paloalto TECHDOCS

WildFire 设备管理

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 设备概述

WildFire™ 通过结合动态和静态分析，提供对零天恶意软件的检测和预防，以监测威胁并创建保护，阻挡恶意软件。WildFire 将扩展 Palo Alto Networks 下一代防火墙的功能，以确定和阻止目标性和未知恶意软件。

关于 WildFire 设备

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

WildFire 设备提供了本地 WildFire 私有云，能够让您在沙盒环境中分析可疑文件，而无需防火墙将文件发送至网络之外。如需使用 WildFire 设备来托管 WildFire 专有云，请配置防火墙提交样本至 WildFire 设备进行分析。WildFire 设备将本地所有文件收集在沙盒中，并使用与 WildFire 公共云系统所用引擎相同的引擎来分析它们的可疑行为。数分钟内，专有云会将分析结果返回至防火墙 **WildFire Submissions (WildFire** 提交情况**)**日志。

WildFire 设备管理涵盖了 *WildFire* 设备的设置和配置，但与 *WildFire* 公共云共享许多操作设计和功能。有关 *WildFire* 分析功能的更多信息，请参阅高级 *WildFire* 管理。

您可以启用 WildFire 设备以便：

- ❑ 为发现的恶意软件本地生成防病毒软件和 DNS 签名，并分配一个 URL 类别至恶意链接。然后，您可以启用连接的防火墙每五分钟检索一次最新的签名和 URL 类别。
- ❑ 提交恶意软件至 WildFire 公共云。WildFire 公共云重新分析样本并生成签名来检测恶意软件—此签名可在数分钟内准备好以保护全球用户
- ❑ 提交本地生成的恶意软件报告（无需发送原始样本内容）至 WildFire 公共云，以便为恶意软件的统计信息和威胁情报作出贡献。

您可以使用有效的 WildFire 订阅配置多达 100 个 Palo Alto Networks 防火墙，以转发至单个 WildFire 设备。除了 WildFire 防火墙订阅之外，无需额外的 WildFire 订阅即可启用 WildFire 专有云部署。

您可以通过本地设备 CLI 管理 WildFire 设备，或您可以集中通过 Panorama 管理 WildFire 设备。从 PAN-OS 8.0.1 开始，您也可以将 WildFire 设备分组至 WildFire 设备集群并本地管理集群，或从 Panorama 进行管理。

WildFire 私有云

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

在 Palo Alto Networks 专有云部署中，Palo Alto Networks 防火墙会转发文件至用于托管专有云分析位置的企业网络上的 WildFire 设备。WildFire 专有云就可以接收和分析从 100 多个 Palo Alto Networks 防火墙转发的文件。

由于 WildFire 专有云是一个本地沙盒，它分析的良性软件、灰色软件和网络钓鱼样本从未离开您的网络。同时在默认条件下，此专有云也不会向您网络之外的其他环境发送已发现的恶意软件，但您可选择以自动方式将恶意软件转发至 WildFire 公共云，以生成和分发签名。在此情况下，WildFire 公共云会对样本进行重新分析，生成一个签名来识别样本，并将此签名分发至配备有威胁防范或 WildFire 许可证的所有 Palo Alto Networks 防火墙。

如果您不希望 WildFire 专有云将恶意样本转发到您的网络之外，您可以：

- 启用 WildFire 设备将恶意软件报告（并非样本自身）转发至 WildFire 公共云。WildFire 报告将提供一些统计信息，用以辅助 Palo Alto Networks 评估恶意软件的普遍性和传播程度。有关更多详细信息，请参阅从 WildFire 设备提交恶意软件或报告。
- 手动上传文件至 WildFire 门户而非自动转发所有恶意软件，或者使用 WildFire API 将文件提交至 WildFire 公共云。

您也可以在 WildFire 设备上启用生成本地签名和 URL 类别。WildFire 设备生成的签名会被分发至已连接的防火墙，以使防火墙能够在下一次检测到恶意软件时进行有效的阻止。

WildFire 专有云分析不支持 Android 应用程序包 (APK) 和 MAC OSX 文件。

WildFire 混合云

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

WildFire 混合云部署中的防火墙可以转发特定样本至 Palo Alto Networks 托管的 WildFire 公共云之一，并将其他样本转发至 WildFire 设备托管的 WildFire 专有云。借助 WildFire 混合云部署，可灵活选择在本地和网络内进行专有文档分析，同时通过 WildFire 公共云对来自互联网的文件进行分析。例如，仅向 WildFire 专有云转发支付卡行业 (PCI) 和受保护的健康信息 (PHI) 等数据，用以对其进行分析，同时将可移植可执行文件 (PE) 转发至 WildFire 公共云进行分析。在 WildFire 混合云部署中，将文件卸载至公共云进行分析可让您获得之前在 WildFire 公共云中处理的文件的快速判定结果，同时也能释放 WildFire 设备的容量，用以处理敏感内容。此外，您也可将 Android 应用程序包 (APK) 等特定的文件类型转发至当前尚不支持 WildFire 设备分析的 WildFire 公共云。

在 WildFire 混合云部署中，可能出现单个文件同时符合公共云分析和专有云分析的情况；这种情况下，为了谨慎起见，该文件仅被提交至专有云进行分析。

要设置混合云转发，请参见 转发文件进行 WildFire 设备分析。

WildFire 设备接口

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

WF-500 设备背面配有四个 RJ-45 以太网端口。这些端口带有 **MGT**、**1**、**2** 和 **3** 标记，并与特定接口对应。

WildFire 设备拥有三个接口：

- 管理 — 用于接收防火墙所转发的所有文件，并将结果的日志详细信息返回给防火墙。请参阅配置 WildFire 设备。
- 虚拟机接口（**VM** 接口）— 提供了对 WildFire 沙盒系统的网络访问权，以使样本文件能够与 Internet 通信，这将使 WildFire 能够更好地分析样本的行为。配置 VM 接口后，WildFire 可以观察恶意软件不访问网络通常就不会表现出来的恶意行为，如回拨活动。但为防止恶意软件从沙盒进入网络，需在隔离网络上通过 Internet 连接配置 VM 接口。您还可以启用 Tor 选项以对样本访问的恶意站点隐藏您公司使用的公共 IP 地址。有关 VM 接口的详细信息，请参见 设置 WildFire 设备虚拟机接口。
- 集群管理接口——提供 WildFire 设备节点之间，集群范围内的通讯，这些节点是 WildFire 设备集群的成员。此接口与防火墙操作的管理 (MGT) 接口不同。您可以配置以太网 2 几口或以太网 3 几口（分别标记为 **2** 和 **3**）作为集群管理接口。

从网络管理员获取在管理端口、虚拟机接口和集群管理接口（仅限 WildFire 设备集群）中配置网络连接所需的信息（IP 地址、子网掩码、网关、主机名、DNS 服务器）。防火墙与设备之间的所有通信都通过管理端口进行，包括文件提交、WildFire 日志传送和设备管理。因此，请确保防火墙能够连接到设备的管理端口。此外，必须能够将设备连接到 updates.paloaltonetworks.com 以检索其操作系统软件更新。

WildFire 设备文件类型支持

下表列出了支持在 WildFire 设备私有云中以及通过 WildFire 门户直接上传来进行分析的文件类型。

支持分析的文件类型	**WildFire** 专有云（**WildFire** 设备）	**WildFire** 门户 **| API**（直接上传；所有地区）
电子邮件中的链接	✓	✓
Android 应用程序包 (APK) 文件	✗	✓
Adobe Flash 文件	✓	✓
Java 压缩 (JAR) 文件	✓	✓
Microsoft Office 文件（包括 SLK 和 IQY 文件**）	✓	✓
可移植的可执行文件（包括 MSI 文件**）	✓	✓
可移植文档格式 (PDF) 文件	✓	✓
Mac OS X 文件	✗	✓
Linux（ELF 文件和 Shell 脚本）文件	✗	✓
存档（RAR、7-Zip、ZIP）文件*	✓	✓
脚本（BAT、JS、VBS、PS1 和 HTA）文件	✓	✓
脚本（Perl 和 Python）脚本	✗	✓

支持分析的文件类型	**WildFire** 专有云（**WildFire** 设备）	**WildFire** 门户	**API**（直接上传；所有地区）
存档（ZIP [直接上传] 和 ISO）文件*	✗	✓

* 不会将 ZIP 文件直接转发到 Wildfire 云进行分析。防火墙会先对其进行解码，然后单独转发与 WildFire 分析配置文件条件匹配的文件以进行分析。

** WildFire 设备不支持 MSI、IQY 和 SLK 文件分析。

设置和管理 WildFire 设备

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

WildFire™ 设备可配置为本地主机的 WildFire 专有云。以下主题将介绍如何准备 WildFire 设备来接收文件进行分析，如何管理该设备，以及如何启用该设备以在本地生成威胁签名和 URL 类别。

配置 WildFire 设备

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

本节主要介绍将 WildFire 设备集成至网络中并执行基本设置所需的步骤。

STEP 1 | 机架式安装 WildFire 设备并连接电缆。

有关说明，请参阅《WildFire 设备硬件参考指南》。

STEP 2 | 使用管理端口或控制台端口将一台计算机连接到设备并启动设备。

1. 连接到控制台端口或管理端口。这两个端口都位于设备的背面。
   - 控制台端口 — 这是一个 9 针串行连接器。在控制台应用程序中使用以下设置：9600-8-N-1。将所提供的电缆连接到管理计算机上的串行端口或 USB 到串行转换器。
   - 管理端口 — 这是一个以太网 RJ-45 端口。默认情况下，管理端口的 IP 地址为 192.168.1.1。管理计算机上的接口必须在与管理端口相同的子网中。例如，将管理计算机的 IP 地址设置为 192.168.1.5。
2. 启动设备。

   将电源连接到第一个电源装置后，设备会立即通电，并会发出警告的哔声，直至连接第二个电源装置。如果设备已插入且处于关机状态，可以使用设备前面的电源按钮启动。

STEP 3 | 注册 WildFire 设备。

1. 从设备上的 S/N 标签获取序列号，或运行以下命令并参阅 `serial` 字段：

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

2. 从浏览器中导航至 Palo Alto Networks 支持门户并登录。
3. 按下述步骤注册设备：
   - 如果这是您注册的第一台 Palo Alto Networks 设备，并且您尚未获得登录信息，请单击页面底部的 **Register**（注册）。

     要进行注册，请提供电子邮件地址和设备的序列号。收到提示时，设置用于访问 Palo Alto Networks 支持社区的用户名和密码。
   - 如果已有帐户，请先登录，然后单击 **My Devices**（我的设备）。向下滚动到屏幕底部的 **Register Device**（注册设备）部分，输入设备的序列号、城市和邮政编码，然后单击 **Register Device**（注册设备）。
4. 如需在 WildFire 设备上确认 WildFire 注册，请使用 SSH 客户端或通过使用控制台端口登录至该设备。在设备上输入用户名/密码：admin/admin，再输入以下命令：

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

下面的输出表明已将设备注册到其中一台 Palo Alto Networks WildFire 云服务器。

```
Test wildfire wildfire registration: successful download
 server list:  successful select the best server: cs-
s1.wildfire.paloaltonetworks.com
```

STEP 4 | 重置管理密码。

1. 通过运行以下命令设置新密码：

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

2. 键入旧密码，按 Enter 键，然后输入并确认新密码。提交配置以确保新密码在重启后保存。

   从 *PAN-OS 9.0.4* 开始，在首次登录到设备时，必须更改预定义的默认管理员密码 *(admin/admin)*。新密码至少包含 *8* 个字符，其中至少 *1* 个小写字母和 *1* 个大写字母以及 *1* 个数字或特殊字符。

   请务必使用密码强度最佳实践确保密码的强度。
3. 键入 **exit** 以注销，然后重新登录以确认设置的新密码。

STEP 5 | 配置管理接口设置。

本示例中使用了以下 IPv4 的值，但设备同样支持 IPv6 地址：

- IPv4 地址 - 10.10.0.5/22
- 子网掩码 - 255.255.252.0
- 默认网关 - 10.10.0.1
- 主机名-wildfire-corp1
- DNS 服务器 - 10.0.0.246

1. 使用 SSH 客户端或通过使用控制台端口登录到设备，然后进入配置模式：

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

2. 设置 IP 信息：

```
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
```

通过在上述命令中使用辅助服务器替换主服务器来配置辅助 *DNS* 服务器，不包括其他 *IP* 参数。例如：

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

3. 设置主机名（在本示例中为 wildfire-corp1）：

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

4. 提交配置以激活新的管理 (MGT) 端口的配置：

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

5. 将管理接口端口连接到网络交换机。
6. 在公司网络或要求访问管理网络上设备的任何网络中还原管理计算机。
7. 从管理计算机中，使用 SSH 客户端连接到新的 IP 地址或分配给设备管理端口的主机名。在本示例中，IP 地址为 10.10.0.5。

STEP 6 | 使用从 Palo Alto Networks 收到的 WildFire 授权代码激活设备。

即使 *WildFire* 设备无需身份验证代码即可工作，但若无有效的身份验证代码则不能检索软件更新。

1. 更改为操作模式：

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

2. 获取并安装 WildFire 许可证：

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

3. 验证许可证：

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

将显示有关支持站点和支持合同日期的信息。请确认显示的日期是否有效。

STEP 7 | 设置 WildFire 设备时钟。

有两种方法可进行设置。您可以手动设置日期、时间和时区，或者您可以配置 WildFire 设备以与 Network Time Protocol (NTP) 服务器同步其本地时钟。

- 要手动设置时钟，请输入以下命令：

```
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>
```

出现在 *WildFire* 详细报告中的时间戳将使用在设备上设置的时区。如果各区域的管理员都会查看报告，请考虑将时区设置为 *UTC*。

- 要配置 WildFire 设备与 NTP 服务器同步，请输入下列命令：

```
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 设备不会优先主 *NTP* 服务器或辅助 *NTP* 服务器，而会与其中之一同步。

STEP 8 | （NTP 配置可选）设置 NTP 验证。

- 禁用 NTP 身份验证：

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

- 使用对称式密钥交换（共享密钥）对 NTP 服务器的时间更新进行身份验证：

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

  继续输入 **key-ID** (1 - 65534)，选择要在 NTP 身份验证（**MD5** 或 **SHA1**）中使用的算法，然后输入并确认身份验证算法 **authentication-key**。

- 使用自动密钥（公钥加密）对 NTP 服务器的时间更新进行身份验证：

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

STEP 9 | 选择设备分析文件使用的虚拟机映像。

此映像应基于能最准确代表最终用户计算机上所装软件的属性。每个虚拟映像都包含不同版本的操作系统和软件，如 Windows XP 或 Windows 7 32 位（或 64 位）、特定版本的 Adobe Reader 和 Flash。尽管可将设备配置为使用一个虚拟机映像配置，但设备会使用映像的多个实例来提高性能。

- 查看可用虚拟机的列表以确定最能代表所用环境的虚拟机映像：

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

- 运行以下命令查看当前虚拟机映像，并参阅 `Selected VM`（所选 VM）字段：

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

- 选择设备用于分析的映像：

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

  例如，使用 vm-5:

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

STEP 10 | 启用 WildFire 设备来观察所分析文件尝试访问网络时表现的恶意行为。

设置 WildFire 设备虚拟机接口。

STEP 11 | #unique_16

STEP 12 | （可选）启用 WildFire 设备执行快速判定查找并将判定与 WildFire 公共云同步。

下列 CLI 命令会启用 WildFire 设备执行判定查找并将判定与 WildFire 公共云同步。此功能默认为禁用；设置此命令为 **yes** 以启用此功能。

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

STEP 13 | （可选）启用 WildFire 设备以获得 Palo Alto Networks 每日内容更新，以促进和改善恶意软件分析。

启用 WildFire 设备分析功能

STEP 14 | （可选）启用 WildFire 设备 以生成 DNS 和防病毒软件签名和 URL 类别，并分配新的签名和 URL 类别至连接的防火墙。

启用生成本地签名和 URL 类别

STEP 15 | （可选）自动将 WildFire 专有云发现的恶意软件提交至 WildFire 公有云，以支持对恶意软件的全球保护。

提交恶意软件至 WildFire 公共云。

STEP 16 | （可选）或者，如果您不希望将恶意软件样本转发至 WildFire 专有云之外，您也可选择将 WildFire 分析报告提交至 WildFire 公共云。

如果您不希望将本地发现的将恶意软件提交至 *WildFire* 公共云，则可采用的最佳方案是启用恶意软件分析报告提交功能，以加强或改善 *WildFire* 威胁情报服务。

提交分析报告至 WildFire 公共云。

STEP 17 | （可选）允许其他用户管理 WildFire 设备。

可以分配两个角色类型：超级用户和超级读者。超级用户相当于管理帐户，超级读者仅拥有读权限。

在本示例中，将为用户 bsimpson 创建一个超级读者帐户：

1. 进入配置模式：

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

2. 创建用户帐户：

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

3. 输入并确认新密码。
4. 分配超级读者角色：

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

STEP 18 | 针对管理员访问配置 RADIUS 身份验证。

1. 使用以下选项创建 RADIUS 配置文件：

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

（配置 RADIUS 服务器和其他属性。）

2. 创建身份验证配置文件：

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

3. 将配置文件分配给本地管理帐户：

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

转发文件进行 WildFire 设备分析

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

配置 Palo Alto Networks 防火墙以转发未知文件或电子邮件链接，并阻挡匹配现有防病毒签名的文件以进行分析。使用 **WildFire Analysis**（**WildFire** 分析）配置文件，定义将转发至 WildFire 私有云（或者，也可以是混合云部署的公共云），然后将配置文件附加至安全规则，以便触发针对零日恶意软件进行的检查。

根据使用中的应用程序、检测到的文件类型、电子邮件消息中包含的链接，或样本传输方向（上传、下载或二者皆有），指定待转发进行分析的流量。例如，您可设置防火墙以转发可移植可执行文件 (PE)，或用户在 Web 浏览会话期间尝试下载的任何文件。除了未知样本外，防火墙还转发匹配现有防病毒前面的已阻挡文件。这为 Palo Alto Networks 提供了威胁情报的有价值来源，其基于前面成功阻止的恶意软件变量，但 WildFire 或防火墙之前均未见过此恶意软件。

通过配置防火墙，继续将敏感文件转发到您的 WildFire 私有云来进行本地分析，并将不太敏感或不受支持的文件类型转发到 WildFire 公共云，您可以将 WildFire 分析资源扩展到 WildFire 混合云。

此外，您可以将 WildFire 设备资源专用于分析特定文件类型：可以是文档（Microsoft Office 文件和 PDF）或可移植可执行文件。例如，部署 WildFire 混合云 来分析本地文件以及某一 WildFire 公共云中的可移植可执行文件时，您可以将所有分析环境专门用于文档分析。这样您可以离线分析公共云可移植可执行文件，让您可以将额外的 WildFire 设备资源分配用于处理敏感文档。

准备工作：

- ❑ 如果在您正配置进行文件转发的防火墙与 WildFire 云或 WildFire 设备之间存在其他防火墙，请确保处于中间位置的防火墙可允许以下端口进行的操作：

端口	使用情况
443	• 注册 • PCAP 下载 • 样本下载 • 报告检索 • 文件提交 • PDF 报告下载
10443	动态更新

STEP 1 | （仅适用于 PA-7000 系列防火墙）如需启用 PA-7000 系列防火墙，以转发样本进行 WildFire 分析，则您必须首先将 NPC 上的数据端口配置为日志卡接口。如果您的 PA-7000 系列设备配备了 LFC（日志转发卡），则必须配置 LFC 使用的端口。配置后，在转发 WildFire 样本时，日志卡端口或 LFC 接口优先于管理端口。

STEP 2 | 指定要将示例转发到的 WildFire 私有云或混合云。

选择 **Device**（设备） > **Setup**（设置） > **WildFire** 并根据 WildFire 云部署（私有或混合）编辑常规设置。

WildFire 专有云：

1. 在 **WildFire Private Cloud**（**WildFire** 专有云）字段输入 WildFire 设备的 IP 地址或 FQDN。

WildFire 混合云：

1. 输入 **WildFire Public Cloud**（**WildFire** 公共云） URL：
   - 美国：**wildfire.paloaltonetworks.com**
   - 欧洲：**eu.wildfire.paloaltonetworks.com**
   - 日本：**jp.wildfire.paloaltonetworks.com**
   - 新加坡：**sg.wildfire.paloaltonetworks.com**
   - 英国：**uk.wildfire.paloaltonetworks.com**
   - 加拿大：**ca.wildfire.paloaltonetworks.com**
   - 澳大利亚：**au.wildfire.paloaltonetworks.com**
   - 德国：**de.wildfire.paloaltonetworks.com**
   - 印度：**in.wildfire.paloaltonetworks.com**
   - 瑞士：**ch.wildfire.paloaltonetworks.com**
   - 波兰：**pl.wildfire.paloaltonetworks.com**
   - 印度尼西亚：**id.wildfire.paloaltonetworks.com**
   - 中国台湾：**tw.wildfire.paloaltonetworks.com**
   - 法国：**fr.wildfire.paloaltonetworks.com**
   - 卡塔尔：**qatar.wildfire.paloaltonetworks.com**
   - 韩国：**kr.wildfire.paloaltonetworks.com**
   - 以色列：**il.wildfire.paloaltonetworks.com**
   - 沙特阿拉伯：**sa.wildfire.paloaltonetworks.com**
   - 西班牙：**es.wildfire.paloaltonetworks.com**
2. 在 **WildFire Private Cloud**（**WildFire** 专有云）字段输入 WildFire 设备的 IP 地址或 FQDN。

STEP 3 | 定义防火墙转发和配置 WildFire 日志记录和报告设置的文件大小限制。

继续编辑 WildFire 常规设置（**Device**（设备） > **Setup**（设置） > **WildFire**）。

- 查看从防火墙转发文件的 **File Size Limits**（文件大小限制）。

  建议的 WildFire 最佳措施是将 *PE* 的 ***File Size***（文件大小）限制设置为最大 *10 MB*，将其他所有文件类型 ***File Size***（文件大小）限制保留默认值。

- 选择 **Report Benign Files**（报告良性文件），以对收到 WildFire 良性判定结果的文件进行记录。
- 选择 **Report Grayware Files**（报告灰色软件文件），以对收到 WildFire 灰色软件判定结果的文件进行记录。
- 通过编辑会话信息设置，定义 WildFire 分析报告中记录的会话信息。在默认情况下，所有会话信息均将显示在 WildFire 分析报告中。取消选中复选框，以从 WildFire 分析报告中删除相应的字段，然后单击 **OK**（确认）保存设置。

STEP 4 | （仅限 Panorama）配置 Panorama 以收集从防火墙上的来的样本信息，该防火墙在运行 PAN-OS 7.0 之前运行的是 PAN-OS 版本。

对于运行更早软件版本的防火墙提交的样本，PAN-OS 7.0 中推出的某些 WildFire Submissions（WildFire 提交情况）日志字段不填充。如果您正在使用 Panorama 管理运行软件版本早于 PAN-OS 7.0 的防火墙，则 Panorama 可与 WildFire 通信，以便为这些来自定义的 **WildFire Server**（**WildFire** 服务器）的防火墙提交的样本收集完整分析信息，以完整日志详情。

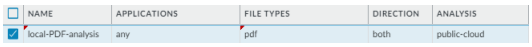
如果您希望修改默认设置，允许 Panorama 从指定的 WildFire 云或者从 WildFire 设备收集详细信息，请选择**Panorama** > **Setup**（设置） > **WildFire** 并输入一台 **WildFire Server**（**WildFire** 服务器）。

STEP 5 | 定义待转发进行 WildFire 分析的流量。

如果您已配备 *WildFire* 设备设置，则您可在混合云部署中使用专有云和公共云。在您的网络上对敏感文件进行本地分析，同时将其他所有未知文件发送至 *WildFire* 公共云，以进行全面分析并即时返回判定结果。

1. 选择 **Objects**（对象） > **Security Profiles**（安全性配置文件） > **WildFire Analysis**（**WildFire** 分析），**Add**（添加） 新的 WildFire 分析配置文件，再为其输入描述性 **Name**（名称）。
2. **Add**（添加）配置文件规则，以定义待转发进行分析的流量，然后再为此规则输入描述性**Name**（名称），如 local-PDF-analysis。
3. 定义配置文件规则，以匹配未知流量并根据以下几个方面进行样本转发：
   - **Applications**（应用程序） — 根据正在使用的应用程序，转发文件进行分析。
   - **File Types**（文件类型） — 根据文件类型来转发文件进行分析，包括在电子邮件消息中包含的链接。例如，选择 **PDF** ，即可转发防火墙检测到的未知 PDF 进行分析。
   - **Direction**（方向） — 根据文件传输方向（上传、下载或二者皆有），转发文件进行分析。例如，选择 **both**（皆有），即可转发所有未知 PDF 进行分析，不论其传输方向如何。
4. 设置防火墙将与规则相匹配的文件转发的目的**Analysis**（分析）位置。
   - 选择**public-cloud**（公共云），以将匹配的样本转发至 WildFire 公共云进行分析。
   - 选择**private-cloud**（专有云），以将匹配的样本转发至 WildFire 专有云进行分析。

     例如，如需分析可能含有敏感或专有信息的 PDF，而不将此类文档发送至您的网络之外，请将 local-PDF-analysis 规则的**Analysis**（分析）位置设置为**private-cloud**（专有云）。



不同规则可将匹配的样本转发至不同分析位置，具体取决于您的需求。上述样本显示一种规则，它将敏感文件类型转发至 *WildFire* 专有云以进行本地分析。您可以创建另一种规则，将敏感度较低的文件类型（比如 *PE*）转发至 *WildFire* 公共云。此灵活性由 WildFire 混合云部署提供支持。

在混合云部署中，与 ***private-cloud***（专有云）和 ***public-cloud***（公共云）规则相匹配的文件将仅被转发至专有云，以作警示。

5. （可选）必要时，继续添加规则至 WildFire 分析配置文件。例如，您可向此配置文件添加第二项规则，以将 Android 应用程序包 (APK)、可移植可执行文件 (PE) 和 Flash 文件转发至 WildFire 公共云进行分析。
6. 单击 **OK**（确定）以保存 WildFire 分析配置文件。
7. （可选）必要时，继续添加规则至 WildFire 分析配置文件。例如，您可向此配置文件添加第二项规则，以将 Android 应用程序包 (APK)、可移植可执行文件 (PE) 和 Flash 文件转发至 WildFire 公共云进行分析。

8. 单击 **OK**（确定）以保存 WildFire 分析配置文件。

STEP 6 | （可选）分配 WildFire 设备资源分析文档或可执行文件。

如果您正在部署混合云以分析本地和 *WildFire* 公共云中的特定文件类型，您可以将分析环境专用于处理一种文件类型。这样您可以更好地根据您的分析环境配置分配资源。如果您不需要将资源专用于某种分析环境，则通过默认设置分配资源。

使用以下 CLI 命令：

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

并从以下选项中选择：

- 文件 — 将分析资源专用于同时分析 25 个文档、1 个可移植可执行文件和 2 个电子邮件链接。
- 可执行文件 — 将分析资源专用于同时分析 25 个可移植可执行文件、1 个文档和 2 个电子邮件链接。
- 默认 — 设备同时分析 16 个文档、10 个可移植可执行文件和 2 个电子邮件链接。

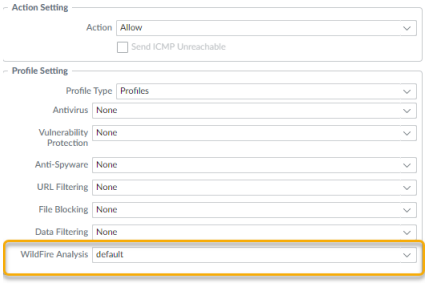
确认所有 WildFire 设备程序通过下列命令运行：

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

STEP 7 | 将 WildFire 分析配置文件附加至安全策略规则。

安全策略规则允许的流量将根据附加的 WildFire 分析配置文件予以评估，防火墙将转发与该配置文件相匹配的流量来进行 WildFire 分析。

1. 选择 **Policies**（策略） > **Security**（安全性），然后**Add** （添加） 或修改策略规则。
2. 单击策略规则中的 **Actions**（操作）选项卡。
3. 在 Profile Settings（配置文件设置）部分中，选择作为 **Profile Type**（配置文件类型）的 **Profiles**（配置文件），然后选择 **WildFire Analysis**（**WildFire** 分析）配置文件以附加至策略规则



STEP 8 | 确保启用防火墙以同时转发解密后的 SSL 通信进行 WildFire 分析。

这是建议的 WildFire 最佳措施。

STEP 9 | 查看并执行 WildFire 最佳措施。

STEP 10 | 单击 **Commit**（提交）应用设置。

STEP 11 | （可选）验证 WildFire 提交。

STEP 12 | 选择下一步...

- 验证 WildFire 提交情况，确认防火墙是否已成功转发文件进行 WildFire 分析。
- 从 WildFire 设备提交恶意软件或报告启用此功能以将 WildFire 专有云中识别的恶意软件转发至 WildFire 公共云。随后，WildFire 公共云会重新分析此样本，然后在确定此样本为恶意软件时生成一个签名。该签名将通过 Wildfire 签名更新分发至全球的用户。
- 监控 WildFire 设备活动 评估针对恶意软件报告的警报和详细信息。

从 WildFire 设备提交恶意软件或报告

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

启用 WildFire 设备的云智能功能，即可将 WildFire 专有云中发现的恶意软件样本自动提交至 WildFire 公共云。随即，WildFire 公共云将对恶意软件进行进一步分析并生成可用于识别样本的签名。之后，签名会被添加至 WildFire 签名更新，然后分发给全球的用户，以免日后再受此威胁的影响。或者，如果您不希望将恶意软件样本转发至您的网络之外，您也可选择仅提交 WildFire 对在您网络上发现的恶意软件给出的报告，以此为 WildFire 统计分析和威胁情报提供信息。

提交恶意软件至 WildFire 公共云

从 WildFire 设备执行以下 CLI 命令，即可使该设备自动提交恶意软件样本至 WildFire 公共云：

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

如果原本提交样本进行 *WildFire* 专有云分析的防火墙已启用数据包捕获 *(PCAP)*，则针对恶意软件的 *PCAP* 也可转发至 *WildFire* 公共云。

提交恶意软件报告至 WildFire 公共云

如果已启用 *WWildFire* 设备来提交恶意软件至 WildFire 公共云，则您无需再启用该设备以向公共云提交报告。当恶意软件被提交至 *WildFire* 公共云时，公共云将针对相关样本生成一份新的恶意软件报告。

要让 WildFire 设备能自动向 WildFire 公共云提交恶意软件报告（而非恶意软件样本），请在 WildFire 设备上执行以下 CLI 命令：

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

验证云智能设置

如需确认是否已启用云智能将恶意软件或恶意软件报告提交至 WildFire 公共云，请运行以下命令：

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

请参考提交示例和提交报告字段。

在独立 WildFire 设备上使用自定义证书设置身份验证

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

默认情况下，WildFire 设备使用预定义证书进行相互身份验证，以建立用于管理访问和设备间通信的 SSL 连接。但是，您可以使用自定义证书配置身份验证。自定义证书允许您建立唯一的信任链，以确保您的 WildFire 设备和防火墙或 Panorama 之间的相互身份验证。您可以在 Panorama 或防火墙上本地生成这些证书，从受信任的第三方证书颁发机构 (CA) 获取，或是从企业私钥基础设施 (PKI) 获取。

以下主题是介绍如何配置不受 Panorama 管理的独立 WildFire 设备。要为 Panorama 管理的 WildFire 设备和 WildFire 集群配置自定义证书，请参阅 《Panorama 管理员指南》 。

- WildFire 设备相互 SSL 身份验证
- 在 WildFire 设备上使用自定义证书配置身份验证

WildFire 设备相互 SSL 身份验证

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

当防火墙或 Panorama 向 WildFire 设备发送样本进行分析时，防火墙充当客户端，而 WildFire 则充当服务器。要实现相互身份验证，每台设备都应提供一个证书，向其他设备标识自己。

要在部署中部署用于相互身份验证的自定义证书，您需要：

- **SSL/TLS** 服务配置文件 — SSL/TLS 服务配置文件通过引用您的自定义证书并建立服务器设备用于与客户端设备通信所使用的 SSL/TLS 协议版本来定义连接的安全性。
- 服务器证书和配置文件—WildFire 设备需要证书和证书配置文件向其他设备标识自己。您可以从企业公钥基础结构 (PKI) 部署此证书，从受信任的第三方 CA 购买证书或在本地生成自签名证书。服务器证书必须在证书通用名 (CN) 或主题备用名称中包含 WildFire 设备管理接口的 IP 地址或 FQDN。防火墙与服务器针对 WildFire 设备的 IP 地址或 FQDN 提供的证书中的 CN 或主题备用名称相匹配，以 WildFire 设备的身份。

  另外，可使用证书配置文件定义 证书撤销状态 (OCSP/CRL)，并根据撤销状态采取操作。

- 客户端证书和配置文件 — 每个防火墙都需要客户端证书和证书配置文件。客户端设备使用其证书向服务器设备标识自己。您可以使用简单证书注册协议 (SCEP)，从受信任的第三方 CA 购买证书或在本地生成自签名证书，从企业 PKI 部署证书。

  自定义证书对于每个客户端设备可以是唯一的，或者在所有设备上通用。唯一的设备证书使用受管设备和 CN 的序列号的散列。服务器会将 CN 或主题备用名称与客户端设备的已配置序列号进行匹配。对于基于 CN 发生的客户端证书验证，必须将用户名设置为主题通用名。

在 WildFire 设备上使用自定义证书配置身份验证

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

使用以下工作流程将您的 WildFire 部署中的预定义证书替换为自定义证书。当防火墙或 Panorama 向 WildFire 设备发送样本进行分析时，防火墙充当客户端，而 WildFire 则充当服务器。

STEP 1 | 获取密钥对和证书颁发机构 (CA) 颁发的用于 WildFire 设备、和防火墙或 Panorama 的证书。

STEP 2 | 导入 CA 证书以验证防火墙证书。

1. 登录到 WildFire 设备上的 CLI，并进入配置模式。

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

2. 使用 TFTP 或 SCP 导入证书。

```
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 | 使用 TFTP 或 SCP 导入包含用于 WildFire 设备的服务器证书和私钥的密钥对。

```
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 | 配置包含根 CA 和中间 CA 的证书配置文件。该证书配置文件定义 WildFire 设备和防火墙将相互进行身份验证的方式。

1. 登录到 WildFire 设备上的 CLI，并进入配置模式。

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

2. 命名证书配置文件。

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

3. 配置 CA。

   命令 *default-ocsp-url* 和 *ocsp-verify-cert* 是可选的。

```
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 | 配置用于 WildFire 设备的 SSL/TLS 配置文件。该配置文件定义 WildFire 设备和防火墙用于 SSL/TLS 服务的证书和 SSL/TLS 协议范围。

1. 标识 SSL/TLS 配置文件。

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

2. 选择证书。

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

3. 定义 SSL/TLS 范围。

   PAN-OS 8.0 或以上版本仅支持 *TLS1.2* 和更高版本的 *TLS* 版本。您必须将最高版本设置为 *TLS1.2* 或更高版本。

```
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 | 在 WildFire 设备上配置安全服务器通信。

1. 设置 SSL/TLS 配置文件。该 SSL/TLS 服务配置文件适用于 WildFire 和客户端设备之间的所有 SSL 连接。

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

2. 设置证书配置文件。

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

设置 WildFire 设备虚拟机接口

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

虚拟机接口（vm 接口）用于提供源自 WildFire 设备中沙盒虚拟机的外部网络连接，以便观察所分析文件尝试网络访问所表现的恶意行为。以下各节介绍 VM 接口及其配置所需的步骤。您可以通过 VM 接口选择启用 Tor 功能，这将掩盖通过 VM 接口从 WildFire 设备发送的任何恶意流量，以便流量可能被发送到的恶意软件站点无法检测您的公开 IP 地址。

此外，本节还介绍将 VM 接口连接到 Palo Alto Networks 防火墙上的专用端口以启用 Internet 连接所需的步骤。

- 虚拟机接口概述
- 在 WildFire 设备上配置 VM 接口
- 连接防火墙至 WildFire 设备 VM 接口

虚拟机接口概述

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

VM 接口（在设备背面标记为 **1**）供 WildFire 用于改善恶意软件检测功能。此接口可让在 WildFire 虚拟机上运行的文件样本与 Internet 进行通信，使 WildFire 设备能够更好地分析样本文件的行为，以确定它是否展现出恶意软件的特征。

- 尽管我们建议启用 *VM* 接口，但不将接口连接到允许访问任何服务器/主机的网络也很重要，因为在 *WildFire* 虚拟机中运行的恶意软件可能会使用此接口自行传播。
- 此连接可以是专用的 *DSL* 线路，或者是仅允许从 *VM* 接口直接访问 *Internet* 和严格限制访问任何内部服务器/客户端主机的网络连接。
- 如果您的 *WildFire* 设备以 *FIPS/CC* 模式运行，则会禁用 *vm-interface*。

下图显示了用于将 VM 接口连接到网络的两个选项。

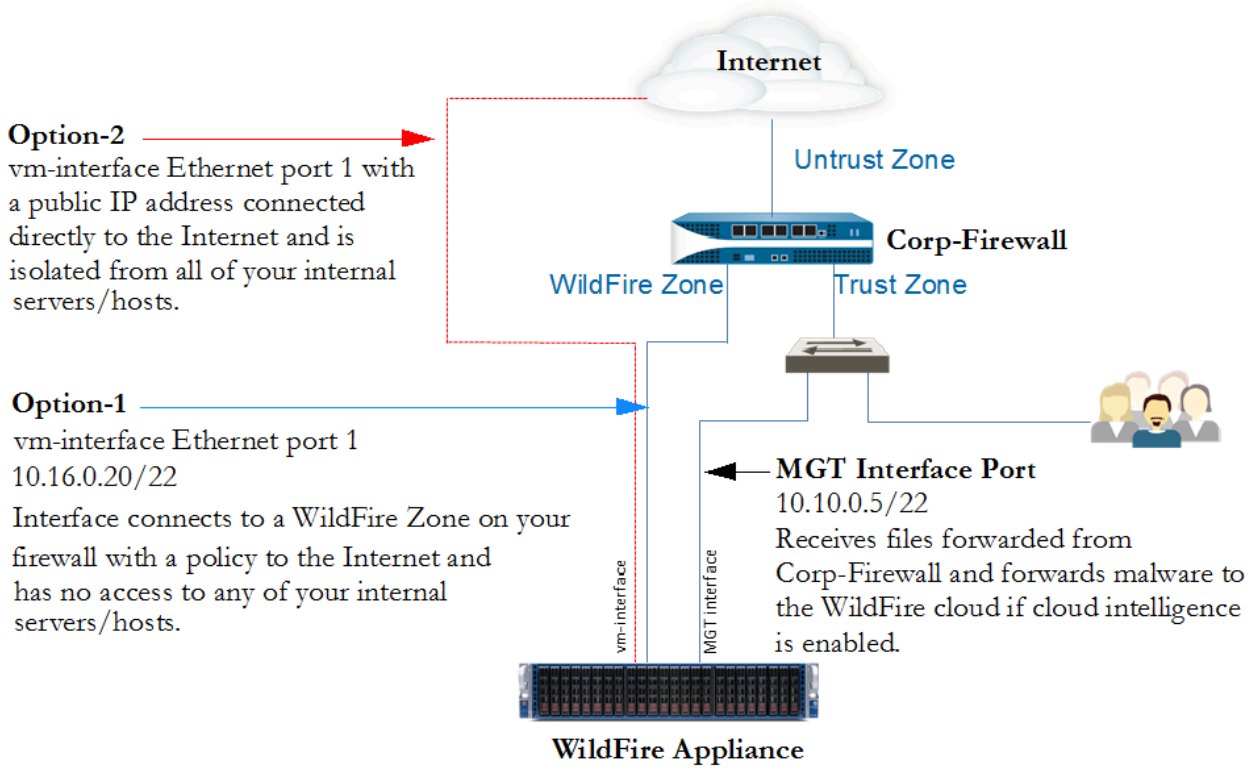


图 **1:** 虚拟机接口示例

- 选项 **1**（建议）— 将 VM 接口连接到其策略仅允许访问 Internet 的防火墙上专用区域的接口。此接口非常重要，因为在 WildFire 虚拟机上运行的恶意软件可能会使用它来自行传播。该选项是推荐选项，因为防火墙日志将提供通过 VM 接口所生成的所有流量的可见性。
- 选项 **2** — 使用专用 Internet 服务提供商连接（如 DSL 连接）将 VM 接口连接到 Internet。确保无法从此连接访问内部服务器/主机。尽管这是一个简单的解决方案，但不会记录通过 VM 接口以外的恶意软件所生成的流量，除非在 WildFire 设备与 DSL 连接之间放置防火墙或流量监控工具。

在 WildFire 设备上配置 VM 接口

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

本节介绍在 WildFire 设备上使用虚拟机接口示例中介绍的选项 1 配置来配置 VM 接口所需的步骤。在使用此选项配置 VM 接口后，还必须配置从 VM 接口路由流量所使用的 Palo Alto Networks 防火墙接口，如连接防火墙至 WildFire 设备 VM 接口所述。

默认情况下，VM 接口具有以下设置：

- IP 地址：192.168.2.1
- 网络掩码：255.255.255.0
- 默认网关：192.168.2.254
- DNS：192.168.2.254

如果想要启用该接口，请使用网络的相应设置来进行配置。如果不想使用该接口，请保留默认设置。注意，此接口必须配置网络值，否则提交将失败。

STEP 1 | 设置 WildFire 设备上 VM 接口的 IP 信息。本示例中使用了以下 IPv4 值，但设备同样支持 IPv6 地址：

- IP address - 10.16.0.20/22
- 子网掩码 - 255.255.252.0
- 默认网关 - 10.16.0.1
- DNS 服务器 - 10.0.0.246

VM 接口与管理接口 *(MGT)* 不能在相同的网络中。

1. 进入配置模式：

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

2. 设置 VM 接口的 IP 信息：

```
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
```

只能对此 *VM* 接口配置一个 *DNS* 服务器。作为最佳做法，使用 *ISP* 中的 *DNS* 服务器或开放 *DNS* 服务。

STEP 2 | 启用 VM 接口。

1. 启用 VM 接口：

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

2. 提交配置：

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

STEP 3 | 测试 VM 接口连接。

Ping 系统，然后指定 VM 接口作为源接口。例如，如果 VM 接口 IP 地址为 10.16.0.20，则运行以下命令，其中 *ip-or-hostname* 是启用 Ping 的服务器/网络的 IP 或主机名：

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

例如：

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

STEP 4 | （可选）将恶意软件生成的任何恶意流量发送至 Internet。Tor 网络掩盖您的面向公共的 IP 地址，以便恶意站点所有者无法确定流量的来源。

1. 启用 Tor 网络：

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

2. 提交配置：

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

STEP 5 | （可选）验证 Tor 网络是否启用且正常运行。

1. 发出以下 CLI 命令以在设备日志中搜索 Tor 事件 ID。正确配置和操作的 WildFire 设备应不会生成任何事件 ID：
   - **admin@WF-500(active-controller)>showlog system direction equal backward | match anonymous-network-unhealthy**—Tor 服务已关闭或无法运行。考虑重新启动 Tor 服务，并验证其是否运行正常。
   - **admin@WF-500(active-controller)>show log systemdirection equal backward | match anonymous-network-unavailable**—Tor 服务运行正常，但无法连接 WildFire 设备的 VM 接口。验证您的网络连接和设置，并重新测试。

STEP 6 | 连接防火墙至 WildFire 设备 VM 接口。

连接防火墙至 WildFire 设备 VM 接口

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

以下工作流示例介绍了如何将 VM 接口连接到 Palo Alto Networks 防火墙上的端口。在将 VM 接口连接到防火墙之前，必须已将防火墙的不信任区域连接到 Internet。在本示例中，已配置名为 wf-vm-zone 的新区域，其中包含用于将设备的 VM 接口连接到防火墙的接口。与 wf-vm-zone 相关的策略将只允许从 VM 接口到不信任区域的通信。

STEP 1 | 配置 VM 接口将要连接的防火墙上的接口，并设置虚拟路由器。

wf-vm-zone 只能包含用于将设备的 *VM* 接口连接到防火墙的接口（在本示例中为 *ethernet1/3*）。执行此操作旨在避免让恶意软件生成的任何流量进入其他网络。

1. 从防火墙的 Web 界面中，选择 **Network**（网络）> **Interfaces**（界面），然后选择接口（如 **Ethernet1/3**（以太网 **1/3**））。
2. 在 **Interface Type**（接口类型）下拉列表中，选择 **Layer3**（第 **3** 层）。
3. 在 **Config**（配置）选项卡上，从 **Security Zone**（安全区域）下拉框中选择 **New Zone**（新建区域）。
4. 在“区域”对话框的 **Name**（名称）字段中，输入 wf-vm-zone，然后单击 **OK**（确定）。
5. 在 **Virtual Router**（虚拟路由器）下拉框中，选择 **default**（默认）。
6. 若要为接口分配 IP 地址，请选择 **IPv4** 或 **IPv6** 选项卡，单击 IP 部分中的 **Add**（添加），然后输入要分配给接口的 IP 地址和网络掩码，如 10.16.0.0/22 (IPv4) 或 2001:db8:123:1::1/64 (IPv6)。
7. 要保存接口配置，请单击 **OK**（确定）。

STEP 2 | 在防火墙中创建安全策略以允许从 VM 接口访问 Internet，并阻止所有传入流量。在本示例中，策略名称为 WildFire VM Interface。因为您不会创建从不信任区域到 wf-vm-interface 区域的安全策略，因此默认情况下已阻止所有入站流量。

1. 选择 **Policies**（策略）> **Security**（安全），并单击 **Add**（添加）。
2. 在 **General**（常规）选项卡中，输入 **Name**（名称）。
3. 在源选项卡中，将源区域设置为 **wf-vm-zone**。
4. 在 **Destination**（目标）选项卡中，将 **Destination Zone**（目标区域）设置为 **Untrust**（不信任）。
5. 在**Application**（应用程序）和**Service/URL Category**（服务/**URL** 类别）选项卡中，保留默认值为**Any**（任何）。
6. 在 **Actions**（操作）选项卡中，将 **Action Setting**（操作设置）设置为 **Allow**（允许）。
7. 在 **Log Setting**（日志设置）下，选中 **Log at Session End**（会话结束日志）复选框。

如果担心有人可能会在无意中将其他接口添加到 *wf-vm-zone*，则克隆 *WildFire VM Interface* 安全策略，然后在所克隆规则的***Action***（操作）选项卡中选择***Deny***（拒绝）。确保已在 *WildFire VM Interface* 策略的下方列出此新的安全策略。此策略将覆盖隐式区域内允许规则（允许在同一区域中两个接口之间通信），并将拒绝/阻止所有区域内通信。

STEP 3 | 连接电缆。

使用直通 RJ-45 电缆将 WildFire 设备上的 VM 接口物理连接到在防火墙上配置的端口（在本示例中为 Ethernet 1/3）。VM 接口在设备的背面标记为 **1**。

启用 WildFire 设备分析功能

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

- 设置 WildFire 设备内容更新
- 启用生成本地签名和 URL 类别
- 提交本地发现的恶意软件或报告至 WildFire 公共云

设置 WildFire 设备内容更新

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

配置 WildFire 设备的日常内容更新WildFire 内容更新功能可为该设备提供威胁情报，以便于准确地检测到恶意软件，提升设备区分恶意样本和良性样本的能力，从而确保设备拥有生成签名所需的最新信息。

- 直接从更新服务器安装 WildFire 内容更新
- 从启用 SCP 的服务器安装 WildFire 内容更新

直接从更新服务器安装 **WildFire** 内容更新

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

STEP 1 | 验证从设备到更新服务器的连接，并确定要安装的内容更新。

1. 登录到 WildFire 设备，并运行以下命令以显示当前内容版本：

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

2. 确认设备可与 Palo Alto Networks 更新服务器通信，并查看可用更新：

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

此命令会查询 Palo Alto Networks 更新服务器，提供有关可用更新的信息，并确定设备当前已安装的版本。

```
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
```

如果设备无法连接到更新服务器，则需要允许从设备到 Palo Alto Networks (updates.paloaltonetworks.com) 更新服务器的连接，或使用 SCP 下载并安装更新，如从 启用 SCP 的服务器安装 WildFire 内容更新中所述 。

STEP 2 | 下载并安装最新内容更新。

1. 下载最新内容更新：

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

2. 查看下载的状态：

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

可以通过运行 **show jobs pending** 查看挂起的作业。以下输出显示了下载（作业 ID 5）已完成 (Status FIN)：

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

3. 下载完成后，安装更新：

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

再次运行 **show jobs all** 命令以监控安装状态。

STEP 3 | 验证内容更新。

运行以下命令，并参阅 `wf-content-version` 字段：

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

以下内容显示了所安装内容更新版本 2-253 的输出示例：

```
admin@WF-500> show system info hostname: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 | （可选）设定每天或每周执行一次内容更新的安装。

1. 为设备计划下载和安装内容更新：

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

   例如，每天上午 8:00 下载和安装更新：

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

2. 提交配置

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

从启用 SCP 的服务器安装 WildFire 内容更新

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

以下步骤将介绍如何在未直接连接至 Palo Alto Networks 更新服务器的 WildFire 设备上安装威胁情报内容更新。您需要使用已启用安全复制 (SCP) 的服务器来临时存储内容更新。

STEP 1 | 从更新服务器中检索内容更新文件。

1. 登录到 Palo Alto Networks 支持门户，然后单击**Dynamic Updates**（动态更新）。
2. 在“WildFire 设备”部分，找到最新 WildFire 设备内容更新，然后下载此更新。
3. 将内容更新文件复制到启用 SCP 的服务器，然后记下文件名和目录路径。

STEP 2 | 在 WildFire 设备上安装内容更新。

1. 登录到 WildFire 设备，然后从 SCP 服务器中下载内容更新文件：

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

   例如：

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

   如果 *SCP* 服务器是在非标准端口上运行，或者您需要指定源 *IP*，则还可以在 ***scp import*** 命令中定义这些选项。

2. 安装更新：

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

3. 查看安装的状态：

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

STEP 3 | 验证内容更新。

验证内容版本：

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

以下输出现在显示版本 2-253：

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

启用生成本地签名和 URL 类别

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

WildFire 设备可根据从相连防火墙和 WildFire API 收到的样本，在本地生成签名，而不再将恶意软件发送至公共云以生成签名。此设备将生成以下类型的签名，以便防火墙可用其阻止恶意软件及其他任何相关的命令，进而控制流量：

- 防病毒签名 — 检测和阻止恶意文件。WildFire 会将这些签名添加到 WildFire 和防病毒内容更新中。
- **DNS** 签名 — 检测和阻止命令的回调域，控制与恶意软件相关的流量。WildFire 会将这些签名添加到 WildFire 和防病毒内容更新中。
- **URL** 类别 — 将回调域归类为恶意软件，并在 PAN-DB 中更新 URL 类别。

配置防火墙，使其每分钟检索一次 WildFire 设备生成的签名。您也可选择将恶意软件样本发送至 WildFire 公共云，以便通过 Palo Alto Networks 内容发布在全球范围内分发签名。

如果您正在使用 *WildFire* 设备进行本地文件分析，您还可以 启用连接的防火墙来接收 WildFire 公共云发布的最新签名 。

STEP 1 | 设置 WildFire 设备内容更新。

这样 WildFire 设备可从 Palo Alto Networks 接收最新的威胁情报。

STEP 2 | 启用生成签名和 URL 类别。

1. 登录到设备，然后键入 **configure** 以进入配置模式。
2. 启用所有威胁阻止选项：

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

3. 提交配置：

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

您可以通过以下命令，显示 *WildFire 8.0.1* 或以上环境中所生成签名的签名状态：

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

WildFire 应用程序无法显示升级至 WildFire 8.0.1 之前所生产的签名状态。

STEP 3 | 设置连接的防火墙接收 WildFire 设备生成的签名和 URL 类别的计划。

可选的最佳措施是配置防火墙从 *WildFire* 公共云和 *WildFire* 设备检索内容更新。这将确保防火墙可根据全球范围内检测到的威胁来接收签名，而不只是您本地设备生成的签名。

- 对于由 Panorama 管理的多个防火墙：

  启动 Panorama 并选择 **Panorama** > **Device Deployment**（设备部署）> **Dynamic Updates**（动态更新），单击 **Schedules**（计划），然后为托管设备 **Add**（添加）计划的内容更新。

  详细了解如何使用 Panorama 来设置托管防火墙从 WildFire 设备接收签名和 URL 类别，请参阅《使用 Panorama 对设备计划内容更新》。

- 对于单个防火墙：

  1. 登录至防火墙 Web 界面，然后选择 **Device**（设备）> **Dynamic Updates**（动态更新）。

     对于已配置转发文件至 WildFire 设备的防火墙（不论是在 WildFire 专有云还是混合云部署中），会显示出 WF-Private 部分。

  2. 设置防火墙的 **Schedule**（计划），以从 WildFire 设备下载、安装内容更新。

提交本地发现的恶意软件或报告至 WildFire 公共云

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

启用 WildFire 设备以将恶意软件样本自动提交至 WildFire 公共云。随即，WildFire 公共云将对恶意软件进行进一步分析并生成可用于识别样本的签名。之后，签名会被添加至 WildFire 签名更新，然后分发给全球的用户，以免日后再受此威胁的影响。或者，如果您不希望将恶意软件样本转发至您的网络之外，您也可选择仅提交 WildFire 对在您网络上发现的恶意软件给出的报告，以此为 WildFire 统计分析和威胁情报提供和改善信息。

提交恶意软件至 WildFire 公共云。

1. 从 WildFire 设备执行以下 CLI 命令，即可使该设备自动提交恶意软件样本至 WildFire 公共云：

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

   如果原本提交样本进行 *WildFire* 专有云分析的防火墙已启用数据包捕获 *(PCAP)*，则针对恶意软件的 *PCAP* 也可转发至 *WildFire* 公共云。

2. 前往 WildFire 门户，查看自动提交至 WildFire 公共云的恶意软件的分析报告。当恶意软件被提交至 WildFire 公共云时，公共云将针对相关样本生成一份新的分析报告。

提交分析报告至 WildFire 公共云

要自动向 WildFire 公共云提交恶意软件报告（而非恶意软件样本），请在 WildFire 设备上执行以下 CLI 命令：

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

如果您已经启用 *WildFire* 设备以将恶意软件自动提交至 *WildFire* 公共云，您无需启用此选项 — *WildFire* 公共云将针对相关样本生成一份新的分析报告。

可在 WildFire 门户上查看提交至 WildFire 公有云的报告。WildFire 门户仅显示 WildFire 公有云报告。

验证恶意软件和报告提交设置

如需确认是否已启用云智能将恶意软件或报告提交至 WildFire 公共云，请运行以下命令：

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

请参考提交示例和提交报告字段。

升级 WildFire 设备

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

使用下列工作流升级 WildFire 设备的操作系统。如果您想要升级已属于 WildFire 集群一部分的设备，请参阅在集群内升级 WildFire 设备。设备一次只能使用一个环境分析样本，因此在升级设备后，查看可用 VM 映像列表，然后选择最适合您的环境的映像。对于 Windows 7，如果您的环境使用混合的 Windows 7 32 位和 Windows 7 64 位系统，则建议您选择 Windows 7 64 位映像，以使 WildFire 能够分析 32 位和 64 位 PE 文件。尽管可将设备配置为使用一个虚拟机映像配置，但设备会使用映像的多个实例来执行文件分析。

根据 WildFire 设备分析和存储的样本数量，升级设备软件的时间也有所不同；这是由于升级需要迁移所有恶意软件样本和 14 天的良性样本。为生产环境下使用的 WildFire 设备留出 30 至 60 分钟升级时间。

以下过程使用 PAN-OS 10.2.2 版本中的示例文件名。在 WildFire 设备上安装的版本的实际文件名可能因具体版本而异。

STEP 1 | 如果您是首次设置 WildFire 设备，请从配置 WildFire 设备开始。

STEP 2 | 临时暂停样本分析。

1. 停止防火墙转发任何新样本至 WildFire 设备。
    1. 登录到防火墙 Web 界面。
    2. 选择 **Device**（设备） > **Setup**（设置） > **WildFire**，然后编辑 **General Settings**（常规设置）。
    3. 清空 **WildFire Private Cloud**（**WildFire** 专有云）字段。
    4. 单击 **OK**（确定）和 **Commit**（提交）。
2. 确认防火墙提交至设备的样本分析已完成：

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

如果您不想要等待 *WildFire* 设备完成对最近提交样本的分析，您可以直接继续下一步。但是，需要考虑到 *WildFire* 设备可能漏掉分析队列的挂起样本。

STEP 3 | 安装最新的 WildFire 设备内容更新。该更新为设备提供最新的威胁信息，以准确检测恶意软件。

在旧设备上，此过程最多可能需要 *6* 小时或更长时间才能完成。

1. 验证是否正在 WildFire 设备上运行最新的内容更新。

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

2. 下载最新的 WildFire 内容更新包。

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

如果您未直接连接 Palo Alto Networks 更新服务器，您可以从启用 SCP 的服务器下载并安装 WildFire 内容更新。

3. 查看下载状态。

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

4. 下载完成后，安装更新。

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

STEP 4 | （升级到 PAN-OS 10.2.2 时需要）升级 WildFire 设备上的虚拟机映像。

1. 登录并访问 Palo Alto Networks 客户支持门户软件下载页面。通过转到 **Updates**（更新） > **Software Updates**（软件更新），您还可以从支持主页手动导航到软件下载页面。
2. 在软件更新页面中，选择 **WF-500 Guest VM Images** 文件并下载以下 VM 映像文件：

   Palo Alto Networks 定期更新虚拟机映像文件；因此，特定文件名会根据可用的版本而更改。请务必下载最新版本，文件名中的 *m-x.x.x* 表示版本号；此外，还可以交叉引用一个发布日期以帮助确定最新版本。

   - 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. 将 VM 映像上传到 WildFire 设备。
   1. 从 SCP 服务器导入虚拟机映像：

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

      例如：

      ```
      admin@WF-500>scp import wildfire-vm-image from
       user1@10.0.3.4:/tmp/WFWin7_64Addon1_m-1.0.1.7_64addon1
      ```
   2. 如需检查下载状态，请使用以下命令：

      ```
      admin@WF-500>show jobs all
      ```
   3. 对其余 VM 映像重复此操作。
4. 安装 VM 映像。
   1. ```
      admin@WF-500>request system wildfire-vm-image upgrade
       install file <vm_image_filename>
      ```
   2. 对其余 VM 映像重复此操作。
5. 确认已在 WildFire 设备上正确安装和启用 VM 映像。
   1. （可选）查看可用虚拟机映像的列表：

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

      输出显示可用的虚拟机映像。
   2. 提交配置：
      ```

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

3. 通过运行以下命令来查看活动 VM 映像：

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

STEP 5 | 将 PAN-OS 10.2.2 软件版本下载到 WildFire 设备。

升级 WildFire 设备时，您不可跳过任何主要版本。例如，如果您想要从 PAN-OS 6.1 升级至 PAN-OS 7.1，您必须首先下载并安装版本 7.0。

此过程中的示例演示如何升级到 PAN-OS 10.2.2。将 10.2.2 替换成目标升级版本。

下载 10.2.2 软件版本：

- 直接互联网连接：
  1. ```
     admin@WF-500> request system software download version 10.2.2
     ```
  2. 如需检查下载状态，请使用以下命令：

     ```
     admin@WF-500> show jobs all
     ```
- 无互联网连接：
  1. 导航到 Palo Alto Networks 支持站点，在工具部分，点击 **Software Updates**（软件更新）。
  2. 将要安装的 WildFire 设备软件映像文件下载到运行 SCP 服务器软件的计算机。
  3. 从 SCP 服务器导入软件映像：

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

     例如：

     ```
     admin@WF-500> scp import software from user1@10.0.3.4:/tmp/
     WildFire_m-10.2.2
     ```
  4. 如需检查下载状态，请使用以下命令：

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

STEP 6 | 确认所有服务正在运行。

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

STEP 7 | 安装 10.2.2 软件版本。

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

STEP 8 | 完成软件升级。

1. 确认是否已完成升级。运行以下命令，然后查找作业类型 `Install` 和状态 `FIN`：

```
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. 重新启动设备：

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

升级程序可能需要 *10* 分钟至一个小时以上，具体取决于 *WildFire* 设备上存储的样本数。

STEP 9 | 检查 WildFire 设备是否继续，可继续样本分析。

1. 验证 `sw-version` 字段是否显示有 10.2.2：

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

2. 确认所有程序正在运行。

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

3. 确认自动提交 (`AutoCom`) 工作已完成：

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

STEP 10 | （可选）启用 WildFire 设备使用的虚拟机映像以执行分析。每个可用的虚拟机映像代表一个单一的操作系统，并支持基于该操作系统的若干不同分析环境。

- 如果您的网络环境使用混合的 *Windows 7 32* 位和 *Windows 7 64* 位系统，则建议您选择 *Windows 7 64* 位映像，以使 *WildFire* 能够分析 *32* 位和 *64* 位 *PE* 文件。
- *vm-3 (Windows XP)*、*vm-5 (Windows 7 64* 位*)* 和 *vm-7*（*Windows 10 64* 位）是目前可用的分析环境。

- 运行以下命令来查看当前虚拟机映像，并参阅 `SelectedVM`（所选 `VM`）字段：

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

- 查看可用虚拟机映像的列表：

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

以下输出显示 `vm-5` 是 Windows 7 64-位映像：

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

- 设置用于分析的映像：

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

例如，要使用 vm-5，请运行以下命令：

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

提交配置：

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

STEP 11 | 后续步骤：

- （可选）将防火墙升级到 PAN-OS 10.2.2。参见 PAN-OS 10.2 新功能指南中的防火墙升级说明。运行 PAN-OS 10.2.2 之前版本的防火墙仍可以继续转发样本至运行 10.2.2 的 WildFire 设备。
- （故障排查）如果您在升级后发现数据迁移问题或错误，重新启动 WildFire 设备以重启升级程序——重新启动 WildFire 设备不会引起数据丢失。

通过 Internet 连接安装 WildFire 设备设备证书

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证 ❑ 具有以下用户角色之一的客户支持门户 (CSP) 帐户： 超级用户、标准用户、有限用户、威胁研究人员、AutoFocus 试用角色、组超级用户、组标准用户、组有限用户、组威胁研究人员、授权支持中心 (ASC) 用户和 ASC 全方位服务用户。 ❑ WildFire 设备的超级用户访问权限

要在 Internet 连接可用时获取 WF-500 设备上的设备证书，您必须登录 Palo Alto Networks 支持门户以生成用于访问证书的一次性密码。随后，此 OTP 用于检索特定设备上的设备证书。

WF-500B 设备配有可信平台模块 *(TPM)*，用于安全地识别自身并自动获取设备证书，无需用户干预即可管理 *WF-500B* 设备证书。

如果您正在运行 WildFire 私有云 且未连接到任何 WildFire 服务，则无需更新 WildFire 设备证书。WildFire 设备使用预定义证书进行相互身份验证，以建立用于管理访问权限和设备间通信的 SSL 连接，但是，您可以在独立 WildFire 设备上使用自定义证书设置身份验证。

如果您的 *WF-500B* 设备未连接到 *Internet*，则可能发现由于设备重复尝试检索设备证书而导致作业失败。

为了在防火墙成功安装设备证书，您的网络必须允许使用以下 FQDN 和端口。

FQDN	端口
• 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

FQDN	端口
• *.gpcloudservice.com	TCP 444 和 TCP 443

STEP 1 | 验证您是否正在 WildFire 设备上运行以下 PAN-OS 版本之一：

- PAN-OS 11.0.1 及更高版本
- PAN-OS 10.2.4 及更高版本
- PAN-OS 10.1.10 及更高版本（WF-500B 设备不支持）
- PAN-OS 10.0.12 及更高版本（WF-500B 设备不支持）
- PAN-OS 9.1.17 及更高版本（WF-500B 设备不支持）

STEP 2 | 生成一次性密码 (OTP)。

1. 使用有权生成 OTP 的用户角色登录到客户支持门户。
2. 选择 **Products**（产品） > **Device Certificates**（设备证书）和 **Generate OTP**（生成 **OTP**）。
3. 对于 **Device Type**（设备类型），选择 **Generate OTP for WF-500**（为 **WF-500** 生成 **OTP**）。
4. 选择 **WF-500 Device**（**WF-500** 设备）序列号。
5. **Generate OTP**（生成 **OTP**）并复制该 OTP。

STEP 3 | 使用超级用户管理权限访问 WF-500 设备 CLI。

STEP 4 | 配置 WildFire 设备，以便与 NTP 服务器同步：

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

STEP 5 | 使用以下 CLI 命令下载并安装 WF-500 设备设备证书（请记住，使用在客户支持门户中生成的正确一次性密码）：

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

STEP 6 | 您的 WF-500 设备成功检索并安装了设备证书。

STEP 7 | （可选）使用以下 CLI 命令验证设备证书是否已成功下载和安装：

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

设备证书安装成功时会显示以下响应：

```
设备证书信息：当前设备证书状态：有效，之前无效：2022/11/30 15:17:47 PST 在以下时间后失效：2023/02/28 15:17:47 PST 上次获取时间戳：2022/11/30 15:29:42 PST 上次获取状态：成功，上次获取信息：已成功获取设备证书
```

STEP 8 | 使用以下 CLI 命令刷新 WildFire 设备设置，以使用更新的设备证书建立与 Advanced WildFire 云的连接：

表 **1:**

在 **WildFire** 设备上运行的 **PAN-OS** 版本	**CLI** 命令
• PAN-OS 11.0.1 及更高版本 • PAN-OS 10.2.5 及更高版本 • PAN-OS 10.1.10 及更高版本	`admin@WF-500> test wildfire registration`
• PAN-OS 10.2.4 • PAN-OS 10.0.12 及更高版本 • PAN-OS 9.1.17 及更高版本	`admin@WF-500> request restart system` 此过程最多可能需要 *20* 分钟才能完成。
配置为 WildFire 集群节点的任何版本	`admin@WF-500(active-controller)> request cluster reboot-local-node`

在 **WildFire** 设备上运行的 **PAN-OS** 版本	**CLI** 命令

	您可以使用以下 *CLI* 命令查看 *WildFire* 控制器节点上的重新启动任务的状态：
	`admin@WF-500(active-controller)> show cluster task pending`
	没有剩余的挂起任务时，使用以下 *CLI* 命令验证是否成功重新启动：
	`admin@WF-500(active-controller)> show cluster task history`
	完成后，您会看到以下状态：*Finished: success at YYYY-MM-DD HH:MM:SS UTC*，表示重新启动过程已完成。

监控 WildFire 设备活动

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

通过访问提交示例的防火墙（如果您集中管理多个防火墙，则访问 Panorama）或使用 WildFire API，您可以查看提交到 WildFire 设备的示例的分析结果。

在 WildFire 完成样本分析并对恶意、网络钓鱼、灰色软件或良性软件进行判定后，会对每个样本生成一份详细的分析报告。在提交样本的防火墙上查看的 WildFire 分析报告中也包括检测样本期间所进行会话的详细信息。对于被识别为恶意软件的样本，WildFire 分析报告中会包括现有 WildFire 签名的详细信息，此类签名可能关系到新识别的恶意软件，以及指示样本属于恶意样本的文件属性、行为及活动方面的信息。

请参阅以下主题，以了解如何使用监控 WildFire 的提交情况、查看样本的 WildFire 分析报告，并设置警报以及基于提交情况和分析结果的通知：

- 关于 WildFire 日志和报告
- 使用 WildFire CLI 监控 WildFire 设备
- 使用防火墙监视 WildFire 设备提交

关于 WildFire 日志和报告

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

您可以通过 WildFire 门户或 WildFire API 在防火墙上监控 WildFire 活动。

对于 WildFire 分析的每一个样本，WildFire 会将样本划分为恶意软件、网络钓鱼、灰色软件或良性文件，同时也会在 WildFire 分析报告中提供详细的样本信息和行为。在提交样本的防火墙或对其进行分析的 WildFire 云（公共云或专有云）中可以找到 WildFire 分析报告，也可以使用 WildFire API 检索：

- 在防火墙上 — 所有由防火墙提交用于进行 WildFire 分析的样本均会被记录为 WildFire 提交情况条目（**Monitor**（监控） > **WildFire Submissions**（**WildFire** 提交情况））。WildFire 提交情况日志中的操作列显示文件被防火墙允许或阻挡。对于每一条 WildFire 提交情况条目，您均可打开详细的日志视图，以查看相关样本的 WildFire 分析报告或将其下载为 PDF 文件。
- 在 WildFire 门户上 — 监控 WildFire 活动，包括各样本的 WildFire 分析报告等（也可将其下载为 PDF 文件）。在 WildFire 专有云部署中，WildFire 门户可提供各样本的详细信息，包括手动上传至 WildFire 门户的样本，以及经启用了云智能的 WildFire 设备所提交的样本。

  在门户上查看 *WildFire* 分析报告仅支持已启用云情报功能的 *WildFire* 设备。

- 使用 WildFire API — 从 WildFire 设备或从 WildFire 公共云检索 WildFire 分析报告。

使用 WildFire 设备监控样本分析状态

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

使用 WildFire CLI（命令行接口）监控 WildFire 设备上与分析相关的详细信息。您可以查看分析平台利用率信息、当前样本队列和样本处理详细信息。

请参阅以下章节，了解有关使用 WildFire 设备监控 WildFire 活动的详细信息：

- 查看 WildFire 分析环境利用率
- 查看 WildFire 样本分析处理详细信息

查看 WildFire 分析环境利用率

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

WildFire 设备使用各种分析环境来检测样本中的恶意行为。您可以查看正在使用哪些分析环境、有多少可用以及有多少文件在排队等待分析。如果特定分析环境的利用率始终处于（或接近）最大工作负载容量，请考虑将敏感度较低的文件的分析卸载至 Palo Alto Networks 托管的 WildFire 公共云，更新文件转发策略或重新定义文件转发限制（Palo Alto Networks 建议对所有文件类型使用默认文件转发值）。

STEP 1 | 根据要查看其利用率统计信息的分析环境，访问 CLI 和以下命令之一。

- 可迁移可执行分析环境利用率—**show wildfire wf-vm-pe-utilization**
- 文档分析环境利用率—**show wildfire wf-vm-doc-utilization**
- 电子邮件链接分析环境利用率—**show wildfire wf-vm-elinkda-utilization**
- 存档分析环境利用率—**show wildfire wf-vm-elinkda-utilization**

对于给定的分析环境，设备会显示有多少正在使用以及有多少可用：

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

STEP 2 | 查看等待分析的 WildFire 设备样本数量和详细信息。分析环境可用时，对样本进行处理。

show wildfire wf-sample-queue-status

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

查看 WildFire 样本分析处理详细信息

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

WildFire 设备会保留事件日志中的分析活动记录。您可以查看有关网络中哪些连接的服务或设备分析了特定样本的详细信息，以及在给定时间范围内分析了多少个样本。您可以使用这些信息来监控活动并制定应对恶意活动的政策和对策。异常活跃的活动可能是可疑活动。还可考虑使用 AutoFocus 等威胁情报工具来调查和确定威胁性质。

STEP 1 | 查看指定时间范围内或基于最大样本数量的本地处理样本数量。

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

```
Latest samples information:
 +-------------------------------------------------------------------
+---------------------+-----------+------------+-----------
+------------+--------------------+ | 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
 |
 +-------------------------------------------------------------------
+---------------------+-----------+------------+-----------
+------------+--------------------+
```

STEP 2 | 标识提交特定样本以供 WildFire 分析的设备。

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

```
 Sample
 1024609813c57fe174722c53b3167dc3cf5583d5c7abaf4a95f561c686a2116e
 last seen on following devices:
 +-------------------------------------------------------------------
```

```
+-----------+-----------+---------------------+ |
 SHA256 | Device ID | Device IP | Submitted Time |
 +-------------------------------------------------------------------
+-----------+-----------+---------------------+ |
 1024609813c57fe174722c53b3167dc3cf5583d5c7abaf4a95f561c686a2116e
 | Manual | Manual | 2019-08-05 19:24:39 |
 +-------------------------------------------------------------------
+-----------+-----------+---------------------+
```

使用 WildFire CLI 监控 WildFire 设备

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

使用 WildFire™ CLI（命令行接口）查看内部系统日志。您可以查看日志记录事件，以监控 WildFire 组件（如集群节点、核心和分析器服务）的运行状况和状态，以及进行故障排除和验证系统配置。了解有关其他 PAN-OS 命令的信息，请参阅《PAN-OS CLI 快速入门》。

- 查看 WildFire 设备系统日志

查看 WildFire 设备系统日志

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

使用终端仿真器（如 PuTTY），通过安全壳连接 (SSH) 或从管理计算机上的串行接口到设备上的控制台端口的物理直接串行连接，连接到 WildFire 设备。

STEP 1 | 启动终端仿真软件并选择连接类型（串行连接或 SSH）。

- 要建立 SSH 连接，请输入要连接设备的 WildFire 主机名或 IP 地址，并将端口设置为 **22**。
- 要建立串行连接，请将管理计算机上的串行接口连接到设备上的控制台端口。终端仿真软件中的串行连接设置配置如下：
  - 数据速率：**9600**
  - 数据位：**8**
  - 奇偶校验：无
  - 停止位：**1**
  - 流量控制：无

STEP 2 | 当提示登录时，请输入您的管理凭据。

STEP 3 | 在 WildFire 设备上，输入以下命令：

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

该命令会按从最旧到最新的顺序显示所有归类为防火墙设备子类型的 WildFire 日志事件。

- 通过添加命令参数 `direction equal backward`，可以反向显示从最新到最旧的日志。
- WildFire 设备 CLI 返回的日志消息可以包括许多子类型。您可以根据常见关键字过滤日志。使用以下命令参数来根据特定字符串进行过滤：`match queue < keyword>`

  以下 WildFire 设备日志会显示启动期间的系统初始化进程。

```
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
```

使用防火墙监视 WildFire 设备提交

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

防火墙转发的样本（到 WildFire 私有云和/或公有云）将作为条目添加到 **WildFire** 提交日志中。每个 WildFire Submissions（WildFire 提交情况）条目的扩展视图中都会显示详细的 WildFire 分析报告。有关使用防火墙监视恶意软件的详细信息，请参阅监视 WildFire 活动。

查看 WildFire 设备日志和分析报告

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

WildFire 日志包含有关 WildFire 分析的样本（文件和电子邮件链接）的相关信息。其中包括工件，这些工件是与记录的事件相关联的属性、活动或行为，例如攻击者的应用程序类型或 IP 地址，以及 WildFire 特定的质量，例如高级分析结果，包括将样本分类为恶意软件、网络钓鱼、灰色软件或良性，并详细说明样本信息。查看 WildFire 提交日志还可以指示您网络中的用户是否下载了可疑文件。WildFire 分析报告将显示详细的样本信息、目标用户的相关信息、电子邮件标题信息（如已启用）、交付文件的应用程序，以及所有与文件命令和控制活动相关的 URL。它通知您文件是否存在恶意、是否修改注册表项、读/写文件、创建新文件、打开网络通信通道、导致应用程序崩溃、产生进程、下载文件或表现出其他恶意行为。

STEP 1 | 转发文件进行 WildFire 设备分析.

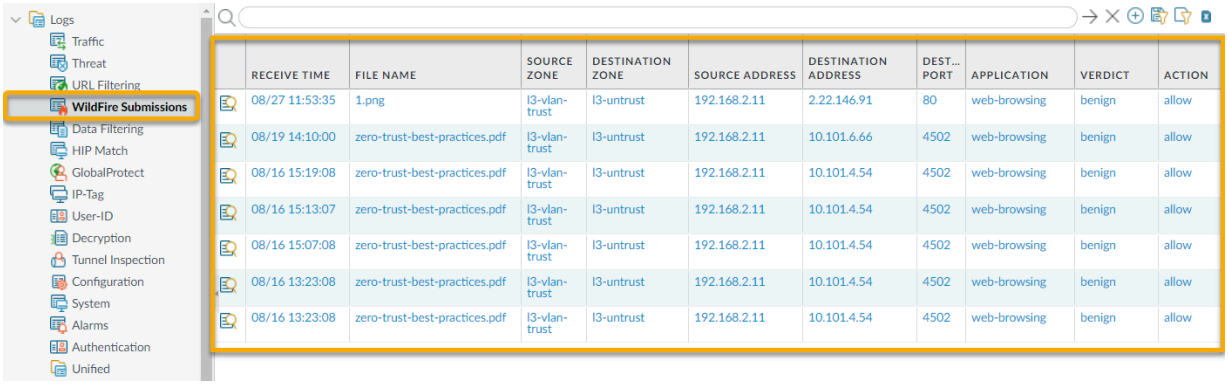
STEP 2 | 配置 WildFire 提交情况日志的设置。

STEP 3 | 要查看防火墙向 WildFire 公共、专有或混合云提交的样本，请选择 **Monitor**（监控） > **Logs**（日志） > **WildFire Submissions**（**WildFire** 提交）。WildFire 样本分析完成后，其结果会发送回提交样本的防火墙，且可在 WildFire 提交情况日志中进行查看。提交日志包含给定样本的详细信息，包括以下信息：

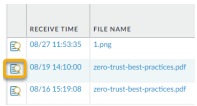
- Verdict（判定）列将显示样本是属于良性、恶性、网络钓鱼还是灰色软件。
- Action（操作）列显示防火墙已允许或阻挡了样本。

- 严重性列显示样本对组织的威胁，通过下列值显示：关键、高、中、低和参考。

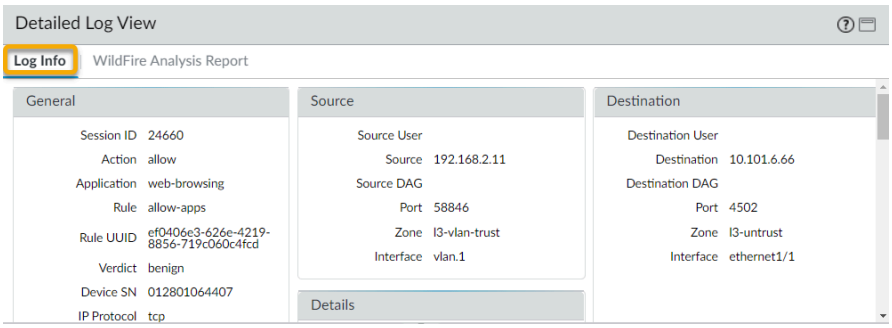
  以下严重性级别的值根据判定和操作值组合确定。
  - 低 — 操作设置为允许的灰色软件样本。
  - 高 — 操作设置为允许的恶意软件样本。
  - 参考：
    - 操作设置为允许的良性软件样本。
    - 带其操作设置为阻止的任何判定的样本。



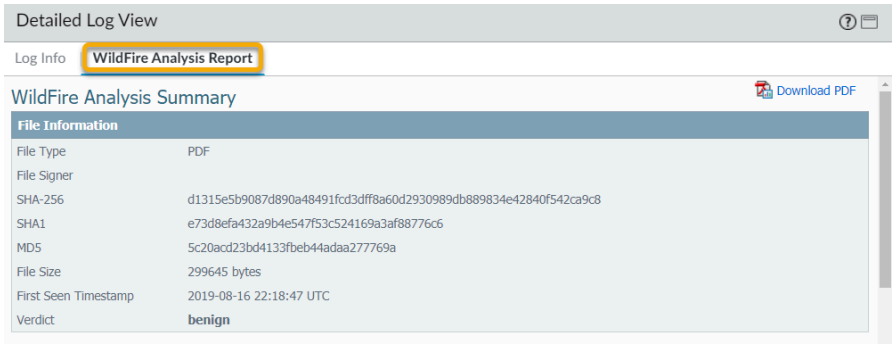
STEP 4 | 对于所有条目，选择 Log Details（日志详细信息）图标，即可打开对应条目的详细日志视图：



详细日志视图将显示 Log Info（日志信息）和对应条目的 WildFire 分析报告。如果防火墙已启用数据包捕获 (PCAP)，则样本的数据包捕获 (PCAP) 结果也会予以显示。



对于所有样本，WildFire 分析报告都会显示文件和会话的详细信息。对于恶意软件样本，WildFire 分析报告将进一步纳入可指示文件为恶意文件的文件属性和行为信息。



STEP 5 | （可选）**Download PDF**（下载 **PDF**） 形式的 WildFire 分析报告。

WildFire 设备集群

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

WildFire 设备集群是 WildFire 设备的互联分组，通过聚集资源增加样本分析和存储能力，支持较大的防火墙分组，并简化多台 WildFire 设备的配置和管理。在不允许访问 WildFire 公共云的情况下，此方法尤其有用。您可以配置和管理最多二十台 WildFire 设备，作为单一网络上的 WildFire 设备集群。集群还可以提供由集群分发至所有已连接防火墙的单一签名包，容错高可用性 (HA) 基础架构，以及通过 Panorama 集中管理集群的能力。您也可以通过 Panorama 管理独立 WildFire 设备。

要创建 WildFire 设备集群，您希望在集群内部署的所有 WildFire 设备都必须运行 PAN-OS 8.0.1 或以上版本。当使用 Panorama 管理 WildFire 设备集群时，Panorama 也必须运行 PAN-OS 8.0.1 或以上版本。您无需独立授权以创建和管理 WildFire 设备集群。

- WildFire 设备集群复原和规模
- WildFire 设备群集管理
- 在 WildFire 设备上本地配置集群
- 配置 WildFire 设备到设备加密
- 监控 WildFire 集群
- 在集群内升级 WildFire 设备
- 对 WildFire 集群的故障排查

WildFire 设备集群复原和规模

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

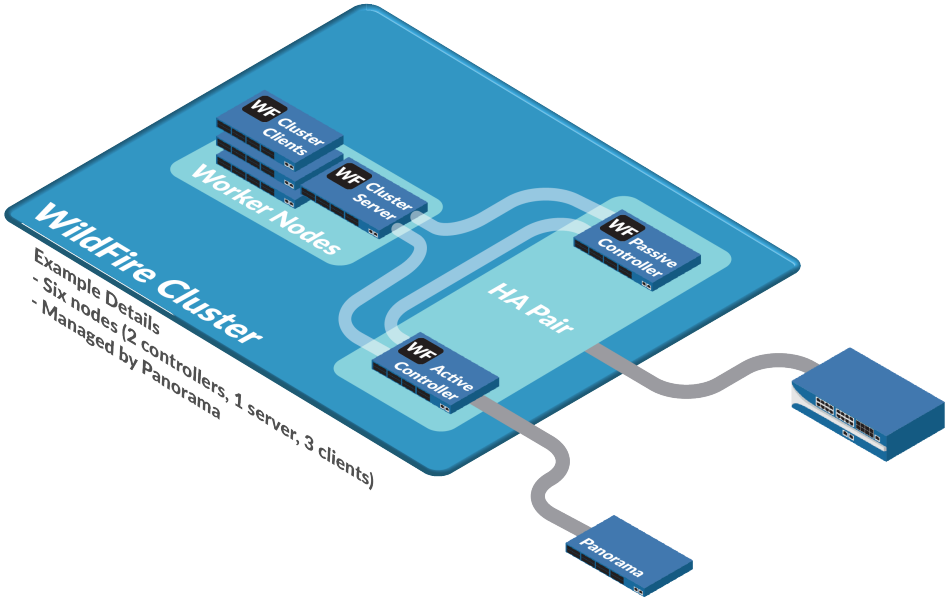
WildFire 设备集群将最多二十台 WildFire 设备的样本分析和存储能力聚合在一起，以让您可以支持单一网络上的大型防火墙部署。通过 CLI，您可以在 WildFire 设备上进行灵活地本机管理和配置集群，或在 Panorama M 系列或虚拟设备服务器上集中管理和配置集群。WildFire 设备集群环境包括：

- 2 至 20 台您希望分组并作为一个集群管理的 WildFire 设备。在高可用 (HA) 对中，至少一个集群必须有两台 WildFire 设备。
- 转发样本至集群进行流量分析和签名生成的防火墙。
- （可选）当您选择不在本地管理集群时，进行中央集群管理的一至两台 Panorama 设备。若要提供高可用性，请使用两台被配置为一个高可用对的 Panorama 设备。

您添加至 WildFire 设备集群的各 WildFire 设备成为该集群内的一个节点（与独立的 WildFire 设备相对）。Panorama 最多可管理 10 台 WildFire 设备，合计 200 个 WildFire 集群节点（10 个集群，每个最多 20 个节点）。

Panorama 也可以管理独立 WildFire 设备和 *WildFire* 设备集群。*Panorama* 可以管理的独立 *WildFire* 设备和 *WildFire* 设备集群节点总数为 *200*。例如，当 *Panorama* 管理三个总共带有 *15* 个 *WildFire* 集群节点的集群，和八个独立的 *WildFire* 设备时，则 *Panorama* 总共管理 *23* 台 *WildFire* 设备，并且最多还可多管理 *177* 台 *WildFire* 设备。

连接 *Panorama* 的 *WildFire* 设备无注册限制——您可以连接任意数量的设备，而不会对您的功能许可证造成影响。关于 *Panorama* 授权的更多信息，请参阅注册 Panorama 和安装许可证。



集群节点履行下列三种职能之一：

- 控制器节点——两个控制器节点管理队列服务和数据库，生成签名，以及在您未使用 Panorama M 系列或虚拟设备管理集群时，执行集群的本地管理。每个集群最多可以有两个控制器节点。为了容错，每个 WildFire 设备集群应至少有两个节点，分别配置为主控制器节点和控制器备份节点高可用对。除了正常维护或故障情况下，各集群都应有两个控制器节点。
- 工作节点（集群客户端）——非控制器节点的集群节点即工作节点。工作节点增加集群的分析能力、存储能力和数据弹性。
- 服务器节点（集群服务器）——WildFire 集群内的第三个节点被自动配置为服务器节点，这是一种特殊的工作节点，除了提供标准的工作节点功能外，还提供数据和基础架构冗余功能。

当防火墙通过集群节点注册，或当您添加一个已注册防火墙的 WildFire 设备至集群时，该集群推送注册列表至连接的防火墙。注册列表包括集群内的每一个节点。如果集群节点发生故障，连接该节点的防火墙通过另一个集群节点重新注册。此类弹性是创建 WildFire 设备集群的优势之一。

优点	说明
规模	WildFire 应用程序集群增加了单一网络上可用的分析吞吐量和存储容量，让您可以在不将您的网络分段的情况下，使用较大的防火墙网路。
高可用性	如果集群节点出现故障，高可用性配置提供容错，以防关键数据和服务丢失。如果您通过 Panorama 集中管理集群，Panorama 高可用性配置提供集中管理容错。
单一签名包分配	所有连接集群的防火墙接收相同的签名包，且无论集群节点是否接收或分析了数据。签名包基于所有集群成员活动和结果，这意味着各连接的防火墙从组合集群知识获益。

优点	说明
集中管理 (Panorama)	当使用 Panorama 管理 WildFire 设备集群时，您可以节约时间并简化管理程序。与使用 CLI 和应用脚本管理 WildFire 设备或集群不同，Panorama 提供您网络设备的单一窗口视图。您也可以推送普通配置、配置更新和软件更新至多个 WildFire 设备集群，并且您可以通过 Panorama 网络接口而非 WildFire 设备 CLI 完成这些操作。
负载均衡	当集群有两个或两个以上活动节点时，集群自动分配和装载均衡分析、报告生成情况、签名创建情况、存储和节点之间的 WildFire 内容分配。

WildFire 集群高可用性

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

高可用性是 WildFire 设备集群的关键性优势，因为高可用性可以防止关键数据和服务的丢失。高可用性集群在节点之间复制并分发关键数据，如分析结果、报告和签名，因此，当某个节点出现问题时，不会导致数据丢失。高可用性集群还提供冗余的关键服务，如分析功能、WildFire API 和签名生成，因此，某个节点出现问题时不会导致服务中断。一个集群必须至少有两个节点，以提供高可用性的优势。集群节点故障不会影响防火墙，因为故障节点所注册的防火墙使用该集群注册表注册另一个集群节点。

高可用对中的两个设备由用户配置为主要设备和次要设备。基于此初始优先值配置，WildFire 也将指派主动操作状态至主要设备，并将被动操作状态指派至次要设备。此状态确定了哪一台 WildFire 设备被作为管理和基础架构控制的接触点。被动设备始终与主动设备同步，并在系统或网络发生故障时继续该职能。例如，当主动状态（主活动）的主要设备发生故障时，将进行故障转移，并转至主被动状态，同时，次要设备转为次要主动状态。无论设备状态如何，原先指派的优先值保持不变。

当高可用对不可互相通信、无响应或遇到致命错误时，执行故障转移。WildFire 高可用对可尝试自动解决小型中断，而重大事件则需要用户干预。当控制器被用户暂停或解除授权时，也可以触发故障转移。

请勿配置只有一个控制器节点的集群。每个集群都应具有一个高可用性控制器对。集群仅在临时情况下带有单一的控制器节点，例如，当您交换控制器节点或某个控制器节点故障时。

在双节点集群高可用对中，如果一个控制器节点故障，其他控制器节点将无法处理样本。要让剩余集群节点处理样本，您必须将其配置为独立的 WildFire 设备：删除剩余集群节点上的 HA 和集群配置，并重启节点。该节点将作为独立 WildFire 设备重新上线。

三节点集群与服务器节点一起操作高可用对，以提供额外的冗余。服务器操作相同的数据库，且服务器基础架构被作为控制器使用，但不生成签名。当控制器节点故障时，此部署让集群可以正常运行。

添加至 WildFire 集群的其他节点可作为工作或服务器节点。第三个节点被自动配置为服务器，后续部分则作为工作节点添加。

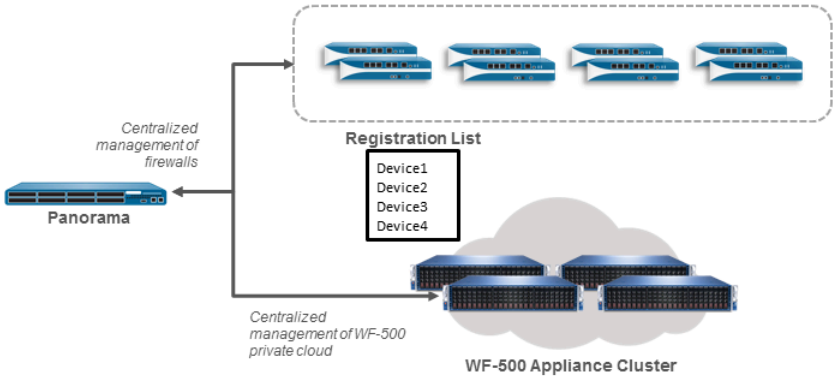
通过 Panorama 管理 WildFire 集群的优点

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

如果您通过 Panorama 管理 WildFire 设备集群，您可以 配置两台 Panorama M 系列或虚拟设备作为 HA 对 以提供管理冗余。如果您不配置冗余 Panorama 设备，且 Panorama 发生故障，您仍可以从控制器节点本地管理集群。

如果您使用 Panorama HA 对管理集群且一台 Panorama 故障，另一台 Panorama 设备接管集群管理。如果 Panorama HA 对端故障，尽快从故障的 Panorama 对端恢复服务以恢复管理 HA。

提供复习、存储和集中管理 HA 需要至少两台配置为集群控制器和控制器备份节点的 WildFire 设备，以及两台 Panorama M 系列或虚拟设备。



防火墙接收包含所有 WildFire 设备（这些设备都是集群成员）的注册列表。防火墙可以通过任何节点在集群内注册，集群自动均衡节点之间的负载。

WildFire 设备群集管理

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

要管理 WildFire 设备集群，您需要了解集群能力和管理建议。

类别	说明
集群操作和配置	为所有集群节点进行相同配置，以确保分析和设备间通讯的一致性： • 所有集群节点必须运行相同版本的 PAN-OS（PAN-OS 8.0.1 或以上版本）。Panorama 必须运行与集群节点相同的，或更新的软件版本。防火墙可运行相同的软件版本，以使其可以提交样本至 WildFire 设备。防火墙无需特定的软件版本以提交样本至 WildFire 设备集群。 • 集群节点从控制器节点沿用其配置，接口配置的情况除外。当控制器节点执行更新配置时，集群成员监控控制器节点配置并更新其自身的配置。工作节点沿用的设置包括，内容更新服务器设置、WildFire 云放弃设置、样本分析图像、样本数据保留时间框架、分析环境设置、签名生成设置、日志设置、验证设置，以及 Panorama 服务器、DNS 服务器 和 NTP 服务器设置。 • 当您通过 Panorama 管理集群时，Panorama 设备推送一致的配置至所有集群节点。虽然您可以在 WildFire 设备节点上进行配置的本地变更，Palo Alto Networks 并不建议您这么做，因为下次 Panorama 设备推送配置时，其将更换节点上的运行配置。Panorama 管理的，对集群节点的本地变更通常引起不同步的错误。 • 如果两个控制器节点上的集群节点成员列表不相同，集群将生成不同步警告。要避免两个控制器节点持续为另一个节点更新不同步成员列表的情况，停止集群成员强制状态。当出现此情况时，您可以从控制器和控制器备份节点上的本地 CLI 同步集群成员列表，做法是运行操作命令 **`request high-availability sync-to-remote running-configuration`**。如果主控制器节点配置和控制器备份节点配置不匹配，主控制器节点上的配置将覆盖控制器备份节点上的配置。在各控制器节点上，运行 **`show cluster all-peers`** 并对比和纠正成员列表。 • 集群只可以有两个控制器节点（主节点和备份节点）；尝试本地添加第三个控制器节点将导致集群故障。（Panorama 网络接口自动阻

类别	说明
	止您添加第三个控制器节点。）添加到集群的第三个和所有后续节点都必须是工作节点。 • 高可用性配置特征之一是，集群分配并保留多个数据库复制、队列服务和提交情况，以在集群节点发生故障时提供冗余部分。运行所需的额外服务以提供高可用冗余会对吞吐量造成轻微影响。 • 集群自动检查分析环境网络使用的重复 IP 地址。 • 如果节点属于某个集群，且您想要将其移动到一个不同的集群，您必须首先从其当前集群移除该节点。 • 不得更改集群内正在运行的 WildFire 设备 IP 地址。否则将导致相关防火墙从节点上注销。
集群数据保留政策	数据保留政策决定 WildFire 设备集群存储不同样本类型的时长。 • 良性和灰色软件样本——集群保留良性和灰色软件样本 1 至 90 天（默认为 14 天）。 • 恶意样本——集群至少保留恶意样本 1 天（默认为无限天数——从不删除）。恶意样本可能包括网络钓鱼判定样本。 在集群内配置相同的数据保留策略（4 参见 本地配置常规集群设置 或 4 参见 Panorama 上配置常规集群设置）。
网络	WildFire 设备集群之间不允许通讯。节点在给定的集群内互相通讯，但不得与其他集群的节点通讯。 所有集群成员必须： • 使用集群管理和通讯专用的集群管理接口（Panorama 中强制）。 • 在相同子网下具有静态 IP 地址。 • 在集群节点之间使用低延迟连接。连接的最大延迟不应超过 500 ms。
专属集群管理接口	专属集群管理接口让控制器节点可以管理集群，并且是与标准管理接口（以太网 0 ）不同的接口。Panorama 强制配置专属集群管理接口。 如果双节点配置中的两个控制器节点之间集群管理链接发生故障，控制器备份节点服务和样本分析继续运行，即使此时与主控制器节点已无管理通讯。这是由于当集群管理链接发生故障时，控制器备份节点不知道主控制器节点是否仍可运行，从而导致出现脑裂状况。控制器备份节点必须持续提供集群服务，以免主控制器节点不运行。当集群管理链接恢复时，来自各控制器节点的数据被合并。

类别	说明
DNS	您可以使用 WildFire 设备集群内的控制器节点作为该集群的授权 DNS 服务器。（授权 DNS 服务器作为集群成员的实际 IP 地址，与递归 DNS 服务器相对，后者查询授权 DNS 服务器，并将请求信息发送至作出初始请求的主机。） 提交样本至 WildFire 设备集群的防火墙应发送 DNS 查询至其常规 DNS 服务器，例如内部企业 DNS 服务器。内部 DNS 服务器将 DNS 查询转发至 WildFire 设备集群控制器（基于查询域）。使用集群控制器作为 DNS 服务器具有许多优点： • 自动负载均衡——当集群控制器解析服务广告主机名称时，主机集群节点顺序为随机，从而具有在节点上有机平衡负载的效果。 • 容错——如果一个集群节点故障，该集群控制器自动将其从 DNS 响应中移除，从而让防火墙发送新请求至正常运行的节点。 • 管理灵活、简单——当您添加节点至集群时，由于控制器自动更新 DNS 响应，您无需对防火墙进行任何更改，请求自动发往新节点和之前存在的节点。 尽管 DNS 记录不应缓存，为了进行故障排查，如果 DNS 查询成功，TTL 将变为 0。但是，当 DNS 查询回传 NXDOMAIN 时，TTL 和“最小 TTL”均变为 0。
管理	您可以通过本地 WildFire CLI 或 Panorama 管理 WildFire 集群。在 WildFire 集群节点上有两种本地管理角色可用： • 超级读取器——只读访问。 • 超级用户——读写访问。
防火墙注册	WildFire 设备集群推送注册列表至连接集群节点的各防火墙，该列表包含集群内的所有节点。当您通过集群内的设备注册防火墙时，该防火墙收到注册列表。当您添加独立 WildFire 设备至集群，且该设备已有连接的防火墙，并使其成为集群节点时，这些已连接的防火墙将收到注册列表。 如果节点故障，连接的防火墙使用注册列表，通过列表上的下一个节点注册。
数据迁移	要提供数据冗余，集群内的 WildFire 设备节点分享数据库、队列服务和样本提交内容，但此数据的准确位置视乎集群拓扑结构而定。因此，当拓扑结构发生改变时，集群内的 WildFire 设备需要进行数据迁移和数据重排。拓扑结构变更包括添加和移除节点，以及变更之前节点的角色。当数据库被转为新的版本时，如从 WildFire 7.1 升级至 8.0 时，也将发生数据迁移。

类别	说明
	可通过从 WildFire CLI 发布状态命令来查看数据迁移状态。此过程可能需要数小时的时间，具体取决于 WildFire 设备上的数据量。

部署 WildFire 集群

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

要部署 WildFire 设备集群，您必须升级所有将加入集群的设备，创建 WildFire 集群，然后配置设置以符合您的需要。您可以从 WildFire 设备 CLI 或通过 Panorama，本地执行这些任务，让您可以快速应用配置更改和升级至连接的 WildFire 设备。

下列程序显示了如何创建和配置 WildFire HA（高可用性）对和添加额外的设备节点至集群。

STEP 1 | 本地升级您的 WildFire 设备至 PAN-OS 8.0.1 或以上，这是最早支持集群操作的版本。

STEP 2 | 创建、配置并添加节点至 WildFire 设备集群。

- 本地配置集群和添加节点
- 在 Panorama 上配置集群和添加节点

STEP 3 | 配置常规 WildFire 设备集群设置。

- 本地配置常规集群设置
- 在 Panorama 上配置常规集群设置

STEP 4 | （可选）加密 WildFire 集群设备到设备通信。

- 通过 CLI 使用预定义证书对设备到设备加密进行配置
- 通过 CLI 使用自定义证书对设备到设备加密进行配置
- 使用预定义证书在 Panorama 上集中配置设备到设备加密
- 使用自定义证书在 Panorama 上集中配置设备到设备加密

STEP 5 | 验证您的 WildFire 设备是否正常运行。

- 通过 CLI 查看 WildFire 集群状态
- 通过 Panorama 查看 WildFire 集群状态

STEP 6 | （可选）升级已加入集群的 WildFire 设备。

- 通过互联网连接本地升级集群
- 不通过互联网连接本地升级集群
- 通过互联网连接在 Panorama 上集中升级集群
- 不通过互联网连接在 Panorama 上集中升级集群

在 WildFire 设备上本地配置集群

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

在您本地配置 WildFire 设备集群之前，将两个 WildFire 设备配置为高可用性控制器节点对，其他额外的 WildFire 设备作为工作节点，增加分析、存储量，以及集群的弹性。

如果 WildFire 设备是新的，检查 WildFire 入门的快速流程以确保您完成基本步骤，如确认您的 WildFire 授权已激活，启用日志记录、连接防火墙至 WildFire 设备，并配置基本 WildFire 功能。

如果您正在使用 Panorama 管理 WildFire 设备集群，则还可以在 Panorama 上集中配置 WildFire 集群。

要创建 *WildFire* 设备集群，您必须升级所有 WildFire 设备至 *PAN-OS 8.0.1* 或以上版本，这些设备是您希望在集群内部署的设备。在您想要添加至集群的各 *WildFire* 设备上，在 *WildFire* 设备 *CLI* 上运行 ***show system info | match version***，确保此设备正在运行 *PAN-OS 8.0.1* 或以上版本。

当您的 WildFire 设备可用时，执行相应的任务：

- 本地配置集群和添加节点
- 本地配置常规集群设置
- 从集群本地移除节点

本地配置集群和添加节点

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

当您添加节点至集群时，集群基于您为控制器节点配置的接口，自动设置节点之间的通讯。

STEP 1 | 确保您想要添加至集群的各 WildFire 设备运行 PAN-OS 8.0.1 或以上版本。

在各 WildFire 设备上，运行：

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

STEP 2 | 验证 WildFire 设备未分析样本，并处于独立状态（非其他集群成员）。

1. 在各设备上，显示设备是否正在分析样本：

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

不得有样本显示为挂起。所有样本都应处于完成状态。如果样本挂起，等待它们完成分析。挂起样本独立于恶意和非恶意样本显示。完成日期显示分析完成的日期和时间。

2. 在每台设备上，确认所有进程都正在运行：

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

3. 在各设备上，检查确保设备处于独立状态，且不属于某个集群。

```
admin@WF-500> show cluster membership Service Summary:
 wfpc signature Cluster name:address: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.
```

突出显示的行表示节点处于独立模式，并准备从独立设备转为集群节点。

这些事例中的 *12* 位序列号 *(000000000000)* 是通用示例，而非真实的序列号。您网络内的 *WildFire* 设备具有唯一的真实序列号。

STEP 3 | 配置主控制器节点。

包括配置节点作为 HA 对的主控制器、启用 HA 和定义设备用于 HA 控制链接和集群通讯、管理的接口。

1. 启用高可用性并配置控制链接接口链接至控制器备份节点，例如，在接口 eth3 上：

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

2. 配置设备作为主控制器节点：

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

3. （可选）配置控制器节点和控制器备份节点之间的备份高可用性接口，例如，在管理接口上：

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

4. 配置集群内通讯和管理的专属接口，包括指定集群名称和设置控制器节点的节点角色：

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

此示例使用 eth2 作为专属的集群通讯端口。

集群名称必须是最大长度为 63 个字符的有效子域名。仅允许使用小写字母和数字，连词符和点号不得出现在集群名称的开头和末尾处。

STEP 4 | 配置控制器备份节点。

包括配置节点作为 HA 对的备份控制器、启用 HA 和定义设备用于 HA 控制链接和集群通讯、管理的接口。

1. 启用高可用性并在主控制器节点使用的相同接口上，配置控制链接接口连接至主控制器节点（此示例中是 eth3）：

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

2. 配置设备作为控制器备份节点：

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

3. （建议）配置控制器备份节点和控制器节点之间的备份高可用性接口，例如，在管理接口上：

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

4. 配置集群内通讯和管理的专属接口，包括指定集群名称和设置控制器节点的节点角色：

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

STEP 5 | 在两个控制器节点上提交配置。

在各控制器节点上：

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

在两个控制器节点上提交配置以形成双节点集群。

STEP 6 | 验证主控制器节点上的配置。

在主控制器节点上：

```
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:JoinedCluster
 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.
```

提示 (`active-controller`) 和突出显示应用程序状态行显示节点处于控制器模式，就绪，并且是主控制器节点。

STEP 7 | 验证次控制器节点上的配置。

在次控制器节点上：

```
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:JoinedCluster  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.
```

提示 (`passive-controller`) 和突出显示应用程序状态行显示节点处于控制器模式，就绪，并且是备份控制器节点。

STEP 8 | 测试节点配置。

验证控制器节点 API 密钥可从任意位置查看：

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

应可以查看两台设备的 API 密钥。

STEP 9 | 在控制器节点上手动同步高可用性配置。

同步控制器节点确保配置匹配，且仅需要完成一次。高可用性配置同步完成后，控制器节点保持配置同步，且您无需再次同步。

1. 在主控制器节点上，同步高可用性配置至远程对端控制器节点：

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

如果主控制器节点配置和控制器备份节点配置不匹配，主控制器节点上的配置将覆盖控制器备份节点上的配置。

2. 提交配置：

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

STEP 10 | 验证集群正常运行。

要验证防火墙相关信息，您必须通过选择 ***Device***（设备） > ***Setup***（设置） > ***WildFire***和编辑 ***General Settings***（常规设置） 指向节点，以先连接至少一个防火墙至集群节点。

1. 显示集群对端以确保两个控制器均为集群成员：

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

2. 显示来自两个节点的 API 密钥（如果您创建了 API 密钥），来自任一控制器节点：

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

3. 从任一控制器节点访问样本：

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

4. 防火墙可以注册并上传文件至两个节点。确认防火墙已成功转发样本。
5. 两个节点可以下载并分析文件。
6. 集群创建后所有分析的文件显示两个存储位置，每个节点一个。

STEP 11 | （可选）配置工作节点并添加至集群。

工作节点使用控制器节点设置，因此集群配置保持一致。您可以添加最多 18 个工作节点至集群，即一个集群最多 20 节点。

1. 在主控制器节点上，添加工作节点至控制器节点的工作节点列表：

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

<*ip*> 是您想要添加到集群的工作节点的集群管理接口 IP 地址。使用单独的命令添加各工作节点至集群。

2. 在控制器节点上提交配置：

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

3. 在您想要转为集群工作节点的 WildFire 设备上，配置集群以加入，设置集群通讯接口，并将设备转为工作模式：

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

集群通讯接口必须为相同的，控制器节点上从集通讯的指定接口。此示例中，`eth2` 是配置用于控制器节点上集群通讯的接口。

4. 在工作节点上提交配置：

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

5. 等待工作节点上的所有服务恢复。运行 **`show cluster membership`** 并检查 `Applicationstatus`，当所有服务上线时，其显示所有服务和 `siggen-db`均为 `Ready` 状态。
6. 在任一集群控制器节点上，检查确保工作节点已添加：

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

您添加的工作节点显示在集群节点列表中。如果您意外添加了错误的 WildFire 设备至集群，您可以从集群本地移除节点。

STEP 12 | 在工作节点上验证配置。

1. 在工作节点上，检查确保节点模式字段显示该节点处于工作模式：

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

2. 验证防火墙可以在工作节点上注册，且该工作节点可以下载和分析文件。

本地配置常规集群设置

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

部分常规设置为可选，而部分常规设置通过默认值自动填充。建议至少对这些设置进行检查，以确保集群配置符合您的需要。常规设置包括：

- 连接至 WildFire 公共云和提交样本至公共云：
- 配置数据保留政策。
- 配置日志。
- 设置分析环境（最符合您环境的 VM 映像）和自定义分析环境，以适用于防火墙提交至 WildFire 的样本类型。
- 为 DNS 服务器、NTP 服务器等设置 IP 地址。

通过 CLI 配置 WildFire 设置，其位于集群主控制器节点上。剩余的集群节点使用集群控制器上配置的设置。

STEP 1 | 配置 WildFire 集群的常规设置。此过程与配置 WildFire 设备设置类似。

1. （建议）重置管理密码。
2. 配置管理接口设置。设置 WildFire 设备集群节点 IP 地址和默认网关。各 WildFire 设备集群节点必须在相同子网内有一个静态 IP 地址。还需设置 DNS 服务器 IP 地址。
3. 设置 WildFire 设备时钟。手动设置时钟或通过制定 NTP 服务器设置，并设置 NTP 服务器验证。
4. 选择设备分析文件使用的虚拟机映像。
5. （可选）允许其他用户管理 WildFire 设备。添加管理员账户并分配角色以管理集群。
6. 针对管理员访问配置 RADIUS 身份验证。

STEP 2 | （可选）连接集群至 WildFire 公共云并配置集群将使用的云服务。

如果商业原因未阻止您连接 WildFire 设备至公共 WildFire 云，将集群连接至云可提供下列优点：

- 使用云资源，通过不同方法在多种环境下执行样本分析。
- 在执行本地分析之前，自动查询云的判定以卸载集群工作。（默认禁用。）
- 从全球 WildFire 社区情报获得收益，并对其作出贡献。

此表中所述功能非集群指定，您也可以在独立的 *WildFire* 设备上配置这些功能。

1. 从所有连接的 WildFire 设备收集的情报获益：

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

WildFire 公共云服务器主机名称的默认值是 `wildfire-public-cloud`。您可以转发 WildFire 分析用的文件至任何公共 WildFire 云。

2. 如果您连接集群至 WildFire 公共云，配置是否在执行本地分析前，自动查询公共云判定。先查询公共云可以减少本地 WildFire 集群的负载：

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

3. 如果您连接集群至 WildFire 公共云，配置信息类型，并为该类型消息提交本地发现恶意软件或报告至 WildFire 公共云（诊断数据、关于恶意软件分析的 XML 报告、恶意软件样本）。如果您发送恶意软件样本，集群不会发送报告。

```
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 | （可选）配置控制器节点以通过 DNS 协议发布服务状态。

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

STEP 4 | （可选）为恶意软件和良性或灰色软件样本配置数据保留策略。

1. 选择保留不同数据类型的时间：

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

保留恶意样本的默认设置是无限（不删除）。保留非恶意（良性和灰色软件）样本的默认设置是 14 天。

STEP 5 | （可选）配置首选分析环境。

1. 如果您的分析环境基本上分析的是可执行样本或文档样本，您可以分配大部分的集群资源用于分析此类样本类型：

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

对于集群内的各 WildFire 设备：

- 默认 选项同时分析 16 个文档、10 个可移植可执行文件和 2 个电子邮件链接。
- 文档选项同时分析 25 个文档、1 个可移植可执行文件和 2 个电子邮件链接。
- 可执行文件选项同时分析 25 个可移植可执行文件、1 个文档和 2 个电子邮件链接。

您可以为集群内的各节点配置不同的首选分析环境。（如果您从 Panorama 管理集群，Panorama 可以设置整个集群的分析环境。）

STEP 6 | 配置节点分析设置。

1. （可选）设置内容更新以改进恶意软件分析。
2. 设置 VM 界面以启用集群来观察所分析样本尝试访问网络时表现的恶意行为。
3. （可选）启用本地前面和 URL 类别生成以生成 DNS 和防病毒签名，以及 URL 类别。

STEP 7 | 配置日志。

1. 配置 WildFire 提交情况日志的设置。

从集群本地移除节点

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

您可以通过本地 CLI 从集群移除节点。双节点集群移除节点的步骤与三个或三个以上节点集群的步骤不同。

从有三个或三个以上成员节点的集群移除工作节点。

1. 从工作节点 CLI 对工作节点解除授权：

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

   Decommission 命令仅适用于有三个或三个以上节点的集群。请勿使用 *decommission* 从双节点集群移除节点。

2. 确认节点接触授权是否已成功：

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

   在工作节点从集群被移除后，此命令报告 `decommission: success`。如果此命令未显示成功接触授权，等待几分钟以允许解除授权结束，然后再次运行此命令。

3. 从工作节点 CLI 删除集群配置：

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

4. 提交配置：

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

5. 检查所有程序是否正在运行：

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

6. 从控制器节点工作列表移除工作节点：

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

7. 提交配置：

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

8. 在控制器节点上，检查确保工作节点已被移除：

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

   您移除的工作节点不显示在集群节点列表中。

从双节点集群移除控制器节点。

正常情况下，在高可用性配置中各集群必须有两个控制器节点。但是，维护或切换控制器节点可能需要通过 CLI 从集群移除控制器节点：

1. 暂停您想要移除的控制器节点：

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

2. 在您想要移除的控制器节点上，删除高可用性配置。此示例显示了控制器备份节点的移除：

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

3. 删除集群配置：

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

4. 提交配置：

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

5. 等待服务恢复。运行 **show cluster membership** 并检查 Application status，当所有服务上线时，其显示所有服务和 siggen-db 均为 Ready 状态。Node mode 应为 stand_alone。
6. 在剩余集群节点上，检查确保节点已被移除：

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

您移除的控制器节点不显示在集群节点列表中。

7. 如果您有另一个就绪的 WildFire 设备，尽快将其添加至集群以恢复高可用性（本地配置集群和添加节点）。

如果您没有其他就绪的更换移除集群节点用 WildFire 设备，您应从剩余集群移除高可用性和集群配置，因为不建议使用单节点集群，且这样无法提供高可用性。将单台 WildFire 设备作为独立设备管理而非单节点集群管理效果更好。

要从剩余节点移除高可用性和集群配置（此示例中是主控制器节点）：

```
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
```

等待服务恢复。运行 **show cluster membership** 并检查 Application status，当所有服务上线时，其显示所有服务和 siggen-db 均为 Ready 状态。Node mode 应为 stand_alone。

配置 WildFire 设备到设备加密

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

您可以在集群内部署的设备之间加密 WildFire 通信。当 WildFire 设备与管理设备和 WildFire 集群对等设备之间进行通信时，默认通过明文发送数据。您可以通过 IKE/IPsec 协议使用预定义证书或自定义证书来对 WildFire 对等设备之间的连接进行身份验证。预定义证书符合当前 FIPS/CC/UCAPL 批准的证书和合规要求。相反，如果您想使用自定义证书，则必须选择 FIPS/CC/UCAPL 合规证书，否则您将无法导入证书。

您可以使用 WildFire CLI 本地配置 WildFire 设备到设备加密，也可以通过 Panorama 集中配置 WildFire 设备到设备加密。请记住，给定集群内的所有 WildFire 设备必须运行支持加密通信的 PAN-OS 版本。

如果您的集群中的 *WildFire* 设备使用 *FIPS/CC* 模式，则应使用预定义证书自动启用加密。

根据您想要部署的设备到设备加密的方式，可以执行以下任务之一：

- 使用预定义证书在 Panorama 上集中配置设备到设备加密
- 使用自定义证书在 Panorama 上集中配置设备到设备加密
- 通过 CLI 使用预定义证书对设备到设备加密进行配置
- 通过 CLI 使用自定义证书对设备到设备加密进行配置

通过 CLI 使用预定义证书对设备到设备加密进行配置

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

通过 CLI 对设备到设备加密进行配置时，您必须从指定为主动控制器的 WildFire 设备发出所有命令。配置更改将主动分发给被动控制器。如果您正在操作具有 3 个或以上节点的集群，则还必须对具有主动控制器相同设置，且充当服务器节点的 WildFire 集群进行配置。

STEP 1 | 将每个受管 Wildfire 设备 升级 到 PAN-OS 9.0。

STEP 2 | 检验您的 WildFire 设备集群是否已正确配置，且在正常状态下运行。

STEP 3 | 启用指定为主动控制器的 WildFire 设备上的安全集群通信。

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

STEP 4 | （推荐）启用 HA 流量加密。该设置（可选）可对 HA 对之间的 HA 流量进行加密，也是 Palo Alto Networks 推荐的最佳做法。

在 *FIPS/CC* 模式下运行时，不得禁用 *HA* 流量加密。

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

STEP 5 | （仅限具有 3 个或以上节点的设备集群）对集群中注册的第三个 WildFire 设备服务器节点重复步骤 2-4。

通过 CLI 使用自定义证书对设备到设备加密进行配置

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

通过 CLI 对设备到设备加密进行配置时，您必须从指定为主动控制器的 WildFire 设备发出所有命令。配置更改将主动分发给被动控制器。如果您正在操作具有 3 个或以上节点的集群，则还必须对具有主动控制器相同设置，且充当服务器节点的 WildFire 集群进行配置。

STEP 1 | 将每个受管 Wildfire 设备 升级 到 PAN-OS 9.0。

STEP 2 | 检验您的 WildFire 设备集群是否已正确配置，且在正常状态下运行。

STEP 3 | 使用私钥或其 CA 证书导入（或生成）证书。请记住，如果您先前已使用自定义证书完成 WildFire 设备和防火墙配置为进行安全通信，则还可以使用该自定义证书来实现 WildFire 设备之间的安全通信.

1. 要导入自定义证书，请从 WildFire 设备 CLI 输入以下命令：**scp import certificate from <value> file <value> remote-port <1-65535> source-ip <ip/netmask> certificate-name <value> passphrase <value> format <value>**
2. 要生成自定义证书，请从 WildFire 设备 CLI 输入以下内容：**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 | 导入包含服务器证书和私钥的 WildFire 设备密钥对。

```
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 | 配置并指定 SSL/TLS 配置文件，以定义 WildFire 设备用于 SSL/TLS 服务的证书和协议。

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

1. 创建 SSL/TLS 配置文件。

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

2. 指定自定义证书。

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

3. 定义 SSL/TLS 范围。

   ```
   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. 指定 SSL/TLS 配置文件。此 SSL/TLS 服务配置文件适用于 WildFire 设备之间，以及 WildFire 对等设备之间所有连接。

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

STEP 6 | 配置并指定证书配置文件，以定义 WildFire 设备用于 SSL/TLS 服务的证书和协议。

1. 创建证书配置文件。

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

2. （可选）设置主题名称（共用名）或主题备用名称。

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

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

3. （可选）设置用户域。

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

4. 配置 CA。

```
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. 指定证书配置文件。

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

STEP 7 | 导入证书和私钥对。

STEP 8 | 在 Panorama 上配置防火墙 安全通行设置，将 WildFire 设备集群与防火墙自定义证书相关联。这便为防火墙和 WildFire 设备集群之间创建一条安全通信通道。如果您已成功配置防火墙和 WildFire 设备集群之间的安全通信，且正在使用现有的自定义证书，请前进至步骤 9。

1. 选择 **Device**（设备） > **Certificate Management**（证书管理） > **Certificate Profile**（证书配置文件）。
2. 配置证书配置文件。
3. 选择 **Device**（设备） > **Setup**（设置） > **Management**（管理） > **Secure Communication Settings**（安全通信设置），单击 **Secure Communication Settings**（安全通信设置） 中的 **Edit**（编辑） 图标，以便配置防火墙自定义证书设置。
4. 从相应的下拉列表中选择 **Certificate Type**（证书类型）、 **Certificate**（证书） 和 **Certificate Profile**（证书配置文件），然后进行配置，以便使用在步骤 2 中创建的自定义证书。
5. 在自定义通信中，选择 **WildFire Communication**（**WildFire** 通信）。
6. 单击 **OK**（确定）。

STEP 9 | 禁止使用预定义证书。

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

STEP 10 | 指定用于自定义证书中找到的身份验证的 DNS 名称（通常是主题名称或主题备用名称）。例如，默认域名为 **wfpc.service.mycluster.paloaltonetworks.com**。

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

STEP 11 | （仅限具有 3 个或以上节点的设备集群）对集群中注册的第三个 WildFire 设备服务器节点重复步骤 2-10。

监控 WildFire 集群

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

您可以通过 CLI 或 Panorama 检查您的 WildFire 集群操作状态。这允许您验证给定节点上运行的应用程序和服务是否正常运行。为了让 WildFire 集群正常运行，必须在各节点上激活相应的服务和应用程序，且必须为正常状态。在这些参数以外运行的集群可能未在最优条件下运行，或可能代表着其他问题和配置问题。

CLI 显示无法从 *Panorama* 获得的信息。当对集群相关问题进行故障排查时，强烈建议使用 *WildFire CLI*。

您可以通过从 WildFire CLI 执行显示命令查看 WildFire 控制器节点的当前状态。命令显示配置详情、当前运行在设备上的应用程序和服务，以及状态/错误消息。您可以将这些详情用于确定您的集群状态。查看状态不会中断任何 WildFire 服务并随时可以运行。

有关监控 WildFire 设备的详细信息，请参阅以下部分：

- 通过 CLI 查看 WildFire 集群状态
- 通过 Panorama 查看 WildFire 集群状态
- WildFire 应用程序状态
- WildFire 服务状态

通过 CLI 查看 WildFire 集群状态

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

要确认您的 WildFire 集群在正常操作参数内运行，您必须执行下列显示命令：

- **show cluster controller**—显示主动/被动 WildFire 集群节点状态。
- **show cluster all-peers**—显示关于给定 WildFire 集群内所有成员的信息。
- **show cluster membership**—为集群和独立节点显示 WildFire 设备信息。
- **show cluster data-migration-status**—显示数据迁移过程的当前状态。
- **show log system**—显示 WildFire 事件日志，包括系统状态详细信息。

STEP 1 | 在 WildFire 设备控制器节点上，运行：

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

正常的 WildFire 集群显示下列详细信息：

- 设备加入的集群名称，及其配置角色。
- 当内部集群接口功能正常时，`K/V API online status` 显示 `True`。`False` 状态表示节点配置不当或出现网络问题。
- `Task processing` 在主动控制器（主）上显示 `True` 并且在被动控制器（备份）上显示 `False`。
- 集群内所有 WildFire 节点的 IP 地址列于 `App Service Avail` 下。
- 最多三个 `Good Core Servers`。`Good Core Servers` 数量取决于集群上运行的节点数。如果集群内有第三个节点正在运行，其自动被配置为服务器节点，以最大化集群完整性。
- 无 `Suspended Nodes`。
- `Current Task` 提供关于集群层级操作的背景信息，如重启、解除授权以及暂停任务。

下列示例展示了双节点 WildFire 集群内配置的，正常状态下主动控制器输出：

```
Cluster name:WildFire_Cluster K/V API online:True Task
 processing: on Active Controller:True DNS Advertisement:App
 Service DNS Name:App Service Avail:2.2.2.14, 2.2.2.15 Core
 Servers:009701000026:2.2.2.15 009701000043:2.2.2.14 Good Core
 Servers:2 Suspended Nodes:Current Task: * Showing latest completed
 task Request: startup from qa14 (009701000043/80025) at 2017-09-18
 21:43:34 UTC null Response: permit by qa15 at 2017-09-18 21:45:15
 UTC 1/2 core servers available.Finished: success at 2017-09-18
 21:43:47 UTC
```

STEP 2 | 在 WildFire 设备控制器节点上，运行：

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

正常的 WildFire 集群显示下列详细信息：

- 关于集群内 WildFire 节点的常规信息列于 `Address`、`Mode`、`Server`、`Node` 和 `Name` 下。
- 所有 WildFire 集群节点正在运行 `wfpc` 服务，这是一种内部文件样本分析服务。
- 作为主动、被动节点或服务器运行的节点在状态旁会显示已应用服务器角色。如果已将节点配置为服务器，但未作为服务器运行，状态旁会显示已分配服务器角色。

  在 *3* 节点部署中，第三个服务器节点被归类为工作节点。

- 最近移除的节点可能存在，但显示为 `Disconnected`。断开连接的节点从集群节点列表中移除需要数天。
- 主动控制器节点显示 `siggen-db:ReadyMaster`。
- 被动控制器节点显示 `siggen-db:ReadySlave`。

  关于常规 *WildFire* 应用程序和服务状态详情的更多信息，请参阅 WildFire 应用程序状态和 WildFire 服务状态。

- `Diag report` 显示集群系统事件和错误消息：

错误消息	说明
`Unreachable`	此节点无法从集群控制器访问。
`Unexpected member`	此节点不是集群配置的一部分。此节点可能最近从集群配置中被删除，或配置不当。
`Left cluster`	此节点无法继续从集群控制器访问。
`Incorrect cluster name`	此节点集群名称配置错误。
`Connectivity unstable`	此节点与集群控制器的连接不稳定。
`Connectivity lost`	此节点与集群控制器的连接丢失。
`Unexpected server serial number`	检测到意外的服务器节点。

下列示例展示了正常状态下运行的 3 节点 WildFire 集群：

```
Address Mode Server Node Name ------- ---- ------ ---------
 2.2.2.15 controller Self True qa15 Service: infra signature
 wfcore wfpc Status:Connected, Server role applied Changed:Mon, 18
```

```
 Sep 2017 15:37:40 -0700 WF App: global-db-service:JoinedCluster
 wildfire-apps-service:Stopped global-queue-service:JoinedCluster
 wildfire-management-service:Done siggen-db:ReadySlave 2.2.2.14
 controller Peer True qa14 Service: infra signature wfcore wfpc
 Status:Connected, Server role applied Changed:Mon, 18 Sep 2017
 15:37:40 -0700 WF App: global-db-service: commit-lock wildfire-
apps-service:Stopped global-queue-service:ReadyStandalone wildfire-
management-service:Done siggen-db:ReadyMaster 2.2.2.16 worker True
 wf6240 Service: infra wfcore wfpc Status:Connected, Server role
 applied Changed:Wed, 22 Feb 2017 11:11:15 -0800 WF App: wildfire-
apps-service:Ready global-db-service:JoinedCluster global-queue-
service:JoinedCluster local-db-service:DataMigrationFailed Diag
 report:2.2.2.14: reported leader '2.2.2.15', age 0. 2.2.2.15:
 local node passed sanity check.
```

STEP 3 | 在 WildFire 设备控制器节点上，运行：

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

正常的 WildFire 集群显示下列详细信息：

- 常规 WildFire 设备配置详情，如集群名称、设备 IP 地址、序列号等。
- `Server role` 表示 WildFire 设备是否作为集群服务器运行。集群服务器运行额外的基础架构应用程序和服务。每个集群您最多可以有三台服务器。
- `Node mode` 描述了 WildFire 设备的角色。加入集群的 WildFire 设备可以是 `controller` 或 `worker` 节点，具体取决于您的配置和您部署中的节点数。非集群一部分的设备显示 `stand_alone`。
- 基于集群节点角色操作下列 `Services`：

节点类型	节点上运行的服务
控制器节点（主动或被动）	• 结构 • wfpc • 签名 • wfcore
服务器节点	• 结构 • wfpc • wfcore
工作节点	• 结构 • wfpc

- `HA priority` 根据其配置角色显示主要或次要，但此设定与设备当前高可用状态无关。

- `Work queue status` 显示了样本分析积压工作以及正被分析的样本。这也可以表示某台 WildFire 设备接收的负载量。

关于 *WildFire* 应用程序和服务状态详情的更多信息，请参阅 WildFire 应用程序状态和 WildFire 服务状态。

下列示例展示了正常状态下运行的 WildFire 控制器：

```
Service Summary: wfpc signature Cluster name: qa-auto-0ut1
 Address:2.2.2.15 Host name: qa15 Node name: wfpc-009701000026-
internal Serial number:009701000026 Node mode: controller Server
 role:True HA priority: secondary Last changed:Fri, 22 Sep 2017
 11:30:47 -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:Ready Work queue status: sample anaysis queued:0 sample
 anaysis running:0 sample copy queued:0 sample copy running:0 Diag
 report:2.2.2.14: reported leader '2.2.2.15', age 0. 2.2.2.15:
 local node passed sanity check.
```

STEP 4 | 在 WildFire 设备控制器节点上，运行：

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

WildFire 设备显示以下数据迁移详细信息：

- 数据迁移时，请勿转发文件到 WildFire 设备集群。数据迁移完成时，会显示完成时间戳。
- 拓扑更改为 WildFire 集群（例如，添加或删除节点和更改节点角色）后，将触发数据迁移事件。
- 升级至新版 WildFire 时，可以进行数据迁移。升级后，请务必检查 WildFire 集群的运行状态，以验证功能是否正常。

以下示例显示了 WildFire 设备集群中的数据迁移过程：

```
admin@WF-500(active-controller)>: show data-migration-status 100%
 completed on Mon Sep 9 21:44:48 PDT 2019
```

STEP 5 | 在 WildFire 设备主动、被动和服务器节点上，运行：

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

该命令会按从最新到最旧的顺序显示所有归类为防火墙设备子类型的 WildFire 日志事件。

- 您必须向集群中的所有节点发出该命令。例如，如果您正在操作 3 个节点集群，则必须验证主动控制器、被动控制器和服务器节点上的状态。
- WildFire 设备 CLI 返回的日志消息可以包括许多子类型。您可以根据常见子类型关键字过滤日志。使用以下命令参数并根据特定组件进行过滤：
  - global-queue—**matchqueue**, for example **show log system directionequal backward | match queue**
  - global-database—**match global**, for example **show log system direction equal backward | matchglobal**
  - signature-generation—**match signature**, for example **show log system direction equal backward| match signature**
- 正常运行的 WildFire 设备会返回有关 2 个节点集群中每个节点的以下状态。正常运行的 WildFire 集群节点基于设备角色具有不同的状态读数。

  使用以下检查清单验证 WildFire 设备服务是否在集群部署中正常运行。

  - 主动控制器

组件	主动控制器状态
global-queue	☐ infowildfire cluster 0 Global queue (rabbitmq) cluster formation succeeded withstatus ReadyLeader ☐ info general general 0 Setup policy for global-queue service
global-database	☐ infogeneral general 0 I'm cluster leader, bootstrap for global-db service ☐ info general general 0 Setup policy for global-queue service
signature-generation	☐ infowildfir cluster 0 Signature generation service status set to ReadyMaster ☐ info wildfir cluster 0 Signature generationservice status set to ReadyMaster

组件	主动控制器状态

WildFire 设备返回的日志信息按从新到旧的顺序显示。如果您不使用以上步骤中所示的命令参数 ***direction equal backward***，则 *WildFire* 设备 *CLI* 会按从最旧到最新的顺序返回日志消息。

- 被动控制器

组件	被动控制器状态示例
global-queue	infogeneral general 0 Setup policy for global-queue service info wildfire cluster 0 Global queue (rabbitmq)cluster formation succeeded with status JoinedCluster info general general 0 Join cluster for global-queueservice - succeeded info general general 0 Setup policy for global-queue service
global-database	infogeneral general 0 Setup policy for global-queue service info general general 0 Restore applications:done, For global-db bootstrap and join cluster info general general 0 Start vm_mgr, For global-dbbootstrap and join cluster info general general 0 Start uwsgi, For global-dbbootstrap and join cluster info general general 0 Start wf_services, Forglobal-db bootstrap and join cluster info general general 0 Suspend applications:done, For global-db bootstrap and join cluster info general general 0 Stop vm_mgr, For global-dbbootstrap and join cluster info general general 0 Stop uwsgi, For global-dbbootstrap and join cluster info general general 0 Stop wf_services, Forglobal-db bootstrap and join cluster

组件	被动控制器状态示例
	❑ info general general 0 Bootstrap and join clusterfor global-db service
signature-generation	❑ infowildfir cluster 0 Signature generation service status set to ReadySlave ❑ info wildfir cluster 0 Signature generationservice status set to ReadySlave

WildFire 设备返回的日志信息按从新到旧的顺序显示。如果您不使用以上步骤中所示的命令参数 ***direction equal backward***，则 *WildFire* 设备 *CLI* 会按从最旧到最新的顺序返回日志消息。

- 正常运行的 WildFire 设备会返回有关 3 个节点集群中每个节点的以下状态。正常运行的 WildFire 集群节点基于设备角色具有不同的状态读数。

  使用以下检查清单验证 WildFire 设备服务是否在集群部署中正常运行。

  - 主动控制器

组件	主动控制器状态
global-queue	❑ infowildfire cluster 0 Global queue (rabbitmq) cluster formation succeeded withstatus JoinedCluster ❑ info general general 0 Join cluster for global-queueservice - succeeded ❑ info general general 0 Setup policy for global-queue service
global-database	❑ infogeneral general 0 Restore applications: done, For global-db bootstrap andjoin cluster ❑ info general general 0 Start vm_mgr, For global-dbbootstrap and join cluster ❑ info general general 0 Start uwsgi, For global-dbbootstrap and join cluster ❑ info general general 0 Start wf_services, Forglobal-db bootstrap and join cluster ❑ info general general 0 Suspend applications:done, For global-db bootstrap and join cluster ❑ info general general 0 Stop vm_mgr, For global-dbbootstrap and join cluster

组件	主动控制器状态
	❑ info general general 0 Stop uwsgi, For global-dbbootstrap and join cluster ❑ info general general 0 Stop wf_services, Forglobal-db bootstrap and join cluster ❑ 2019/07/19 14:40:19 info general general 0Bootstrap and join cluster for global-db service
signature-generation	❑ infowildfire cluster 0 Signature generation service status set to ReadyMaster

WildFire 设备返回的日志信息按从新到旧的顺序显示。如果您不使用以上步骤中所示的命令参数 ***direction equal backward***，则 *WildFire* 设备 *CLI* 会按从最旧到最新的顺序返回日志消息。

- 被动控制器

组件	被动控制器状态
global-queue	❑ infogeneral general 0 Setup policy for global-queue service ❑ info general general 0 Setup policy for global-queue service ❑ info wildfire cluster 0 Global queue (rabbitmq)cluster formation succeeded with status ReadyLeader ❑ info general general 0 Setup policy for global-queue service
global-database	❑ infogeneral general 0 I'm cluster leader, bootstrap for global-db service ❑ info general general 0 Setup policy for global-queue service
signature-generation	❑ infowildfire cluster 0 Signature generation service status set to ReadySlave ❑ info wildfire cluster 0 Signature generationservice status set to ReadySlave

组件	被动控制器状态

WildFire 设备返回的日志信息按从最新到最旧的顺序显示。如果您不使用以上步骤中所示的命令参数 ***direction equal backward***，则 *WildFire* 设备 *CLI* 会按从最旧到最新的顺序返回日志消息。

- 服务器节点

组件	服务器节点状态
global-queue	❑ infowildfire cluster 0 Global queue (rabbitmq) cluster formation succeeded withstatus JoinedCluster ❑ info general general 0 Join cluster for global-queueservice - succeeded ❑ info general general 0 Setup policy for global-queue service ❑ info wildfire cluster 0 Global queue (rabbitmq)cluster formation succeeded with status StandbyAsWorker
global-database	❑ infogeneral general 0 Restore applications: done, For global-db bootstrap andjoin cluster ❑ info general general 0 Start vm_mgr, For global-dbbootstrap and join cluster ❑ info general general 0 Start uwsgi, For global-dbbootstrap and join cluster ❑ info general general 0 Start wf_services, Forglobal-db bootstrap and join cluster ❑ info general general 0 Suspend applications:done, For global-db bootstrap and join cluster ❑ info general general 0 Stop vm_mgr, For global-dbbootstrap and join cluster ❑ info general general 0 Stop uwsgi, For global-dbbootstrap and join cluster ❑ info general general 0 Stop wf_services, Forglobal-db bootstrap and join cluster ❑ 2019/07/19 14:32:50 info general general 0Promote worker node and join cluster for global-db service

组件	服务器节点状态
signature-generation	❑ infowildfire cluster 0 Signature generation service status set to Stopped ❑ critical wildfire cluster 0 Signature DataMigrationDone

WildFire 设备返回的日志信息按从新到旧的顺序显示。如果您不使用以上步骤中所示的命令参数 ***direction equal backward***，则 *WildFire* 设备 *CLI* 会按从最旧到最新的顺序返回日志消息。

WildFire 应用程序状态

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

WildFire 设备运行一系列的内部应用程序，以管理和协调样本数据的处理。在查看 WildFire 设备集群状态时，显示这些应用程序及其必备项状态。

下表显示了集群组件、目的和状态条件：

名称	说明	可能的状态条件	定义
global-db-service	此应用程序数据库用于存储 WildFire 分析数据。	AcquiringSessionSpinLock	等待会话旋转锁，直至获取锁或超时。
		引导	样本数据库应用程序目前处于引导状态。
		BootstrappingNoMeet	本地样本数据库服务启动，且未与其他 WildFire 设备形成集群。
		FailedToBecomeWorker	以工作节点加入集群失败。
		FailedToBootstrap	引导进程失败。
		FailedToJoinCluster	加入集群失败。
		FailedToStartServices	内部数据库服务启动失败。

名称	说明	可能的状态条件	定义
		MaintenanceDecommission	开始数据库服务的解除授权进程。
		MaintenanceDecommissionDone	数据库服务已解除授权。
		MaintenanceFailover	启动进程以降级本地服务和故障转移备份副本。
		MaintenanceFailed	服务故障转移失败。
		MaintenanceFailoverDone	服务故障转移完成。
		MaintenanceRecoverFromSplitbrain	如果 WildFire 设备当前处于裂脑模式，数据库服务状态将在服务开始时设置为 MaintenanceRecoverFromSplitbrain。
		MaintenanceSuspend	由于用户发出下列命令之一，数据库服务被暂停：调试集群暂停或请求集群解除授权。
		MaintenanceSuspendDone	数据库服务已完成暂停进程。
		DataMigration	本地数据库内容正与主数据库合并。当 WildFire 设备加入集群时发生此情况。
		DataMigrationDone	数据迁移进程完成。
		DataMigrationFailed	数据迁移进程失败。
		JoinedCluster	本地数据库服务已加入集群。
		Ready	数据库服务处于就绪状态。
		ReadyLeader	数据库服务处于就绪状态，且此设备被设为引导设备。

名称	说明	可能的状态条件	定义
		ReadyStandalone	数据库服务处于就绪状态，且此设备正作为独立设备运行。
		Splitbrain	已检测到裂脑状态，且数据库服务已进入裂脑模式。服务即将转换至 ReadyStandalone。
		StandbyAsWorker	工作节点数据库服务处于待机状态。
		WaitingforLeaderReady	本地节点正等待加入引导节点。

名称	说明	可能的状态条件	定义
global-queue-service	处理发送给 WildFire 进行分析的样本的管理和优先。	引导	队列服务应用程序目前处于引导状态。
		FailedToBecomeWorker	以工作节点加入集群失败。
		FailedToBootstrap	引导进程失败。
		FailedToJoinCluster	加入集群失败。
		FailedToStartServices	内部队列服务启动失败。
		MaintenanceDecommission	开始队列服务的解除授权进程。
		MaintenanceDecommissionDone	队列服务已解除授权。
		MaintenanceFailover	启动进程以降级本地服务和故障转移备份副本。
		MaintenanceFailed	服务故障转移失败。
		MaintenanceFailoverDone	服务故障转移完成。

名称	说明	可能的状态条件	定义
		MaintenanceRecoverFromSplitbrain	如果 WildFire 设备当前处于脑裂模式，队列服务状态将被设为
		MaintenanceSuspend	由于用户发出下列命令之一，队列服务被暂停：调试集群暂停或请求集群解除授权。
		MaintenanceSuspendDone	队列服务已完成暂停进程。
		JoinedCluster	队列服务已加入集群。
		Ready	队列服务处于就绪状态。
		ReadyLeader	队列服务处于就绪状态，且此设备被设为引导设备。
		ReadyStandalone	队列服务处于就绪状态，且此设备正作为独立设备运行。
		Splitbrain	已检测到裂脑状态，且队列服务已进入裂脑模式。服务即将转换至 ReadyStandalone。
		StandbyAsWorker	工作节点队列服务处于待机状态。

名称	说明	可能的状态条件	定义
siggen-db	生成 WildFire 专有签名和分析样本。	DatabaseFailover	当发生高可用性故障转移时，被动控制器变为主动控制器。被动控制器中的签名服务变为主导，且状态被设为 DatabaseFailover。
		DatabaseFailoverFaild	签名数据库故障转移失败。

名称	说明	可能的状态条件	定义
		DataMigration	本地签名数据库内容正与主数据库合并。当 WildFire 设备加入集群时发生此情况。
		DataMigrationDone	数据迁移进程完成。
		DataMigrationFailed	数据迁移进程失败。
		已注销	签名数据库服务被注销。
		MaintenanceDecommission	开始签名数据库服务的解除授权进程。
		MaintenanceDecommissionDone	队列服务已解除授权。
		MaintenanceFailover	启动进程以降级本地服务和故障转移备份副本。
		MaintenanceFailoverDone	服务故障转移完成。
		MaintenanceSuspend	由于用户发出下列命令之一，签名数据库服务被暂停：调试集群暂停或请求集群解除授权。
		MaintenanceSuspendDone	签名数据库服务已完成暂停进程。
		MigrateMalwareDatabase	当 PAN-OS 从版本 7.1 升级至 8.0 时，样本数据被转为不同格式。这些状态表示了数据迁移程序的进度。
		MigrateSiggenDatabaseStage1	
		MigrateSiggenDatabaseStage2	
		MigrateSiggenDatabaseStage3	
		Ready	签名数据库服务处于就绪状态。
		ReadyMaster	签名数据库服务处于主模式，且在主动控制器上运行。

名称	说明	可能的状态条件	定义
		ReadySlave	签名数据库服务处于备份模式，且在被动控制器上运行。
		ReadyStandalone	签名数据库服务处于就绪状态，且此设备正作为独立设备运行。
		Splitbrain	已检测到裂脑状态，且签名数据库服务已进入裂脑模式。服务即将转换至 ReadyStandalone。
		已停止	签名数据库服务已在设备上停止。

名称	说明	可能的状态条件	定义
wildfire-management-service	WildFire 工作模式管理服务。	运行	WildFire 管理服务处于操作状态。
		完成	WildFire 管理服务已完成运行。

名称	说明	可能的状态条件	定义
wildfire-apps-service	WildFire 基础架构应用程序。	已注销	WildFire 应用程序服务已注销。
		Ready	WildFire 应用程序服务处于就绪状态。
		还原	WildFire 应用程序服务已完成维护程序。
		正在计划	WildFire 应用程序服务处于计划状态。
		设置样本存储	当 WildFire 从 7.1 倍升级至 8.0 时，此 WildFire 应用程序服务运行。

名称	说明	可能的状态条件	定义
		已停止	WildFire 应用程序服务已在设备上停止。
		挂起	WildFire 应用程序服务已暂停以进行维护。

WildFire 服务状态

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

WildFire 设备运行一系列的内部服务，以管理和协调样本数据的处理。在查看 WildFire 设备集群状态时，显示这些服务及其必备项状态。

以下列表显示了 WildFire 服务组件、说明、状态条件和其他相关详细信息：

名称	目的	受影响节点	状态
结构	表示 WildFire 集群基础架构服务正在给定的节点上运行。	所有节点	服务运行时，在 CLI 状态屏幕中显示。如果这些服务未向给定的节点提供，请验证设备的配置。
`wfpc`	表示文件样本分析服务（WildFire 专有云）可以进行文件分析和报告生成。		
签名	生成 WildFire 专有签名和分析样本。	主动（主要）/被动（备份）控制器	
`wfcore`	表示此节点正作为 WildFire 集群基础架构服务的服务器运行。	服务器节点	

在集群内升级 WildFire 设备

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

您可以使用 CLI 单独升级加入集群的 WildFire 设备，或使用 Panorama 按组升级集群。

根据 WildFire 设备分析和存储的样本数量，升级设备软件的时间也有所不同；这是由于升级需要迁移所有恶意软件样本和 14 天的良性样本。为每台在生产环境下使用的 WildFire 设备留出 30 至 60 分钟。

- 集群内的所有节点必须运行相同版本的操作系统。
- *Panorama* 可以管理运行 *PAN-OS* 软件版本 *8.0.1* 或以上的 *WildFire* 设备和设备集群。
- 确保设备连接至可靠的电源。升级时断电可能导致设备无法使用。

根据您的部署，执行下列任务之一，以升级您的 WildFire 集群：

- 通过互联网连接在 Panorama 上集中升级集群
- 不通过互联网连接在 Panorama 上集中升级集群
- 通过互联网连接本地升级集群
- 不通过互联网连接本地升级集群

通过互联网连接本地升级集群

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

要本地升级集群，您必须单独升级加入集群的各 WildFire 设备。当设备升级完成时，其自动重新加入之前被指派的集群。

STEP 1 | 临时暂停样本分析。

1. 停止防火墙转发任何新样本至 WildFire 设备。
   1. 登录到防火墙 Web 界面。
   2. 选择**Device**（设备） > **Setup**（设置） > **WildFire**，然后编辑**General Settings (**常规设置**)**。
   3. 清空 **WildFire Private Cloud**（**WildFire** 专有云）字段。
   4. 单击 **OK**（确定）和 **Commit**（提交）。

2. 确认防火墙提交至设备的样本分析已完成：

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

如果您不想要等待 *WildFire* 设备完成对最近提交样本的分析，您可以直接继续下一步。但是，需要考虑到 *WildFire* 设备可能漏掉分析队列的挂起样本。

STEP 2 | 安装最新的 WildFire 设备内容更新。该更新为设备提供最新的威胁信息，以准确检测恶意软件。

在旧设备上，此过程最多可能需要 *6* 小时或更长时间才能完成。

1. 验证是否正在 WildFire 设备上运行最新的内容更新。

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

2. 下载最新的 WildFire 内容更新包。

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

如果您未直接连接 Palo Alto Networks 更新服务器，您可以从启用 SCP 的服务器下载并安装 WildFire 内容更新。

3. 查看下载状态。

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

4. 下载完成后，安装更新。

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

STEP 3 | （升级到 PAN-OS 10.2.2 时需要）升级 WildFire 设备上的虚拟机映像。

1. 登录并访问 Palo Alto Networks 客户支持门户软件下载页面。通过转到 **Updates**（更新） > **Software Updates**（软件更新），您还可以从支持主页手动导航到软件下载页面。
2. 在软件更新页面中，选择 **WF-500 Guest VM Images** 文件并下载以下 VM 映像文件：

   Palo Alto Networks 定期更新虚拟机映像文件；因此，特定文件名会根据可用的版本而更改。请务必下载最新版本，文件名中的 *m-x.x.x* 表示版本号；此外，还可以交叉引用一个发布日期以帮助确定最新版本。

   - 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. 将 VM 映像上传到 WildFire 设备。
   1. 从 SCP 服务器导入虚拟机映像：

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

      例如：

      ```
      admin@WF-500>scp import wildfire-vm-image from
       user1@10.0.3.4:/tmp/WFWin7_64Addon1_m-1.0.1.7_64addon1
      ```
   2. 如需检查下载状态，请使用以下命令：

      ```
      admin@WF-500>show jobs all
      ```
   3. 对其余 VM 映像重复此操作。
4. 安装 VM 映像。
   1. ```
      admin@WF-500>request system wildfire-vm-image upgrade
       install file <vm_image_filename>
      ```
   2. 对其余 VM 映像重复此操作。
5. 确认已在 WildFire 设备上正确安装和启用 VM 映像。
   1. （可选）查看可用虚拟机映像的列表：

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

      输出显示可用的虚拟机映像。
   2. 提交配置：
      ```

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

3. 通过运行以下命令查看活动 VM 映像：

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

STEP 4 | 检验您想要安装的 WildFire 设备软件版本是否可用。

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

STEP 5 | 将 PAN-OS 10.2.2 软件版本下载到 WildFire 设备。

升级 WildFire 设备时，您不可跳过任何主要版本。例如，如果您想要从 PAN-OS 6.1 升级至 PAN-OS 7.1，您必须首先下载并安装版本 7.0。此过程中的示例演示如何升级到 PAN-OS 10.2.2。将 10.2.2 替换成目标升级版本。

下载 10.2.2 软件版本。

```
admin@WF-500(passive-controller)> request system software download
 version 10.2.2
```

如需检查下载状态，请使用以下命令

```
admin@WF-500(passive-controller)> show jobs all
```

STEP 6 | 确认所有服务正在运行。

```
admin@WF-500(passive-controller)> show system software status
```

STEP 7 | 安装 10.2.2 软件版本。

```
admin@WF-500(passive-controller)> request system software install
 version 10.2
```

STEP 8 | 完成软件升级。

1. 确认是否已完成升级。运行以下命令，然后查找作业类型 **Install** 和状态 **FIN**：

```
admin@WF-500(passive-controller)> show jobs all
 Enqueued Dequeued ID Type Status Result Completed
```

```
---------------------------------------------------- 14:53:15
14:53:15 5 Install FIN OK 14:53:19
```

2. 重启设备：

```
admin@WF-500(passive-controller)> request cluster reboot-
local-node
```

升级程序可能需要 *10* 分钟至一个小时以上，具体取决于 *WildFire* 设备上存储的样本数。

STEP 9 | 对群集中的每个 WildFire 工作器节点重复步骤 1-8。

STEP 10 | （可选）查看 WildFire 控制器节点上的重启任务状态。

在 WildFire 集群控制器上，运行以下命令，然后查找作业类型 **Install** 和状态 **FIN**：

```
admin@WF-500(active-controller)> show cluster task pending
```

STEP 11 | 检查 WildFire 设备是否继续，可继续样本分析。

1. 验证 sw 版本字段是否显示有升级的发行版本：

```
admin@WF-500(passive-controller)> show system info | match sw-
version
```

2. 确认所有程序正在运行。

```
admin@WF-500(passive-controller)> show system software status
```

3. 确认自动提交 (**AutoCom**) 工作已完成：

```
admin@WF-500(passive-controller)> show jobs all
```

4. 确认数据迁移已成功完成。运行 `show cluster data-migration-status`以查看数据库合并进度。数据合并完成后，完成时间戳将会显示：

```
100% completed on Mon Sep 9 21:44:48 PDT 2019
```

数据合并市场取决于 *WildFire* 设备上存储的数据量。确保至少留出几个小时用于恢复，因为数据合并可能是一个较长的过程。

不通过互联网连接本地升级集群

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

要本地升级集群，您必须单独升级加入集群的各 WildFire 设备。当设备升级完成时，其自动重新加入之前被指派的集群。

STEP 1 | 临时暂停样本分析。

1. 停止防火墙转发任何新样本至 WildFire 设备。
   1. 登录到防火墙 Web 界面。
   2. 选择**Device**（设备） > **Setup**（设置） > **WildFire**，然后编辑**General Settings (**常规设置**)**。
   3. 清空 **WildFire Private Cloud**（**WildFire** 专有云）字段。
   4. 单击 **OK**（确定）和 **Commit**（提交）。
2. 确认防火墙提交至设备的样本分析已完成：

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

如果您不想要等待 *WildFire* 设备完成对最近提交样本的分析，您可以直接继续下一步。但是，需要考虑到 *WildFire* 设备可能漏掉分析队列的挂起样本。

STEP 2 | 从更新服务器中检索内容更新文件。

1. 登录到 Palo Alto Networks 支持门户，然后单击**Dynamic Updates**（动态更新）。
2. 在“WildFire 设备”部分，找到最新 WildFire 设备内容更新，然后下载此更新。
3. 将内容更新文件复制到启用 SCP 的服务器，然后记下文件名和目录路径。

STEP 3 | 在 WildFire 设备上安装内容更新。

1. 登录到 WildFire 设备，然后从 SCP 服务器中下载内容更新文件：

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

例如：

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

如果 *SCP* 服务器是在非标准端口上运行，或者您需要指定源 *IP*，则还可以在 ***scp import*** 命令中定义这些选项。

2. 安装更新：

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

3. 查看安装的状态：

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

STEP 4 | 验证内容更新。

验证内容版本：

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

以下输出现在显示版本 2-253：

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

STEP 5 | （升级到 PAN-OS 10.2.2 时需要）升级 WildFire 设备上的虚拟机映像。

1. 登录并访问 Palo Alto Networks 客户支持门户软件下载页面。通过转到 **Updates**（更新） > **Software Updates**（软件更新），您还可以从支持主页手动导航到软件下载页面。
2. 在软件更新页面中，选择 **WF-500 Guest VM Images** 文件并下载以下 VM 映像文件：

   Palo Alto Networks 定期更新虚拟机映像文件；因此，特定文件名会根据可用的版本而更改。请务必下载最新版本，文件名中的 *m-x.x.x* 表示版本号；此外，还可以交叉引用一个发布日期以帮助确定最新版本。

   - 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. 将 VM 映像上传到 WildFire 设备。
   1. 从 SCP 服务器导入虚拟机映像：

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

      例如：

      ```
      admin@WF-500>scp import wildfire-vm-image from
       user1@10.0.3.4:/tmp/WFWin7_64Addon1_m-1.0.1.7_64addon1
      ```
   2. 如需检查下载状态，请使用以下命令：

      ```
      admin@WF-500>show jobs all
      ```
   3. 对其余 VM 映像重复此操作。
4. 安装 VM 映像。
   1. ```
      admin@WF-500>request system wildfire-vm-image upgrade
       install file <vm_image_filename>
      ```
   2. 对其余 VM 映像重复此操作。
5. 确认已在 WildFire 设备上正确安装和启用 VM 映像。
   1. （可选）查看可用虚拟机映像的列表：

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

      输出显示可用的虚拟机映像。
   2. 提交配置：
      ```

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

3. 通过运行以下命令来查看活动 VM 映像：

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

STEP 6 | 检验您想要安装的 WildFire 设备软件版本是否可用。

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

STEP 7 | 将 PAN-OS 10.2.2 软件版本下载到 WildFire 设备。

升级 WildFire 设备时，您不可跳过任何主要版本。例如，如果您想要从 PAN-OS 6.1 升级至 PAN-OS 7.1，您必须首先下载并安装版本 7.0。此过程中的示例演示如何升级到 PAN-OS 10.2.2。将 10.2.2 替换成目标升级版本。

下载 10.2.2 软件版本：

1. 导航到 Palo Alto Networks 支持站点，在工具部分，点击 **Software Updates**（软件更新）。
2. 将要安装的 WildFire 设备软件映像文件下载到运行 SCP 服务器软件的计算机。
3. 从 SCP 服务器导入软件映像：

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

例如：

```
admin@WF-500> scp import software from user1@10.0.3.4:/tmp/
WildFire_m-10.2.2
```

4. 如需检查下载状态，请使用以下命令：

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

STEP 8 | 确认所有服务正在运行。

```
admin@WF-500(passive-controller)> show system software status
```

STEP 9 | 安装 10.2.2 软件版本。

```
admin@WF-500(passive-controller)> request system software install
 version 10.2.2
```

STEP 10 | 完成软件升级。

1. 确认是否已完成升级。运行以下命令，然后查找作业类型 **Install** 和状态 **FIN**：

```
admin@WF-500(passive-controller)> show jobs all
 Enqueued Dequeued ID Type Status Result Completed
 ------------------------------------------------- 14:53:15
 14:53:15 5 Install FIN OK 14:53:19
```

2. 重启设备：

```
admin@WF-500(passive-controller)> request cluster reboot-
local-node
```

升级程序可能需要 *10* 分钟至一个小时以上，具体取决于 *WildFire* 设备上存储的样本数。

STEP 11 | 对群集中的每个 WildFire 工作器节点重复步骤 1-10。

STEP 12 | （可选）查看 WildFire 控制器节点上的重启任务状态。

在 WildFire 集群控制器上，运行以下命令，然后查找作业类型 **Install** 和状态 **FIN**：

```
admin@WF-500(active-controller)> show cluster task pending
```

STEP 13 | 检查 WildFire 设备是否继续，可继续样本分析。

1. 验证 sw 版本字段是否显示有升级的发行版本：

```
admin@WF-500(passive-controller)> show system info | match sw-
version
```

2. 确认所有程序正在运行。

```
admin@WF-500(passive-controller)> show system software status
```

3. 确认自动提交 (**AutoCom**) 工作已完成：

```
admin@WF-500(passive-controller)> show jobs all
```

4. 确认数据迁移已成功完成。运行 `show cluster data-migration-status`以查看数据库合并进度。数据合并完成后，完成时间戳将会显示：

```
100% completed on Mon Sep 9 21:44:48 PDT 2019
```

数据合并市场取决于 *WildFire* 设备上存储的数据量。确保至少留出几个小时用于恢复，因为数据合并可能是一个较长的过程。

对 WildFire 集群的故障排查

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

参阅以下主体以诊断并对 WildFire 集群问题进行故障排查：

- WildFire 裂脑状况故障排查

WildFire 裂脑状况故障排查

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

当一个节点（或两个高可用对等机）认定另一个未运行时，WildFire 双节点 HA（高可用性）集群出现裂脑状况。当由于网络连接或配置问题，导致 HA 和集群连接失败时会出现此状况，但仍允许设备继续处理样本。当出现此状况时，两台 WildFire 设备接管主动（或主）控制器的角色，而无需备份，使得 HA 部署的优点无效，如冗余和负载均衡。此外，这还阻止了 WildFire 设备高效利用分析资源。当 WildFire 集群遇到小的干扰时，其自动尝试从裂脑状况中恢复。更多严重事件将需要手动干预。

当发生脑裂时，会出现以下情况：

- WildFire 对端设备既不知道另一个对端设备的状态，也不知道其高可用性角色。
- 两个 WildFire 对端设备成为主服务器，并继续接收来自防火墙的样本，但作为独立的设备运行。
- 当 HA 不可用时，集群相关任务被暂停。

正确配置的 *3* 节点 *WildFire* 设备集群不会遇到裂脑状况，因为第三个服务器节点提供了额外的冗余。

引起脑裂状况的原因？

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

脑裂状况是对双节点集群但节点故障的纠正性响应，此故障中 WildFire 高可用对无法再互相通讯，但仍可提供有限的功能。当高可用性和负载均衡功能不再可用时，您仍可以转发样本至 WildFire 进行分析。发生脑裂的原因如下：

- 硬件问题或断电。
- 网络连接问题，如交换机/路由器故障，网络摆动或网络分区。
- WildFire 设备配置和连接问题。

  Palo Alto Networks 建议为 *HA1* 和集群接口链接使用直接缆线连接。

- 异常的 WildFire 节点。

确定 WildFire 集群是否处于裂脑状况

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

当 WildFire 双节点集群中的设备进入裂脑状况时，服务失败导致 WildFire CLI 和管理 Panorama（如适用）中生成警报。

STEP 1 | （仅限 WildFire 设备 CLI）在 WildFire 设备控制器上，运行：

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

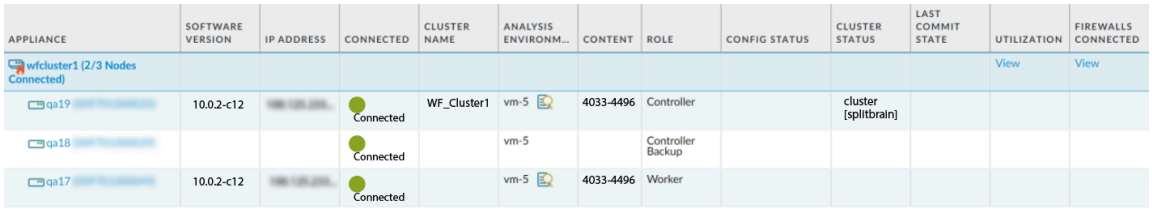
受影响的 WildFire 集群节点显示 `Cluster:splitbrain`，与 `Service Summary` 相邻。

下列示例展示了裂脑状况下的双节点 WildFire 集群内节点：

```
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 | （仅限 Panorama）在管理 WildFire 集群的 Panorama 设备上：

1. 选择 **Panorama > Managed WildFire Clusters**（受管理的 **WildFire** 集群）。
2. 在 **Cluster Status**（集群状态）列中，检查是否存在 **cluster [splitbrain]**（集群**[**裂脑**]**）。这表示设备处于裂脑模式中。



从脑裂状况恢复

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

要解决脑裂状况，请调试网络问题，并恢复 WildFire 高可用性对之间的连接。WildFire 设备集群自动尝试从裂脑状况恢复，但当措施失败时，您必须手动启动恢复过程。

STEP 1 | 验证您的网络运行正常，且 WildFire 设备正在收发流量。

1. 启用 ping WildFire 设备接口的能力。
   - 在特定设备接口上启用 Ping — `setdeviceconfig system <interface_number> service disable-icmp no`
   - 在所有设备接口上启用 Ping — `setdeviceconfig system service disable-icmp no`
2. 从 WildFire 接口生成 ping 流量至外部设备。验证收发的计数器增量。

   ```
   ping source <wildfire-interface-ip> host<destination-ip-address>
   ```

STEP 2 | 确定异常的 WildFire 设备。参阅通过 CLI 查看 WildFire 集群状态或通过 Panorama 查看 WildFire 集群状态以查看设备状态。

STEP 3 | 通过下列命令重启异常节点：

```
request cluster reboot-local-node
```

重启的 WildFire 设备应自动加入其配置的 WildFire 集群。

裂脑模式下的剩余控制器节点必须为正常状态。

STEP 4 | 等待数据迁移完成。运行 `show cluster data-migration-status`以查看数据库合并进度。数据合并完成后，完成时间戳将会显示：

```
100% completed on Mon Sep 9 21:44:48 PDT 2019
```

数据合并市场取决于 *WildFire* 设备上存储的数据量。确保至少留出几个小时用于恢复，因为数据合并可能是一个较长的过程。

STEP 5 | 在 Panorama 上或通过 WildFire 设备 CLI 验证集群状态。

使用 WildFire 设备 CLI

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

以下主题描述了特定于 WildFire™ 设备软件的 CLI 命令。所有其他命令（如配置接口、提交配置和设置系统信息）与 PAN-OS 完全相同，并且也以层次结构显示。了解有关 PAN-OS 命令的信息，请参阅《PAN-OS CLI 快速入门》。

- WildFire 设备软件 CLI 概念
- WildFire CLI 命令模式
- 访问 WildFire 设备 CLI
- WildFire 设备 CLI 操作
- WildFire 设备配置模式命令参考
- WildFire 设备操作模式命令参考

WildFire 设备软件 CLI 概念

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

本节介绍和说明如何使用 WildFire 设备软件命令行界面 (CLI)：

- WildFire 设备软件 CLI 结构
- WildFire 设备软件 CLI 命令约定
- WildFire 设备 CLI 命令消息
- WildFire 设备命令选项符号
- WildFire 设备特权级别

WildFire 设备软件 CLI 结构

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

WildFire 设备软件 CLI 用于管理设备。CLI 是设备唯一的界面。该界面用于查看设备状态和配置信息，以及修改设备的配置。通过 SSH 或使用控制台端口的直接控制台访问可访问 WildFire 设备软件 CLI。

WildFire 设备软件 CLI 以下面两种模式工作：

- 操作模式 — 查看系统的状态，导航 WildFire 设备软件 CLI，并输入配置模式。
- 配置模式 — 查看并修改配置层次结构。

WildFire 设备软件 CLI 命令约定

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

此基本命令提示符包含了设备的用户名和主机名：

```
username@hostname>
```

示例：

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

进入“配置模式”时，提示符从 > 更改为 #：

```
username@hostname> (Operational mode) username@hostname> configure
 Entering configuration mode [edit] username@hostname# (Configuration
 mode)
```

在“配置模式”下，发出命令时，方括号中显示的 [edit...] 横幅显示当前层次结构上下文。

WildFire 设备 CLI 命令消息

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

发出命令时可能会显示消息。这些消息可提供上下文信息，帮助用户更正无效的命令。在下面的示例中，消息以粗体显示。

示例：未知命令

```
username@hostname# application-group Unknown command: application-
group [edit network] username@hostname#
```

示例：更改模式

```
username@hostname# exit Exiting configuration mode
 username@hostname>
```

示例：无效语法

```
username@hostname> debug 17 Unrecognized command Invalid syntax.
 username@hostname>
```

CLI 会检查每条命令的语法。如果语法正确，则会执行命令，同时记录待选层次结构更改。如果语法不正确，则会显示语法无效的消息，如以下示例所示：

```
username@hostname# set deviceconfig setting wildfire cloud-
intelligence submit-sample yes Unrecognized command Invalid syntax.
 [edit] username@hostname#
```

WildFire 设备命令选项符号

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

选项前面的符号可提供命令语法相关的额外信息。

符号	说明
*	这是必要选项。
>	此命令有其他嵌套选项。
+	此命令在该级别有其他命令选项。
立即注册即可享受全部会议活动 400 美元的优惠 | 在浏览器中查看	有一个指定 "except value" 或 "match value" 的选项，用于限制命令。
“ “	虽然双引号不是命令选项符号，但是在 CLI 命令中输入多个词的短语时必须使用此符号。例如，要创建名为“测试组”的地址组，并将名称 user1 添加到该组，则必须按如下所述对组名加双引号： set address-group "Test Group" user1。 如果您没有给组名加上双引号，则 CLI 会将 Test 一词解译为组名，而将 Group 解译为用户名，并显示以下错误：`test` 不是有效的名称。 此示例中使用单引号无效。

以下示例显示如何使用这些符号。

示例：在下面的命令中，关键词 `from` 是必填字段：

```
username@hostname> scp import configuration ? + remote-port SSH
 port number on remote host * from Source (username@host:path)
 username@hostname> scp import configuration 示例：此命令输出中显示了
以 + 和 > 指定的选项。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
```

列出的带有 + 的每个选项都能添加到命令中。

配置文件关键词（带有 >）有其他选项：

```
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 设备特权级别

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

特权级别可确定允许用户执行的命令以及允许用户查看的信息。

级别	说明
superreader	对设备具有完整的只读访问权限。
超级用户	对设备具有完整的读写访问权限。

WildFire CLI 命令模式

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

以下主题介绍用于与 WildFire 设备软件 CLI 交互的模式：

- WildFire 设备 CLI 配置模式
- WildFire 设备 CLI 操作模式

WildFire 设备 CLI 配置模式

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

在配置模式中输入命令可修改待选配置。设备正在运行时，修改后的待选配置保存在设备内存中并进行维护。

每个配置命令均包含一个操作，可能还包含关键字、选项和值。

本节介绍配置模式和配置层次结构。

- 配置模式命令的使用
- 配置层次结构
- 层次结构路径
- 导航层次结构

配置模式命令的使用

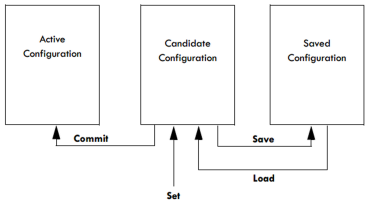
在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

使用以下命令可保存和应用配置更改：

- `save` — 将待选配置保存在设备非易失性存储中。保留保存的配置，直到后面的 **save** 命令覆盖该配置。请注意，此命令不会使配置处于活动状态。
- `commit` — 将待选配置应用到设备中。提交的配置成为设备的主动配置。
- `set` — 更改待选配置中的值。

- `load` — 将上次保存的配置或指定的配置指定为待选配置。

  如果退出配置模式而不发出 ***save*** 或 ***commit*** 命令，则当设备断电时，配置更改可能会丢失。



与传统 CLI 架构相比，维护待选配置和将保存步骤和提交步骤分开可带来巨大的优势。

- 区分 save 和 commit 概念可允许同时进行多项更改，并减少系统的漏洞。
- 对于类似的功能，对命令进行简单地调整即可。例如，配置两个以太网接口（每个都有不同的 IP 地址）时，您可以编辑第一个接口的配置、复制命令、只修改接口和 IP 地址，然后将更改应用到第二个接口。
- 命令结构始终一致。

由于待选配置始终是唯一的，因此对待选配置的所有授权更改会彼此一致。

配置层次结构

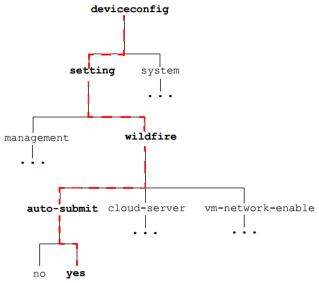
在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

设备的配置以层次结构进行组织。要显示当前的层次结构级别部分，请使用 `show` 命令。输入 show 可显示完整的层次结构，而输入 `show` 及关键字则可显示层次结构的部分。例如，从配置模式的最高级运行命令 `show` 时，会显示整个配置。运行命令 `edit mgt-config` 以及输入 `show` 时，或通过运行 **`show mgt-config`**，只显示层次结构的管理配置部分。

层次结构路径

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

输入命令时，通过层次结构追踪路径，如下所示：

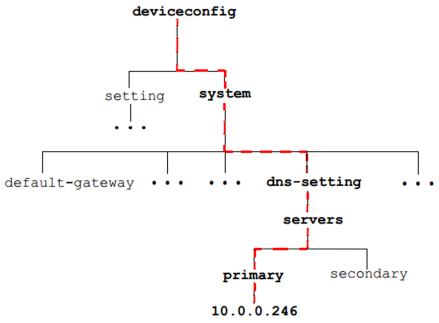


例如，以下命令会为设备分配主 DNS 服务器 10.0.0.246：

```
[edit] username@hostname# set deviceconfig system dns-setting servers
 primary 10.0.0.246
```

此命令会在层次结构和以下 show 命令的输出中生成一个新的要素：

```
[edit] username@hostname# show deviceconfig system dns-settings dns-
setting { servers { primary 10.0.0.246 } } [edit] username@hostname#
```



导航层次结构

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

配置模式命令提示行下面显示的 [edit...] 横幅可显示当前的层次结构上下文。

```
[edit]
```

表示相关的上下文是层次结构的最高级别，其中

```
[edit deviceconfig]
```


表示相关的上下文处于 deviceconfig 级别。

使用列出的命令通过配置的层次结构进行导航。

级别	说明
编辑	在命令层次结构中设置配置的上下文。
up	在层次结构中将上下文更改为下一个较高的级别。
顶部	在层次结构中将上下文更改为最高的级别。

使用 ***up*** 和 ***top*** 命令后发出的 ***set*** 命令会从新的上下文开始。

WildFire 设备 CLI 操作模式

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

在第一次登录设备时，WildFire 设备软件 CLI 以操作模式打开。操作模式命令涉及立即执行的操作。这些操作不涉及对配置的更改，同时也不需要保存或提交。

“操作模式”命令有以下几种类型：

- 网络访问 — 打开另一个主机的窗口。支持 SSH。
- 监控和故障排除 — 执行诊断和分析。包括 `debug` 和 `ping` 命令。
- 显示命令 — 显示或清除当前的信息。包括 `clear` 和 `show` 命令。
- **WildFire** 设备软件 **CLI** 导航命令 — 进入“配置模式”或退出 WildFire 设备软件 CLI。包括 `configure`、`exit` 和 `quit` 命令。
- 系统命令 — 发出系统级别的请求或重启。包括 `set` 和 `request` 命令。

访问 WildFire 设备 CLI

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

本节将介绍如何访问 WildFire 设备软件 CLI：

- 建立直接控制台连接
- 建立 SSH 连接

建立直接控制台连接

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

对于直接控制台连接，请使用以下设置：

- 数据速率：9600
- 数据位：8
- 奇偶校验：无
- 停止位：1
- 流控制：None

建立 SSH 连接

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

要访问 WildFire 设备软件 CLI，请执行以下操作：

STEP 1 | 使用终端模拟软件建立与 WildFire 设备之间的 SSH 控制台连接。

STEP 2 | 输入管理用户名。默认为 admin。

STEP 3 | 输入管理密码。默认为 admin。

在“操作模式”下打开 WildFire 设备软件 CLI 时，会显示 CLI 提示符：

```
username@hostname>
```


WildFire 设备 CLI 操作

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

- 访问 WildFire 设备操作和配置模式
- 显示 WildFire 设备软件 CLI 命令选项
- 限制 WildFire 设备 CLI 命令消息输出
- 设置 WildFire 设备配置命令的输出格式

访问 WildFire 设备操作和配置模式

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

登录时，WildFire 设备软件 CLI 以“操作模式”打开。您可以随时在操作模式和配置模式之间导航。

- 要从“操作模式”进入“配置模式”，请使用 **configure** 命令：

```
username@hostname> configure Entering configuration mode [edit]
 username@hostname#
```

- 要退出“配置模式”并返回“操作模式”，请使用 **quit** 或 **exit** 命令：

```
username@hostname# quit Exiting configuration mode
 username@hostname>
```

要在处于“配置模式”时输入“操作模式”命令，请使用 **run** 命令。例如，要从配置模式中显示系统资源，请使用 **run show system resources**。

显示 WildFire 设备软件 CLI 命令选项

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

根据上下文，使用 **?**（或 Meta-H）显示命令选项列表：

- 要显示操作命令列表，请在命令提示符处输入 **?**。

```
username@hostname> ? clear 清除运行时参数 configure 操作软件配置信息
 create 创建命令 debug 调试和诊断 delete 从硬盘中移除文件 disable 禁用命令
 edit 编辑命令 exit 退出此会话 find 查找带有关键字 的 CLI 命令 grep 搜索文
件中包含模式匹配的行 less 检查调试文件内容 ping Ping 主机和网络 quit 退出此
会话 request 发出系统级别的请求 scp 使用 scp 导入/导出文件 set 设置操作参数
 show 显示操作参数 ssh 启动安全 shell 至另一台主机 submit 提交命令 tail 打
印调试文件最后 10 行 telnet 启动 telnet 会话至另一台主机 test 使用测试用例验
证系统设置 tftp 使用 tftp 导入/导出文件 traceroute 打印路由数据包到网络主机
 username@hostname>
```

- 要显示指定命令的可用选项，请在 **?** 后输入以下命令。

示例：

```
username@hostname> ping ? + bypass-routing 绕过路由表，使用指定接口 +
 count 要发送的请求数量 (1..2000000000 个数据包) + do-not-fragment 不要
将回显请求数据包分段 (IPv4) + interval 请求之间的延迟（秒） + no-resolve 不
要尝试象征性地打印地址 + pattern 十六进制填充模式 + size 请求数据包的大小
 (0..65468 字节) + source 回显请求的源地址 + tos IP 服务类型值 (0..255) +
 ttl IP 生存时间值 (IPv6 跃点限制值) (0..255 个跃点) + verbose 显示详细输出
 * host 远程主机的主机名或 IP 地址
```

限制 WildFire 设备 CLI 命令消息输出

某些操作命令包括限制显示的输出的选项。要限制输出，请在 **except**或 **match** 以及要排除在外或包含在内的值前输入分隔符：

示例：

以下示例输出适用于 show system info 命令：

```
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 platform-family:
 m operational-mode: normal username@hostname> The following sample
 displays only the system model information: username@hostname> show
 system info | match model model:WF-500 username@hostname>
```

设置 WildFire 设备配置命令的输出格式

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

通过在操作模式下使用 **`set cli config-output-format`** 命令可更改配置命令的输出格式。选项包括默认格式、json（JavaScript 对象通知）、set 格式和 XML 格式。默认格式为层次结构格式，其中配置部分会缩进，并用波形括号括起来。

WildFire 设备配置模式命令参考

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

本节包含以下特定于 WildFire 设备软件的配置模式命令的命令参考信息。WildFire 设备软件中包含的所有其他命令与 PAN-OS 中相同，具体如《PAN-OS 11.0 CLI 快速入门》中所述。

- 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

说明

在 WildFire 设备上配置 Wildfire 设备集群设置。您可以配置集群名称、集群通讯用接口以及集群内的设备模式（角色）——控制器或工作设备。在您配置为集群控制器的 WildFire 设备上，您可以添加 WildFire 设备至集群并设置控制器是否在其管理接口上提供 DNS 服务。

层次结构位置

```
set deviceconfig
```

语法

```
cluster { cluster-name <name>; interface {eth2 | eth3}; mode
 { controller { service-advertisement dns-service enabled {no | yes};
 worker-list {ip-address} } worker; } }
```

选项

+ `cluster-name` — 为集群命名。名称必须是有效的域名区段。

+ `interface` — 配置接口以用于集群通讯。集群通讯接口必须与所有集群成员上的一致。

> `mode` — 配置 WildFire 设备作为控制器节点或工作节点。对于控制器节点，配置控制器以确定是否在管理接口上提供 DNS 服务 (`service-advertisement`) 和添加工作节点至集群 (`worker-list`)。各 WildFire 设备集群应有两个控制器节点以提供高可用性。您可以添加两个控制器和最多 18 个工作节点至集群，即最多 20 节点。

示例输出

```
admin@wf-500(active-controller)# show deviceconfig cluster cluster
 { cluster-name sid-6; interface eth2; mode { controller { worker-
list { 2.2.2.115; } } } }
```

所需的特权级别

superuser、deviceadmin

set deviceconfig high-availability

说明

配置 Wildfire 设备集群高可用性 (HA) 设置。

层次结构位置

```
set deviceconfig
```

语法

```
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}; } } }
```

选项

+ `enabled` — 启用两个控制器节点上的 HA 以提供集群容错。各 WildFire 设备集群应有两个被配置为 HA 对的控制器节点。

> `election-option` — 配置抢先、有限和定时器 HA 选项值。

`+ preemptive` — Election 选项以启用被动 HA 对端（控制器备份节点），基于 HA 优先级设置抢占主动 HA 对端（主控制器节点）。例如，如果主控制器节点故障，次（被动）控制器节点接管集群控制。当主控制器节点重新恢复时，如果您不配置抢先级，次控制器继续控制集群，而主控制器则被作为控制器备份节点。但是，如果您在两个 HA 对端上配置抢先级，那么当主控制器重新恢复时，其通过重新接管集群控制的方式抢占次控制器的工作。次控制器恢复其之前控制器备份节点的角色。您必须在两个 HA 端对上配置抢先设置，以启用此功能。

`+ priority` — Election 选项以配置 HA 对中各控制器的抢先优先级。配置 HA 控制器对两个成员的抢先。

`> timers` — 配置 HA election 选项的定时器。WildFire 设备提供两种预配置定时器选项（主动和建议设置），或您可以单独配置各定时器。高级定时器让您可以单独配置各值：

- `Heartbeat-interval` 设置发送 heartbeat ping 的毫秒单位时间。该值的范围是 1000-60,000 ms，默认值为 2000 ms。
- `hello-interval` 设置发送问候消息的毫秒单位时间。该值的范围是 8000-60,000 ms，默认值为 8000 ms。
- `Preemption-hold-time` 设置在抢占主动（主）控制器节点之前，保持被动（控制器备份）模式的时间长度（分钟）。该值的范围是 1-60 分钟，默认值为 1 分钟。
- `Promtion-hold-time` 设置从被动（控制器备份）更改至主动（主）状态的时间（毫秒）。该值的范围是 0-60,000 ms，默认值为 2000 ms。

`> interface` — 配置主 (`ha1`) 和备份 (`ha1-backup`) 控制链接接口的 HA 接口设置。控制链接接口让 HA 控制器对可以保持同步，并在主控制器节点故障时准备好进行故障转移。配置 `ha1` 接口和 `ha1-backup` 接口可在链接故障时提供控制器之间的冗余连接。设置：

- `peer-ip-address`。为每个接口，配置 HA 对端的 IP 地址。`Ha1` 接口对端是 HA 对中另一个控制器节点上的 `ha1` 接口 IP 地址。`Ha1-backup` 接口对端是 HA 对中另一个控制器节点上的 `ha1-backup` 接口 IP 地址。
- `port`。在各控制器节点上，配置 `ha1` 接口和 `ha-backup` 接口使用的端口。您可以为 HA 控制链接接口使用 `eth2`、`eth3` 或 `management` 端口 (eth0)。您不能将分析环境网络接口 (eth1) 作为 `ha1` 或 `ha1-backup` 控制链接接口使用。在两个 HA 对端上使用相同的接口作为 `ha1` 接口，并在两个 HA 对端上使用相同的接口（但非 `ha1` 接口）作为 `ha1-backup` 接口。例如，配置 `eth3` 作为两个控制器节点上的 `ha1` 接口，并配置 `management` 接口作为两个控制器节点上的 `ha1-backup` 接口。

示例输出

```
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 } } }
```

所需的特权级别

superuser、deviceadmin

set deviceconfig setting management

说明

在 WildFire 设备上配置行政管理会话设置。您可以配置超时以结束行政会话，以应对会话空闲时间过长，还可以设置锁定管理员的输入重试次数（失败的登录尝试次数）。

层次结构位置

```
set deviceconfig setting
```

语法

```
management { idle-timeout {0 | <value>} admin-lockout { failed-
attempts <value> lockout-time <value> } }
```

选项

`+ idle-timeout` — 默认管理会话空闲超时（分钟）。配置 1-1440 分钟的空闲超时，或设置超时值为 0（零）至会话永不超时。

`> admin-lockout` — 配置失败尝试次数以在管理员被系统锁定之前 (0-10) 登录设备，并配置锁定时间（分钟 0-60）以在管理员超出失败尝试阈值后背锁定的时长。

示例输出

```
management { idle-timeout 0; admin-lockout { failed-attempts 3;
 lockout-time 5; } }
```

set deviceconfig setting wildfire

说明

在 WildFire 设备上配置 Wildfire 设置。可以配置转发恶意文件、定义接收恶意软件感染文件的云服务器，以及启用或禁用 vm-interface.

层次结构位置

```
set deviceconfig setting
```

语法

```
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}; } }
```

选项

`+ active-vm` — 选择 WildFire 分析样本所使用的虚拟机环境。每个 vm 有不同的配置，如 Windows XP、特定版本的 Flash、Adobe reader 等。要查看选择的 VM，请运行以下命令：**`show wildfire status`**，然后查看选择的 VM 字段。要查看 VM 环境信息，请运行以下命令：**`show wildfire vm-images.`**

`+ cloud-server` — 设备为重新分析将恶意样本/报告转发到的云服务器的主机名。默认云服务器为 wildfire-public-cloud。要配置转发，请使用以下命令：**`set deviceconfig setting wildfire cloud-intelligence`**。

`+ custom-dns-name` — 配置一个自定义 DNS 名称以在服务器证书和 WildFire 服务器列表中使用，而不是使用默认的 DNS 名称 `wfpc.sevice.<clustername>.<domain>`。

`+ preferred-analysis-environment` — 分配大部分资源至文档分析或可执行文件分析，具体取决于您环境中最长分析的样本类型。默认的分配在文档和可执行样本之间取平衡。例如，要分配大部分分析资源至文档：**`set deviceconfig setting wildfire preferred-analysis-environment Documents`**。

`+ vm-network-enable` — 启用或禁用 vm-network。启用后，在虚拟机沙盒中运行的样本文件可访问 Internet。这样有助于 WildFire 分析恶意软件的行为。

`+ vm-network-use-tor` — 对 vm-interface 启用或禁用 Tor 网络。启用此选项后，在样本分析期间来自 WildFire设备沙盒系统的所有恶意流量都将通过 Tor 网络进行发送。Tor 网络将掩盖您的面向公共的 IP 地址，以便恶意站点所有者无法确定流量的来源。

`> cloud-intelligence` — 配置设备以提交 WildFire 诊断、报告或样本至 Palo Alto Networks WildFire 云，或在执行本地分析以保留 WildFire 设备资源之前，自动查询公共 WildFire 云。提交报告选项会将恶意样本的报告发送到云，进行统计收集。提交样本选项会将恶意样本发送到云。如果启用 submit-sample，则不需要启用 submit-report，因为在云中将重新分析样本，并且如果样本是恶意的，则会生成新报告和签名。

`> file-retention` — 配置保存恶意样本（恶意软件和网络钓鱼）和非恶意样本（灰色软件和良性软件）的时间。恶意样本的默认设置是无限（从不删除）。非恶意样本的默认设置是 14 天。例如，要保留非恶意样本 30 天：**`set deviceconfig setting wildfire file-retention non-malicious 30`**。

`> signature-generation` — 可让设备在本地生成签名，从而消除了需要将所有数据发送到公共云才能阻止恶意内容的问题。WildFire 设备将分析从 Palo Alto Networks 防火墙或 WildFire API 转发来的文件，并将生成防病毒签名和 DNS 签名，用于阻止恶意文件以及相关命令和控制流量。当设备检测到恶意 URL 时，会将此 URL 发送到 PAN-DB，而 PAN-DB 会将其分配到恶意软件类别。

示例输出

下面显示了 WildFire 设置输出示例。

```
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

说明

配置 eth2 接口。

层次结构位置

```
set deviceconfig system
```

语法

```
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}; }
```

选项

+ `default-gateway` — eth2 接口默认网关的 IP 地址。

+ `ip-address` — eth2 接口的 IP 地址。

+ `mtu` — eth2 接口的最大传输单位 (MTU)。

+ `netmask` — eth2 接口的子网络掩码。

+ `speed-duplex` — eth2 接口的接口速度（10Mbps、100Mbps、1Gbps 或自动协商）和双工模式（全双工或半双工）。

> `permitted-ip` — 允许访问 eth2 接口的 IP 地址。如果您指定某个带有 IP 地址的子网掩码，该子网掩码必须采用斜杠地址表示法。例如，要指定 C 级地址，输入：10.10.10.100/24（而非 10.10.10.100 255.255.255.0）。

> `service-disable` — 停用 eht2 接口 ICMP。

示例输出

```
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; }
```

所需的特权级别

superuser、deviceadmin

set deviceconfig system eth3

说明

配置 eth3 接口。

层次结构位置

```
set deviceconfig system
```

语法

```
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}; }
```

选项

+ `default-gateway` — eth3 接口默认网关的 IP 地址。

+ `ip-address` — eth3 接口的 IP 地址。

+ `mtu` — eth3 接口的最大传输单位 (MTU)。

+ `netmask` — eth3 接口的子网络掩码。

+ `speed-duplex` — eth3 接口的接口速度（10Mbps、100Mbps、1Gbps 或自动协商）和双工模式（全双工或半双工）。

> `permitted-ip` — 允许访问 eth3 接口的 IP 地址。如果您指定某个带有 IP 地址的子网掩码，该子网掩码必须采用斜杠地址表示法。例如，要指定 C 级地址，输入：10.10.10.100/24（而非 10.10.10.100 255.255.255.0）。

> `service-disable` — 停用 eht3 接口 ICMP。

示例输出

```
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; }
```

所需的特权级别

superuser、deviceadmin

set deviceconfig system panorama local-panorama panorama-server

说明

配置主 Pnorama 服务器进行 WildFire 设备或设备集群管理。

层次结构位置

```
set deviceconfig system panorama local-panorama
```

语法

```
panorama-server {IP address | FQDN};
```

选项

`+ panorama-server` — 配置您将用于管理 WildFire 设备或设备集群的主 Panorama 服务器 IP 地址或完全限定的域名 (FQDN)。

示例输出

输出被缩短以仅显示 Panorama 服务器设定的输出部分。

```
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; } ...
```

所需的特权级别

superuser、deviceadmin

set deviceconfig system panorama local-panorama panorama-server-2

说明

配置备份 Pnorama 服务器进行 WildFire 设备或设备集群管理。配置备份 Panorama 服务器可以提供集群或单独设备管理的高可用性。

层次结构位置

```
set deviceconfig system panorama local-panorama
```

语法

```
panorama-server-2 {IP address | FQDN};
```

选项

`+ panorama-server-2` — 配置您将用于管理 WildFire 设备或设备集群的备份 Panorama 服务器 IP 地址或完全限定的域名 (FQDN)。

示例输出

输出被缩短以仅显示 Panorama 服务器设定的输出部分。

```
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; } ...
```

所需的特权级别

superuser、deviceadmin

set deviceconfig system update-schedule

说明

在 WildFire 设备上计划内容更新。这些内容更新为此设备准备了最新威胁信息，以便准确检测恶意软件和增强设备区分恶意和良性的能力。

层次结构位置

```
set deviceconfig system update-schedule
```

语法

```
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}; } }
```

选项

> `wf-content` — WildFire 内容更新。

> `daily` — 计划每天更新。

+ `action` — 指定要执行的操作。可以为设备计划下载和安装更新，或仅下载，然后手动安装。

+ `at` — 时间规范 hh:mm（例如 20:10）。

> `hourly` — 计划每小时更新。

+ `action` — 指定要执行的操作。可以为设备计划下载和安装更新，或仅下载，然后手动安装。

+ `at` — 超过小时的分钟数。

> `weekly` — 计划一周更新一次。

+ `action` — 指定要执行的操作。可以为设备计划下载和安装更新，或仅下载，然后手动安装。

+ `at` — 时间规范 hh:mm（例如 20:10）。

+ `day-of-week` — 星期几（星期五、星期一、星期六、星期日、星期四、星期二、星期三）。

示例输出

```
admin@WF-500# show update-schedule { wf-content { recurring
 { weekly { at 19:00; action download-and-install; day-of-week
 friday; } } } }
```

所需的特权级别

superuser、deviceadmin

set deviceconfig system vm-interface

说明

在 WildFire 设备虚拟机沙盒上运行的恶意软件使用 vm-interface 访问 Internet。我们推荐激活此端口，如果恶意软件访问 Internet 执行回拨活动或其他活动时，这有助于 WildFire 更好地识别恶意活动。重要的是，此接口具有隔离的 Internet 连接。如果您的 WildFire 设备以 FIPS/CC 模式运行，则会禁用 vm-interface。如需更多信息，请参见设置 WildFire 设备 VM 接口。

配置 vm-interface 后，通过运行以下命令启用：

```
set deviceconfig setting wildfire vm-network-enable yes
```

层次结构位置

```
set deviceconfig system
```

语法

```
set vm-interface { default-gateway <ip_address>; dns-server
 <ip_address>; ip-address <ip_address>; link-state; mtu; netmask
 <ip_address>; speed-duplex; {
```

选项

+ `default-gateway` — VM 接口默认网关。
+ `dns-server` — VM 接口的 dns 服务器。
+ `ip-address` — VM 接口的 IP 地址。
+ `link-state` — 将链接状态设置为连接或断开。
+ `mtu` — VM 接口的最大传输单位。
+ `netmask` — VM 接口的 IP 网络掩码。
+ `speed-duplex` — VM 接口的速度和双工。

示例输出

下面是已配置的 vm-interface：

```
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; }
```

所需的特权级别

superuser、deviceadmin

WildFire 设备操作模式命令参考

在何处可以使用？	需要提供什么？
• WildFire 设备	❑ WildFire 许可证

本节包含以下特定于 WildFire 设备软件的操作模式命令的命令参考信息。WildFire 设备软件中包含的所有其他命令与 PAN-OS 中相同。有关这些命令的信息，请参阅《PAN-OS 11.0 CLI 快速入门》。

- clear high-availability
- create wildfire api-key
- delete high-availability-key
- delete wildfire api-key
- delete wildfire-metadata
- disable wildfire
- edit wildfire api-key
- load wildfire api-key
- request cluster decommission
- request cluster reboot-local-node
- request high-availability state
- request high-availability sync-to-remote
- request system raid
- request wildfire sample redistribution
- request system wildfire-vm-image
- request wf-content
- save wildfire api-key
- set wildfire portal-admin
- show cluster all-peers
- show cluster controller
- show cluster membership
- show cluster task
- 显示集群数据迁移状态
- 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

说明

清除 WildFire 设备集群控制器节点上的高可用性 (HA) 控制链接统计信息和转移统计信息。

语法

```
create { high-availability { control-link { statistics; }
 transitions; } }
```

选项

`> control-link>` — 清除 HA 控制链接统计信息。

`> transitions>` — 清除 HA 转移统计信息（HA 切换过程中发生的事件）。

示例输出

在去除控制链接或转移统计信息后，WildFire 集群重置所有值为零 (0)。

```
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
```

所需的特权级别

superuser、deviceadmin

create wildfire api-key

说明

在 WildFire 设备上生成 API 密钥，此密钥在外部系统上可用于将样本提交到设备、查询报告或从设备中检索样本和数据包捕获 (PCAP)。

语法

```
create { wildfire { api-key { key <value>; name <value>; { { {
```

选项

+ `key` — 通过手动输入密匙值创建 API 密钥。该值必须是 64 个阿尔法字符 (a-z) 或数字 (0-9)。如果没有指定密钥选项，则设备会自动生成密钥。

+ `name` — 可选择输入 API 密钥的名称。API 密钥名称仅用于标记密钥，以便更轻松地确定针对特定用途分配的密钥，对密钥功能没有任何影响。

示例输出

以下输出显示了设备有三个 API 密钥，一个密钥名为 `my-api-key`。

```
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 | +---------
+---------------------+---------------------+
```

所需的特权级别

superuser、deviceadmin

delete high-availability-key

说明

删除 WildFire 设备集群控制器节点的集群控制链接上高可用性 (HA) 所用的对端加密密钥。

语法

```
delete { high-availability-key; }
```

选项

无其他选项。

示例输出

输出中突出显示行显示 HA 控制链接上的加密未启用。

```
admin@wf-500(active-controller)> show high-availability state High-
Availability:Local Information:版本：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:Software
 Version: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
```

所需的特权级别

superuser、deviceadmin

delete wildfire api-key

说明

从 WildFire 设备中删除 API 密钥。删除密钥后，配置为使用 API 在设备上执行 API 功能的系统不能再访问此设备。

语法

```
delete { wildfire { api-key { key <value>; { { {
```

选项

`+ key <value>` — 要删除的密钥的密钥值。要查看 API 密钥列表，请运行以下命令：

```
admin@WF-500> show wildfire global api-keys all
```

示例输出

```
admin@WF-500> delete wildfire api-key key <API KEY> APIKey <API Key>
 deleted
```

所需的特权级别

superuser、deviceadmin

delete wildfire-metadata

说明

在 WildFire 设备上删除内容更新。有关内容更新和如何安装它们的详细信息，请参阅 request wf-content。

语法

```
delete { wildfire-metadata update <value>; {
```

选项

`+ update <value>` — 定义要删除的内容更新。

示例输出

随后的输出显示了删除更新名为：

```
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
```

所需的特权级别

superuser、deviceadmin

disable wildfire

说明

禁用域签名或样本签名，以便将其从下一个 WildFire 内容包版本中排除。

语法

```
disable wildfire { domain-signature { domain <value>; } OR... sample-
signature { sha256 { equal <value>; } }
```

选项

> `domain-signature`— 设置域签名状态为禁用，将其从下一个 WildFire 内容版本中排除。

> `sample-signature`— 设置样本签名状态为禁用，将其从下一个 WildFire 内容版本中排除。

示例输出

成功禁用的样本或域不会显示任何输出。

```
admin@WF-500> disable wildfire sample-signature sha256 equal
 d1378bda0672de58d95f3bff3cb42385f2d806a4a15b89cdecfedbdb1ec08228
```

所需的特权级别

superuser、deviceadmin

edit wildfire api-key

说明

在 WildFire 设备上修改 API 密钥名称或密钥状态（已启用/已禁用）。

语法

```
edit { wildfire { api-key [name | status] key <value>; { {
```

选项

+ `name`— 更改 API 密钥的名称。

+ `status`— 启用或禁用 API 密钥。

* `key`— 指定要修改的密钥。

示例输出

密钥值在此命令中是必需的。例如，要将名为 `stu` 的密钥名称更改为 `stu-key1`，请输入以下命令：

在以下命令中，不需要输入旧密钥名称；仅输入新密钥名称。

```
admin@WF-500> edit wildfire api-key name stu-key1 key <API
 KEY> To change the status of stu-key1 to disabled, enter the
 following command: 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 | +----------+---------------------+---------------------+
```

所需的特权级别

superuser、deviceadmin

load wildfire api-key

说明

将 API 密钥导入 WildFire 设备后，必须使用 load 命令才能使密钥可用。使用此命令可替换所有现有 API 密钥，您也可以合并导入文件中的密钥和现有密钥数据库。

语法

```
load { wildfire { from <value> mode [merge | replace]; { {
```

选项

* `from`— 指定要导入的 API 密钥的文件名。密钥文件使用 .keys 文件扩展名。例如，my-api-keys.keys。要查看可用于导入的密钥的列表，请输入以下命令：

```
admin@WF-500> load wildfire api-key from ?
```

+ `mode` — 可选择输入导入的模式 (merge/replace)。例如，要将设备的密钥数据库替换为新密钥文件的内容，请输入以下命令：

```
admin@WF-500> load wildfire api-key mode replace from my-api-
keys.keys
```

如果不指定 **mode** 选项，则默认操作是合并密钥。

所需的特权级别

superuser、deviceadmin

request cluster decommission

说明

从有三个或三个以上成员节点的集群移除 WildFire 设备集群节点。请勿使用此命令从双节点集群移除节点。相反，从集群本地移除节点时使用 `delete deviceconfig high-availability` 和 `delete deviceconfig cluster` 命令。

层次结构位置

request cluster

语法

```
request { cluster { decommission { show; start; stop; } } }
```

选项

`Show`—— 显示节点解除授权工作的状态。

`Start`—— 开始节点解除授权工作。

`Stop`—— 终止节点解除授权工作。

示例输出

`Node mode` 字段确认集群节点解除授权生效，因为模式为 `stand_alone` 而非 `controller` 或 `worker`。

```
admin@wf-500> show cluster membership Service Summary: wfpc signature
 Cluster name:address: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
```

所需的特权级别

superuser、deviceadmin

request cluster reboot-local-node

说明

重启本地 WildFire 集群节点。

层次结构位置

```
request cluster
```

语法

```
request { cluster { reboot-local-node; } }
```

选项

无其他选项。

示例输出

您可以通过几种方式验证本地集群节点已重启，或正在重启：

- `show cluster task local`— 显示本地节点上请求的任务。
- `show cluster task current`— 显示本地节点上目前正在运行的任务或上一次完成的任务（仅限控制器节点）。
- `show cluster task pending`— 显示队列中，但尚未在本地节点上运行的任务（仅限控制器节点）。
- `show cluster task history`— 显示已在本地节点上运行的任务（仅限控制器节点）。

例如，下列命令显示了已成功完成的两个集群节点重启任务：

```
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
```

所需的特权级别

superuser、deviceadmin

request high-availability state

说明

在 WildFire 设备集群上，使本地控制器节点或对端控制器节点的高可用性 (HA) 状态可正常运行。

层次结构位置

```
request high-availability
```

语法

```
request { high-availability { state { functional; } peer
 {    functional; } } }
```

选项

> `functional`— 使本地控制器节点的 HA 状态可正常运行。

> `peer`— 使对端控制器节点的 HA 状态可正常运行。

示例输出

输出中突出显示的行表示本地控制器节点的 HA 状态可在主动（主）控制器角色中运行，且对端控制器节点 HA 状态可在被动（备份）控制器节点中正常运行。

```
admin@wf-500(active-controller)> show high-availability state
 High-Availability:Local Information:版本：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:Software Version: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
```

所需的特权级别

superuser、deviceadmin

request high-availability sync-to-remote

说明

在 WildFire 应用程序集群中，同步本地控制器节点的候选配置或运行配置，或本地控制器节点时钟（时间和日期）至远程高可用 (HA) 对端控制器节点。

层次结构位置

request high-availability

语法

```
request { high-availability { sync-to-remote { candidate-config;
 clock; running-config; } } }
```

选项

> `candidate-config`— 在本地对端控制器节点上同步候选配置至远程 HA 对端控制器节点。

> `clock`— 在本地对端控制器节点上同步时钟（时间和日期）至远程 HA 对端控制器节点。

> `running-config`— 在本地对端控制器节点上同步运行的配置至远程 HA 对端控制器节点。

示例输出

输出中突出显示的行表示 HA 配置状态在 HA 对端控制器节点上同步。

```
admin@wf-500(active-controller)> show high-availability state
 High-Availability:Local Information:版本: 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:Software Version: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
```

所需的特权级别

superuser、deviceadmin

request system raid

说明

使用此选项可管理安装在 WildFire 设备中的 RAID 对。WF-500 设备在前四个驱动器托架（A1、A2、B1、B2）中随附四个驱动器。驱动器 A1 和 A2 是一组 RAID 1 对，驱动器 B1 和 B2 是另一组 RAID 1 对。

层次结构位置

request system

语法

```
raid { remove <value>; OR... copy { from <value>; to <value>; } OR...
 add {
```

选项

> `add`— 添加驱动器至对应的 RAID 磁盘对

> `copy`— 在驱动器托架中，从一个驱动器向另一个驱动器复制和迁移

> `remove`— 从 RAID 磁盘对移除驱动器

示例输出

下面的输出内容显示了包含正确配置 RAID 的 WF-500 设备。

```
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
```

所需的特权级别

superuser、deviceadmin

request wildfire sample redistribution

说明

从本地 WildFire 设备集群节点重新分配样本至其他集群节点，同时选择在本地节点上保留样本。

层次结构位置

```
request system
```

语法

```
request { wildfire { sample { redistribution {    keep-local-copy {no
 | yes};    serial-number <value>; } } } }
```

选项

* keep-local-copy— 在本地 WildFire 应用程序节点上保留或不保留重新分配的样本副本。
* serial-number— 您重新分配的样本节点序列号。

示例输出

Storage Nodes 显示本地节点重新分配样本的其他节点。如果本地节点未重新分配样本，仅显示存储节点位置。如果本地节点重新分配样本，Storage Nodes 显示两个存储节点位置。突出显示的输出展示了存储样本的两个存储节点（本地节点和本地节点重新分配样本的节点），并验证是否正在重新分配样本。

```
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
```

所需的特权级别

superuser、deviceadmin

request system wildfire-vm-image

对用于分析文件的 WildFire 设备虚拟机 (VM) 沙盒映像执行升级。要从 Palo Alto Networks 更新服务器检索新 VM 映像，必须先手动下载映像，在启用 SCP 的服务器上托管它，然后使用 SCP 客户端从设备中检索此映像。将映像下载到设备后，可以使用此命令安装它。

层次结构位置

request system

语法

```
request { system { wildfire-vm-image { upgrade install file
 <value>; } } }
```

选项

`> wildfire-vm-image`— 安装虚拟机 (VM) 映像。

`+ upgrade install file`— 对 VM 映像执行升级。在此文件选项后键入 ? 可查看可用 VM 映像的列表。例如，运行以下命令列出可用映像：

```
admin@WF-500> request system wildfire-vm-image upgrade install file ?
```

示例输出

要列出可用 VM 映像，请运行以下命令：

```
admin@WF-500> request system wildfire-vm-image upgrade install
 file ?要安装虚拟机映像（本例中为 Windows 7 64 位），请运行以下命
令：admin@WF-500> request system wildfire-vm-image upgrade install
 file WFWin7_64Base_m-1.0.0_64base
```

所需的特权级别

superuser、deviceadmin

request wf-content

在 WildFire 设备上执行内容更新。这些内容更新为此设备准备了最新威胁信息，以便准确检测恶意软件和增强设备区分恶意和良性的能力。如需将内容更新计划为自动安装，请参阅 set deviceconfig system update-schedule，而如需在 WildFire 设备上删除内容更新，请参阅 delete wildfire-metadata 。

层次结构位置

```
request
```

语法

```
request wf-content { downgrade install {previous | <value>}; upgrade
 { check download latest info install { file <filename> version
 latest; } } }
```

选项

> `downgrade` — 安装之前的内容版本。使用 previous 选项安装之前安装的内容数据包，或输入一个要降级到特定内容数据包的版本号值。

> `upgrade` — 执行内容更新功能

> `check` — 从 Palo Alto Networks 更新服务器中获取可用内容数据包的信息

> `download` — 下载内容数据包

> `info` — 显示可用内容数据包的相关信息

> `install` — 安装内容数据包

> `file` — 指定包含内容数据包的文件的名称

> `version` — 基于内容数据包的版本号下载或升级

示例输出

要列出可用内容更新，请运行以下命令：

```
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
```

所需的特权级别

superuser、deviceadmin

save wildfire api-key

说明

使用 save 命令将 WildFire 设备上的所有 API 密钥保存到文件中。然后可以导出密钥文件进行备份，也可以批量修改密钥。有关在 WildFire 设备上使用 WildFire API 的详细信息，请参阅《WildFire API 参考》。

层次结构位置

```
save
```

语法

```
save { wildfire { api-key to <value>; { {
```

选项

* `to` — 输入用于导出密钥的文件名。例如，要将 WildFire 设备上的所有 API 密钥导出到名为 my-wf-keys 的文件中，请输入以下命令：

```
admin@WF-500> save wildfire api-key to my-wf-keys
```

所需的特权级别

superuser、deviceadmin

set wildfire portal-admin

说明

设置管理员用于查看 WildFire 设备所生成 WildFire 分析报告的门户管理帐户密码。在防火墙上或在 Panorama 中通过选择**Monitor**（监控） > **WildFire Submissions**（**WildFire** 提交） > **View WildFire Report**（查看 **WildFire** 报告） 查看报告时，帐户名称 (admin) 和密码是必需的。默认的用户名和密码为 admin/admin。

门户管理帐户是在设备上配置的，用于从防火墙或 *Panorama* 中查看报告的唯一帐户。您不能创建新帐户，或更改帐户名称。这不是用于管理设备的同一管理员帐户。

层次结构位置

```
set wildfire
```

语法

```
set { wildfire { portal-admin { password <value>; } }
```

示例输出

以下所示为此命令的输出内容。

```
admin@WF-500> set wildfire portal-admin password Enter
 password:Confirm password:
```

所需的特权级别

superuser、deviceadmin

show cluster all-peers

说明

在 WildFire 设备集群控制器节点上，显示所有 WildFire 设备集群成员状态，包括 WildFire 设备模式（控制器或工作设备）、连接状态和应用程序服务状态。

层次结构位置

```
show cluster
```

语法

```
all-peers;
```

选项

无其他选项。

示例输出

```
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.
```

所需的特权级别

superuser、deviceadmin

show cluster controller

说明

在 WildFire 设备集群控制器节点上，显示 WildFire 设备集群控制器状态，包括集群名称和本地控制器节点角色（如果 `Active Controller` 字段显示 `True`，本地控制器即为主控制器，如果 `Active Controller` 字段显示 `False`，本地控制器为备份控制器）。

层次结构位置

```
show cluster
```

语法

```
controller;
```

选项

无其他选项。

示例输出

```
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
```

所需的特权级别

superuser、deviceadmin

显示集群数据迁移状态

说明

从 WildFire 设备集群控制器节点使用该命令可显示当前数据迁移状态。该命令会显示何时启动数据迁移及其过程。数据迁移完成时，该命令会显示完成时间戳。如果数据迁移失败，状态将显示为 `0%` 已完成。

层次结构位置

```
show cluster
```

语法

```
data-migration-status;
```

选项

无其他选项。

示例输出

```
adminWF-500(active-controller)> show cluster data-migration-status
 100% completed on Mon Sep 9 21:44:48 PDT 2019
```

所需的特权级别

superuser、deviceadmin

show cluster membership

说明

显示集群节点或独立 WildFire 设备的 WildFire 设备集群成员信息，包括 IP 地址、主机名称、WildFire 设备序列号、设备角色（节点模式）、高可用优先级和应用程序状态。

层次结构位置

```
show cluster
```

语法

```
membership;
```

选项

无其他选项。

示例输出

您可以显示 WildFire 应用程序集群节点成员（控制器和工作节点）和独立 WildFire 设备的集群成员信息，以检查其应用程序状态、是否属于某个集群，以及其他本地主机信息。输出根据 WildFire 设备角色的不同而略显不同。区别为：

- 提示指示主动（主）控制器节点和被动（备份）控制器节点，但不指示工作节点或独立角色。
- 节点模式指示 WildFire 设备为控制器节点、工作节点或 `stand_alone` WildFire 设备。

- `HA` 优先级显示主动控制器节点的主要状态、被动（备份）控制器节点的次要状态，以及工作节点和独立 WildFire 设备的字段为空。
- `Application status` 字段在某些字段显示不同的值。对于 `global-db-service` 和 `global-queue-service`，集群成员显示 `ReadyLeader` 或 `JoinedCluster`，且独立设备显示 `ReadyStandalone`。

  对于 `siggen-db`，WildFire 设备集群主控制器节点显示 `ReadyMaster`，WildFire 设备集群次控制器节点显示 `ReadySlave`，WildFire 设备集群工作节点显示 `Ready`，且独立 WildFire 设备显示 `ReadyMaster`。

各 *WildFire* 设备序列号的后四位在显示屏中更改为“*xxxx*”以避免显示真实的序列号。

WildFire 设备集群内主控制器节点上的输出：

```
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 设备集群内控制器备份节点上的输出：

```
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 设备集群内工作节点上的输出：

```
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
```

独立 WildFire 设备上的输出（非 WildFire 设备集群成员）：

```
admin@max> show cluster membership Service Summary: wfpc signature
 Cluster name:address: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
```

所需的特权级别

superuser、deviceadmin

show cluster task

说明

显示本地集群节点或所有集群节点的 WildFire 设备集群任务信息，或显示已完成的集群任务历史记录或挂起的集群任务。

层次结构位置

```
show cluster
```

语法

```
task { current; history; local; pending; }
```

选项

> `current`— 显示 WildFire 设备集群上当前允许的任务。仅在集群控制器节点上可用。

> `history`— 显示完成的集群任务。仅在集群控制器节点上可用。

> `local`— 显示本地 WildFire 设备集群节点上挂起的任务。

> `pending`— 显示整个 WildFire 设备集群的挂起任务。仅在集群控制器节点上可用。

示例输出

```
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.Progress:
 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
```

所需的特权级别

superuser、deviceadmin

show high-availability all

说明

显示所有 WildFire 设备集群高可用性 (HA) 信息，包括 HA 控制链接、HA 状态、HA 转换信息、对端软件、内容更新和防病毒兼容性信息，以及对端连接和角色信息。

层次结构位置

```
show high-availability
```

语法

```
all;
```

选项

无其他选项。

示例输出

```
admin@thing1(active-controller)> show high-availability all High-
Availability:Local Information:版本：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 地址：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:Software
 Version: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 地址：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
```

所需的特权级别

superuser、deviceadmin

show high-availability control-link

说明

显示主要和备份控制器节点之间，HA 控制链接的 WildFire 设备集群高可用性 (HA) 统计，包括 HA 控制链接上传输和接收的不同消息类型数量、连接故障以及 ping 活动。

层次结构位置

```
show high-availability
```

语法

```
control-link { statistics; }
```

选项

`> statistics`— 显示 WildFire 设备集群控制器节点 HA 控制链接统计。

示例输出

```
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 :1
```

所需的特权级别

superuser、deviceadmin

show high-availability state

说明

显示本地和对端集群控制器节点的 WildFire 设备集群高可用性 (HA) 状态信息，包括控制器节点是主动（主）或被动（备份），控制器节点处于该状态多长时间，本地和对端控制器节点配置是否同步，以及软件、内容更新和控制器节点对端设备之间的防病毒版本兼容性。

层次结构位置

```
show high-availability
```

语法

```
state;
```

选项

无其他选项。

示例输出

```
admin@thing1(active-controller)> show high-availability state
 High-Availability:Local Information:版本: 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:Software Version: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
```

所需的特权级别

superuser、deviceadmin

show high-availability transitions

说明

显示关于 HA 切换集群控制器节点时所发生事件的 WildFire 设备集群高可用性 (HA) 转换信息。

层次结构位置

```
show high-availability
```

语法

```
transitions;
```

选项

无其他选项。

示例输出

```
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
```

所需的特权级别

superuser、deviceadmin

show system raid

说明

显示 WildFire 设备的 RAID 配置。WF-500 设备在前四个驱动器托架（A1、A2、B1、B2）中随附四个驱动器。驱动器 A1 和 A2 是一组 RAID 1 对，驱动器 B1 和 B2 是另一组 RAID 1 对。

层次结构位置

```
show system
```

语法

```
raid { detail; {
```

选项

无其他选项。

示例输出

下面显示了正在运行的 WF-500 设备上的 RAID 配置。

```
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
```

所需的特权级别

superuser, superreader

submit wildfire local-verdict-change

说明

更改本地生成的，防火墙提交的样本 WildFire 判定。判定更改仅适用于提交至 WildFire 设备的样本，且相同样本的判定在 WildFire 公共云内保持不变。您可以通过显示 wildfire 全球命令查看带有更改判定的样本。

WildFire 专有云内容包更新以反映您（在防火墙上）所做的任何判定更改（选择 **Device**（设备） > **Dynamic Updates**（动态更新） > **WF-Private**（**WF-**专有）以启用 WildFire 专有云内容更新）。当

您更改样本判定为恶意时，WildFire 设备生成新签名以检测恶意软件并添加该签名至 WildFire 专有云内容包。当您更改样本判定为良性时，WildFire 设备从 WildFire 专有云内容包移除签名。

还有一个可用于更改本地样本判定的 API 调用。有关详细信息，请参见 WildFire API 参考文件。

层次结构位置

```
submit wildfire
```

语法

```
submit { wildfire { local-verdict-change { hash <value>; verdict
 <value>; comment <value>; } }
```

选项

* `hash` — 指定您要更改判定的 SHA-256 文件哈希。
* `verdict` — 输入新的文件判定：0 表示良性样本；1 表示恶意软件；2 表示灰色软件。
* `comment` — 包括描述判定更改的注释。

示例输出

以下所示为此命令的输出内容。

```
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)
```

所需的特权级别

superuser、deviceadmin

show wildfire

说明

显示关于 WildFire 设备的各种信息，如全球和本地设备以及样本相关详情、设备状态以及被选择执行分析的虚拟机。

层次结构位置

```
show wildfire
```

语法

```
status | vm-images | wf-vm-pe-utilization | wf-vm-doc-utilization
 | wf-vm-email-link-utilization | wf-vm-archive-utilization | wf-
sample-queue-status }
```

选项

`> status` — 显示设备状态以及配置信息，如用于样本分析的虚拟机 (VM)、样本/报告是否已发送到云、vm 网络和注册信息。

`> vm-images` — 显示用于样本分析的可用虚拟机映像的属性。若要查看当前活动映像，请运行以下命令：

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

，然后查看 `VM` 字段。

`> wf-sample-queue-status` — 显示等待分析的 WildFire 设备样本数量和详细信息。

`> wf-vm-doc-utilization` — 显示有多少用于处理文档文件的分析环境可用或正在使用。

`> wf-vm-elinkda-utilization` — 显示有多少用于处理电子邮件链接的分析环境可用或正在使用。

`> wf-vm-pe-utilization` — 显示有多少用于处理可迁移可执行文件的分析环境可用或正在使用。

示例输出

下面是此命令的输出内容。

```
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, }
```

所需的特权级别

superuser, superreader

show wildfire global

说明

显示关于全球设备和样本状态的各种信息，例如，可用的 API 密钥、注册信息、样本判定更改、活动、样本设备原始信息和设备最近分析的样本等。

层次结构位置

```
show wildfire global
```

语法

```
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>; } }
```

选项

`> api-keys` — 显示在 WildFire 设备上生成的 API 密钥的相关详细信息。可以查看上次使用密钥的时间、密钥名称、状态（已启用或已禁用）以及生成密钥的日期/时间。

`> devices-reporting-data` — 显示最近的注册活动的列表。

`> last-device-registration` — 显示最近的注册活动的列表。

`> local-verdict-change` — 显示带更改判定的样本。

`> sample-analysis` — 显示最多 1000 个样本的 WildFire 分析结果。

`> sample-status` — 显示 WildFire 样本状态。输入文件的 SHA256 值，以查看当前分析状态。

`> sample-device-lookup` — 显示发送指定 SHA256 样本的防火墙。

`> signature-status` — 显示 WildFire 签名状态。输入文件的 SHA256 值，以查看当前分析状态。

示例输出

下面是此命令的输出内容。

```
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 | +---------------+--------------------
+---------+-------------+----------+
```

所需的特权级别

superuser, superreader

show wildfire local

说明

显示关于本地设备和样本、活动、设备分析的近期样本以及基本 WildFire 统计的各种信息。

层次结构位置

```
show wildfire local
```

语法

```
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>; }
```

选项

> `latest` — 显示最近的 30 项活动，包括最近的 30 项分析活动、最近的 30 个分析文件、分析文件和上传到公共云服务器的文件上的网络会话信息。

> `sample-processed` — 显示指定时间范围内的本地处理样本数量或最大样本数量。

> `sample-status` — 显示 WildFire 样本状态。输入文件的 SHA256 值，以查看当前分析状态。

> `statistics` — 显示基本 WildFire 统计信息。

示例输出

下面是此命令的输出内容。

```
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 | 0 || |
+-------------------------------------------------------------------------------
+| || docx | 0 | 0 | 0 | 0 | 0 | 0 | 0 || |
+-------------------------------------------------------------------------------
+| || pptx | 0 | 0 | 0 | 0 | 0 | 0 | 0 || |
+-------------------------------------------------------------------------------
+| || xlsx | 0 | 0 | 0 | 0 | 0 | 0 | 0 || |
+-------------------------------------------------------------------------------
+| || rtf | 0 | 0 | 0 | 0 | 0 | 0 | 0 || |
+-------------------------------------------------------------------------------
+| || 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
 ||| ||+---------------------------+-------------------------+||
```

所需的特权级别

superuser, superreader

test wildfire registration

说明

执行测试以检查 WildFire 设备或 Palo Alto Networks 防火墙在 WildFire 服务器中的注册状态。如果测试成功，则会显示 WildFire 服务器的 IP 地址或服务器名称。必须成功注册，WildFire 设备或防火墙才能将文件转发到 WildFire 服务器。

语法

```
test { wildfire { registration; } }
```

选项

无其他选项。

示例输出

下面显示了可与 WildFire 设备通信的防火墙上的成功输出。如果这是指向 Palo Alto Networks WildFire 云的 WildFire 设备，则其中一个云服务器的服务器名称在 `select the best server:` 字段中显示。

```
Testing wildfire Public Cloud wildfire registration: successful
 download server list: successful select the best server: ca-
s1.wildfire.paloaltonetworks.com
```

所需的特权级别

superuser, superreader