig system eth2

説明

eth2 インターフェイスの設定

階層内の場所

```
set deviceconfig system
```

構文

```
eth2 { default-gateway <ip-address>; ip-address <ip-address>; mtu
 <value>; netmask <ip-netmask>; speed-duplex {100Mbps-full-duplex
 | 100Mbps-half-duplex | 10Mbps-full-duplex | 10Mbps-half-duplex |
 1Gbps-full-duplex | 1Gbps-half-duplex | auto-negotiate}; permitted-
ip <ip-address/netmask>; service disable-icmp {no | yes}; }
```

オプション

`+ default-gateway` —eth2インターフェイスのデフォルトゲートウェイのIPアドレス。

`+ ip-address` — eth2インターフェースのIPアドレス。

`+ mtu` — eth2インタフェースの最大伝送ユニット（MTU）。

+ `netmask` —eth2インターフェースのネットマスク。

+ `speed-duplex` — eth2インターフェイスのインターフェイス速度（10Mbps、100Mbps、1Gbps、または自動ネゴシエーション）およびデュプレックスモード（フルまたはハーフ）。

> `permitted-ip` — eth2インターフェースへのアクセスが許可されているIPアドレス。IPアドレスでネットマスクを指定する場合、ネットマスクはスラッシュ表記でなければなりません。たとえば、クラスCのアドレスを指定するには、次のように入力します。10.10.10.100/24 (not 10.10.10.100 255.255.255.0).

> `service-disable` — eth2インターフェイスのICMPを無効にします。

サンプル出力

```
admin@wf-500(active-controller)# show deviceconfig system eth2 eth2
 { ip-address 10.10.10.120; netmask 255.255.255.0; service { disable-
icmp no; } speed-duplex auto-negotiate; mtu 1500; }
```

必要な権限レベル

superuser, deviceadmin

set deviceconfig system eth3

説明

eth3 インターフェイスの設定

階層内の場所

```
set deviceconfig system
```

構文

```
eth3 { default-gateway <ip-address>; ip-address <ip-address>; mtu
 <value>; netmask <ip-netmask>; speed-duplex {100Mbps-full-duplex
 | 100Mbps-half-duplex | 10Mbps-full-duplex | 10Mbps-half-duplex |
 1Gbps-full-duplex | 1Gbps-half-duplex | auto-negotiate}; permitted-
ip <ip-address/netmask>; service disable-icmp {no | yes}; }
```

オプション

+ `default-gateway` —eth3インターフェイスのデフォルトゲートウェイのIPアドレス。

+ `ip-address` — eth3インターフェースのIPアドレス。

+ `mtu` — eth3インタフェースの最大伝送ユニット（MTU）。

+ `netmask` —eth3インターフェースのネットマスク。

+ `speed-duplex` — eth3インターフェイスのインターフェイス速度（10Mbps、100Mbps、1Gbps、または自動ネゴシエーション）およびデュプレックスモード（フルまたはハーフ）。

> `permitted-ip` — eth3インターフェースへのアクセスが許可されているIPアドレス。IPアドレスでネットマスクを指定する場合、ネットマスクはスラッシュ表記でなければなりません。たとえば、クラスCのアドレスを指定するには、次のように入力します。10.10.10.100/24 (not 10.10.10.100 255.255.255.0).

> `service-disable` — eth3インターフェイスのICMPを無効にします。

サンプル出力

```
admin@wf-500(active-controller)# show deviceconfig system eth3 eth3
 { ip-address 10.10.20.120; netmask 255.255.255.0; service { disable-
icmp no; } speed-duplex auto-negotiate; mtu 1500; }
```

必要な権限レベル

superuser, deviceadmin

set deviceconfig system panorama local-panorama panorama-server

詳説

WildFireアプライアンスまたはアプライアンスクラスタを管理するためのプライマリパノラマサーバを設定します。

階層内の場所

```
set deviceconfig system panorama local-panorama
```

構文

```
panorama-server {IP address | FQDN};
```

オプション

+ `panorama-server` — WildFireアプライアンスまたはアプライアンスクラスタの管理に使用するプライマリパノラマサーバのIPアドレスまたは完全修飾ドメイン名（FQDN）を設定します。

サンプル出力

出力は、パノラマサーバー設定を表示する出力スタンザのみを表示するように切り捨てられます。

```
admin@wf-500(active-controller)# show deviceconfig system
 system { panorama-server 10.10.10.100; panorama-server-2
 10.10.10.110 hostname myhost; ip-address 10.10.20.120; netmask
 255.255.255.0; default-gateway 10.10.10.1; update-server
 updates.paloaltonetworks.com; service { disable-icmp no; disable-ssh
 no; disable-snmp yes; } ...
```

必要な権限レベル

superuser, deviceadmin

set deviceconfig system panorama local-panorama panorama-server-2

詳説

WildFireアプライアンスまたはアプライアンスクラスタを管理するためのバックアップPanoramaサーバを設定します。バックアップの設定パノラマサーバは、クラスタまたは個々のアプライアンス管理の高可用性を提供します。

階層内の場所

```
set deviceconfig system panorama local-panorama
```

構文

```
panorama-server {IP address | FQDN};
```

オプション

`+ panorama-server-2` — WildFireアプライアンスまたはアプライアンスクラスタの管理に使用するプライマリパノラマサーバのIPアドレスまたは完全修飾ドメイン名（FQDN）を設定します。

サンプル出力

出力は、パノラマサーバー設定を表示する出力スタンザのみを表示するように切り捨てられます。

```
admin@wf-500(active-controller)# show deviceconfig system
 system { panorama-server 10.10.10.100; panorama-server-2
 10.10.10.110 hostname myhost; ip-address 10.10.20.120; netmask
 255.255.255.0; default-gateway 10.10.10.1; update-server
```

```
updates.paloaltonetworks.com; service { disable-icmp no; disable-ssh
no; disable-snmp yes; } ...
```

必要な権限レベル

superuser, deviceadmin

set deviceconfig system update-schedule

説明

WildFireアプライアンスでコンテンツ更新のスケジュールを決定します。これらのコンテンツ更新により、マルウェアを正確に検出するための最新の脅威情報をアプライアンスに取り込み、有害なコンテンツと安全なコンテンツを区別するアプライアンスの性能を高めることができます。

階層内の場所

```
set deviceconfig system update-schedule
```

構文

```
wf-content recurring { daily at <value> action {download-and-install
 | download-only}; weekly { action {download-and-install | download-
only}; at <value>; day-of-week {friday | monday | saturday | sunday |
 thursday | tuesday | wednesday}; } }
```

オプション

`> wf-content` — WildFireコンテンツ更新。

`> daily` — 毎日更新をスケジュールします。

`+ action` — 実行するアクションを指定します。アプライアンスをダウンロードしてインストールするか、ダウンロードのみを実行し、手動でインストールするようにアプライアンスをスケジュールできます。

`+ at` — 時間指定hh：mm（たとえば、20:10）。

`> hourly` — 毎時更新をスケジュールします。

`+ action` — 実行するアクションを指定します。アプライアンスをダウンロードしてインストールするか、ダウンロードのみを実行し、手動でインストールするようにアプライアンスをスケジュールできます。

`+ at` — 該当する時間を過ぎた後の分間。

`> weekly` — 1週間に1回更新をスケジュールします。

+ `action` — 実行するアクションを指定します。アプライアンスをダウンロードしてインストールするか、ダウンロードのみを実行し、手動でインストールするようにアプライアンスをスケジュールできます。

+ `at` — 時間指定hh：mm（たとえば、20:10）。

+ `day-of-week`— 曜日（金曜日、月曜日、土曜日、日曜日）

サンプル出力

```
admin@WF-500# show update-schedule { wf-content { recurring
 { weekly { at 19:00; action download-and-install; day-of-week
 friday; } } } }
```

必要な権限レベル

superuser, deviceadmin

set deviceconfig system vm-interface

説明

vm-interface は、WildFireアプライアンス 仮想マシンのサンドボックスで実行されているマルウェアにより、インターネットにアクセスするために使用されます。このポートを有効にすることをお勧めします。マルウェアが電話やその他のアクティビティでインターネットにアクセスした場合、WildFireは悪意のあるアクティビティをよりよく識別しやすくなります。このインターフェイスに、インターネットへの隔離された接続が確立されていることは重要です。ご利用のWildFireアプライアンスがFIPS/CCモードで運用されている場合は、vm-interfaceは無効です。詳細については、Set Up the WildFire Appliance VM InterfaceWildFire（アプライアンスVMインターフェイスの設定）を参照してください。

vm-interface　を設定したら、以下のコマンドを実行して有効にします。

```
set deviceconfig setting wildfire vm-network-enable yes
```

階層内の場所

```
set deviceconfig system
```

構文

```
set vm-interface { default-gateway <ip_address>; dns-server
 <ip_address>; ip-address <ip_address>; link-state; mtu; netmask
 <ip_address>; speed-duplex; {
```

オプション

+ `default-gateway` — VMインターフェイスのデフォルトゲートウェイ。

+ `dns-server` — VMインターフェイス用のDNSサーバ。

+ `ip-address` — VMインタフェースのIPアドレス。

+ `link-state`— リンクの状態を上下に設定します。

+`Mtu` — VMインタフェースの最大伝送単位。

+ `netmask` — VMインタフェースのIPネットマスク。

+ `speed-duplex` — VMインタフェースの速度とデュプレックス。

サンプル出力

以下の出力には、設定された vm-interface が表示されています。

```
vm-interface { ip-address 10.16.0.20; netmask 255.255.252.0; default-
gateway 10.16.0.1; dns-server 10.0.0.246; }
```

必要な権限レベル

superuser, deviceadmin

WildFire アプライアンス設定モードのコマンド リファレンス

どこで使用できますか?	何が必要ですか?
• WildFireアプライアンス	❑ WildFire アライセンス

このセクションには、以下の　WildFire　アプライアンス　ソフトウェア固有の操作モード　コマンドに関するコマンド　リファレンス情報が含まれます。WildFire アプライアンス software の一部である他のすべてのコマンドは、PAN-OS と同じです。これらのコマンドについてはPAN-OS 11.0 CLI クイック・スタートを参照してください。

- clear high-availability
- create wildfire api-key
- delete high-availability-key
- delete wildfire api-key
- delete wildfire-metadata
- disable wildfire
- edit wildfire api-key
- load wildfire api-key
- request cluster decommission
- request cluster reboot-local-node（要求クラスタ再起動 - ローカルノード）
- request high-availability state functional
- request high-availability sync-to-remote
- request system raid
- request wildfire sample redistribution
- request system wildfire-vm-image
- request wf-content
- save wildfire api-key
- set wildfire portal-admin
- show cluster all-peers
- show cluster all-peers
- show cluster membership
- show cluster task
- show cluster data migration status
- show high-availability all

- show high-availability control-link
- show high-availability state
- show high-availability transitions
- show system raid
- show wildfire
- show wildfire global
- show wildfire local
- submit wildfire local-verdict-change
- test wildfire registration

clear high-availability

説明

高可用性（HA）制御リンク統計情報を消去し、WildFireアプライアンスクラスタのコントローラノードの統計を遷移させます。

構文

```
create { high-availability { control-link { statistics; }
 transitions; } }
```

オプション

`> control-link>` — HA制御リンクの統計情報をクリアします。

`> transitions>` — HA移行統計（HAスイッチオーバー中に発生するイベント）をクリアします。

サンプル出力

コントロールリンクまたはトランジションの統計情報を消去すると、WildFireクラスタはすべての値をゼロ(0)にリセットします。

```
admin@wf-500(active-controller)> show high-availability control-link
 statistics High-Availability:Control Link Statistics:HA1：Messages-
TX :0 Messages-RX :0 Capability-Msg-TX :0 Capability-Msg-RX :0
 Error-Msg-TX :0 Error-Msg-RX :0 Preempt-Msg-TX :0 Preempt-Msg-
RX :0 Preempt-Ack-Msg-TX :0 Preempt-Ack-Msg-RX :0 Primary-Msg-
TX :0 Primary-Msg-RX :0 Primary-Ack-Msg-TX :0 Primary-Ack-Msg-
RX :0 Hello-Msg-TX :0 Hello-Msg-RX :0 Hello-Timeouts :0 Hello-
Failures :0 MasterKey-msg-TX :0 MasterKey-msg-RX :0 MasterKey-Ack-
Msg-TX :0 MasterKey-Ack-Msg-RX :0 Connection-Failures :0 Connection-
Tries-Failures :0 Connection-Listener-Tries :0 Connection-Active-
Tries :0 Ping-TX :0 Ping-Fail-TX :0 Ping-RX :0 Ping-Timeouts :0 Ping-
Failures :0 Ping-Error-Msgs :0 Ping-Other-Msgs :0 Ping-Last-Rsp :0
 admin@wf-500(active-controller)> show high-availability transitions
```

```
 High-Availability:Transition Statistics:Unknown :0 Suspended :0
 Initial :0 Non-Functional :0 Passive :0 Active :0
```

必要な権限レベル

superuser, deviceadmin

create wildfire api-key

説明

外部システムでアプライアンスにサンプルを送信したり、レポートをクエリしたり、アプライアンスからサンプルとパケットキャプチャ（PCAPS）を取得するために使用するWildFireアプライアンスにAPIキーを生成します。

構文

```
create { wildfire { api-key { key <value>; name <value>; { { {
```

オプション

+ `key` — 手動でキー値を入力してAPIキーを作成します。値は64文字のアルファベット（a～z）または数字（0～9）でなければなりません。キーオプションを指定しないと、アプライアンスは自動的にキーを生成します。

+ `name` — オプションで、APIキーの名前を入力します。An API key name is simply used to label the keys to make it easier to identify keys assigned for specific uses and has no impact on the functionality of the key.

サンプル出力

以下の出力は、アプライアンスに 3 つの API キーがあり、1 つのキーの名前が `my-api-key` であることを示しています。

```
admin@WF-500> show wildfire global api-keys all
 +-----------------------------------------------------+------------+
 | Apikey | Name |
 +-----------------------------------------------------
+------------+ | <API KEY> | my-api-key | | <API
 KEY> | my-api-key | | <API KEY> | my-api-key |
 +-----------------------------------------------------+------------
+ +---------+---------------------+---------------------+ | Status
 | Create Time | Last Used Time | +---------+---------------------
+---------------------+ | Enabled | 2017-03-02 19:14:36 | 2017-03-02
 19:14:36 | | Enabled | 2016-02-06 12:13:22 | 2017-03-01 12:10:20 |
 | Enabled | 2014-08-04 17:00:42 | 2017-03-01 11:12:52 | +---------
+---------------------+---------------------+
```

必要な権限レベル

superuser, deviceadmin

delete high-availability-key

説明

WildFireアプライアンスクラスタのコントローラノードのクラスタ制御リンク上の高可用性（HA）に使用されるピア暗号化キーを削除します。

構文

```
delete { high-availability-key; }
```

オプション

追加のオプションはありません。

サンプル出力

出力の強調表示された行は、HA制御リンクで暗号化が有効になっていないことを示しています。

```
admin@wf-500(active-controller)> show high-availability state
 High-Availability:Local Information:バージョン：1 State: active-
controller (last 1 days) Device Information:Management IPv4
 Address:10.10.10.14/24 Management IPv6 Address:HA1 制御リンク ジョイン
ト構成: Encryption Enabled: no Election Option Information::Priority:
 primary Preemptive: no Version Compatibility:ソフトウェアバー
ジョン：Match Application Content Compatibility:Match Anti-
Virus Compatibility:Match Peer Information:Connection status:
 up Version:1 State: passive-controller (last 1 days) Device
 Information:Management IPv4 Address:10.10.20.112/24 Management
 IPv6 Address:Connection up; Primary HA1 link Election Option
 Information:Priority: secondary Preemptive: no Configuration
 Synchronization:Enabled: yes Running Configuration: synchronized
```

必要な権限レベル

superuser, deviceadmin

delete wildfire api-key

説明

WildFire アプライアンスから API キーを削除します。アプライアンスで API を使用して API 関数を実行する様に設定されているシステムは、キーを削除すると、そのアプライアンスにアクセスできなくなります。

構文

```
delete { wildfire { api-key { key <value>;{ { {
```

オプション

+ キー `<value>` — 削除するキーのキー値。API キーのリストを表示するには、次のコマンドを実行します:

```
admin@WF-500> show wildfire global api-keys all
```

サンプル出力

```
admin@WF-500> delete wildfire api-key key <API KEY> APIKey <API Key>
 deleted
```

必要な権限レベル

superuser, deviceadmin

delete wildfire-metadata

説明

WildFire アプライアンスでコンテンツ更新を削除します。コンテンツ更新およびそのインストール方法の詳細は、request wf-content（wfコンテンツをリクエスト）を参照してください。

構文

```
delete { wildfire-metadata update <value>; {
```

オプション

+ 更新 `<value>` — 削除するコンテンツの更新を定義します。

サンプル出力

次の出力は、名前の付いた更新プログラムの削除を示しています。

```
panup-all-wfmeta-2-181.candidate.tgz. admin@WF-500> delete wildfire-
metadata update panup-all-wfmeta-2-181.candidate.tgz successfully
 removed panup-all-wfmeta-2-181.candidate.tgz
```

必要な権限レベル

superuser, deviceadmin

disable wildfire

説明

ドメインシグネチャまたはサンプルシグネチャを無効にして、次のWildFireコンテンツパッケージのリリースから除外します。

構文

```
disable wildfire { domain-signature { domain <value>; } OR... sample-signature { sha256 { equal <value>; } }
```

オプション

`> domain-signature`（ドメインシグネチャ）—ドメインシグネチャのステータスをdisabledに設定し、次のWildFireコンテンツリリースから除外します。

`> sample-signature`（サンプルシグネチャ）—サンプルシグネチャのステータスを無効に設定し、次のWildFireコンテンツリリースから除外します。

サンプル出力

正常に無効になったサンプルまたはドメインには出力が表示されません。

```
admin@WF-500> disable wildfire sample-signature sha256 equal
 d1378bda0672de58d95f3bff3cb42385f2d806a4a15b89cdecfedbdb1ec08228
```

必要な権限レベル

superuser, deviceadmin

edit wildfire api-key

説明

WildFire アプライアンスで、API キーの名前、または、キーの状態（enabled/disabled）を変更します。

構文

```
edit { wildfire { api-key [name | status] key <value>; { {
```

オプション

`+Name` — APIキーの名前を変更します。

`+ status` —APIキーを有効または無効にします。

* key —変更するキーを指定します。

サンプル出力

このコマンドのキー値は必須です。たとえば、stu という名前のキーの名前を stu-key1 に変更するには、以下のコマンドを入力します。

以下のコマンドでは、古いキー名を入力する必要はありません。新しいキー名のみを入力してください。

```
admin@WF-500> edit wildfire api-key name stu-key1 key <API
 KEY> stu-key1 のステータスを無効に変更するには、次のコマンドを入力
します: admin@WF-500> edit wildfire api-key status disable
 key <API KEY> Example output that shows that stu-key1 is
 disabled: admin@WF-500> show wildfire global api-keys all
 +-----------------------------------------------------+------------+
 | Apikey | Name |
 +-----------------------------------------------------+------------+
 | <API KEY> | stu-key1 |
 +-----------------------------------------------------+------------
+ +----------+---------------------+---------------------+ | Status
 | Create Time | Last Used Time | +----------+---------------------
+---------------------+ | Disabled | 2017-03-02 19:14:36 | 2017-03-02
 19:14:36 | +----------+---------------------+---------------------+
```

必要な権限レベル

superuser, deviceadmin

load wildfire api-key

説明

APIキーをWildFireアプライアンスにインポートした後、ロードコマンドを使用してキーを使用可能にする必要があります。このコマンドを使用して既存のすべての API キーを置き換えるか、既存のキー データベースを使用してインポート ファイルにキーをマージすることができます。

構文

```
load { wildfire { from <value> mode [merge | replace]; { {
```

オプション

* from — インポートしたいAPIキーファイル名を指定キーファイルは.keysファイル拡張を使用します。例えば、 my-api-keys.keysです。インポートが可能なキーのリストを見るためには以下のコマンドを入力します。

```
admin@WF-500> load wildfire api-key from ?
```

+ mode — オプションとしてインポートのモードを入力 (merge/replace).例えば、新しいキーファイルの内容にアプライアンスのキーデータベースを置き換えるには、以下のコマンドを入力します。

```
admin@WF-500> load wildfire api-key mode replace from my-api-keys.keys
```

mode（モード） オプションを指定しない場合は、デフォルトのアクションによってキーがマージされます。

必要な権限レベル

superuser, deviceadmin

request cluster decommission

説明

ノードが3つ以上あるクラスタからWildFireアプライアンスクラスタノードを削除します。2ノードクラスタからノードを削除する場合は、このコマンドを使用しないでください。代わりに、delete deviceconfig high-availability（deviceconfig高可用性を削除）およびdelete deviceconfig cluster（deviceconfig クラスタを削除）コマンドを使用して、 Remove a Node from a Cluster Locally（クラスタからノードをローカルで削除）します。

階層内の場所

request cluster

構文

```
request { cluster { decommission { show; start; stop; } } }
```

オプション

show（表示） —ノード廃止ジョブのステータスを表示します。

start（開始） —ノード廃止ジョブを開始します。

stop（中止）—ノード廃止ジョブを中止します。

サンプル出力

Node mode（ノードモード）フィールドは、モードがcontroller（コントローラ）ノードまたはworker（ワーカー）ではなくstand_aloneであるため、クラスタノードの廃止が成功したことを確認します。


```
admin@wf-500> show cluster membership Service Summary: wfpc signature
 Cluster name:アドレス:10.10.10.86 Host name: wf-500 Node name:
 wfpc-009707000xxx-internal Serial number:009707000xxx Node mode:
 stand_alone Server role:True HA priority:Last changed:Wed, 15
 Feb 2017 00:05:11 -0800 Services: wfcore signature wfpc infra
 Monitor status:Serf Health Status: passing Agent alive and
 reachable Application status: wildfire-apps-service:Ready global-db-
service:ReadyStandalone global-queue-service:ReadyStandalone local-
db-service：ReadyMaster
```

必要な権限レベル

superuser, deviceadmin

request cluster reboot-local-node（要求クラスタ再起動 - ローカルノード）

説明

ローカルのWildFireクラスタノードを正常に再起動します。

階層内の場所

```
request cluster
```

構文

```
request {cluster {reboot-local-node; }}
```

オプション

追加のオプションはありません。

サンプル出力

次のいくつかの方法で、ローカルクラスタノードが再起動したか、または再起動中であることを確認できます。

- `show cluster task local`（ローカルクラスタタスクを表示）—ローカルノードで要求されたタスクを表示します。
- `show cluster task current`（現在のクラスタタスクを表示）—現在実行中のタスクをローカルノードまたは最後に完了したタスク（コントローラノードのみ）で表示します。
- `show cluster task pending`（待機中のクラスタタスクを表示）—キューに登録されているが、まだローカルノード上で実行されていないタスクを表示します（コントローラノードのみ）。

- `show cluster task history`（クラスタタスクの履歴を表示）—ローカルノード上で実行されたタスクを表示します（コントローラノードのみ）。

たとえば、次のコマンドは、2つのクラスタノードの再起動タスクが正常に完了したことを示しています。

```
admin@qa15(passive-controller)> show cluster task history
 Request:        reboot from qa16 (009701000044/35533) at
 2017-02-17 19:21:53 UTC                 Reboot requested
 by admin Response:       permit by qa15 at 2017-02-17
 22:11:31 UTC                request not affecting
 healthy core server.Progress:       Wait for kv store
 ready for query...               KV store is ready, wait
 for cluster leader available...                Cluster
 leader is 2.2.2.16...              Checking is sysd and
 clusterd are alive...              Checking if cluster-
mgr is ready...              Checking global-db-cluster
 readiness...               Stopping global-queue server and
 leaving cluster...               Stopping global-db servers
 and doing failover...                rebooting...Finished:
  success at 2017-02-17 22:17:56 UTC Request:        reboot
 from qa16 (009701000044/35535) at 2017-02-17 22:45:50 UTC
                Reboot requested by admin Response:
 permit by qa15 at 2017-02-17 23:06:44 UTC
 request not affecting healthy core server.Progress:       Wait
 for kv store ready for query...                KV store is
 ready, wait for cluster leader available...
 Cluster leader is 2.2.2.15...                Checking is sysd
 and clusterd are alive...              Checking if cluster-
mgr is ready...              Checking global-db-cluster
 readiness...               Stopping global-queue server and leaving
 cluster...               Stopping global-db servers and doing
 failover...                rebooting...Finished:       success at
 2017-02-17 23:12:53 UTC
```

必要な権限レベル

superuser, deviceadmin

request high-availability state functional

説明

WildFireアプライアンスクラスタでは、ローカルコントローラノードまたはピアコントローラノードの高可用性（HA）状態を機能的に設定します。

階層内の場所

```
request high-availability
```

構文

```
request { high-availability { state { functional; } peer {
 functional; } } }
```

オプション

> functional（機能 ）—ローカルコントローラノードのHA状態を機能させる。

> peer（ピア）—ピア・コントローラ・ノードのHA状態を機能的にします。

サンプル出力

出力のハイライト表示された行は、ローカルコントローラノードのHA状態がアクティブ（プライマリ）コントローラの役割で機能し、ピアコントローラノードのHA状態がパッシブ（バックアップ）コントローラの役割で機能していることを示しています。

```
admin@wf-500(active-controller)> show high-availability state
 High-Availability:Local Information:バージョン：1 State: active-
controller (last 1 days) Device Information:Management IPv4
 Address:10.10.10.14/24 Management IPv6 Address:HA1 Control Links
 Joint Configuration:Encryption Enabled: no Election Option
 Information:Priority: primary Preemptive: no Version Compatibility:ソフトウェアバージョン：Match Application Content Compatibility:Match
 Anti-Virus Compatibility:Match Peer Information:Connection status:
 up Version:1 State: passive-controller (last 1 days) Device
 Information:Management IPv4 Address:10.10.20.112/24 Management
 IPv6 Address:Connection up; Primary HA1 link Election Option
 Information:Priority: secondary Preemptive: no Configuration
 Synchronization:Enabled: yes Running Configuration: synchronized
```

必要な権限レベル

superuser, deviceadmin

request high-availability sync-to-remote

説明

Wildfireアプライアンスクラスタでは、ローカルコントローラノードの候補設定または実行コンフィギュレーション、またはローカルコントローラノードのクロック（時刻と日付）をリモートの高可用性（HA）ピアコントローラノードと同期させます。

階層内の場所

request high-availability

構文

```
request { high-availability { sync-to-remote { candidate-config;
 clock; running-config; } } }
```

オプション

> `candidate-config`（候補設定）—ローカルピアコントローラノードの候補設定をリモートHAピアコントローラノードに同期させます。

> `clock`（クロック）—ローカルピアコントローラノードのクロック（時刻と日付）をリモートHAピアコントローラノードに同期させます。

> `running-config`（実行設定）—ローカルピアコントローラノードの実行設定をリモートHAピアコントローラノードに同期させます。

サンプル出力

出力のハイライト表示された行は、HAの設定状態がHAのピアコントローラノードで同期されていることを示しています。

```
admin@wf-500(active-controller)> show high-availability state
 High-Availability:Local Information:バージョン：1 State: active-
controller (last 1 days) Device Information:Management IPv4
 Address:10.10.10.14/24 Management IPv6 Address:HA1 Control Links
 Joint Configuration:Encryption Enabled: no Election Option
 Information:Priority: primary Preemptive: no Version Compatibility:ソフトウェアバージョン：Match Application Content Compatibility:Match
 Anti-Virus Compatibility:Match Peer Information:Connection status:
 up Version:1 State: passive-controller (last 1 days) Device
 Information:Management IPv4 Address:10.10.20.112/24 Management
 IPv6 Address:Connection up; Primary HA1 link Election Option
 Information:Priority: secondary Preemptive: no Configuration
 Synchronization:Enabled: yes Running Configuration: synchronized
```

必要な権限レベル

superuser, deviceadmin

request system raid

説明

このオプションは、WildFire　アプライアンスにインストールされた　RAID　ペアを管理するために使用します。WF-500 アプライアンスには、最初の 4 つのドライブ ベイ（A1、A2、B1、B2）に 4 台のドライブが設置された状態で出荷されます。ドライブ A1 と A2 が RAID 1 ペア、ドライブ B1 と B2 が 2 つ目の RAID 1 ペアになります。

階層内の場所

request system

構文

```
raid { remove <value>; OR... copy { from <value>; to <value>; } OR...
 add {
```

オプション

> add（追加）—ドライブを対応する RAID ディスク ペアに追加する

> copy（コピー）— ベイの一方のドライブから、もう一方のドライブにコピーして移行する

> remove（削除）—RAID ディスク ペアからドライブを削除する

サンプル出力

以下の出力は、RAIDが正しく設定されたWF-500アプライアンスを示します。

```
admin@WF-500> show system raid Disk Pair A Available Disk id A1
 Present Disk id A2 Present Disk Pair B Available Disk id B1 Present
 Disk id B2 Present
```

必要な権限レベル

superuser, deviceadmin

request wildfire sample redistribution

説明

必要に応じてサンプルをローカルノードに保持しながら、ローカルのWildFireアプライアンスクラスタノードから別のクラスタノードにサンプルを再配布します

階層内の場所

```
request system
```

構文

```
st { wildfire { sample { redistribution {   keep-local-copy {no |
 yes};   serial-number <value>; } } } }
```

オプション

* keep-local-copy—再配布されたサンプルのコピーをローカルのWildFireアプライアンスノードに保持するか、保持しない。

* serial-number—サンプルを再配布するノードのシリアル番号。

サンプル出力

Storage Nodesには、ローカルノードがサンプルを再配布する他のノードが表示されます。ローカルノードがサンプルを再配布していない場合、ストレージノードの場所は1つだけ表示されます。ローカルノードがサンプルを再配布している場合、Storage Nodesには2つのストレージノードの場所が表示されます。ハイライト表示された出力は、サンプル（ローカルノードとローカルノードがサンプルを再配布するノード）を格納する2つのストレージノードを示し、サンプルの再配布が行われていることを確認します。

```
admin@WF-500> show wildfire global sample-
analysis Last Created 100 Malicious Samples
 +-------------------------------------------------------------------------
+ | SHA256 | Finish Date | Create Date | Malicious |
 +-------------------------------------------------------------------------
+ | <HASH VALUE> | 2017-03-24 17:27:40 | 2017-03-24 15:41:47 | Yes |
  | <HASH VALUE> | 2017-03-24 17:26:46 | 2017-03-24 15:41:45 | Yes |
  | <HASH VALUE> | 2017-03-24 17:26:54 | 2017-03-24 15:41:45 | Yes |
  | <HASH VALUE> | 2017-03-24 17:25:12 | 2017-03-24 15:41:44 | Yes |
  | <HASH VALUE> | 2017-03-24 17:24:28 | 2017-03-24 15:41:44 | Yes |
  | <HASH VALUE> | 2017-03-24 17:23:58 | 2017-03-24 15:41:44 | Yes |
  | <HASH VALUE> | 2017-03-24 17:26:52 | 2017-03-24 14:55:23 | Yes |
  | <HASH VALUE> | 2017-03-24 17:23:32 | 2017-03-24 14:55:23 | Yes |
  | <HASH VALUE> | 2017-03-24 17:24:58 | 2017-03-24 14:55:23 | Yes |
  | <HASH VALUE> | 2017-03-24 17:22:02 | 2017-03-24 14:55:23 | Yes |
 +-------------------------------------------------------------------------
+
 +-------------------------------------------------------------------
+ | Storage Nodes | Analysis Nodes | Status | File Type |
 +-------------------------------------------------------------------
+ | 0907:ld2_2,065:ld2_2 | qa116 | Notify Finish | Java JAR |
  | 0097:ld2_2,004:ld2_2 | qa117 | Notify Finish | Java Class
  | | 0524:ld2_2,006:ld2_2 | qa117 | Notify Finish | Java
 Class | | 0656:ld2_2,524:ld2_2 | qa117 | Notify Finish |
 Java Class | | 0024:ld2_2,056:ld2_2 | qa117 | Notify Finish
 | DLL | | 0324:ld2_2,006:ld2_2 | qa117 | Notify Finish |
 Java JAR | | 0682:ld2_2,006:ld2_2 | qa116 | Notify Finish |
 Java JAR | | 0092:ld2_2,016:ld2_2 | qa116 | Notify Finish |
 DLL | | 0682:ld2_2,002:ld2_2 | qa116 | Notify Finish | DLL
 | | 0056:ld2_2,824:ld2_2 | qa117 | Notify Finish | DLL |
 +-------------------------------------------------------------------
* lines 1-10
```

必要な権限レベル

superuser, deviceadmin

request system wildfire-vm-image

ファイルを分析するために使用されるWildFireアプライアンス仮想マシン（VM）サンドボックスイメージのアップグレードを実行します。Palo Alto Networks 更新サーバーから新しい VM イメージを取得するには、まずイメージを手動でダウンロードし、SCP が有効なサーバーでそのイメージをホストし、SCP クライアントを使用してアプライアンスからイメージを取得する必要があります。イメージをアプライアンスにダウンロードしたら、以下のコマンドを使用してインストールすることができます。

階層内の場所

request system

構文

```
request { system { wildfire-vm-image { upgrade install file
 <value>; } } } }
```

オプション

`> wildfire-vm-image` — 仮想マシン(VM)イメージをインストールします。

`+ upgrade install file` — VMイメージに更新します。ファイルオプションタイプの後は？使用可能なVMイメージのリストを表示します。例えば、使用可能なイメージのリストを作成する場合は以下のコマンドを実行します。

```
admin@WF-500> request system wildfire-vm-image upgrade install file ?
```

サンプル出力

使用可能な VM イメージをリストするには、以下のコマンドを実行します。

```
admin@WF-500> request system wildfire-vm-image upgrade install
 file ?VM イメージ (この例では Windows 7 64 ビット) をインストールするには、
次のコマンドを実行します: admin@WF-500> request system wildfire-vm-image
 upgrade install file WFWin7_64Base_m-1.0.0_64base
```

必要な権限レベル

superuser, deviceadmin

request wf-content

WildFireアプライアンスでコンテンツ更新を実行します。これらのコンテンツ更新により、マルウェアを正確に検出するための最新の脅威情報をアプライアンスに取り込み、有害なコンテンツと安全なコンテンツを区別するアプライアンスの性能を高めることができます。WildFire アプライアンスで自動的にインストールされる様にコンテンツ更新をスケジュールする場合はset

deviceconfig system update-schedule（deviceconfigシステム更新スケジュールを設定）を、コンテンツ更新を削除する場合はdelete wildfire-metadata（wildfireメタデータを削除）を参照してください。

階層内の場所

要求

構文

```
request wf-content { downgrade install {previous | <value>}; upgrade
 { check download latest info install { file <filename> version
 latest; } } }
```

オプション

> `downgrade` — 以前のコンテンツバージョンをインストールします。以前にインストールしたコンテンツパッケージをインストールするためにprevious optionを使うか特定のコンテンツパッケージ番号にダウンロードするために値を入力します。

> `upgrade` — コンテンツアップグレードを実行します。

> `check` — パロアルトネットワークス更新サーバから使用可能なコンテンツパッケージ情報を入手します。

> `download` — コンテンツパッケージをダウンロードします。

> `info` — 使用可能なコンテンツパッケージの情報を表示します。

> `install` — コンテンツパッケージをインストールします。

> `file` — コンテンツパッケージのファイル名を指定します。

> `version` — コンテンツパッケージのバージョン番号指定でダウンロードまたはアップグレードします。

サンプル出力

使用可能なコンテンツ更新をリストするには、以下のコマンドを実行します。

```
admin@WF-500> request wf-content upgrade check
 Version Size Released on Downloaded Installed
 ------------------------------------------------------------------------------
 2-217 58MB 2014/07/29 13:04:55 PDT yes current 2-188 58MB 2014/07/01
 13:04:48 PDT yes previous 2-221 59MB 2014/08/02 13:04:55 PDT no no
```

必要な権限レベル

superuser, deviceadmin

save wildfire api-key

説明

save （保存）コマンドを使用して、WildFire アプライアンス上のすべての API キーをファイルに保存します。その後、バックアップ目的でキー ファイルをエクスポートしたり、キーを一括して変更したりすることができます。WildFire アプライアンスでの WildFire API の使用法の詳細は、WildFire API Reference（WildFire API参照） を参照してください。

階層内の場所

保存

構文

```
save { wildfire { api-key to<value> ;{ {
```

オプション

* `to` — キーエクスポートのファイル名を入力例えば、my-wf-keysというファイル名にWildFireアプライアンスの全APIキーをエクスポートするために以下のコマンドを入力します。

```
admin @ WF-500>save wildfire api-key to my-wf-keys
```

必要な権限レベル

superuser, deviceadmin

set wildfire portal-admin

説明

WildFire プライアンスによって生成された WildFire 分析レポートを表示するために管理者が使用する、ポータル管理者アカウントのパスワードを設定します。**Monitor (**監視**)** > **WildFire Submissions (WildFire** への送信**)** > **View WildFire Report (WildFire** レポートの表示**)**においてファイアウォールや Panorama でレポートを表示する場合には、アカウント名（admin）とパスワードが必要になります。デフォルトのユーザー名/パスワードは admin/admin です。

ファイアウォールまたは *Panorama* からレポートを表示するためにアプライアンスで設定するアカウントは、ポータル管理者アカウントのみです。新規アカウントを作成したり、アカウント名を変更したりすることはできません。これは、アプライアンスの管理に使用する管理者アカウントとは別のアカウントです。

階層内の場所

```
set wildfire
```

構文

```
set { wildfire { portal-admin { password <value>; } }
```

サンプル出力

以下は、このコマンドの出力内容です。

```
admin@WF-500> set wildfire portal-admin password Enter
 password:Confirm password:
```

必要な権限レベル

superuser, deviceadmin

show cluster all-peers

説明

WildFireアプライアンスクラスタコントローラノードでは、WildFireアプライアンスモード（コントローラまたはワーカー）、接続ステータス、アプリケーションサービスステータスなど、すべてのWildFireアプライアンスクラスタメンバーのステータスを表示します。

階層内の場所

```
show cluster
```

構文

```
all-peers;
```

オプション

追加のオプションはありません。

サンプル出力

```
admin@thing1(active-controller)> show cluster all-peers Address
 Mode Server Node Name ------- ---- ------ --------- 10.10.10.14
  controller Self True thing1 Service: infra signature wfcore
 wfpc Status:Connected, Server role applied Changed:Wed, 15 Feb
```



```
 2017 09:12:01 -0800 WF App: wildfire-apps-service:Ready global-
db-service:JoinedCluster global-queue-service:JoinedCluster
 siggen-db:ReadyMaster 10.10.10.112   controller Peer True thing2
 Service: infra signature wfcore wfpc Status:Connected, Server role
 applied Changed:Wed, 15 Feb 2017 09:13:00 -0800 WF App: wildfire-
apps-service:Ready global-db-service:ReadyLeader global-queue-
service:ReadyLeader siggen-db:ReadySlave Diag report:10.10.10.112:
 reported leader '10.10.10.112', age 0. 10.10.10.14: local node
 passed sanity check.
```

必要な権限レベル

superuser, deviceadmin

show cluster all-peers

説明

WildFireアプライアンスのクラスタコントローラノードで、クラスタ名とローカルコントローラノードの役割を含むWildFireアプライアンスクラスタコントローラのステータスを表示します（`Active Controller`（アクティブコントローラ）フィールドが`True`（正）、ローカルコントローラがプライマリコントローラの場合、`Active Controller`（アクティブコントローラ）のフィールドに`False`（誤）と表示されます。ローカルコントローラはバックアップコントローラです）。

階層内の場所

```
show cluster
```

構文

```
controller;
```

オプション

追加のオプションはありません。

サンプル出力

```
admin@thing1(active-controller)> show cluster controller
 Cluster name: satriani1 K/V API online:True Task processing:
 on Active Controller:True DNS Advertisement:App Service
 DNS Name:App Service Avail:10.10.10.112, 10.10.10.14 Core
 Servers:009707000742:10.10.10.112 009701000043:10.10.10.14 Good Core
 Servers:2 Suspended Nodes:Current Task: no tasks found
```

必要な権限レベル

superuser, deviceadmin

show cluster data migration status

詳説

WildFireアプライアンスのクラスターコントローラーノードからこのコマンドを使用して、現在のデータ移行ステータスを表示します。コマンドは、データ移行がいつ開始されたか、および進行状況を表示します。データ移行が完了すると、コマンドは完了タイムスタンプを表示します。データの移行が失敗した場合、ステータスには `0% completed`（完了）と表示されます。

階層内の場所

```
show cluster
```

構文

```
data-migration-status;
```

オプション

追加のオプションはありません。

サンプル出力

```
adminWF-500(active-controller)> show cluster data-migration-status
 100% completed on Mon Sep 9 21:44:48 PDT 2019
```

必要な権限レベル

superuser, deviceadmin

show cluster membership

説明

IPアドレス、ホスト名、WildFireアプライアンスのシリアル番号、アプライアンスの役割（`Node mode`（ノードモード））、高可用性の優先順位、アプリケーションの状態など、クラスタノードまたはスタンドアロンのWildFireアプライアンスのWildFireアプライアンスクラスタメンバシップ情報を表示します。

階層内の場所

```
show cluster
```

構文

```
membership;
```

オプション

追加のオプションはありません。

サンプル出力

WildFireアプライアンスのクラスタノードメンバー（コントローラおよびワーカーノード）とスタンドアロンのWildFireアプライアンスのクラスタメンバーシップ情報を表示して、クラスタに属しているかどうか、アプリケーションステータス、およびその他のローカルホスト情報を確認できます。出力は、WildFireアプライアンスの役割によってわずかに異なります。違いは次のとおりです：

- プロンプトはアクティブ（プライマリ）コントローラノードとパッシブ（バックアップ）コントローラノードを示しますが、ワーカーノードまたはスタンドアロンの役割は示しません。
- `Node mode`（ノードモード）は、WildFireアプライアンスが`controller node`（コントローラノード）、`worker node`（ワーカーノード）、または`stand_alone` WildFireアプライアンスであるかどうかを示します。
- `HA priority`（HAプライオリティ）は、アクティブコントローラノードの`primary`（プライマリ）、パッシブ（バックアップ）コントローラノードの`secondary`（セカンダリ）を表示し、ワーカーノードおよびスタンドアロンWildFireアプライアンスのフィールドは空白です。
- `Application status`（アプリケーションステータス）フィールドには、いくつかのフィールドに異なる値が表示されます。`global-db-service`および`global-queue-service`の場合、クラスタメンバーには`ReadyLeader`または`JoinedCluster`が表示され、スタンドアロンアプライアンスには`ReadyStandalone`が表示されます。

  `siggen-db`の場合、WildFireアプライアンスクラスタのプライマリコントローラノードは`ReadyMaster`を表示し、WildFireアプライアンスクラスタのセカンダリコントローラノードは`ReadySlave`を表示し、WildFireアプライアンスクラスタワークノードは`Ready`を表示し、スタンドアロンWildFireアプライアンスは`ReadyMaster`を表示します。

  実際のシリアル番号を隠すため、各*WildFire*アプライアンスのシリアル番号の最後の*4*桁が「*xxxx*」に変更されています。

WildFireアプライアンスクラスタのプライマリコントローラノードの出力：

```
admin@thing1(active-controller)> show cluster membership Service
 Summary: wfpc signature Cluster name: satriani1 Address:10.10.10.14
 Host name: thing1 Node name: wfpc-00970100xxxx-internal Serial
 number:00970100xxxx Node mode: controller Server role:True HA
 priority: primary Last changed:Wed, 15 Feb 2017 09:12:01 -0800
 Services: wfcore signature wfpc infra Monitor status:Serf Health
 Status: passing Agent alive and reachable Application status:
 wildfire-apps-service:Ready global-db-service:JoinedCluster global-
queue-service:JoinedCluster siggen-db:ReadyMaster
```

WildFireアプライアンスクラスタのコントローラバックアップノードでの出力：

```
admin@thing2(passive-controller)> show cluster membership Service
 Summary: wfpc signature Cluster name: satriani1 Address:10.10.10.112
 Host name: thing2 Node name: wfpc-00970700xxxx-internal Serial
 number:009707000xxxx Node mode: controller Server role:True HA
 priority: secondary Last changed:Wed, 15 Feb 2017 09:13:10 -0800
 Services: wfcore signature wfpc infra Monitor status:Serf Health
 Status: passing Agent alive and reachable Application status:
 wildfire-apps-service:Ready global-db-service:ReadyLeader global-
queue-service:ReadyLeader siggen-db:ReadySlave
```

WildFireアプライアンスクラスタ内のワーカーノードでの出力：

```
admin@grinch> show cluster membership Service Summary: wfpc Cluster
 name: satriani1 Address:10.10.10.19 Host name: grinch Node name:
 wfpc-00970100xxxx-internal Serial number:00970100xxxx Node mode:
 worker Server role:True HA priority:Last changed:Thu, 09 Feb 2017
 15:55:55 -0800 Services: wfcore wfpc infra Monitor status:Serf
 Health Status: passing Agent alive and reachable Application status:
 wildfire-apps-service:Ready global-db-service:JoinedCluster global-
queue-service:JoinedCluster siggen-db:Ready
```

スタンドアロンのWildFireアプライアンス（WildFireアプライアンスクラスタメンバーではない）の出力

```
admin@max> show cluster membership Service Summary: wfpc signature
 Cluster name:アドレス:10.10.10.90 Host name: max Node name:
 wfpc-00970700xxxx-internal Serial number:00970700xxxx Node mode:
 stand_alone Server role:True HA priority:Last changed:Mon, 13
 Feb 2017 02:54:52 -0800 Services: wfcore signature wfpc infra
 Monitor status:Serf Health Status: passing Agent alive and
 reachable Application status: wildfire-apps-service:Ready global-db-
service:ReadyStandalone global-queue-service:ReadyStandalone siggen-
db:ReadyMaster
```

必要な権限レベル

superuser, deviceadmin

show cluster task

説明

ローカルクラスタノードまたはすべてのクラスタノードのWildFireアプライアンスクラスタタスク情報を表示するか、完了したクラスタタスク履歴または保留中のクラスタタスクを表示します。

階層内の場所

```
show cluster
```

構文

```
task { current; history; local; pending; }
```

オプション

> current—現在、WildFireアプライアンスクラスタで許可されているタスクを表示します。クラスタコントローラノードでのみ使用できます。

> history—完了したクラスタタスクを表示します。クラスタコントローラノードでのみ使用できます。

> local—ローカルのWildFireアプライアンスクラスタノードに保留中のタスクを表示します。

> pending— WildFireアプライアンスクラスタ全体の保留中のタスクを表示します。クラスタコントローラノードでのみ使用できます。

サンプル出力

```
admin@WF-500(active-controller)> show cluster task local
 Request:         reboot from WF-500 (009701000034/74702) at
 2017-02-21 03:06:45 UTC                  Reboot requested by
 admin Queued:          by WF-500                  2/3 core servers
 available. reboot not allowed to maintain quorum Request:
 reboot from WF-500 (009701000034/74704) at 2017-02-21 03:10:27 UTC
                 Reboot requested by admin Queued:          by WF-500
                 2/3 core servers available. reboot not allowed to
 maintain quorum admin@WF-500(active-controller)> show cluster task
 current no tasks found admin@WF-500(active-controller)> show cluster
 task pending Request:         reboot from WF-500 (009701000034/74702)
 at 2017-02-21 03:06:45 UTC                  Reboot requested by
 admin Queued:          by WF-500                  2/3 core servers
 available. reboot not allowed to maintain quorum Request:
 reboot from WF-500 (009701000034/74704) at 2017-02-21 03:10:27 UTC
                 Reboot requested by admin Queued:          by WF-500
                 2/3 core servers available. reboot not allowed to
 maintain quorum admin@WF-500B(passive-controller)> show cluster
```

```
 task history Request:        reboot from WF-500 (009701000044/35533)
 at 2017-02-17 19:21:53 UTC                  Reboot requested by
 admin Response:       permit by WF-500B at 2017-02-17 22:11:31
 UTC                request not affecting healthy core server.経
過:       Wait for kv store ready for query...                KV
 store is ready, wait for cluster leader available...
  Cluster leader is 10.10.10.100...                Checking
 is sysd and clusterd are alive...               Checking if
 cluster-mgr is ready...               Checking global-db-cluster
 readiness...               Stopping global-queue server and leaving
 cluster...               Stopping global-db servers and doing
 failover...                rebooting...Finished:       success at
 2017-02-17 22:17:56 UTC
```

必要な権限レベル

superuser, deviceadmin

show high-availability all

説明

HA制御リンク、HA状態、HA移行情報、ピアソフトウェア、コンテンツ更新、ウイルス対策互換性情報、ピア接続と役割情報など、WildFireアプライアンスクラスタのHA（高可用性）情報をすべて表示します。

階層内の場所

```
show high-availability
```

構文

```
all;
```

オプション

追加のオプションはありません。

サンプル出力

```
admin@thing1(active-controller)> show high-availability all
 High-Availability:Local Information:バージョン：1 State: active-
controller (last 1 days) Device Information:Management IPv4
 Address:10.10.10.14/24 Management IPv6 Address:HA1 Control
 Links Joint Configuration:Link Monitor Interval:3000 ms
 Encryption Enabled: no HA1 Control Link Information:IPアドレ
ス:10.10.10.140/24 MAC Address:00:00:5e:00:53:ff Interface: eth3
 Link State:Up; Setting:1Gb/s-full Key Imported : no Election
 Option Information:Priority: primary Preemptive: no Promotion
```

```
 Hold Interval:2000 ms Hello Message Interval:8000 ms Heartbeat
 Ping Interval:2000 ms Preemption Hold Interval:1 min Monitor Fail
 Hold Up Interval:0 ms Addon Master Hold Up Interval:500 ms Version
 Information:Build Release:8.0.1-c31 URL Database:Not Installed
 Application Content:497-2688 Anti-Virus:0 Version Compatibility:ソ
フトウェアバージョン：Match Application Content Compatibility:Match
 Anti-Virus Compatibility:Match Peer Information:Connection status:
 up Version:1 State: passive-controller (last 1 days) Device
 Information:Management IPv4 Address:10.10.10.30/24 Management IPv6
 Address:HA1 Control Link Information:IPアドレス:10.10.10.130 MAC
 Address:00:00:5e:00:53:00 Connection up; Primary HA1 link Election
 Option Information:Priority: secondary Preemptive: no Version
 Information:Build Release:8.0.1-c31 URL Database:Not Installed
 Application Content:497-2688 Anti-Virus:0 Initial Monitor Hold
 inactive; Allow Network/Links to Settle:Link and path monitoring
 failures honored Configuration Synchronization:Enabled: yes Running
 Configuration: synchronized
```

必要な権限レベル

superuser, deviceadmin

show high-availability control-link

説明

HA制御リンクで送受信されるさまざまなタイプのメッセージ数、接続障害、およびpingアクティビティを含む、プライマリコントローラノードとバックアップコントローラノード間のHA制御リンクのWildFireアプライアンスクラスタ高可用性（HA）統計情報を表示します。

階層内の場所

```
show high-availability
```

構文

```
control-link { statistics; }
```

オプション

`> statistics`—WildFireアプライアンスクラスタコントローラノードのHA制御リンク統計を表示します。

サンプル出力

```
admin@thing1(active-controller)> show high-availability control-link
 statistics High-Availability:Control Link Statistics:HA1：Messages-
TX :13408 Messages-RX :13408 Capability-Msg-TX :2 Capability-Msg-
```

```
RX :2 Error-Msg-TX :0 Error-Msg-RX :0 Preempt-Msg-TX :0 Preempt-Msg-
RX :0 Preempt-Ack-Msg-TX :0 Preempt-Ack-Msg-RX :0 Primary-Msg-TX :1
 Primary-Msg-RX :1 Primary-Ack-Msg-TX：1 Primary-Ack-Msg-RX：1 Hello-
Msg-TX :13402 Hello-Msg-RX :13402 Hello-Timeouts :0 Hello-Failures :0
 MasterKey-Msg-TX :1 MasterKey-Msg-RX :1 MasterKey-Ack-Msg-TX：1
 MasterKey-Ack-Msg-RX：1 Connection-Failures :0 Connection-Tries-
Failures :12 Connection-Listener-Tries :1 Connection-Active-Tries :12
 Ping-TX：53614 Ping-Fail-TX：0 Ping-RX：53613 Ping-Timeouts :0 Ping-
Failures :0 Ping-Error-Msgs :0 Ping-Other-Msgs :0 Ping-Last-Rsp：{{{防
御>防御<防御}>{防御>防御<防御}<{防御>防御<防御}}>{{防御>防御<防御}>{防御>防
御<防御}<{防御>防御<防御}}<{{防御>防御<防御}>{防御>防御<防御}<{防御>防御<防
御}}}
```

必要な権限レベル

superuser, deviceadmin

show high-availability state

説明

コントローラノードがアクティブ（プライマリ）かパッシブ（バックアップ）か、コントローラノードがその状態になっているかどうかを含む、ローカルおよびピアクラスタコントローラノードのWildFireアプライアンスクラスタの高可用性（HA）状態情報を表示すると、HA 構成、ローカルとピアのコントローラノードの構成が同期されているかどうか、コントローラノードのピア間のソフトウェア、コンテンツ更新、およびウイルス対策のバージョンの互換性が含まれます。

階層内の場所

```
show high-availability
```

構文

```
state;
```

オプション

追加のオプションはありません。

サンプル出力

```
admin@thing1(active-controller)> show high-availability state
 High-Availability:Local Information:バージョン：1 State: active-
controller (last 1 days) Device Information:Management IPv4
 Address:10.10.10.14/24 Management IPv6 Address:HA1 Control Links
 Joint Configuration:Encryption Enabled: no Election Option
 Information:Priority: primary Preemptive: no Version Compatibility:ソ
```

```
フトウェアバージョン：Match Application Content Compatibility:Match
 Anti-Virus Compatibility:Match Peer Information:Connection status:
 up Version:1 State: passive-controller (last 1 days) Device
 Information:Management IPv4 Address:10.10.10.30/24 Management
 IPv6 Address:Connection up; Primary HA1 link Election Option
 Information:Priority: secondary Preemptive: no Configuration
 Synchronization:Enabled: yes Running Configuration: synchronized
```

必要な権限レベル

superuser, deviceadmin

show high-availability transitions

説明

クラスタコントローラノードのHAスイッチオーバー中に発生するイベントに関するWildFireアプライアンスクラスタの高可用性（HA）移行情報を表示します。

階層内の場所

```
show high-availability
```

構文

```
transitions;
```

オプション

追加のオプションはありません。

サンプル出力

```
admin@thing1(active-controller)> show high-availability transitions
 High-Availability:Transition Statistics:Unknown :1 Suspended :0
 Initial :0 Non-Functional :0 Passive :0 Active :3
```

必要な権限レベル

superuser, deviceadmin

show system raid

説明

WildFire アプライアンスの RAID 設定を表示します。WF-500 アプライアンスには、最初の 4 つのドライブ ベイ（A1、A2、B1、B2）に 4 台のドライブが設置された状態で出荷されます。ドライブ A1 と A2 が RAID 1 ペア、ドライブ B1 と B2 が 2 つ目の RAID 1 ペアになります。

階層内の場所

```
show system
```

構文

```
raid { detail; {
```

オプション

追加のオプションはありません。

サンプル出力

以下の出力には、稼働中の WF-500 アプライアンス上の　RAID 設定が表示されています。

```
admin@WF-500> show system raid detail Disk Pair A Available Status
 clean Disk id A1 Present model :ST91000640NS size :953869 MB
 partition_1 : active sync partition_2 : active sync Disk id A2
 Present model :ST91000640NS size :953869 MB partition_1 : active
 sync partition_2 : active sync Disk Pair B Available Status
 clean Disk id B1 Present model :ST91000640NS size :953869 MB
 partition_1 : active sync partition_2 : active sync Disk id B2
 Present model :ST91000640NS size :953869 MB partition_1 : active
 sync partition_2 : active sync
```

必要な権限レベル

superuser, superreader

submit wildfire local-verdict-change

説明

ファイアウォールから送信されたサンプルのローカルで生成されたWildFireの判定を変更します。評決の変更は WildFire アプライアンスに送信されたサンプルにのみ適用され、同じサンプルの評決は WildFire パブリック クラウドで変更されません。show wildfire global（wildfire グローバルを表示）コマンドを使用して、変更された判定のあるサンプルを表示できます。

WildFire プライベート クラウド コンテンツ パッケージ は、設定した変更を反映して更新されます (ファイアウォールで、デバイス > 動的更新 > **WF-Private** を選択して WildFire プライベート クラウド コンテンツの更新を有効にします)。サンプルの判定を悪意のあるものに変更すると、WildFireアプライアンスは新しいシグネチャを生成してマルウェアを検出し、そのシグネチャをWildFireプライベートクラウドコンテンツパッケージに追加します。サンプルの判定を無効に変更すると、WildFireアプライアンスはWildFireプライベートクラウドコンテンツパッケージからシグネチャを削除します。

ローカルサンプルの判定を変更するために使用できるAPI呼び出しもあります。詳細については、 WildFire API Reference（WildFire APIリファレンス）を参照してください。

階層内の場所

```
submit wildfire
```

構文

```
submit { wildfire { local-verdict-change { hash <value>; verdict
 <value>; comment <value>; } }
```

オプション

* `hash` — 判定を変更するファイルの SHA-256 ハッシュを指定します。

* `verdict` —新しいファイルの判定を入力します：0は良性のサンプルを示し、 1はマルウェアを示します。 2はグレーウェアを示します。

* `comment` — 評決の変更を説明するコメントを含みます。

サンプル出力

以下は、このコマンドの出力内容です。

```
admin@WF-500> submit wildfire local-verdict-change comment test hash
 c323891a87a8c43780b0f2377de2efc8bf856f02dd6b9e46e97f4a9652814b5c
 verdict 2 Please enter 'Y' to commit: (y or n) verdict is changed
 (old verdict:1, new verdict:2)
```

必要な権限レベル

superuser, deviceadmin

show wildfire

説明

グローバルおよびローカルデバイス、サンプル関連の詳細、アプライアンスのステータス、分析を実行するために選択された仮想マシンなど、WildFireアプライアンスに関するさまざまな情報を表示します。

階層内の場所

```
show wildfire
```

構文

```
status | vm-images | wf-vm-pe-utilization | wf-vm-doc-utilization
 | wf-vm-email-link-utilization | wf-vm-archive-utilization | wf-
sample-queue-status }
```

オプション

`> status` —アプライアンスの状況だけでなくサンプル解析に使用された仮想マシン(VM)のコンフィグ情報、クラウドへのサンプル/レポートの送付の有無、VMネットワークや登録情報を表示します。

`> vm-images` — サンプル解析のための使用可能な仮想マシンの特性の表示現在アクティブなイメージを表示するには、次のコマンドを実行します

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

そして、VMフィールドを表示します。

`> wf-sample-queue-status` — 解析待ちのWildFireアプライアンスサンプルの数と内訳を表示します。

`> wf-vm-doc-utilization` — ドキュメントファイルの処理に使用され、使用されている解析環境の数を表示します。

`> wf-vm-elinkda-utilization` — 電子メールリンクの処理に使用され、使用されている解析環境の数を表示します。

`> wf-vm-pe-utilization` — Portable Executable(ポータブル実行可能-PE)ファイルの処理に使用され、使用されている解析環境の数を表示します。

サンプル出力

以下は、このコマンドの出力です。

```
admin@WF-500> show wildfire status Connection info:Wildfire
 cloud: s1.wildfire.paloaltonetworks.com Status:Idle Submit
 sample: disabled Submit report: disabled Selected VM: vm-5 VM
 internet connection: disabled VM network using Tor: disabled Best
 server:                    s1.wildfire.paloaltonetworks.com Device
 registered: yes Service route IP address:10.3.4.99 Signature
 verification: enable Server selection: enable Through a proxy: no
 admin@WF-500> show wildfire vm-images Supported VM images: vm-1
 Windows XP, Adobe Reader 9.3.3, Flash 9, Office 2003.Support PE,
 PDF, Office 2003 and earlier vm-2 Windows XP, Adobe Reader 9.4.0,
 Flash 10n, Office 2007.Support PE, PDF, Office 2007 and earlier
 vm-3 Windows XP, Adobe Reader 11, Flash 11, Office 2010.Support PE,
 PDF, Office 2010 and earlier vm-4 Windows 7 32bit, Adobe Reader 11,
 Flash 11, Office 2010.Support PE, PDF, Office 2010 and earlier vm-5
 Windows 7 64bit, Adobe Reader 11, Flash 11, Office 2010.Support
 PE, PDF, Office 2010 and earlier vm-6 Windows XP, Internet Explorer
 8, Flash 11.Support E-MAIL Links admin@WF-500> show wildfire wf-
sample-queue-status DW-ARCHIVE:4、DW-DOC：2、DW-ELINK：0、DW-PE：21、DW-
URL_UPLOAD_FILE：2, admin@WF-500> show wildfire wf-vm-pe-utilization
 { available:2、in_use：1, }
```

必要な権限レベル

superuser, superreader

show wildfire global

説明

利用可能なAPIキー、登録情報、検体の判定の変更、アクティビティ、検体のデバイス元、アプライアンスが解析した最近のサンプルなど、グローバルデバイスと検体のステータスに関するさまざまな情報が表示されます。

階層内の場所

```
show wildfire global
```

構文

```
api-keys { all { details; } key <value>; } devices-reporting-data;
 last-device-registration { all; } local-verdict-change { all; sha256
 <value>; } } sample-analysis { number; type; } } sample-device-
lookup { sha256 { equal <value>; } sample-status { sha256 { equal
 <value>; } } signature-status { sha256 { equal <value>; } }
```

オプション

`> api-keys` —WildFire アプライアンスで生成されたAPIキーの詳細を表示します。キーが最後に使用された時刻、キー名、ステイタス（有効または無効）キーが生成された日付/時刻を確認できます。

`>devices-reporting-data` —最新の登録作業のリストの表示

`> last-device-registration` —最新の登録作業のリストの表示

`> local-verdict-change` — 評決が変更されたサンプルを表示します。

`> sample-analysis` —最大1,000サンプルまでの森林火災分析結果を表示します。

`> sample-status`—wildfireのサンプル状況の表示ファイルのSHA256値を入力して現在のアナライザを表示する。

`> sample-device-lookup` — 特定のSHA256検体を送信したファイアウォールを表示します。

`> signature-status` —wildfireのサンプル状況の表示ファイルのSHA256値を入力して現在のアナライザを表示する。

サンプル出力

以下は、このコマンドの出力です。

```
admin@WF-500> show wildfire global api-keys all +------------
+-----------+---------+----------------------+----------------------
+ | Apikey | Name | Status | Create Time | Last Used Time |
 +------------+-----------+---------+---------------------
+----------------------+ | <API KEY> | happykey1 | Enabled |
 2017-03-01 23:21:02 | 2017-03-01 23:21:02 | +------------
+-----------+---------+----------------------+----------------------
+ admin@WF-500> show wildfire global devices-reporting-data
 +--------------+---------------------+-------------+------------
+----------+--------+ | _Device ID | Last Registered | Device IP | SW
 Version | HW Model | Status | +--------------+----------------------
+-------------+------------+----------+--------+ | 000000000000
 | 2017-03-01 22:28:25 | 10.1.1.1 | 8.1.4 | PA-220 | OK |
 +--------------+---------------------+-------------+------------
+----------+--------+ admin@WF-500> show wildfire global last-
device-registration all +--------------+---------------------
+-------------+------------+----------+--------+ | Device
 ID | Last Registered | Device IP | SW Version | HW Model |
 Status | +--------------+---------------------+-------------
+------------+----------+--------+ | 000000000000 | 2017-07-31
 12:35:53 | 10.1.1.1 | 8.1.4 | PA-220 | OK | +--------------
+---------------------+-------------+------------+----------
+--------+ admin@WF-500> show wildfire global local-verdict-change
 +-------------------------------------------------------------------
+---------+--------+ | SHA256 | Verdict | Source |
 +-------------------------------------------------------------------
+---------+--------+ |
```

```
 c883b5d2e16d22b09b176ca0786128f8064d47edf26186b95845aa3678868496| 2
 -> 1 | Yes |
 +-------------------------------------------------------------------
+---------+--------+ admin@WF-500> show wildfire global sample-
analysis Last Created 100 Malicious Samples +--------------
+---------------------+---------------------+-----------+ |
 SHA256 | Finish Date | Create Date | Malicious | +--------------
+---------------------+---------------------+-----------+ |
 <HASH VALUE> | 2017-03-01 23:27:57 | 2017-03-01 23:27:57 | Yes
 | +--------------+---------------------+--------------------
+-----------+ +---------------------+---------------
+---------------+----------------+ | Storage Nodes | Analysis Nodes
 | Status | File Type | +---------------------+---------------
+---------------+----------------+ | 00926ld1_2,0094:d1_2 |
 qa16 | Notify Finish | Elink File | +----------------------
+----------------+--------------+----------------+ Last Created
 100 Non-malicious Samples +--------------+--------------------
+---------------------+-----------+ | SHA256 | Finish Date |
 Create Date | Malicious | +--------------+---------------------
+---------------------+-----------+ | <HASH VALUE> | 2017-03-01
 23:31:15 | 2017-03-01 23:24:29 | No | +--------------
+---------------------+--------------------+-----------+
 +----------------------+----------------+--------------
+--------------------+ | Storage Nodes | Analysis Nodes |
 Status | File Type | +---------------------+---------------
+---------------+--------------------+ | 0712:smp_27,94:smp_7 |
 qa16 | Notify Finish | MS Office document | +----------------------
+----------------+--------------+--------------------+
 admin@WF-500> show wildfire global sample-device-lookup sha256 equal
 d75f2f71829153775fa33cf2fa95fd377f153551aadf0a642704595100efd460
 Sample
 1024609813c57fe174722c53b3167dc3cf5583d5c7abaf4a95f561c686a2116e
 last seen on following devices:
 +-------------------------------------------------------------------
+-----------+-----------+--------------------+ |
 SHA256 | Device ID | Device IP | Submitted Time |
 +-------------------------------------------------------------------
+-----------+-----------+--------------------+ |
 1024609813c57fe174722c53b3167dc3cf5583d5c7abaf4a95f561c686a2116e
 | Manual | Manual | 2019-08-05 19:24:39 |
 +-------------------------------------------------------------------
+-----------+-----------+--------------------+
 admin@WF-500> show wildfire global sample-status sha256 equal
 dc9f3a2a053c825e7619581f3b31d53296fe41658b924381b60aee3eeea4c088
 +---------------------+---------------------+-----------
+---------------------------+ | Finish Date | Create
 Date | Malicious | Storage Nodes | +--------------------
+---------------------+-----------+---------------------------
+ | 2017-03-01 22:34:17 | 2017-03-01 22:28:23 | No |
 009026:smp_27,097010smp_27 | +--------------------
+---------------------+-----------+---------------------------+
 +---------------+--------------+-----------------+ | Analysis
 Nodes | Status | File Type | +---------------+--------------
+-----------------+ | qa15 | Notify Finish | Adobe Flash
 File | +---------------+--------------+-----------------
+ admin@WF-500> show wildfire global signature-status sha256
```

```
 equalc883b5d2e16d22b09b176ca0786128f8064d47edf26186b95845aa3678868496
 Signature Name:Virus/Win32.WPCGeneric.cr Current Status: released
 Release History: +---------------+---------------------+---------
+-------------+----------+ | Build Version | Timestamp | UTID |
 Internal ID | Status | +---------------+---------------------
+---------+-------------+----------+ | 155392 | 2017-02-03 10:11:06 |
 5000259 | 10411 | released | +---------------+---------------------
+---------+-------------+----------+
```

必要な権限レベル

superuser, superreader

show wildfire local

説明

ローカルデバイスとサンプル、アクティビティ、アプライアンスが分析した最近のサンプル、および基本的なWildFireの統計情報に関するさまざまな情報を表示します。

階層内の場所

```
show wildfire local
```

構文

```
latest { analysis { filter malicious|benign; sort-by SHA256|Submit
 Time|Start Time|Finish Time|Malicious|Status; sort-direction asc|
desc; limit 1-20000; days 1-7; } OR... samples { filter malicious|
benign; sort-by SHA256|Create Time|File Name|File Type|File Size|
Malicious|Status; sort-direction asc|desc; limit 1-20000; days
 1-7; } sample-processed { count 1-1000; time {last-1-hr|last-12-
hrs|last-15-minutes|last-24-hrs|last-30-days|last-7-days|last-
calender-day|last-calender-month; } sample-status { sha256 { equal
 <value>; } } statistics days <1-31> | hours <0-24> | minutes
 <0-60>; }
```

オプション

`> latest` —最新の30の作業の表示（最新の30の解析作業、解析された30ファイル、解析されたファイルのネットワークセッション情報とパブリッククラウドにアップロードされたファイルを含みます）

`> sample-processed` — 指定されたタイムスパン内でローカルに処理された検体の数、または検体の最大数を示します。

`> sample-status`—wildfireのサンプル状況の表示ファイルのSHA256値を入力して現在のアナライザを表示する。

`> statistics` — 基本的なwildfireの統計の表示

サンプル出力

以下は、このコマンドの出力です。

```
admin@WF-500> show wildfire latest analysis Latest
 analysis information: +-------------+--------------------
+---------------------+---------------------+ | SHA256 | Submit Time
 | Start Time | Finish Time | +-------------+--------------------
+---------------------+---------------------+ | <HASH VALUE>|
 2017-03-01 14:28:26 | 2017-03-01 14:28:26 | 2017-03-01 14:34:24 | |
 <HASH VALUE>| 2017-03-01 14:28:25 | 2017-03-01 14:28:25 | 2017-03-01
 14:28:41 | | <HASH VALUE>| 2017-03-01 14:28:25 | 2017-03-01 14:28:25
 | 2017-03-01 14:28:26 | +-------------+--------------------
+---------------------+---------------------+ +-----------
+-------------------------------------------------------------
+-----------+ | Malicious | VM Image | Status | +------------
+-------------------------------------------------------------
+-----------+ | Yes | Windows 7 x64 SP1, Adobe Reader
 11, Flash 11, Office 2010 | completed | | No | Java/
Jar Static Analyzer | completed | | Suspicious |
 Java/Jar Static Analyzer | completed | +------------
+-------------------------------------------------------------
+-----------+ admin@WF-500> show wildfire local latest samples
 Latest samples information: +--------------+--------------------
+----------------+---------------+ | SHA256 | Create Time |
 File Name | File Type | +--------------+--------------------
+----------------+---------------+ | <HASH VALUE> | 2017-03-01
 14:28:25 | | JAVA Class | | <HASH VALUE> | 2017-03-01
 14:28:25 | | JAVA Class | | <HASH VALUE> | 2017-03-01
 14:28:25 | | PE | +--------------+--------------------
+----------------+---------------+ +--------------+-----------
+------------------+ | File Size | Malicious | Status |
 +--------------+-----------+------------------+ | 20,407 |
 No | analysis complete | | 1,584 | Yes | analysis complete | |
 259,024 | No | analysis complete | +--------------+-----------
+------------------+ admin@WF-500> show wildfire local sample-
processed count 2 Time Window: last-15-minutes Display Count:2:
 +-----------------------------------------------------------------------
+---------------------+-----------+------------+-----------
+------------+------------------+ | SHA256 | Create Time
 | File Name | File Type | File Size | Malicious | Status |
 +-----------------------------------------------------------------------
+---------------------+-----------+------------
+-----------+-----------+------------------+ |
 ce752b7b76ac2012bdff2b76b6c6af18e132ae8113172028b9e02c6647ee19bb |
 2018-12-09 16:55:53 | | Email Link | 31,522 | | download complete |
 | 349e57e51e7407abcd6eccda81c8015298ff5d5ba4cedf09c7353c133ceaa74b |
 2018-12-09 16:53:40 | | Email Link | 39,679 | | download complete |
 +-----------------------------------------------------------------------
+---------------------+-----------+------------
+-----------+------------+------------------+
 admin@WF-500> show wildfire local sample-status sha256 equal
 0f2114010d00d7fa453177de93abca9643f46604575361148 98c56149f819a9b
```

```
 Sample information: +--------------------+----------
+----------------------------------+ | Create Time | File
 Name | File Type | +--------------------+----------
+----------------------------------+ | 2017-03-01 22:28:24 |
 rmr.doc | Microsoft Word 97 - 2003 Document | +--------------------
+----------+-----------------------------------+ +----------
+----------+------------------+ | File Size | Malicious
 | Status | +----------+----------+------------------+ |
 133120 | Yes | analysis complete | +----------+----------
+------------------+ Analysis information: +--------------------
+--------------------+--------------------+-----------+ | Submit
 Time | Start Time | Finish Time | Malicious | +--------------------
+--------------------+--------------------+-----------+
 | 2017-03-01 22:28:24 | 2017-03-01 22:28:24 | 2017-03-01
 22:28:24 | Suspicious | | 2017-03-01 22:28:24 | 2017-03-01
 22:28:24 | 2017-03-01 22:34:07 | Yes | +--------------------
+--------------------+--------------------+-----------+
 +-------------------------------------------------------------
+----------+ | VM Image | Status |
 +-------------------------------------------------------------
+----------+ | DOC/CDF Static Analyzer | completed | | Windows
 7 x64 SP1, Adobe Reader 11, Flash 11, Office 2010 | completed
 | +-----------------------------------------------------------
+----------+ admin@WF-500> show wildfire local
 statistics Current Time:2017-03-01 17:44:31 Received
 After:2017-02-28 17:44:31 Received Before:2017-03-01 17:44:31
 ---------------------------------------------------------------------------------
 | Wildfire Stats |
 +-------------------------------------------------------------------------------
+ |
+---------------------------------------------------------------------------------
+| || Executable || |
+---------------------------------------------------------------------------------
+| || FileType | Submitted | Analyzed | Pending
 | Malware | Grayware | Benign | Error || |
+---------------------------------------------------------------------------------
+| || exe | 2 | 2 | 0 | 0 | 0 | 2 | 0 || |
+---------------------------------------------------------------------------------
+| || dll | 0 | 0 | 0 | 0 | 0 | 0 | 0 || |
+---------------------------------------------------------------------------------
+| Environment Analysis Summary for Executable:VM Utilization :0/10
 Files Analyzed :2
 +-------------------------------------------------------------------------------
+ || Non-Executable || |
+---------------------------------------------------------------------------------
+| || FileType | Submitted | Analyzed | Pending
 | Malware | Grayware | Benign | Error || |
+---------------------------------------------------------------------------------
+| || pdf | 0 | 0 | 0 | 0 | 0 | 0 | 0 || |
+---------------------------------------------------------------------------------
+| || jar | 0 | 0 | 0 | 0 | 0 | 0 | 0 || |
+---------------------------------------------------------------------------------
+| || doc | 1 | 1 | 0 | 1 | 0 | 0 | 0 || |
+---------------------------------------------------------------------------------
+| || ppt | 0 | 0 | 0 | 0 | 0 | 0 | 0 || |
+---------------------------------------------------------------------------------
```

```
+| || xls | 0 | 0 | 0 | 0 | 0 | 0 || |
+-------------------------------------------------------------------------------
+| || docx | 0 | 0 | 0 | 0 | 0 | 0 || |
+-------------------------------------------------------------------------------
+| || pptx | 0 | 0 | 0 | 0 | 0 | 0 || |
+-------------------------------------------------------------------------------
+| || xlsx | 0 | 0 | 0 | 0 | 0 | 0 || |
+-------------------------------------------------------------------------------
+| || rtf | 0 | 0 | 0 | 0 | 0 | 0 || |
+-------------------------------------------------------------------------------
+| || class | 2 | 2 | 0 | 1 | 0 | 1 | 0 || |
+-------------------------------------------------------------------------------
+| || swf | 1 | 1 | 0 | 0 | 0 | 1 | 0 || |
+-------------------------------------------------------------------------------
+| Environment Analysis Summary for Non-
Executable:VM Utilization :0/16 Files Analyzed :4
 +-------------------------------------------------------------------------------
+ || Links || |
+-------------------------------------------------------------------------------
+| || FileType | Submitted | Analyzed | Pending
 | Malware | Grayware | Benign | Error || |
+-------------------------------------------------------------------------------
+| || elink | 1 | 1 | 0 | 1 | 0 | 0 | 0 || |
+-------------------------------------------------------------------------------
+| Environment Analysis Summary for Links:Files Analyzed :1
 ------------------------------------------------------------ | General
 Stats | +-------------------------------------------------------------
+ Total Disk Usage:67/1283(GB) (5%) ||+--------------------------
+-----------+-+-----------+|| ||| Sample Queue ||| ||
+----------------+------------------+--------------+|| |||
 SUBMITTED | ANALYZED | PENDING ||| ||+--------------------------
+-----------+-+-----------+|| ||| 7 | 7 | 0 ||| ||
+---------------------------+----------+-+----------+||| |
+---------------------------+--------------------------+| |||
 Verdicts ||| ||+--------------------------+-------------------------
+|| ||| Malware | Grayware | Benign | Error ||| ||
+------------------------------+----------------------+|| ||| 3 | 0
 | 4 | 0 ||| ||+--------------------------+----------+-+----------
+||| |+---------------------------+--------------------------+|
 ||| Session and Upload Count ||| ||+--------------------------
+-------------------------+|| ||| Sessions | Uploads ||| ||
+---------------------------+-------------------------+|| ||| 7 | 5
 ||| ||+-------------------------+-------------------------+||
```

必要な権限レベル

superuser, superreader

test wildfire registration

説明

WildFire アプライアンスまたは Palo Alto Networks ファイアウォールの WildFire サーバーへの登録状態を確認するテストを実行します。テストに合格すると、WildFire サーバーの IP アド

レスまたはサーバー名が表示されます。WildFire アプライアンスまたはファイアウォールから WildFire サーバーにファイルを転送できるようにするには、正しく登録されている必要があります。

構文

```
test { wildfire { registration; } }
```

オプション

追加のオプションはありません。

サンプル出力

以下の出力は、ファイアウォールのテストが成功し、WildFire アプライアンスと通信できることを示しています。これが Palo Alto Networks WildFire クラウドを指す WildFire アプライアンスの場合、いずれかのクラウド サーバーのサーバー名が `select the best server:` フィールドに表示されます。

```
Testing wildfire Public Cloud wildfire registration: successful
 download server list: successful select the best server: ca-
s1.wildfire.paloaltonetworks.com
```

必要な権限レベル

superuser, superreader