paloalto TECHDOCS

PAN-OS 升级指南

Version 11.1 & later

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Last Revised

May 22, 2024

Table of Contents

软件和内容更新

PAN-OS 是运行所有 Palo Alto Networks 次世代防火墙的软件。Palo Alto Networks 也会频繁发布更新，为防火墙带来最新的安全功能。防火墙可实施基于内容更新提供的应用程序和威胁签名（等）策略，而无需更新防火墙配置。

成功下载并将 PAN-OS 软件更新安装到物理防火墙上后，一旦该物理防火墙作为软件安装流程的一部分重新启动后，即会验证该软件更新，以确保 PAN-OS 软件的完整性。这样可确保新运行的软件更新是已知良好的，且防火墙不会因远程或物理漏洞利用而受到威胁。

PAN-OS 软件更新

PAN-OS 是运行所有 Palo Alto Networks 次世代防火墙的软件。防火墙运行的 PAN-OS 软件版本显示于防火墙 **Dashboard**（仪表板）上。

您可以在防火墙上直接检查是否有新的 PAN-OS 发布版本，或在 Palo Alto Networks 支持门户网站上查看。要将防火墙升级至 PAN-OS 的最新版本：

STEP 1 | 查看最新 PAN-OS 发行说明以了解有哪些新内容。另请查看升级/降级注意事项以确保您了解 PAN-OS 版本可能引入的所有潜在更改。

STEP 2 | 检查是否有新的 PAN-OS 发行版本：

- **On the support portal**（在支持门户网站上）—前往 support.paloaltonetworks.com，然后在左边的菜单栏选择 **Updates**（更新） > **Software Updates**（软件更新）。下载并保存您想要用于升级防火墙的版本。
- **On the firewall**（在防火墙上）—选择 **Device**（设备） > **Software**（软件）和 **Check Now**（立即检查），让防火墙检查 Palo Alto Networks 升级服务器，查看是否有新的 PAN-OS 发行版本。

检查软件更新有困难吗？请参阅 本文，了解一些常见连接问题的解决方案。

STEP 3 | 在您决定了想要的发布版本之后，按照完整的工作流程来将防火墙升级到 PAN-OS 11.1。您将要采取的步骤可能取决于您当前运行的发行版本，您是否在使用 HA，以及您是否在通过 Panorama 管理防火墙。

动态内容更新

Palo Alto Networks 会经常发布防火墙可用于实施安全策略的更新，无需升级 PAN-OS 软件或更改防火墙配置。通过这些更新，防火墙可配备最新安全功能和威胁情报。

除任何防火墙都可以接收到的应用程序更新和一些防病毒更新外，根据您的订阅，您还可以使用动态内容更新。您可以为每个动态内容更新设置一个时间表，以定义防火墙检查、下载或安装新更新的频率（**Device**（设备） > **Dynamic Updates**（更新））。

动态内容更新	这个包里有什么？
反病毒	防病毒更新每 24 小时发布一次，包括： • 新发现恶意软件的 WildFire 签名。要想每隔五分钟（而非每天）获取一次这些更新，您需要 WildFire 订阅。 • （需要威胁防护）自动生成的命令和控制 (C2) 签名，可检测 C2 流量中的某些模式。即使是 C2 主机未知或变化迅速，防火墙也能通过这些签名检测到 C2 活动。 • （需要威胁防护）用于内置外部动态列表的新的、经过更新的列表条目。这些列表包括恶意 IP 地址、高风险 IP 地址、防弹主机提供的 IP 地址，有助于保护您免遭恶意主机的攻击。 • （需要威胁防护）本地 DNS 签名集更新，可供防火墙用于标识已知的恶意域。如果已设置DNS sinkholing，则防火墙可以标识网络上尝试连接这些域的主机。要允许防火墙根据完整的 DNS 签名数据库检查域，请设置 DNS Security（DNS 安全）。
应用程序	应用程序更新可提供新建和修改过的应用程序签名，或 App-ID。此更新不需要任何额外订阅，但一定需要具备有效的维护/支持合约。新的应用程序更新仅在每个月的第三个星期二发布，让您有时间提前准备任何必要的政策更新。 在极少数情况下，包含新 *App-ID* 的更新可能会延迟一两天发布。 对 App-ID 的修改的发布频率更高。当新建和修改过的 App-ID 使防火墙能够以越来越高地精度执行您的安全策略时，发生的安全策略更改可能会影响应用程序的可用性。要充分利用应用程序更新，请按照我们的提示管理新的和修改后的 App-ID。
应用程序和威胁	包括新的和更新的应用程序和威胁签名。如果您已订阅威胁防护，则可以获得此更新（在这种情况下，您将获得此更新，而不是应用程序更新）。新的威胁更新会经常发布，有时每周发布几次，并附带更新的 App-ID。新的 App-ID 仅在每个月的第三个星期二发布。 在极少数情况下，包含新 *App-ID* 的更新可能会延迟一两天发布。

动态内容更新	这个包里有什么？
	最新的威胁和应用程序更新可用后，防火墙可以在短短 30 分钟内检索到。 有关如何最好启用应用程序和威胁更新以确保应用程序可用性，并防止最新威胁的指导，请查看 应用程序和威胁内容更新的最佳实践。
Device Dictionary 设备目录	设备字典是防火墙在基于 Device-ID（设备 ID）的安全策略规则中使用的 XML 文件。它包含各种设备属性的条目，并定期完全刷新并作为新文件发布在更新服务器上。如果字典条目有任何更改，则会在更新服务器上发布修订后的文件，以便 Panorama 和防火墙在下次检查更新服务器时自动下载并安装该文件，每两个小时自动执行此操作。
GlobalProtect 数据文件	包括供应商特定信息，用于定义和评估 GlobalProtect 应用程序返回的主机信息配置文件 (HIP) 数据。您必须订阅 GlobalProtect 网关才能获取这些更新。此外，您必须在 GlobalProtect 运行前为这些更新创建一个计划表。
GlobalProtect 无客户端 **VPN**	包含新的和更新的应用程序签名，使得无客户端 VPN 能够访问 GlobalProtect 门户的常见 Web 应用程序。您必须订阅 GlobalProtect 才能获取这些更新。此外，您必须在 GlobalProtect 无客户端 VPN 运行前为这些更新创建一个计划表。作为最佳实践，建议 GlobalProtect 无客户端 VPN 始终安装最新内容更新。
WildFire	提供实时访问 WildFire 公共云所生成的恶意软件和防病毒签名的权限。或者，您可以配置 PAN-OS 来检索 WildFire 签名更新包。您可以将防火墙设为每分钟检查一次新的更新，确保防火墙能够在一分钟内检索到最新 WildFire 签名。若未订阅 WildFire，您必须至少等待 24 小时才能获得防病毒更新中提供的签名。
WF - 私有	由于 WildFire 设备执行了分析，从而能几乎实时地提供已创建的恶意软件和防病毒签名。要从 WildFire 设备获取内容更新，防火墙和设备必须同时运行 PAN-OS 6.1 或更高版本，且防火墙必须配置为可以转发文件和电子邮件链接到 WildFire 私有云。

安装内容更新

为了确保您始终不会受到最新威胁（包括尚未发现的威胁）的攻击，您必须确保防火墙始终具有 Palo Alto Networks 发布的最新更新内容及软件。您可以使用的 动态内容更新 取决于您拥有的订阅。

按照以下步骤安装内容更新。此外，您还可以设置内容更新计划，以定义防火墙检索和安装更新的频率。

与其他更新类型相比，应用程序和威胁内容更新的工作方式略有不同 — 要充分利用最新应用程序知识和威胁防护措施，并根据指南以部署应用程序和威胁内容更新，而不是此处所述的步骤。

STEP 1 | 确保防火墙具备防火墙服务器访问权限。

1. 默认情况下，防火墙通过 **`updates.paloaltonetworks.com`** 访问更新服务器，以便防火墙从距离最近的服务器接收内容更新。如果防火墙对互联网的访问受限，则可能需要配置允许列表以允许访问更新下载中涉及的服务器。有关内容更新服务器的详细信息，请参阅动态更新的内容分发网络基础架构。如果您需要更多参考信息或遇到连接和更新下载问题，请参阅 https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000001UtRCAU。

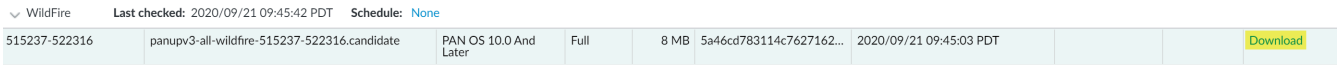
   如果您的设备位于中国大陆，*Palo Alto Networks* 建议使用 ***`updates.paloaltonetworks.cn`*** 服务器来下载更新。

2. （可选）单击 **Verify Update Server Identity**（确认更新服务器身份）进行额外验证，从而启用防火墙检查服务器的 SSL 证书是否由授信机构颁发。默认启用此选项。
3. （可选）如果防火墙需要使用代理服务器才能访问 Palo Alto Networks 更新服务，则请在 **Proxy Server**（代理服务器）窗口中输入：
   - **Server**（服务器）— 代理服务器的 IP 地址或主机名。
   - **Port**（端口）— 代理服务器的端口。范围：1-65535。
   - **User**（用户）— 用于访问此服务器的用户名。
   - **Password**（密码）— 用户用以访问该代理服务器的密码。在 **Confirm Password**（确认密码）中重新输入此密码。
4. （可选）连接失败时，最多可以配置 3 次重新连接尝试。使用 **`debug set-content-download-retry attempts`** 设置连接尝试次数。默认值为 0。

STEP 2 | 检查最新内容更新。

选择 **Device**（设备） > **Dynamic Updates**（动态更新）并单击 **Check Now**（立即检查）（位于窗口的左下角）以检查最新更新。**Action**（操作）列中的链接指示是否有更新可用：

- **Download**（下载） — 指示有新更新文件可用。单击该链接便可以开始将文件直接下载到防火墙。成功下载后，**Action**（操作）列中的链接将从**Download**（下载）更改为**Install**（安装）。



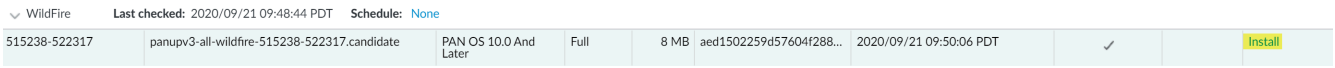
在安装应用程序和威胁更新之前，无法下载防病毒更新。

- **Revert**（还原） — 指示之前安装的内容版本或软件版本可用。您可以选择还原到之前安装的版本。

STEP 3 | 安装内容更新。

在 *PA-220* 防火墙上，最长需要 *10* 分钟来完成安装，而在 *PA-5200* 系列、*PA-7000* 系列或 *VM* 系列防火墙上，最长仅需两分钟即可完成。

单击 **Install**（安装） 连接中的 **Action**（操作） 列。安装完成时，将在 **Currently Installed**（当前已安装）列中显示复选标记。



STEP 4 | 调度每项内容更新。

为您要计划的每项更新重复执行此步骤。

交错执行更新计划，因为防火墙每次只能下载一项更新。如果您计划以相同时间间隔下载这些更新，则只有第一项下载会成功。

1. 通过单击 **None**（无）链接设置每个更新类型的计划。

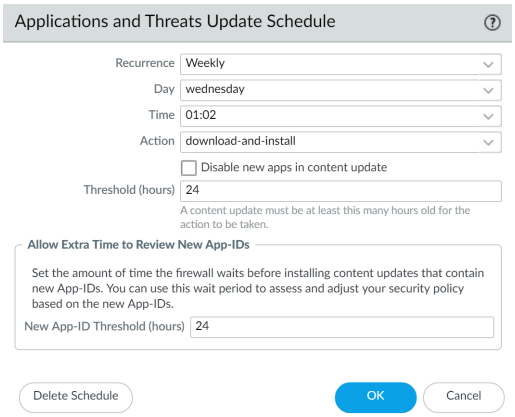
2. 通过从 **Recurrence**（重复）下拉列表中选择值来指定希望更新发生的频率。根据内容类型的不同，可用值会发生变化（WildFire 更新具有**Real-time**（实时）、**Every Minute**（每分钟）、**Every 15 Minutes**（每 **15** 分钟）、**Every 30 minutes**（每 **30** 分钟）或 **Every Hour**（每小时）选项，而应用程序及威胁更新可计划为 **Weekly**（每

周）、**Daily**（每天）、**Hourly**（每小时）或 **Every 30 Minutes**（每 **30** 分钟），防病毒更新可计划为**Hourly**（每小时）、**Daily**（每天）或 **Weekly**（每周））。

您也可以为应用程序和威胁或防病毒更新选择**None (Manual)**（无（手动））。这意味着此项目没有定期时间表，您必须手动安装更新。要完全删除计划节点，请选择 **Delete Schedule**（删除时间表）。

3. 指定 **Time**（时间）（如果是 WildFire，则指定每小时后的分钟数），并且在适用情况下，根据选择的 **Recurrence**（重复）值指定希望更新发生在 **Day**（星期几）。
4. 指定是希望系统 **Download Only**（仅下载），还是 **Download And Install**（下载和安装）（最佳实践）更新。
5. 在 **Threshold (Hours)**（阈值（小时））字段输入发布后执行内容更新的等待时间。在极少数情况下，可能会发现内容更新中存在错误。为此，您可能希望延迟安装新更新，直到更新已经发布一定的时间后才安装。

   如果您的关键任务应用程序必须 *100#* 可用，请将应用程序或应用程序和威胁更新的阈值设置为至少 *24* 小时或更长时间，并遵循应用程序和威胁内容更新的最佳实践。此外，虽然计划内容更新是一次性或不常发生的任务，计划设置完毕后，您将需要继续管理新建和修改过的 App-ID（均包含在内容发布中），因为这些 *App-ID* 可以改变安全策略实施的方式。
6. （可选）输入 **New App-ID Thresholds**（新的 **App-ID** 阈值）（以小时为单位），以设置防火墙在安装包含新 App-ID 的内容更新之前等待的时间。



7. 单击 **OK**（确定）以保存计划设置。
8. 单击**Commit**（提交）以将设置保存到正在运行的配置中。

STEP 5 | 更新 PAN-OS。

始终在更新 *PAN-OS* 前更新内容。所有 *PAN-OS* 版本均具备最低支持内容发行版本。

1. 审核发行说明。
2. 更新 PAN-OS 软件。

应用程序和威胁内容更新

应用程序和威胁内容更新可为防火墙提供最新的应用程序和威胁签名。包内应用程序部分包括新的和修改过的 App-ID，无需许可证。完整的“应用程序和威胁”内容包也包含新的和修改过的威胁签名，需要“威胁防护”许可证。由于防火墙会根据自定义设置自动检索并安装最新的应用程序和威胁签名，因此可以基于最新的 App-ID 和威胁防护执行安全策略，无需任何其他配置。

新的和修改过的威胁签名以及修改过的 App-ID 应至少每周发布一次，通常频率应该更高。新 App-ID 在每个月的第三个星期二发布。

在极少数情况下，包含新 *App-ID* 的更新可能会延迟一两天发布。

由于新的 App-ID 可以更改安全策略实施流量的方式，因此更有限的 App-ID 新版本旨在为您提供可预测窗口，以准备和更新安全策略。此外，内容更新应是累积式的，即，最新内容更新应始终包含先前版本中发布的应用程序和威胁签名。

由于应用程序和威胁签名通过单个包提供（相同的解码器使应用程序签名能够识别应用程序，同时也使威胁签名能够检查流量），您需要考虑是否要一起或单独部署签名。您选择部署内容更新的方式取决于组织的网络安全和应用程序的可用性要求。首先，将您的组织标识为具有以下状态之一（或者两者都有，具体取决于防火墙的位置）：

- 奉行安全第一的组织会优先考虑使用最新威胁签名来进行防护，而非应用程序的可用性。您主要将防火墙用于实现威胁防护功能。其次，对影响安全策略实施应用程序流量的方式的 App-ID 做出的任何更改。
- 任务关键型网络优先考虑应用程序的可用性，而非使用最新威胁签名来进行防护。您的网络绝不容忍停机。防火墙在线部署以实施安全策略。如果您在安全策略中使用 App-ID，则引入任何影响 App-ID 的内容版本的更改都可能会导致停机。

您可以采取任务关键型或安全第一的方式来部署内容更新，或可以将这两种方法相结合来满足业务需求。查看并考虑 应用程序和威胁内容更新的最佳实践以决定您想要如何实施应用程序和威胁更新。然后：

- 部署应用程序和威胁内容更新。
- 遵守我们的 内容更新提示。

虽然计划内容更新是一次性或不常发生的任务，计划设置完毕后，您将需要继续管理新建和修改过的 App-ID（均包含在内容发布中），因为这些 *App-ID* 可以改变安全策略实施的方式。

部署应用程序和威胁内容更新

在执行各步骤以配置应用程序和威胁内容更新之前，请先了解应用程序和威胁内容更新 的工作原理并决定实施应用程序和威胁内容更新的最佳实践的方式。

此外，Panorama 可以让您能轻松快速地部署内容更新到防火墙。如果使用 Panorama 管理防火墙，请遵循部署内容更新的这些步骤，而不是下面的步骤。

STEP 1 | 要解锁完整的“应用程序和威胁”内容数据包，请获取“威胁防护”许可证，并在防火墙上激活许可证。

1. 选择**Device**（设备） > **Licenses**（许可证）。
2. 手动上传许可证密钥，或从 Palo Alto Networks 许可证服务器检索密钥。
3. 检验“威胁防护”许可证是否激活。

STEP 2 | 设置防火墙计划，以检索和安装内容更新。

完成以下步骤后，请务必考虑您的组织是任务关键型或安全第一型组织（或是两者兼而有之），并查看应用程序和威胁内容更新的最佳实践。

1. 选择 **Device**（设备） > **Dynamic Updates**（动态更新）。
2. 选择“应用程序和威胁”内容更新 **Schedule**（计划）。
3. 设置防火墙检查 Palo Alto Networks 更新服务器新“应用程序和威胁”内容发布的频率（**Recurrence**（重复周期）），以及 **Day**（日期）和 **Time**（时间）。
4. 设置防火墙在发现和检索新内容发布时执行的 **Action**（操作）。
5. 设置内容发布的安装 **Threshold**（阈值）。在防火墙可以检索发布并执行在上一步配置的“操作”之前，Palo Alto Networks 更新服务器上的内容发布必须至少在这段时间内可用。
6. 如果使用任务关键型网络，即您对应用程序停机时间零容忍（应用程序的可用性甚至等同于最新威胁防护），则可以设置 **New App-ID Threshold**（新建 **App-ID** 阈值）。仅在新建 App-ID 在这段时间已可用之后，防火墙方检索包含这些新建 App-ID 的内容更新。
7. 单击 **OK**（确定）以保存“应用程序和威胁”内容更新计划，并 **Commit**（提交）。

STEP 3 | 设置日志转发，将 Palo Alto Networks 关键内容警告发送给您用于监控网络和防火墙活动的外部服务。为此，可以确保相应人员收到有关关键内容问题的通知，以便按需采取行动。关键内容警告将记录为带有以下“类型”和“事件”的系统日志条目：(subtype eq content) 及 (eventid eq palo-alto-networks-message)。

STEP 4 | 虽然计划内容更新是一次性或不常发生的任务，计划设置完毕后，您将需要继续管理新建和修改过的 App-ID（均包含在内容发布中），因为这些 App-ID 可以改变安全策略实施的方式。

内容更新提示

Palo Alto Networks 应用程序和威胁内容发布经过严格的性能和质量检查。但是，因为客户网络环境中可能存在诸多变量，因此在极少数情况下，会出现内容发布以意想不到的方式影响网络的事件。请执行以下提示来减轻或解决内容发布带来的问题，尽可能将对您网络的影响降至最低。

- 请执行应用程序和威胁内容更新的最佳实践。

  查看并执行 应用程序和威胁内容更新的最佳实践。您选择部署内容更新的方式取决于您的网络安全和应用程序的可用性要求。

- 确保您运行的是最新内容。

  如果尚未配置可以自动下载和安装的防火墙，请获取最新内容更新。

  防火墙将验证已下载的内容更新是否仍然是安装时 Palo Alto Networks 推荐的更新。默认情况下，当内容更新下载自 Palo Alto Networks 更新服务器（手动或按计划）或是在安装前进行

下载，防火墙执行的这类检查都将非常有用。因为在极少情况下，会出现 Palo Alto Networks 从可用性中删除内容更新的情况，即便是防火墙已成功下载，但该选项仍可以防止防火墙安装 Palo Alto Networks 已经删除的内容更新。如果看到一条“您正在尝试安装的内容更新已不再有效”错误消息，请 **Check Now**（立即检查），获取最新内容更新，并安装该版本（**Device**（设备） > **Dynamic Updates**（动态更新））。

- 打开威胁情报遥测。

  打开防火墙发送给 Palo Alto Networks 的威胁情报遥测。我们使用遥测数据来标识和解决内容更新相关的问题。

  遥测数据有助于我们快速识别在 Palo Alto Networks 客户群中以意想不到的方式影响防火墙性能或安全策略实施的内容更新。越快识别问题，我们就能越快地帮助您避免问题，或减轻对您网络的影响。

  要启动防火墙和 Palo Alto Networks 一起收集和共享遥测数据：

  1. 选择 **Device**（设备） > **Setup**（设置） > **Telemetry**（遥测）。
  2. 编辑 **Telemetry**（遥测）设置，并 **Select All**（选择所有）。
  3. 单击 **OK**（确定）和 **Commit**（提交），保存您的更改。

- 向相应人员转发 **Palo Alto Networks** 内容更新警报。

  启用 Palo Alto Networks 关键内容警报的日志转发，以便将内容发布问题相关的重要消息直接发送给相应的人员。

  现在，Palo Alto Networks 可以将内容更新问题相关的警报直接发送给防火墙 Web 接口，或是在您已启用日志转发功能时，发送给用于监控的外部服务。关键内容警报对问题进行描述，为此，您能够了解它对您的影响，且还包含必要时应采取的操作步骤。

  在防火墙 Web 接口上，关键内容问题警报的显示方式类似于当日消息。当 Palo Alto Networks 发布内容更新相关的关键警报时，警报将会在您登陆至防火墙 Web 接口时默认显示。如果您已成功登陆到防火墙 Web 接口，您会发现，在 Web 接口底部菜单栏上消息图标上会出现一个感叹号，单击消息图标以显示警报。

  关键内容更新警报还可以记录为类型为动态更新，事件为 **palo-alto-networks-message** 的系统日志条目。使用下列筛选器以查看这些日志条目：(subtype eq dynamic-updates) 和 (eventid eq palo-alto-networks-message)。

- 必要时，使用 **Panorama** 回滚到较早的内容版本。

  在看到内容更新相关的问题后，您可以使用 Panorama 快速将受管防火墙恢复至最新内容更新版本，而不是手动恢复每个防火墙的内容版本：从 Panorama 恢复内容更新

应用程序和威胁内容更新的最佳实践

部署内容更新的最佳实践有助于确保策略的无缝实施，同时防火墙可以持续配置新的和修改过的应用程序和威胁签名。即使应用程序和威胁签名一起通过单个内容更新包提供（请阅读更多有关应用程序和威胁内容更新的信息），您也可以根据网络安全和可用性要求灵活地区别部署它们：

- 奉行安全第一的组织会优先考虑使用最新威胁签名来进行防护，而非应用程序的可用性。您主要将防火墙用于实现威胁防护功能。
- 任务关键型网络优先考虑应用程序的可用性，而非使用最新威胁签名来进行防护。您的网络绝不容忍停机。防火墙在线部署以实施安全策略。如果您在安全策略中使用 App-ID，则任何影响 App-ID 的内容的更改都可能会导致停机。

您可以采取任务关键型或安全第一的方式来部署内容更新，或可以将这两种方法相结合来满足业务需求。在应用下列最佳实践以最有效地利用新的和修改过的威胁和应用程序签名时，请考虑您自己的方法：

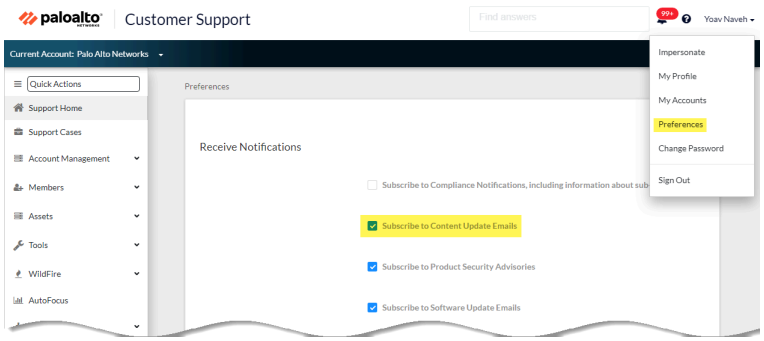
- 内容更新的最佳实践——任务关键型
- 内容更新的最佳实践 ——安全第一

内容更新的最佳实践——任务关键型

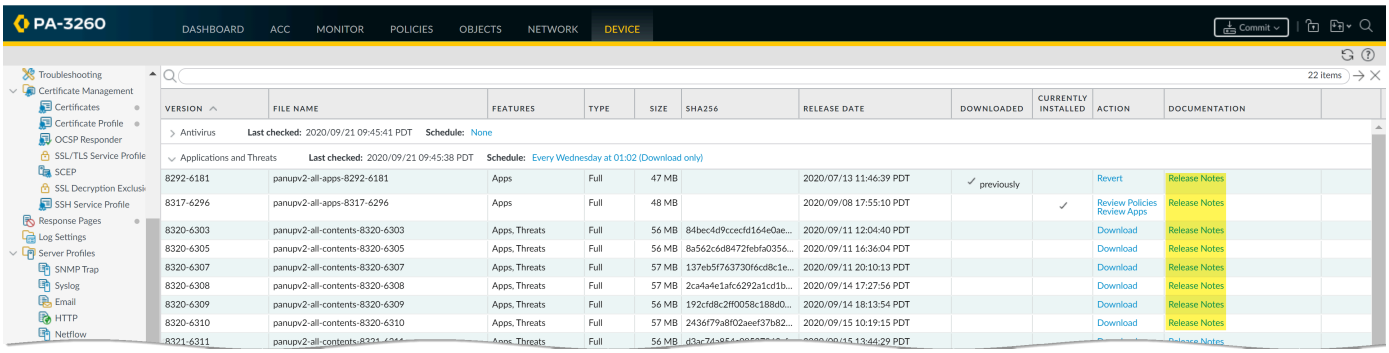
发布新应用程序和威胁签名时，应用程序和威胁内容更新的最佳实践有助于确保策略的无缝实施。当您对应用程序的停机时间零容忍时，请遵循这些最佳实践，在任务关键型网络中部署内容更新。

- 请始终查看“内容发布说明”，了解内容发布中引入的新识别和修改的应用程序和威胁签名列表。内容发布说明还对更新如何影响现有安全策略的实施进行说明，并提供有关如何修改安全策略以实现新功能的最佳利用的建议。

  要订阅获取新内容更新的通知，请访问客户支持门户，编辑您的 **Preferences**（首选项），然后选择 **Subscribe to Content Update Emails**（订阅内容更新电子邮件）。



  您还可以在 Palo Alto Networks 支持门户上查看应用程序和威胁内容发布说明，或是直接在防火墙 Web 界面查看：选择 **Device**（设备）> **Dynamic Updates**（动态更新），打开特定内容发布版本的 **Release Note**（发布说明）。

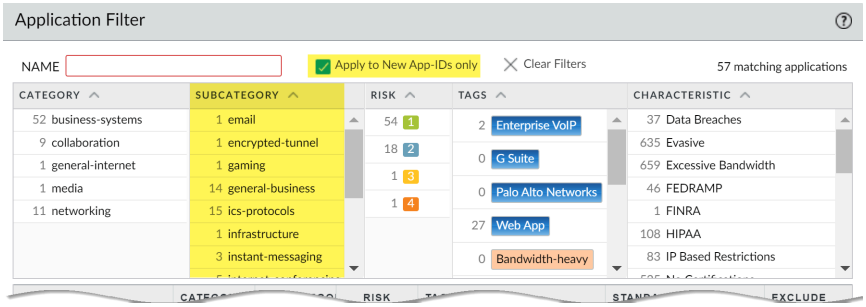


  内容发布说明的“说明”部分着重强调 *Palo Alto Networks* 认为未来可能会对覆盖范围有重大影响的更新：例如，新的 *App-ID* 或解码器。检查这些未来更新，以便在发布之前解决策略带来的任何影响。

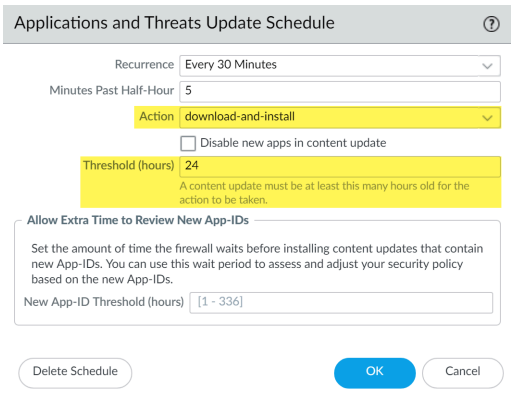
- 创建安全策略规则，始终允许某些类别的新建 App-ID，例如，关键业务功能所依赖的身份验证或软件开发应用程序。也就是说，当内容发布引入或更改重要业务应用程序的覆盖时，防火墙将继续无缝允许应用程序，无需更新安全策略。这就消除了关键类别中 App-ID 的任何潜在可用

性影响，给您提供三十天的时间（新建 App-ID 应每月发布一次）调整安全策略，以允许任务关键型 App-ID。

为此，创建用于关键类别中新 App-ID 的应用程序筛选器（**Objects > Application Filters**（对象> 应用程序筛选器））， 并添加应用程序筛选器至安全策略规则。



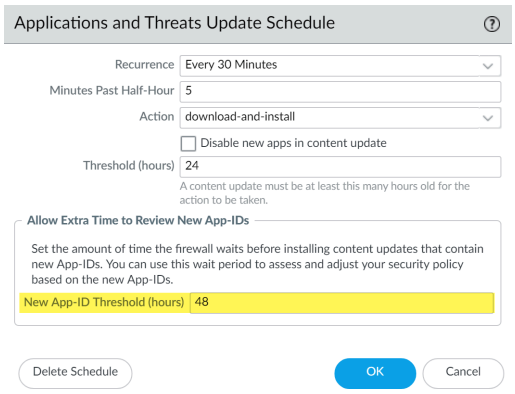
- 为了降低与启用新应用程序和威胁签名相关的安全策略实施的任何影响，可以交错使用新内容。在将新内容部署到具有更高业务风险的位置（例如具有关键应用程序的位置）之前，先将其提供给业务风险较低的位置（用户较少的卫星办公室）。在您的网络中部署之前，先将最新的内容更新部署到某些防火墙，这样便可更容易地解决出现的任何问题。您可以根据组织或位置使用 Panorama 将交错计划和安装阈值推送到防火墙和设备组（使用 Panorama 将更新部署至防火墙）。
- 安排内容更新，以自动**download-and-install**（下载并安装）然后，设置**Threshold**（阈值），确定防火墙在安装最新内容之前需要等待的时间量。在任务关键型网络中，安排的阈值最长为 48 小时。



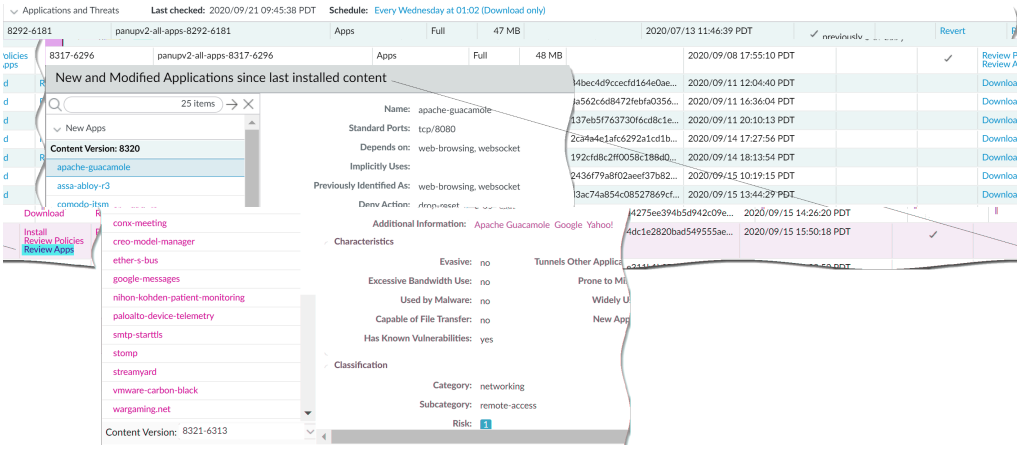
安装延迟，可确保防火墙在指定时间段内仅安装在客户环境中可用且功能正常的内容。要计划内容更新，请选择 **Device**（设备） > **Dynamic Updates**（动态更新） > **Schedule**（计划）。

- 在安装前，请给自己额外的时间根据新建 App-ID 调整您的安全策略。为此，设置仅适用于包含新建 App-ID 的内容更新的安装阈值。带新建 App-ID 的内容更新应每月仅发布一次，

安装阈值应在此时触发。安排内容更新以配置 **New App-ID Threshold**（新建 **App-ID** 阈值）（**Device**（设备） > **Dynamic Updates**（动态更新） > **Schedule**（安排））。

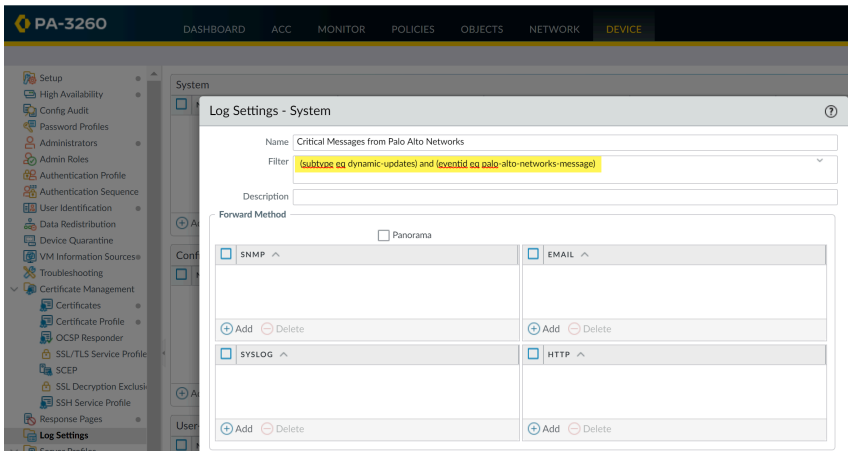


- 始终查看内容发布引入的新建和修改过的 App-ID，以评估更改可能会对安全策略产生的影响。以下主题介绍了您可以在安装新建 App-ID 前后用于更新安全策略的选项。管理新建和修改过的 App-ID。



- 设置日志转发，将 Palo Alto Networks 关键内容警告发送给您用于监控网络和防火墙活动的外部服务。为此，可以确保相应人员收到有关关键内容问题的通知，以便按需采取行动。关

键内容警告将记录为带有以下“类型”和“事件”的系统日志条目：**(subtype eq dynamic-updates)** 及 **(eventid eq palo-alto-networks-message)**。



PAN-OS 8.1.2 将关键内容警告的日志类型从 ***general*** 更改为 ***dynamic-updates***。如果使用 *PAN-OS 8.1.0* 或 *PAN-OS 8.1.1*，则关键内容将记录为带有有以下类型和事件的系统日志条目，同时，应使用下列筛选器设置转发这些警告：***(subtype eq general)*** 和 ***(eventid eq palo-alto-networks-message)***。

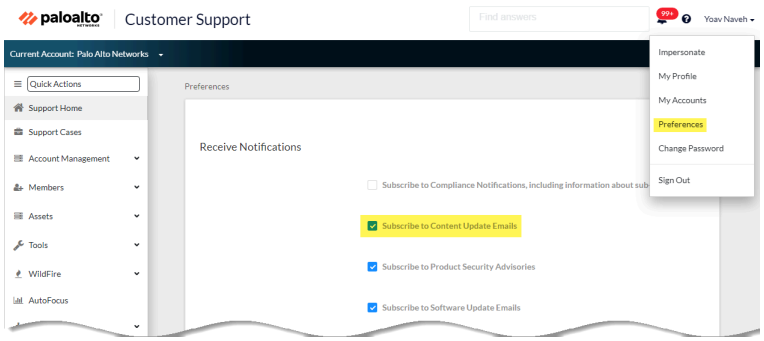
- 在专门的模拟环境中测试新应用程序和威胁内容更新，然后再在生产环境中启用。测试新应用程序和威胁的最简单方法是使用测试防火墙来接入生产流量。在测试防火墙上安装最新内容，并在处理从生产环境复制的流量时监控防火墙。您还可以使用测试客户端和测试防火墙或数据包捕获 (PCAP) 来模拟生产流量。使用 PCAP 可以很好地模拟各种部署的流量，其中防火墙安全策略因位置而异。

内容更新的最佳实践——安全第一

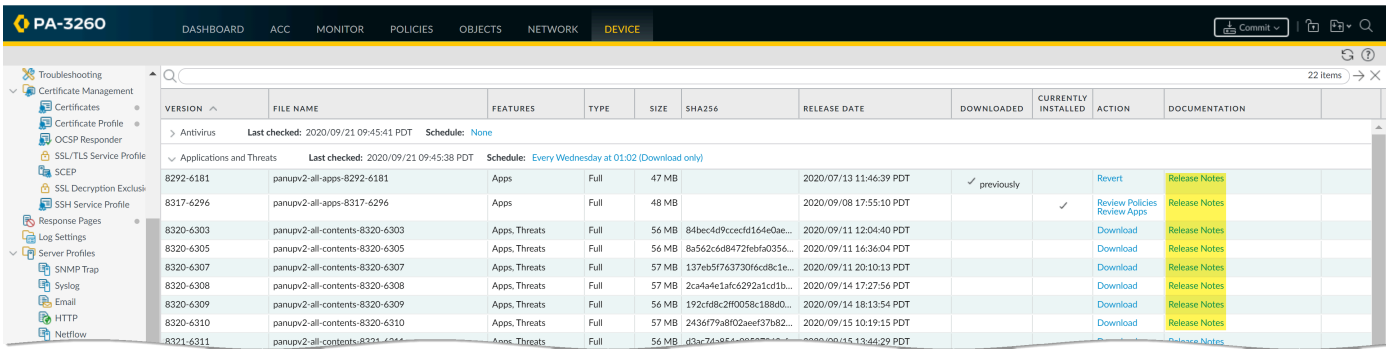
发布新应用程序和威胁签名时，应用程序和威胁内容更新的最佳实践有助于确保策略的无缝实施。当您主要使用防火墙实现威胁防护功能且您的首要任务是预防攻击时，请遵循这些最佳实践，在 *security-first network*（安全第一网络）中部署内容更新。

- 请始终查看“内容发布说明”，了解内容发布中引入的新识别和修改的应用程序和威胁签名列表。内容发布说明还对更新如何影响现有安全策略的实施进行说明，并提供有关如何修改安全策略以实现新功能的最佳利用的建议。

  要订阅获取新内容更新的通知，请访问客户支持门户，编辑您的 **Preferences**（首选项），然后选择 **Subscribe to Content Update Emails**（订阅内容更新电子邮件）。



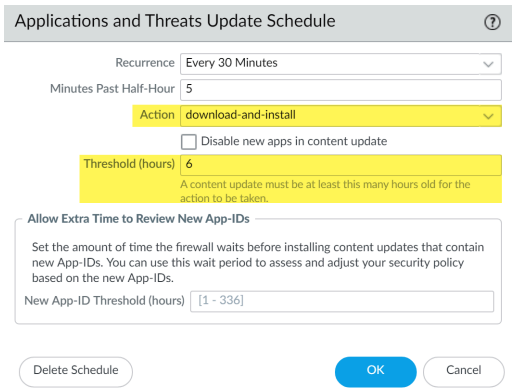
  您还可以在 Palo Alto Networks 支持门户上查看应用程序和威胁内容发布说明，或是直接在防火墙 Web 界面查看：选择 **Device**（设备）> **Dynamic Updates**（动态更新），打开特定内容发布版本的 **Release Note**（发布说明）。



  内容发布说明的“说明”部分着重强调 *Palo Alto Networks* 认为未来可能会对覆盖范围有重大影响的更新：例如，新的 *App-ID* 或解码器。检查这些未来更新，以便在发布之前解决策略带来的任何影响。

- 为了降低与启用新应用程序和威胁签名相关的安全策略实施的任何影响，可以交错使用新内容。在将新内容部署到具有更高业务风险的位置（例如具有关键应用程序的位置）之前，先将其提供给业务风险较低的位置（用户较少的卫星办公室）。在您的网络中部署之前，先将最新的内容更新部署到某些防火墙，这样便可更容易地解决出现的任何问题。您可以根据组织或位置使用 Panorama 将交错计划和安装阈值推送到防火墙和设备组（使用 Panorama 将更新部署至防火墙）。

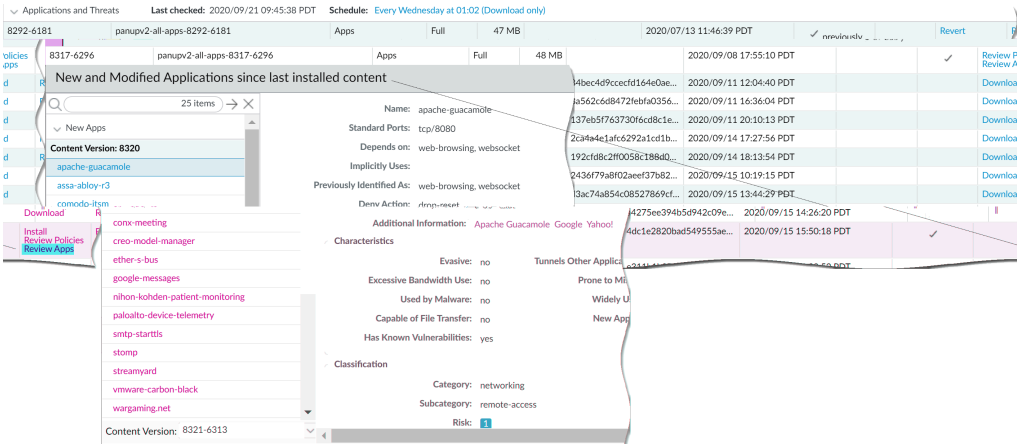
- 安排内容更新，以自动**download-and-install**（下载并安装）然后，设置**Threshold**（阈值），确定防火墙在安装最新内容之前需要等待的时间量。在安全第一的网络中，安排 6 到 12 小时的阈值。



安装延迟，可确保防火墙在指定时间段内仅安装在客户环境中可用且功能正常的内容。要安排内容更新，请选择 **Device**（设备） > **Dynamic Updates**（内容更新） > **Schedule**（安排）。

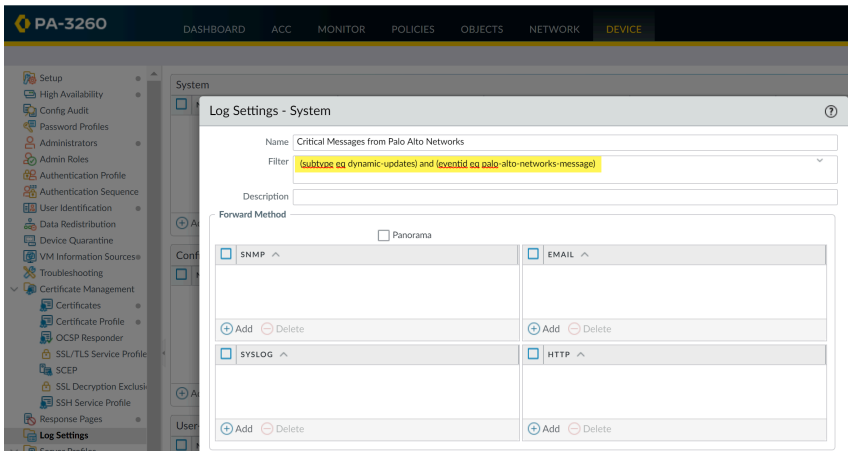
请勿安排 ***New App-ID Threshold***（新建 ***App-ID*** 阈值）。此阈值给予任务关键型组织额外的时间来根据新建 *App-ID* 调整安全策略实施。但是，因为该阈值还会延迟最新威胁防护更新的交付，因此不建议奉行安全第一的组织使用。

- 查看内容发布引入的新建和修改过的 App-ID，以评估更改可能会对安全策略产生的影响。以下主题介绍了您可以在安装新建 App-ID 前后用于更新安全策略的选项。管理新建和修改过的 App-ID。



- 设置日志转发，将 Palo Alto Networks 关键内容警告发送给您用于监控网络和防火墙活动的外部服务。为此，可以确保相应人员收到有关关键内容问题的通知，以便按需采取行动。关

键内容警告将记录为带有以下“类型”和“事件”的系统日志条目：(`subtype eq dynamic-updates`) 及 (`eventid eq palo-alto-networks-message`)。



PAN-OS 8.1.2 将关键内容警告的日志类型从 ***general*** 更改为 ***dynamic-updates***。如果使用 *PAN-OS 8.1.0* 或 *PAN-OS 8.1.1*，则关键内容将记录为带有有以下类型和事件的系统日志条目，同时，应使用下列筛选器设置转发这些警告：***(subtype eq general)*** 和 ***(eventid eq palo-alto-networks-message)***。

内容交付网络基础架构

Palo Alto Networks 维护了一个内容交付网络 (CDN) 基础架构，以便将内容更新交付到 Palo Alto Networks 防火墙。防火墙通过访问 CDN 中的 Web 资源来执行各种内容和应用程序标识功能。

下表列出了防火墙所访问的功能和应用的 Web 资源：

资源	网址	静态地址（如果需要静态服务器）
应用程序数据库 威胁/抗病毒数据库	• updates.paloaltonetworks.com（全球，不包括中国大陆） • updates.paloaltonetworks.cn（仅限中国大陆） 如果您的防火墙对 Internet 的访问受限，请将以下 URL 添加到您的防火墙允许列表： • downloads.paloaltonetworks.com:443 • proditpdownloads.paloaltonetworks.com:443 作为最佳实践，将更新服务器设置为 updates.paloaltonetworks.com。这允许 Palo Alto 网络防火墙从 CDN 基础结构中离它最近的服务器接收内容更新。 如果您需要其他参考信息或遇到连接和更新下载问题，请参阅：https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000001UtRCAU Palo Alto NetworksThreatVault 数据库包含有关漏洞、攻击、病毒和间谍软件威胁的信息。防火墙功能（包括 DNS 安全和防病毒配置文件）使用以下资源来检索威胁 ID 信息以创建例外项： • data.threatvault.paloaltonetworks.com	us-static.updates.paloaltonetworks.com 将以下 IPv4 或 IPv6 静态服务器地址集添加到防火墙允许列表中： • **IPv4**—35.186.202.45:443 和 34.120.74.244:443 • **IPv6**—[2600:1901:0:669::]:443 和 [2600:1901:0:5162::]:443 必须将为给定协议类型提供的两个 *IP* 地址都添加到允许列表中才能正常运行。
PAN-DB URL 筛选 |高级 URL 筛选	*.urlcloud.paloaltonetworks.com 解析到主 URL s0000.urlcloud.paloaltonetworks.com，然后重定向到最近的区域服务器： • s0100.urlcloud.paloaltonetworks.com • s0200.urlcloud.paloaltonetworks.com	不可使用静态 IP 地址。但是，您可以手动将 URL 解析到一个 IP 地址，并允许访问区域服务器 IP 地址。

资源	网址	静态地址（如果需要静态服务器）
	• s0300.urlcloud.paloaltonetworks.com • s0500.urlcloud.paloaltonetworks.com	
云服务	解析为 hawkeye.services-edge.paloaltonetworks.com，然后重定向到最近的区域服务器： • 美国 — **us.hawkeye.services-edge.paloaltonetworks.com** • 欧洲 — **eu.hawkeye.services-edge.paloaltonetworks.com** • 美国 — **uk.hawkeye.services-edge.paloaltonetworks.com** • 亚太地区 — **apac.hawkeye.services-edge.paloaltonetworks.com**	不可使用静态 IP 地址。
DNS 安全	• 云—dns.service.paloaltonetworks.com:443 • 遥测—io.dns.service.paloaltonetworks.com:443 下载允许列表时，dns.service.paloaltonetworks.com 解析为以下服务器： • static.dns.service.paloaltonetworks.com:443 • data.threatvault.paloaltonetworks.com（用于创建 DNS 例外）	不可使用静态 IP 地址。
基于防火墙的内联 ML： • URL 过滤 Inline ML • WildFire Inline ML	• ml.service.paloaltonetworks.com:443	不可使用静态 IP 地址。
WildFire	• 云（报告检索）—wildfire.paloaltonetworks.com:443 WildFire 云区域： • 全球 — wildfire.paloaltonetworks.com • 欧盟—eu.wildfire.paloaltonetworks.com • 日本 — jp.wildfire.paloaltonetworks.com	不可使用静态 IP 地址。

资源	网址	静态地址（如果需要静态服务器）
	• 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 — krv.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	

升级 Panorama

- 安装 Panorama 的内容更新和软件升级
- Panorama 升级问题故障排除
- 使用 Panorama 将更新部署到防火墙、日志收集器和 WildFire 设备

安装 Panorama 的内容更新和软件升级

有效的支持订阅能够让您访问 Panorama 软件映像和发行说明。要充分利用最新的修补程序和安全性增强功能，升级到您的经销商或 Palo Alto Networks 系统工程师为您的部署推荐的最新的软件和内容更新。安装软件和内容更新的步骤取决于 Panorama 是否能够直接访问互联网以及它是否具有高可用性 (HA) 配置。

- 在具有互联网连接的情况下升级 Panorama
- 在没有互联网连接的情况下升级 Panorama
- 在没有互联网连接的情况下自动安装 Panorama 更新
- 在高可用性配置中升级 Panorama
- 安装 PAN-OS 软件补丁
- 将 Panorama 日志迁移到新日志格式
- 升级 Panorama 以提高设备管理容量
- 在 FIPS-CC 模式下升级 Panorama 和受管设备
- 从 Panorama 11.1 降级

在具有互联网连接的情况下升级 Panorama

如果 Panorama™ 具有与互联网的直接连接，则执行以下步骤根据需要安装 Panorama 软件和内容更新。如果 Panorama 在高可用性 (HA) 配置中运行，请在每个对端设备上升级 Panorama 软件（请参阅在高可用性配置中升级 Panorama）。如果要将 FIPS-CC 模式下的 Panorama 和托管设备从 PAN-OS 10.2 或更早版本升级到 PAN-OS® 11.1，则必须采取额外步骤重置 FIPS-CC 模式下设备的安全连接状态（如果添加）在运行 PAN OS 10.2 版本时进行 Panorama 管理。有关在 FIPS-CC 模式下升级 Panorama 和 FIPS-CC 设备的更多详细信息，请参阅在 FIPS-CC 模式下升级 Panorama 和受管设备。

升级 Panorama 虚拟设备上的软件不会更改系统模式；切换到 Panorama 模式或仅管理模式是手动任务，需要您执行设置具有本地日志收集器的 Panorama 虚拟设备时所述的其他设置。

Palo Alto Networks 在升级路径的不同点引入了新的日志数据格式，具体取决于您要升级的 *PAN OS* 版本。

- 从 ***PAN-OS 8.1*** 升级到 ***PAN-OS 9.0***——*PAN-OS 9.0* 为本地和专用日志收集器引入了新的日志数据格式。在升级到 *PAN-OS 11.1* 的路径中，现有日志数据会在从 *PAN-OS 8.1* 升级到 *PAN-OS 9.0* 时自动迁移到新格式。
- 从 ***PAN-OS 10.0*** 升级到 ***PAN-OS 10.1***—*PAN-OS 10.1* 为本地和专用日志收集器引入了一种新的日志格式。在升级到 *PAN-OS 11.1* 的路径上，在 *PAN-OS 8.1* 或更早版本中生成的日志不再可用。这包括作为升级到 *PAN OS 9.0* 的一部分迁移的日志。升级到 *PAN-OS 10.1* 后，您可以选择恢复这些日志并将其迁移到 *PAN-OS 10.1* 日志格式。

同时，您必须在收集器组中更新所有日志收集器，以避免日志数据丢失。如果收集器组内的日志收集器并非全部都运行相同的 PAN-OS 版本，则不会转发日志或日志收集。此外，在所有日志收集器都运行相同的 PAN-OS 版本前，**ACC** 或 **Monitor**（监控）选项卡将不会显示用于收集器组内日志收集器的日志数据。例如，如果在收集器组内有三个日志收集器，且您更新其中的两个，则不会有日志转发到收集器组内任何日志收集器。

在升级 Panorama 前，请参阅发行说明以了解 PAN-OS® 11.1 所需的最低内容发行版本。

STEP 1 | 验证您计划安装的更新适用于您的 Panorama 部署。

Palo Alto Networks 强烈建议 *Panorama*，日志收集器和所有受管防火墙运行相同的内容发布版本。

- 请参阅发布说明以了解 Panorama 软件版本所需的最低内容发布版本。如果您打算升级日志收集器和防火墙到特定版本，则您必须首先将 Panorama 升级到该版本（或更高版本）。
- 对于在管理程序上运行的 Panorama 虚拟设备，请确保该实例满足设置 Panorama 虚拟设备的前提条件。

STEP 2 | 确定升级到 PAN-OS 11.1 的路径.

在从当前运行的 PAN-OS 版本升级到 PAN-OS 11.1 的路径中，您无法跳过任何功能发行版本的安装。

对于您在升级路径中会经过的每个版本，查看发行说明和升级/降级注意事项中的PAN-OS 升级清单、已知问题以及默认行为更改。

STEP 3 | （仅限 Panorama Interconnect 插件）将 Panorama 节点与 Panorama 控制器同步。

在开始升级 Panorama 节点之前，必须同步 Panorama 控制器和 Panorama 节点配置。为了在成功升级后将通用的 Panorama 控制器配置成功推送到 Panorama 节点，需要执行此操作。

STEP 4 | 保存当前 Panorama 配置文件的备份，如果您在升级时遇到问题，可以使用该备份恢复配置。

尽管 *Panorama* 自动创建配置备份，但最佳做法仍是在升级之前创建备份并通过外部方式将其保存。

1. 登录到 Panorama Web 界面。
2. 保存已命名 **Panorama** 配置快照（**Panorama** > **Setup**（设置） > **Operations**（操作）），输入配置的 **Name**（名称），然后单击 **OK**（确定）。
3. **Export named Panorama configuration snapshot**（导出已命名 **Panorama** 配置快照），选择您刚才所保存配置的 **Name**（名称），单击 **OK**（确定），然后将导出文件保存到 Panorama 之外的位置。

STEP 5 | （最佳实践）如果您正在使用 Cortex 数据湖 (CDL)，请安装 Panorama 设备证书。

升级到 PAN-OS 11.1 时，Panorama 会自动切换为使用设备证书向 CDL 摄取和查询端点验证身份。

如果在升级到 *PAN-OS 11.1* 之前没有安装设备证书，*Panorama* 将继续使用现有的日志记录服务证书进行身份验证。

STEP 6 | 在您的网络上启用以下 TCP 端口。

必须在网络上启用这些 TCP 端口，才能允许日志收集器之间进行通信。

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

STEP 7 | 安装最新的内容更新。

如果 *Panorama* 未运行您打算升级到的 *Panorama* 版本所需的最低内容版本，则必须在安装软件更新之前将内容版本更新为最低（或更高）版本。请参阅发布说明以了解 *Panorama* 版本的最低内容发布版本。

Palo Alto Networks® 强烈建议 *Panorama*，日志收集器和所有受管防火墙运行相同的内容发布版本。此外，我们建议您安排自动定期更新，以便始终运行最新的内容版本（请参阅18）。

1. 选择 **Panorama > Dynamic Updates**（动态更新）和 **Check Now**（立即检查）以获取最新更新。如果“操作”列中的值为 **Download**（下载），则表示有更新可用。

   确保 *Panorama* 运行的版本与受管防火墙和日志收集器上运行的内容发布版本相同，但不是更高版本。

2. （在更新 Panorama 上的内容发行版本前，请确保从 Panorama 中将防火墙升级到 PAN-OS 11.1，然后将日志收集器（请参阅在 Panorama 连接到互联网的情况下升级日志收集器）升级到相同（或更高版本）的内容发行版本。

   如果您目前不需要安装内容更新，请跳至下一步。

3. 根据需要安装剩余的内容更新。安装完成后，Currently Installed（当前已安装）列会显示一个复选标记。

   1. **Download**（下载）并 **Install**（安装）应用程序或应用程序和威胁更新。无论您的订阅如何，Panorama 都只安装和需要应用程序内容更新，而无需威胁内容。有关详细信息，请参阅 Panorama、日志收集器、防火墙和 WildFire 的版本兼容性。
   2. 根据需要一次性以任何顺序 **Download**（下载）并 **Install**（安装）其他更新（防病毒软件、WildFire 或 URL 筛选）。

STEP 8 | 对于当前安装在 Panorama 上的所有插件，选择 **Panorama > Plugins**（插件） 并 **Download**（下载）PAN-OS 11.1 上支持的插件版本。

有关目标 PAN-OS 11.1 版本支持的 Panorama 插件版本，请参阅兼容性矩阵。

这是成功地将 Panorama 从 PAN-OS 11.0 升级到 PAN-OS 11.1 所必需的。如果未下载支持的插件版本，将阻止升级到 PAN-OS 11.1。

Panorama 成功升级到 *PAN-OS 11.1* 后，将自动安装升级到 *PAN-OS 11.1* 所需的下载插件。如果下载的插件没有自动安装，则必须在升级到 *PAN-OS 11.1* 后手动安装受影响的插件。

STEP 9 | 在升级到 PAN-OS 11.1 的路径中，将 Panorama 升级到 PAN-OS 版本。

1. 在具有互联网连接的情况下升级 Panorama 到 PAN-OS 9.1。
2. 在具有互联网连接的情况下升级 Panorama 到 PAN-OS 10.0。

   （仅限传统模式下的 *Panorama*）**Download**（下载）*PAN-OS 10.0.0*，然后在继续升级路径之前 **Download**（下载）并 **Install**（安装）*PAN-OS 10.0.8* 或更高版本。

   这是保留存储在 *NFS* 存储分区上的所有日志所必需的。如果您安装 *PAN-OS 10.0.7* 或更早的 *PAN-OS 10.0* 版本，一些存储在传统模式下 *Panorama* 的 *NFS* 存储分区上的日志将被删除。
3. 在具有互联网连接的情况下升级 Panorama 到 PAN-OS 10.1。

   PAN-OS 10.1 引入了一种新的日志格式。从 PAN-OS 10.0 升级到 PAN-OS 10.1 时，您可以选择迁移在 PAN-OS 8.1 或更早版本中生成的日志。否则，在成功升级到 PAN-OS 10.1 时，系统会自动删除这些日志。在迁移期间，ACC 或监视选项卡中不会显示日志数据。在迁移过程中，日志数据会继续转发到相应的日志收集器，但是您可能会遇到一些性能影响。

   （仅限传统模式下的 *Panorama*）**Download**（下载）*PAN-OS 10.1.0*，然后 **Download**（下载）并 **Install**（安装）*PAN-OS 10.1.3* 或更高版本。

   这是保留存储在 *NFS* 存储分区上的所有日志所必需的。如果安装 *PAN-OS 10.1.2* 或更早的 *PAN-OS 10.1* 版本，一些存储在传统模式下 *Panorama* 的 *NFS* 存储分区上的日志将被删除。
4. 在具有互联网连接的情况下升级 Panorama 到 PAN-OS 10.2。
5. 在具有互联网连接的情况下升级 Panorama 到 PAN-OS 11.0。

STEP 10 | 将 Panorama 升级到 PAN-OS 11.1。

1. **Check Now**（立即检查）（**Panorama** > **Software**（软件））最新版本。

   （PAN-OS 11.1.3 及更高版本）默认情况下，显示首选版本和相应的基础版本。要仅查看首选版本，请禁用（清除）**Base Releases**（基础版本）复选框。同样地，要仅查看基础版本，请禁用（清除）**Preferred Releases**（首选版本）复选框。
2. 找到并 **Download**（下载）PAN-OS 11.1.0 映像。成功下载后，已下载映像的 Action（操作）列将从 **Download**（下载）更改为 **Install**（安装）。
3. （仅限 Panorama 模式）如果本地日志收集器包含在 PAN-OS 10.0 或更早版本中生成的日志，则会显示通知。

   在您第一次尝试 **Install**（安装）PAN-OS 11.1.2 或更高版本 11.1 时会显示此通知，关闭后不会再次显示该通知。它会警告您，系统检测到在运行 PAN-OS 10.0 或更早版本时由

Panorama 或托管设备生成的日志，并且将会在升级时删除这些日志。这意味着成功升级后无法查看或搜索受影响的日志。

但您可以在升级后恢复这些受影响的日志。该通知还为您提供以下信息：

- 受影响的日志类型。
- 每种日志类型受影响的时间范围。
- 恢复每种日志类型受影响的日志所需的每个 `debug logdb migrate-lc` 命令。

  在 **Close**（关闭）通知之前复制所列的 `debug logdb migrate-lc` 命令。

Close（关闭）通知。

4. **Install**（安装）下载的映像，然后重新启动。
   1. 安装映像。
   2. 安装成功完成后，请使用以下方法之一重新启动：
      - 如果提示重新启动，请单击 **Yes**（是）。如果系统显示 CMS Login 提示符，按 Enter 键，而不输入用户名或密码。当 Panorama 登录提示符出现后，输入在初始配置期间指定的用户名和密码。
      - 如果没有提示重新启动，单击设备操作部分中的 **Reboot Panorama**（重新启动 **Panorama**）（**Panorama** > **Setup**（设置） > **Operations**（操作））。

   Panorama 成功重启后继续下一步。

STEP 11 | （PAN-OS 11.1.2 及更高版本；仅限 Panorama 模式）登录到日志收集器 CLI，并使用上一步中列出的 `debug logdb migrate-lc` 命令恢复受影响的日志。

这些命令必须按顺序运行，不能同时运行。如果您没有从通知窗口复制 `debug logdb migrate-lc` 命令，请单击 **Tasks**（任务）并查看特定安装失败的作业详细信息。

STEP 12 | 验证您的 Panorama 插件版本是否支持 PAN-OS 11.1。

成功升级 Panorama 后，您必须验证并安装 PAN-OS 11.1 支持的 Panorama 插件版本。有关 PAN-OS 11.1 支持的 Panorama 插件的详细信息，请参阅兼容性矩阵。

1. 登录到 Panorama Web 界面 并查看 **Dashboard**（仪表板）中的 General Information（一般信息）小部件，以验证是否成功安装了兼容 PAN-OS 11.1 的插件版本。

   您还可以 登录到 Panorama CLI 并输入命令 `show plugins installed` 以查看当前安装的插件列表。
2. 选择 **Panorama** > **Plugins**（插件） 并搜索未安装的插件。
3. **Install**（安装）PAN-OS 11.1 支持的插件版本。
4. 重复上述步骤，直到 Panorama 上安装的所有插件都运行 PAN-OS 11.1 支持的版本。

STEP 13 | （如果本地日志收集器位于收集器组）升级收集器组内其他日志收集器。

- 当 Panorama 连接上互联网时升级日志收集器
- 当 Panorama 未连接互联网时升级日志收集器

STEP 14 | （FIPS-CC 模式下的 Panorama 和受管设备）在 FIPS-CC 模式下升级 Panorama 和受管设备。

如果在运行 PAN-OS 11.1 版本时将设备添加到 Panorama 管理中，则在 FIPS-CC 模式下升级 Panorama 和托管设备需要重置 FIPS-CC 模式下设备的安全连接状态。您需要将以下受管设备重新加入 Panorama 管理：

- 使用设备注册身份验证密钥将处于 FIPS-CC 模式的受管设备添加到 Panorama。
- 使用设备注册身份验证密钥将处于正常操作模式的受管设备添加到 Panorama

当受管设备运行 PAN-OS 10.0 或更早版本时，您无需重新加载添加到 Panorama 管理的受管设备。

STEP 15 | 重新生成或重新导入所有证书以遵守 OpenSSL 安全级别 2。

如果您从 PAN-OS 10.1 或更早版本升级到 PAN-OS 11.1，则需要执行此步骤。如果您从 PAN-OS 10.2 升级并且已经重新生成或重新导入了您的证书，请跳过此步骤。

所有证书都必须满足以下最低要求：

- RSA 2048 位或以上，或 ECDSA 256 位或以上
- SHA256 或更高版本的摘要

请参阅 PAN-OS 管理员指南或 Panorama 管理员指南，了解有关重新生成或重新导入证书的更多信息。

STEP 16 | （推荐用于 Panorama 模式）将 Panorama 虚拟设备的内存增加到 64GB。

在 Panorama 模式下成功将 Panorama 虚拟设备升级到 PAN-OS 11.1 后，Palo Alto Networks 建议将 Panorama 虚拟设备的内存增加到 64GB 以满足增加的系统要求，从而避免与配置不足的 Panorama 虚拟设备相关的任何日志、管理和操作性能问题。

STEP 17 | 选择 **Commit**（提交） > **Commit and Push**（提交并推送），然后将 Panorama 管理的配置 **Commit and Push**（提交并推送）到所有托管设备。

成功将 Panorama 和托管设备升级到 PAN-OS 11.1 后，需要完全提交和推送 Panorama 托管配置，然后才能将选择性配置推送到托管设备，并利用针对 Panorama 管理的多 vsys 防火墙改进的共享配置对象管理。

STEP 18 | （最佳做法）调度重复性自动内容更新。

Panorama 不会在高可用性对端设备之间同步内容更新调度。必须同时在主动和被动 *Panorama* 设备上执行此任务。

在每种更新类型的标头行中（**Panorama** > **Dynamic Updates**（动态更新）），**Schedule**（调度）最初设为 **None**（无）。应为每种更新类型执行以下步骤。

1. 单击 **None**（无），选择更新频率（**Recurrence**（重复））。频率选项取决于更新 Type（类型）。
2. 选择调度操作：
   - **Download And Install**（下载并安装）（最佳做法）— Panorama 下载更新后自动安装更新。

     Download Only（仅下载）— 您必须在 Panorama 下载更新后手动安装更新。
3. 根据贵组织的安全态势的最佳实践，配置在 Panorama 下载更新前更新变成可用后的延迟（**Threshold**（阈值））。
4. 单击 **OK**（确定）保存更改。
5. 选择 **Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

在没有互联网连接的情况下升级 Panorama

如果 Panorama™ 不具有与互联网的直接连接，则执行以下步骤根据需要安装 Panorama 软件和内容更新。如果 Panorama 是在高可用性 (HA) 配置中部署的，则必须升级每个对端设备（请参阅在高可用性配置中升级 Panorama）。如果您要从 PAN-OS 10.2 或更早版本将 Panorama 和处于 FIPS-CC 模式的托管设备升级到 PAN-OS 11.1，则在运行 PAN-OS 10.2 版本时，如果将其添加到 Panorama 管理中，则必须采取其他步骤，重置设备在 FIPS-CC 模式下的安全连接状态。有关在 FIPS-CC 模式下升级 Panorama 和 FIPS-CC 设备的更多详细信息，请参阅在 FIPS-CC 模式下升级 Panorama 和受管设备。

升级 Panorama 虚拟设备上的软件不会更改系统模式；切换到 Panorama 模式或仅管理模式是手动任务，需要您执行设置具有本地日志收集器的 Panorama 虚拟设备时所述的其他设置。

Palo Alto Networks 在升级路径的不同点引入了新的日志数据格式，具体取决于您要升级的 *PAN OS* 版本。

- 从 ***PAN-OS 8.1*** 升级到 ***PAN-OS 9.0***——*PAN-OS 9.0* 为本地和专用日志收集器引入了新的日志数据格式。在升级到 *PAN-OS 11.1* 的路径中，现有日志数据会在从 *PAN-OS 8.1* 升级到 *PAN-OS 9.0* 时自动迁移到新格式。
- 从 ***PAN-OS 10.0*** 升级到 ***PAN-OS 10.1***—*PAN-OS 10.1* 为本地和专用日志收集器引入了一种新的日志格式。在升级到 *PAN-OS 11.1* 的路径上，在 *PAN-OS 8.1* 或更早版本中生成的日志不再可用。这包括作为升级到 *PAN OS 9.0* 的一部分迁移的日志。升级到 *PAN-OS 10.1* 后，您可以选择恢复这些日志并将其迁移到 *PAN-OS 10.1* 日志格式。

同时，您必须在收集器组中更新所有日志收集器，以避免日志数据丢失。如果收集器组内的日志收集器并非全部都运行相同的 PAN-OS 版本，则不会转发日志或日志收集。此外，在所有日志收集器都运行相同的 PAN-OS 版本前，**ACC** 或 **Monitor**（监控）选项卡将不会显示用于收集器组内日志收集器的日志数据。例如，如果在收集器组内有三个日志收集器，且您更新其中的两个，则不会有日志转发到收集器组内任何日志收集器。

在更新 Panorama 前，请参阅发行说明以了解 PAN-OS® 11.1 所需的最低内容发行版本。

STEP 1 | 验证您计划安装的更新适用于您的 Panorama 部署。

Palo Alto Networks 强烈建议 *Panorama*，日志收集器和所有受管防火墙运行相同的内容发布版本。

- 请参阅发布说明以了解您必须为 Panorama 发布软件安装的最低内容发布版本。如果您打算升级日志收集器和防火墙到特定版本，则您必须首先将 Panorama 升级到该版本（或更高版本）。
- 对于 Panorama 虚拟设备，请确保该实例满足设置 Panorama 虚拟设备的前提条件。

STEP 2 | 确定升级到 PAN-OS 11.1 的路径.

在从当前运行的 PAN-OS 版本升级到 PAN-OS 11.1 的路径中，您无法跳过任何功能发行版本的安装。

对于您在升级路径中会经过的每个版本，查看发行说明和升级/降级注意事项中的PAN-OS 升级清单、已知问题以及默认行为更改。

STEP 3 | （仅限 Panorama Interconnect 插件）将 Panorama 节点与 Panorama 控制器同步。

在开始升级 Panorama 节点之前，必须同步 Panorama 控制器和 Panorama 节点配置。为了在成功升级后将通用的 Panorama 控制器配置成功推送到 Panorama 节点，需要执行此操作。

STEP 4 | 保存当前 Panorama 配置文件的备份，如果您在升级时遇到问题，可以使用该备份恢复配置。

尽管 *Panorama* 自动创建配置备份，但最佳做法仍是在升级之前创建备份并通过外部方式将其保存。

1. 登录到 Panorama Web 界面。
2. 保存已命名 **Panorama** 配置快照（**Panorama** > **Setup**（设置） > **Operations**（操作）），输入配置的 **Name**（名称），然后单击 **OK**（确定）。
3. **Export named Panorama configuration snapshot**（导出已命名 **Panorama** 配置快照），选择您刚才所保存配置的 **Name**（名称），单击 **OK**（确定），然后将导出文件保存到 Panorama 之外的位置。

STEP 5 | 将最新的内容更新下载到可以通过 SCP 或 HTTPS 连接并将内容上传到 Panorama 的主机。

如果您目前不需要安装内容更新，请跳至 6。

1. 使用能够访问互联网的主机登录到 Palo Alto Networks 客户支持网站。
2. 根据需要下载内容更新：
   1. 在资源部分中单击 **Updates**（更新） > **Dynamic Updates**（动态更新） 。
   2. **Download**（下载）相应内容更新，并将文件保存到主机。对您需要更新的每种内容类型执行此步骤。

STEP 6 | 在您的网络上启用以下 TCP 端口。

必须在网络上启用这些 TCP 端口，才能允许日志收集器之间进行通信。

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

STEP 7 | 安装最新的内容更新。

在安装软件更新之前，必须安装内容更新。首先，您必须从 Panorama 中将防火墙升级到 PAN-OS 11.1；然后升级日志收集器，再将其安装到 *Panorama* 管理服务器。

先安装应用程序或应用程序和威胁更新，然后按照任何顺序一次性安装任何其他更新（防病毒软件、WildFire® 和 URL 筛选）。

无论您的订阅是否同时包括应用程序和威胁内容，*Panorama* 都只安装和需要应用程序内容。有关详细信息，请参阅 Panorama、日志收集器、防火墙和 WildFire 的版本兼容性。

登录 Panorama Web 界面，然后对每种内容类型执行以下步骤：

1. 选择 **Panorama** > **Dynamic Updates**（动态更新）。
2. 单击 **Upload**（上传），选择内容 **Type**（类型），**Browse**（浏览）到将更新下载到的主机上的位置，选择更新，然后单击 **OK**（确定）。
3. 单击 **Install From File**（从文件安装），选择 **Package Type**（数据包类型），然后单击 **OK**（确定）。

STEP 8 | 对于当前安装在 Panorama 上的所有插件，上传 PAN-OS 11.1 支持的插件版本。

有关目标 PAN-OS 11.1 版本支持的 Panorama 插件版本，请参阅兼容性矩阵。

这是成功地将 Panorama 从 PAN-OS 11.0 升级到 PAN-OS 11.1 所必需的。如果未下载支持的插件版本，将阻止升级到 PAN-OS 11.1。

Panorama 成功升级到 *PAN-OS 11.1* 后，将自动安装升级到 *PAN-OS 11.1* 所需的下载插件。如果下载的插件没有自动安装，则必须在升级到 *PAN-OS 11.1* 后手动安装受影响的插件

1. 下载 PAN-OS 11.1 支持的插件版本。
   1. 登录到 Palo Alto Networks 支持门户。
   2. 选择 **Updates**（更新） > **Software Updates**（软件更新），然后从下拉菜单中选择插件。
   3. **Download**（下载） PAN-OS 10.2 支持的插件版本。
   4. 对当前安装在 Panorama 上的所有插件重复此步骤。
2. 登录到 Panorama Web 界面
3. 选择 **Panorama** > **Plugins**（插件）并 **Upload**（上传）您在上一步中下载的插件版本。对当前安装在 Panorama 上的所有插件重复此步骤。

STEP 9 | 在升级到 PAN-OS 11.1 的路径中，将 Panorama 升级到 PAN-OS 版本。

1. 在未连接到互联网的情况下升级 Panorama 到 PAN-OS 9.1。
2. 在未连接到互联网的情况下升级 Panorama 到 PAN-OS 10.0。

   （仅限传统模式下的 *Panorama*）**Download**（下载）*PAN-OS 10.0.0*，然后在继续升级路径之前 **Download**（下载）并 **Install**（安装）*PAN-OS 10.0.8* 或更高版本。

   这是保留存储在 *NFS* 存储分区上的所有日志所必需的。如果您安装 *PAN-OS 10.0.7* 或更早的 *PAN-OS 10.0* 版本，一些存储在传统模式下 *Panorama* 的 *NFS* 存储分区上的日志将被删除。
3. 在未连接到互联网的情况下升级 Panorama 到 PAN-OS 10.1。

   PAN-OS 10.1 引入了一种新的日志格式。从 PAN-OS 10.0 升级到 PAN-OS 10.1 时，您可以选择迁移在 PAN-OS 8.1 或更早版本中生成的日志。否则，在成功升级到 PAN-OS 10.1 时，系统会自动删除这些日志。在迁移期间，ACC 或监视选项卡中不会显示日志数据。在迁移过程中，日志数据会继续转发到相应的日志收集器，但是您可能会遇到一些性能影响。

   （仅限传统模式下的 *Panorama*）**Download**（下载）*PAN-OS 10.1.0*，然后 **Download**（下载）并 **Install**（安装）*PAN-OS 10.1.3* 或更高版本。

   这是保留存储在 *NFS* 存储分区上的所有日志所必需的。如果安装 *PAN-OS 10.1.2* 或更早的 *PAN-OS 10.1* 版本，一些存储在传统模式下 *Panorama* 的 *NFS* 存储分区上的日志将被删除。
4. 在未连接到互联网的情况下升级 Panorama 到 PAN-OS 10.2。
5. 在未连接到互联网的情况下升级 Panorama 到 PAN-OS 11.0。

STEP 10 | 将最新的 PAN-OS 11.1 版本映像下载到可以通过 SCP 或 HTTPS 连接并将内容上传到 Panorama 的主机。

1. 使用能够访问互联网的主机，登录到 Palo Alto Networks 客户支持网站。
2. 下载软件更新：
   1. 在 Palo Alto Networks 客户支持网站的主页上，单击 **Updates**（更新）> **Software Updates**（软件更新）。
   2. 找到特定于型号的最新 PAN-OS 11.1 版本映像。例如，要将 M-Series 设备升级到 Panorama 11.1.0，请下载 `Panorama_m-11.1.0` 映像；要将 Panorama 虚拟设备升级到 Panorama 11.1.0，请下载 `Panorama_pc-11.1.0` 映像。

      您可以通过从 **Content By**（按内容）下拉列表中选择 ***Panorama M Images***（*Panorama M* 映像）（*M-Series* 设备）或 ***Panorama Updates***（*Panorama* 更新）（虚拟设备）快速找到 *Panorama* 映像。

      （*PAN-OS 11.1.3* 及更高版本）默认情况下，结果显示首选版本。在 ***Release type***（版本类型）字段中，单击 ***Other***（其他）以查看其他可用的版本。
   3. 单击文件名并将文件保存到主机。

STEP 11 | 将 Panorama 升级到 PAN-OS 11.1。

1. 登录到 Panorama Web 界面。
2. 选择 **Panorama** > **Software**（软件）并 **Upload**（上传）您在上一步中下载的 PAN-OS 11.1 映像。
3. **Browse**（浏览）到将更新下载到的主机上的位置，选择更新，选择 **Sync To Peer**（同步到对端设备）（如果 Panorama 具有高可用性配置）（以将软件映像推送到辅助对端设备），然后单击 **OK**（确定）。
4. （仅限 Panorama 模式）如果本地日志收集器包含在 PAN-OS 10.0 或更早版本中生成的日志，则会显示通知。

   在您第一次尝试 **Install**（安装）PAN-OS 11.1.2 或更高版本 11.1 时会显示此通知，关闭后不会再次显示该通知。它会警告您，系统检测到在运行 PAN-OS 10.0 或更早版本时由 Panorama 或托管设备生成的日志，并且将会在升级时删除这些日志。这意味着成功升级后无法查看或搜索受影响的日志。

   但您可以在升级后恢复这些受影响的日志。该通知还为您提供以下信息：

   - 受影响的日志类型。
   - 每种日志类型受影响的时间范围。
   - 恢复每种日志类型受影响的日志所需的每个 `debug logdb migrate-lc` 命令。

     在 **Close**（关闭）通知之前复制所列的 `debug logdb migrate-lc` 命令。

   Close（关闭）通知。
5. 安装软件映像并重新启动。

   对于 HA 配置，在高可用性配置中升级 Panorama；否则：

   1. **Install**（安装）上传的映像。
   2. 安装成功完成后，使用以下方法之一重新启动：

      - 如果提示重新启动，请单击 **Yes**（是）。如果系统显示 CMS Login 提示符，按 Enter 键，而不输入用户名或密码。当 Panorama 登录提示符出现后，输入在初始配置期间指定的用户名和密码。
      - 如果没有提示重新启动，单击设备操作部分中的 **Reboot Panorama**（重新启动 **Panorama**）（**Panorama** > **Setup**（设置） > **Operations**（操作））。

   Panorama 成功重启后继续下一步。

STEP 12 | （PAN-OS 11.1.2 及更高版本；仅限 Panorama 模式）登录到日志收集器 CLI，并使用上一步中列出的 `debug logdb migrate-lc` 命令恢复受影响的日志。

这些命令必须按顺序运行，不能同时运行。如果您没有从通知窗口复制 `debug logdb migrate-lc` 命令，请单击 **Tasks**（任务）并查看特定安装失败的作业详细信息。

STEP 13 | 验证您的 Panorama 插件版本是否支持 PAN-OS 11.1。

成功升级 Panorama 后，您必须验证并安装 PAN-OS 11.1 支持的 Panorama 插件版本。有关 PAN-OS 11.1 支持的 Panorama 插件的详细信息，请参阅兼容性矩阵。

1. 登录到 Panorama Web 界面 并查看 **Dashboard**（仪表板）中的 General Information（一般信息）小部件，以验证是否成功安装了兼容 PAN-OS 11.1 的插件版本。

   您还可以 登录到 Panorama CLI 并输入命令 `show plugins installed` 以查看当前安装的插件列表。
2. 选择 **Panorama** > **Plugins**（插件） 并搜索未安装的插件。
3. **Install**（安装）PAN-OS 11.1 支持的插件版本。
4. 重复上述步骤，直到 Panorama 上安装的所有插件都运行 PAN-OS 11.1 支持的版本。

STEP 14 | （如果本地日志收集器位于收集器组）升级收集器组内其他日志收集器。

STEP 15 | （推荐用于 Panorama 模式）将 Panorama 虚拟设备的内存增加到 64GB。

在 Panorama 模式下成功将 Panorama 虚拟设备升级到 PAN-OS 11.1 后，Palo Alto Networks 建议将 Panorama 虚拟设备的内存增加到 64GB 以满足增加的系统要求，从而避免与配置不足的 Panorama 虚拟设备相关的任何日志、管理和操作性能问题。

STEP 16 | （FIPS-CC 模式下的 Panorama 和受管设备）在 FIPS-CC 模式下升级 Panorama 和受管设备。

如果在运行 PAN-OS 11.1 版本时将设备添加到 Panorama 管理中，则在 FIPS-CC 模式下升级 Panorama 和托管设备需要重置 FIPS-CC 模式下设备的安全连接状态。您需要将以下托管设备重新加入 Panorama 管理：

- 使用设备注册身份验证密钥将 FIPS-CC 模式下的托管设备添加到 Panorama。
- 使用设备注册身份验证密钥将处于正常操作模式的托管设备添加到 Panorama

当托管设备运行 PAN-OS 10.0 或更早版本时，您无需重新加入已添加到 Panorama 管理的托管设备。

STEP 17 | （PAN-OS 10.2 及更高版本）重新生成或重新导入所有证书以符合 OpenSSL 安全级别 2。

如果您从 PAN-OS 10.1 或更早版本升级到 PAN-OS 11.1，则需要执行此步骤。如果您从 PAN-OS 10.2 升级并且已经重新生成或重新导入了您的证书，请跳过此步骤。

所有证书都必须满足以下最低要求：

- RSA 2048 位或以上，或 ECDSA 256 位或以上
- SHA256 或更高版本的摘要

请参阅 PAN-OS 管理员指南或 Panorama 管理员指南，了解有关重新生成或重新导入证书的更多信息。

STEP 18 | 选择 **Commit**（提交） > **Commit and Push**（提交并推送），然后将 Panorama 管理的配置 **Commit and Push**（提交并推送）到所有托管设备。

成功将 Panorama 和托管设备升级到 PAN-OS 11.1 后，需要完全提交和推送 Panorama 托管配置，然后才能将选择性配置推送到托管设备，并利用针对 Panorama 管理的多 vsys 防火墙改进的共享配置对象管理。

在没有互联网连接的情况下自动安装 Panorama 更新

自动下载内容更新到物理隔离的网络中的防火墙、日志收集器和 WildFire® 设备，在该网络中，Panorama™ 管理服务器、受管防火墙、日志收集器和 WildFire 设备均不连接至互联网。要实现这一点，您必须部署一个可访问互联网的额外 Panorama 和一个 SCP 服务器。在部署可访问互联网的 Panorama 后，将已连接到互联网的 Panorama 配置为自动下载内容更新到 SCP 服务器。将物理隔离的 Panorama 配置为根据内容更新计划自动从 SCP 服务器下载并安装内容更新。当可访问互联网的 Panorama 下载内容更新到 SCP 服务器或当物理隔离的 Panorama 从 SCP 服务器下载并安装内容更新时，Panorama 会生成一个系统日志。

仅支持从已连接互联网的 Panorama 到无互联网连接的 Panorama 的以下内容更新计划：

在将内容更新文件成功下载到 *SCP* 服务器后，不要操作或更改内容更新文件的名称。*Panorama* 无法下载和安装文件名修改过的内容更新。此外，为使自动内容更新成功，您必须确保 *SCP* 服务器上有足够的磁盘空间、当准备开始下载时 *SCP* 服务器正在运行，以及两个 *Panorama* 均已开启且未处于正在重新启动状态。

本示例显示如何为应用程序和威胁内容更新配置自动内容更新。

STEP 1 | 部署一个 SCP 服务器。

从已连接互联网的 Panorama 为受管防火墙、日志收集器和 WildFire 设备下载内容更新。物理隔离的 Panorama 从 SCP 服务器下载内容更新，然后将更新安装在受管防火墙、WildFire 设备和日志收集器上。

创建用于内容更新的文件夹目录时，最佳实践是为每种类型的动态更新各创建一个文件夹。这是管理大量动态更新的负担，减少了删除不应从 *SCP* 服务器删除的内容更新的可能性。

STEP 2 | 部署已连接互联网的 Panorama。

此 Panorama 与 Palo Alto Networks 更新服务器进行通信，并将内容更新下载到 SCP 服务器。

1. 重新启动 Panorama 管理服务器。
   - 设置 M 系列设备
   - 设置 Panorama 虚拟设备
2. 执行初始 Panorama 配置。
   - 执行 M 系列设备的初始配置
   - 执行 Panorama 虚拟设备的初始配置

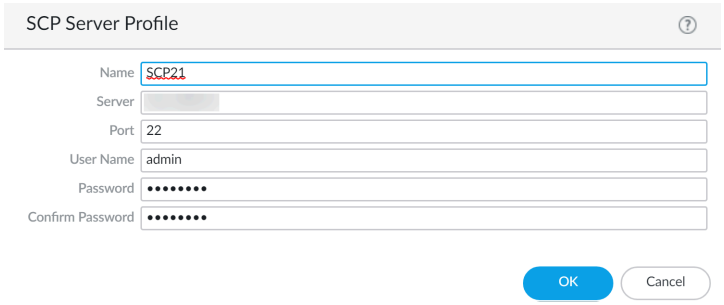
STEP 3 | 部署不具有互联网连接的 Panorama。

此 Panorama 与 SCP 服务器进行通信，以在受管防火墙、日志收集器和 WildFire 设备上下载并安装内容更新。

1. 重新启动 Panorama 管理服务器。
   - 设置 M 系列设备
   - 设置 Panorama 虚拟设备
2. 执行初始 Panorama 配置。
   - 执行 M 系列设备的初始配置
   - 执行 Panorama 虚拟设备的初始配置
3. 添加您的受管防火墙、日志收集器和 WildFire 设备。
   - 添加防火墙作为受管设备
   - 配置受管收集器
   - 添加独立 WildFire 设备以使用 Panorama 进行管理

STEP 4 | 将已连接互联网的 Panorama 配置为下载内容更新到 SCP 服务器。

1. 登录到 Panorama Web 界面。
2. 创建 SCP 服务器配置文件。
   1. 选择 **Panorama** > **Server Profiles**（服务器配置文件） > **SCP**，并 **Add**（添加）新的 SCP 服务器配置文件。
   2. 为 SCP 服务器配置文件输入描述性 **Name**（名称）。
   3. 输入 SCP **Server**（服务器）IP 地址。
   4. 输入 **Port**（端口）。
   5. 输入 SCP 服务器 **User Name**（用户名）。
   6. 输入 SCP 服务器 **Password**（密码）和 **Confirm Password**（确认密码）。
   7. 单击 **OK**（确定）保存更改。

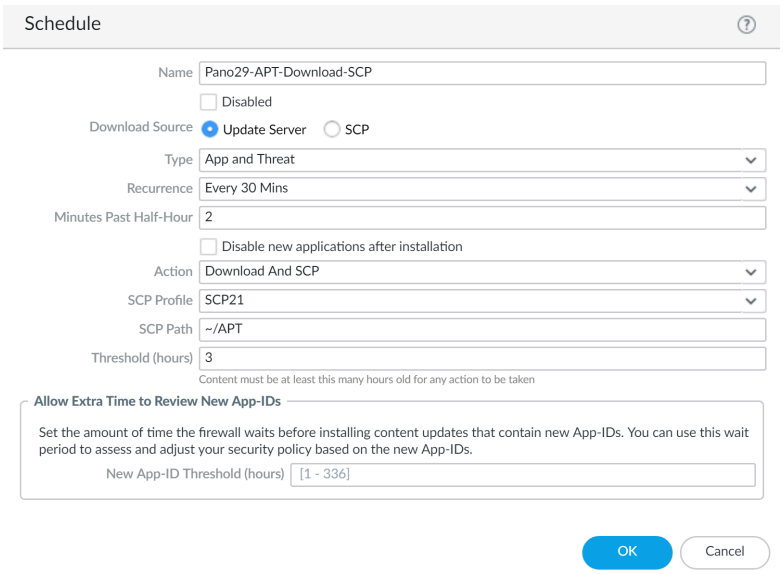


3. 创建内容更新计划以定期将内容更新下载到 SCP 服务器。

   您必须为打算自动下载并安装在受管防火墙、日志收集器和 WildFire 设备上的每种类型内容更新创建计划。

   1. 选择 **Panorama** > **Device Deployment**（设备部署） > **Dynamic Updates**（动态更新），并选择 **Schedules**（计划），然后 **Add**（添加）内容更新计划。
   2. 为内容更新计划输入描述性 **Name**（名称）。
   3. 对于 **Download Source**（下载源），选择 **Update Server**（更新服务器）。
   4. 选择内容更新 **Type**（类型）。
   5. 选择 **Recurrence**（重复）以设置 Panorama 检查 Palo Alto Networks 更新服务器查看新内容更新的间隔。

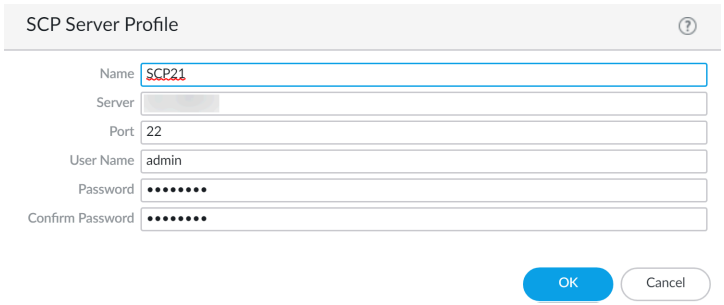
      要配置更精确的重复计划，请输入所选重复间隔之后的分钟数。如果您计划使用相同的重复间隔下载多个内容更新，请交错安排以免 *Panorama* 和 *SCP* 服务器过载。
   6. 对于 **Action**（操作），选择 **Download And SCP**（下载和 **SCP**）。
   7. 选择您在上一步中配置的 **SCP Profile**（**SCP** 配置文件）。
   8. 输入内容更新类型的 **SCP Path**（**SCP** 路径）。
   9. （可选）输入内容更新的 **Threshold**（阈值）（以小时为单位）。Panorama 仅下载达到此存在小时数（或更久）的内容更新
   10. 单击 **OK**（确定）保存更改。



4. **Commit**（提交）更改。

STEP 5 | 配置物理隔离的 Panorama 以从 SCP 服务器下载内容更新，然后将更新安装在受管防火墙、日志收集器和 WildFire 设备上。

1. 登录到 Panorama Web 界面。
2. 创建 SCP 服务器配置文件。
   1. 选择 **Panorama** > **Server Profiles**（服务器配置文件） > **SCP**，并 **Add**（添加）新的 SCP 服务器配置文件。
   2. 为 SCP 服务器配置文件输入描述性 **Name**（名称）。
   3. 输入 SCP **Server**（服务器）IP 地址。
   4. 输入 **Port**（端口）。
   5. 输入 SCP 服务器 **User Name**（用户名）。
   6. 输入 SCP 服务器 **Password**（密码）和 **Confirm Password**（确认密码）。
   7. 单击 **OK**（确定）保存更改。



3. 创建内容更新计划，以定期从 SCP 服务器下载并安装内容更新。

   您必须为打算自动下载并安装在受管防火墙、日志收集器和 WildFire 设备上的每种类型内容更新创建计划。
   1. 选择 **Panorama** > **Device Deployment**（设备部署） > **Dynamic Updates**（动态更新），并选择 **Schedules**（计划），然后 **Add**（添加）内容更新计划。
   2. 为内容更新计划输入描述性 **Name**（名称）。
   3. 对于 **Download Source**（下载源），选择 **SCP**。
   4. 选择您在上一步中配置的 **SCP Profile**（SCP 配置文件）。
   5. 输入内容更新类型的 **SCP Path**（SCP 路径）。
   6. 选择内容更新 **Type**（类型）。
   7. 选择 **Recurrence**（重复）以设置 Panorama 检查 Palo Alto Networks 更新服务器查看新内容更新的间隔。

      要配置更精确的重复计划，请输入所选重复间隔之后的分钟数。如果您计划使用相同的重复间隔下载多个内容更新，请交错安排以免 *Panorama* 和 *SCP* 服务器过载。
   8. 对于 **Action**（操作），选择 **Download**（下载）或 **Download And Install**（下载并安装）。

当 ***Download Source***（下载源）为 ***SCP*** 时，仅支持 ***Download***（下载）和 ***Download and Install***（下载并安装）。

如果您选择 ***Download***（下载），则必须在受管防火墙上手动启动内容更新安装。

9. 选择要在其上安装内容更新的 **Devices**（设备）。
10. （可选）输入内容更新的 **Threshold**（阈值）（以小时为单位）。Panorama 仅下载达到此存在小时数（或更久）的内容更新
11. 单击 **OK**（确定）保存更改。

4. **Commit**（提交）更改。

在高可用性配置中升级 Panorama

要在高可用性 (HA) 配置中更新 Panorama 软件时确保无缝故障转移，主动和被动 Panorama 对端设备必须使用相同的应用程序数据库版本运行相同的 Panorama 版本。以下示例说明如何升级 HA 对端设备（主动对端设备为 Primary_A，被动对端设备为 Secondary_B）。

如果您要从 PAN-OS 10.2 或更早版本将 Panorama 和处于 FIPS-CC 模式的托管设备升级到 PAN-OS 11.1，则在运行 PAN-OS 10.2 版本时，如果将其添加到 Panorama 管理中，则必须采取其他步骤，重置设备在 FIPS-CC 模式下的安全连接状态。有关在 FIPS-CC 模式下升级 Panorama 和 FIPS-CC 设备的更多详细信息，请参阅在 FIPS-CC 模式下升级 Panorama 和受管设备。

在更新 Panorama 前，请参阅 发行说明以了解 PAN-OS 11.0 所需的最低内容发行版本。

STEP 1 | 在 Secondary_B 设备（被动）对端设备上升级 Panorama 软件版本。

在 Secondary_B 对端设备上执行以下任务之一：

- 在具有互联网连接的情况下升级 Panorama
- 在没有互联网连接的情况下升级 Panorama

在升级后，Panorama 将会转换为非运行状态，因为对端设备不再运行相同的软件版本。

STEP 2 | （仅限 Panorama Interconnect 插件）将 Panorama 节点与 Panorama 控制器同步。

在开始升级 Panorama 节点之前，必须同步 Panorama 控制器和 Panorama 节点配置。为了在成功升级后将通用的 Panorama 控制器配置成功推送到 Panorama 节点，需要执行此操作。

STEP 3 | （最佳实践）如果您正在使用 Cortex 数据湖 (CDL)，请在每个 Panorama HA 对等设备上安装 Panorama 设备证书。

升级到 PAN-OS 11.0 时，Panorama 会自动切换为使用设备证书向 CDL 摄取和查询端点验证身份。

如果在升级到 *PAN-OS 11.0* 之前没有安装设备证书，*Panorama* 将继续使用现有的日志记录服务证书进行身份验证。

STEP 4 | 挂起 Primary_A 对端设备以执行故障转移。

在 Primary_A 对端设备上：

1. 在 **Operational Commands**（操作命令）部分中（**Panorama** > **High Availability**（高可用性）），挂起本地 **Panorama**。
2. 核实状态为 `suspended`（显示在 Web 界面的右下角）。

   由此产生的故障转移应导致 Secondary_B 对端设备转换为 `active` 状态。

STEP 5 | 在 Primary_A（当前为被动）对端设备上升级 Panorama 软件版本。

在 Primary_A 对端设备上执行以下任务之一：

- 在具有互联网连接的情况下升级 Panorama
- 在没有互联网连接的情况下升级 Panorama

在重新启动后，Primary_A 对端设备最初仍处于被动状态。然后，如果启用抢先（默认），Primary_A 对端设备自动转换为主动状态，Secondary_B 对端设备恢复为被动状态。

如果您禁用了抢先，手动将主要 Panorama 还原至主动状态。

STEP 6 | 验证两个对端设备现在是否正在运行任何新安装的内容发布版本和新安装的 Panorama 版本。

在每个 Panorama 对端设备的 **Dashboard**（仪表盘）上，检查 Panorama Software Version（Panorama 软件版本）和 Application Version（应用程序版本），并确认它们在两个对端设备上相同且运行的配置已同步。

STEP 7 | （仅限收集器组内的本地日志收集器）升级收集器组内其他日志收集器。

- 当 Panorama 连接上互联网时升级日志收集器
- 当 Panorama 未连接互联网时升级日志收集器

STEP 8 | （推荐用于 Panorama 模式）将 Panorama 虚拟设备的内存增加到 64GB。

在 Panorama 模式下成功将 Panorama 虚拟设备升级到 PAN-OS 11.1 后，Palo Alto Networks 建议将 Panorama 虚拟设备的内存增加到 64GB 以满足增加的系统要求，从而避免与配置不足的 Panorama 虚拟设备相关的任何日志、管理和操作性能问题。

STEP 9 | 选择 **Commit**（提交） > **Commit and Push**（提交并推送），然后将 Panorama 管理的配置 **Commit and Push**（提交并推送）到所有托管设备。

成功将 Panorama 和托管设备升级到 PAN-OS 11.1 后，需要完全提交和推送 Panorama 托管配置，然后才能将选择性配置推送到托管设备，并利用针对 Panorama 管理的多 vsys 防火墙改进的共享配置对象管理。

STEP 10 | （FIPS-CC 模式下的 Panorama 和受管设备）在 FIPS-CC 模式下升级 Panorama 和受管设备。

如果在运行 PAN-OS 11.1 版本时将设备添加到 Panorama 管理中，则在 FIPS-CC 模式下升级 Panorama 和托管设备需要重置 FIPS-CC 模式下设备的安全连接状态。您需要将以下托管设备重新加入 Panorama 管理：

- 使用设备注册身份验证密钥将 FIPS-CC 模式下的托管设备添加到 Panorama。
- 使用设备注册身份验证密钥将处于正常操作模式的托管设备添加到 Panorama

当托管设备运行 PAN-OS 10.0 或更早版本时，您无需重新加入已添加到 Panorama 管理的托管设备。

STEP 11 | 重新生成或重新导入所有证书以遵守 OpenSSL 安全级别 2。

如果您从 PAN-OS 10.1 或更早版本升级到 PAN-OS 11.1，则需要执行此步骤。如果您从 PAN-OS 10.2 升级并且已经重新生成或重新导入了您的证书，请跳过此步骤。

所有证书都必须满足以下最低要求：

- RSA 2048 位或以上，或 ECDSA 256 位或以上
- SHA256 或更高版本的摘要

请参阅 PAN-OS 管理员指南或 Panorama 管理员指南，了解有关重新生成或重新导入证书的更多信息。

安装 PAN-OS 软件补丁

在何处可以使用？	需要提供什么？
• 运行 PAN-OS 11.1.3 或更高版本的 Panorama	☐ 设备管理许可证 ☐ 支持许可证 ☐ PAN-OS 11.1.3 或更高的 11.1 版本

在何处可以使用？	需要提供什么？
	❑ 出站互联网接入

查看 PAN-OS 11.1 发行说明，然后按照以下步骤安装 PAN-OS 软件补丁，以解决当前在 Panorama™ 管理服务器上运行的 PAN-OS 版本中的错误以及公共漏洞和暴露 (CVE)。安装 PAN-OS 软件补丁可修复错误和 CVE，无需安排长期维护，并允许您立即加强安全态势，而不会引入任何新的已知问题或更改安装新 PAN-OS 版本时可能出现的默认行为。此外，您可以恢复当前安装的软件补丁，以卸载安装软件补丁时应用的错误和 CVE 修复程序。

安装或恢复 PAN-OS 软件补丁时会生成系统日志（**Monitor**（监视） > **Logs**（日志） > **System**（系统））。需要出站互联网连接才能从 Palo Alto Networks 客户支持门户下载 PAN-OS 软件补丁。

- 安装
- 恢复

安装

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 选择 **Panorama** > **Software**（软件），然后 **Check Now**（立即检查）以从 Palo Alto Networks 更新服务器检索最新的 PAN-OS 软件补丁。

STEP 3 | 选中（启用）**Include Patch**（包含补丁），以显示所有可用的 PAN-OS 软件补丁。

STEP 4 | 找到当前安装在 Panorama 上的 PAN-OS 版本的软件补丁。

通过 **Version**（版本）名称旁边显示的 `Patch` 标签来表示软件补丁。

STEP 5 | 查看 **More Info**（更多信息），以查看软件补丁的详细信息，例如严重错误和 CVE 修复程序，以及是否需要重新启动下一代防火墙才能应用修复程序。

STEP 6 | **Download**（下载）软件补丁。

（仅限 HA）选中（启用）同步到 HA 对等设备，然后选择 **Continue Download**（继续下载）以下载 PAN-OS 软件补丁。

成功下载软件补丁后单击 **Close**（关闭）。

STEP 7 | **Install**（安装）软件补丁。

成功安装软件补丁后，单击 **Close**（关闭）。

STEP 8 | **Apply**（应用）软件补丁。

当系统提示您确认要将已安装的 PAN-OS 软件补丁应用于 Panorama 时，单击 **Apply**（应用）。

将显示一个状态栏，显示 PAN-OS 软件补丁应用程序的当前进度。成功应用补丁后，单击 **Close**（关闭）。

此时，如果需要重新启动才能将 PAN-OS 软件补丁应用于 Panorama，Panorama 将自动重新启动。

STEP 9 | （仅限 HA）在 Panorama HA 对等设备上安装 PAN-OS 软件补丁。

1. 登录到 HA 对等设备的 Panorama Web 界面。
2. 选择 **Panorama** > **Software**（软件）以及 **Check Now**（立即检查）。
3. **Install**（安装）软件补丁。
4. 如果需要，重新启动 Panorama。

恢复

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 选择 **Panorama** > **Software**（软件），并找到要恢复的 PAN-OS 软件补丁。

STEP 3 | **Revert**（恢复）软件补丁。

当系统提示您确认要恢复 Panorama 上安装的 PAN-OS 软件补丁时，单击 **Revert**（恢复）。

将显示一个状态栏，显示 PAN-OS 软件补丁应用程序的当前进度。成功应用补丁后，单击 **Close**（关闭）。

此时，如果需要重新启动才能将 PAN-OS 软件补丁应用于 Panorama，防火墙将自动重新启动。

将 Panorama 日志迁移到新日志格式

升级到 Panorama 8.0 或更高版本后，Panorama 日志收集器将使用新的日志存储格式。由于 Panorama 在升级后不能再以 8.0 版本之前的日志格式生成报告或 ACC 数据，因此只要将 Panorama 及其日志收集器从 PAN-OS®7.1 或更早版本升级到现有日志，就必须迁移到 PAN-OS 8.0 或更高版本，并且您必须在升级受管防火墙前执行此操作。在升级到 PAN-OS 8.0 或更高版本后，Panorama 将继续在日志迁移过程中从受管设备收集日志，但会将传入日志存储为新日志格式。因此，在 Panorama 完成日志迁移过程前，您只能在 ACC 和报表中看到部分数据。

将日志迁移到新格式是您升级到 *PAN-OS 8.0* 或更高版本时（或是当您将升级到 *PAN-OS 8.0* 作为您的升级路径时）必须执行的一次性任务；升级到更高 *PAN-OS* 版本时，不需要再次执行此迁移。

Panorama 用于完成日志迁移过程的时间取决于写入 Panorama 的新日志的数量以及要迁移的日志数据库的大小。由于日志迁移是一个 CPU 密集型过程，因此在日志记录速率较低时开始迁移。如果您注意到 CPU 利用率较高，则可以在高峰时段始终停止迁移，并在传入日志速率较低时继续迁移。

在您安装 Panorama 的内容和软件更新 和升级日志收集器后，请按以下步骤迁移日志：

查看传入日志记录速率。

为获得最佳效果，请在传入日志速率较低时开始日志迁移。要检查速率，请从日志收集器 CLI 运行以下命令：

```
admin@FC-M500-1> debug log-collector log-collection-stats show
 incoming-logs
```

预计日志迁移期间 *CPU* 利用率较高（接近 *100#*），操作将继续正常运行。在出现资源争用的情况下，日志迁移将受到限制以支持传入日志和其他进程。

开始将每个日志收集器上的日志迁移到新格式。

要开始迁移，请从每个日志收集器的 CLI 输入以下命令：

```
admin@FC-M500-1> request logdb migrate lc serial-number <ser_num>
 start
```

查看日志迁移状态以估计完成将所有现有日志迁移到新格式所需的时间。

```
admin@FC-M500-1> request logdb migrate lc serial-number <ser_num>
 status Slot: all Migration State:进行中完成百分比：0.04 预计剩余时
间：451 小时 47 分
```

停止日志迁移过程。

要暂时停止日志迁移过程，请从日志收集器 CLI 输入以下命令：

```
admin@FC-M500-1 request logdb migrate lc serial-number <ser_num>
 stop
```

升级 Panorama 以提高设备管理容量

升级到 PAN-OS 9.1 或更高版本，以使用 M-600 设备上的现有设备管理许可证管理最多 5,000 个防火墙，或者使用 Panorama™ 虚拟设备管理最多 2,500 个防火墙。

STEP 1 | 如果 Panorama 虚拟设备尚未满足增加设备管理的最低资源要求，则增加 Panorama 虚拟设备的 CPU 和内存。

在升级之前，查看增加的设备管理容量要求以验证您现有的 Panorama 虚拟设备是否满足最低要求。

STEP 2 | 登录到 Panorama 命令行界面。

STEP 3 | 如果此模式下的 Panorama 不可用，则将 Panorama 管理服务器更改为“仅管理”。

- （仅限 M-600 设备）从第 5 步开始在仅管理模式下设置 M 系列设备。

或者

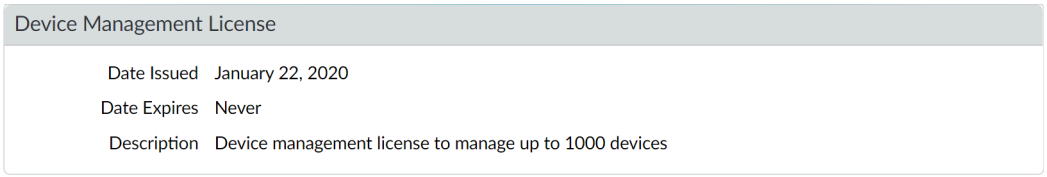
- 在仅管理模式下设置 Panorama 虚拟设备。

STEP 4 | 登录到 Panorama Web 界面。

STEP 5 | 升级 Panorama 管理服务器。

- 在具有互联网连接的情况下升级 Panorama.
- 在没有互联网连接的情况下升级 Panorama.
- 在高可用性配置中升级 Panorama.

STEP 6 | 选择 **Panorama** > **Licenses**（许可证），并验证设备管理许可证成功激活。



如果已激活设备管理许可证并随后升级到 *PAN-OS 9.1* 或更高版本，则可以通过 *M-600* 设备管理最多 *5,000* 个防火墙或者通过 *Panorama* 虚拟设备管理最多 *2,500* 个防火墙，但 *Description*（说明）部分仍会显示 *`Device management license to manage up to 1000 devices`*（设备管理许可证可管理最多 *`1000`* 台设备）。

在 FIPS-CC 模式下升级 Panorama 和受管设备

成功升级到 PAN-OS 11.1 后，FIPS-CC 模式下的所有托管设备以及在设备运行 PAN-OS 10.0 或更早版本时添加到 Panorama 的任何托管设备都必须重新加入 Panorama 管理。这需要您在 FIPS-CC 模式下重置 Panorama 和 FIPS-CC 模式下任何受管设备的安全连接状态。重置安全连接状态后，您必须 使用设备注册身份验证密钥 将添加到 Panorama 的防火墙、日志收集器和 WildFire 设备添加回 Panorama 管理。在运行 PAN OS 10.0 或更早版本时，此过程不是必需的，也不会影响添加到 Panorama 的受管设备。这对于 FIPS-CC 模式下的所有受支持的 Panorama 模式 和 下一代防火墙硬件和 VM 系列模型 都是必需的。

STEP 1 | 使用设备注册身份验证密钥在 FIPS-CC 模式下创建您的受管设备列表以及添加到 Panorama 的任何受管设备。这将帮助您稍后在将受管设备重新加入 Panorama 管理时集中精力。

STEP 2 | 将 Panorama 和托管设备升级到 PAN-OS 11.1。

- 在具有互联网连接的情况下升级 Panorama
- 在没有互联网连接的情况下升级 Panorama
- 在高可用性配置中升级 Panorama

STEP 3 | 成功升级到 PAN-OS 11.1 后，查看 Panorama 上的系统日志，以确定 FIPS-CC 模式下哪些托管设备无法连接到 Panorama。

STEP 4 | 重置 Panorama 上的安全连接状态。

此步骤会重置在运行 PAN-OS 11.1 版本时添加到 Panorama 管理的任何托管设备的连接，并且是不可逆的。此步骤对运行 PAN-OS 10.0 或升级到 PAN-OS 11.1 的更早版本时添加的防火墙的连接状态没有影响。

1. 登录到 Panorama 命令行界面。
2. 重置安全连接状态。

```
admin> request sc3 reset
```

3. 重新启动 Panorama 上的管理服务器。

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

4. （仅限 HA） 对高可用性 (HA) 配置中的每个对端设备重复此步骤。

STEP 5 | 在 FIPS-CC 模式下重置受管设备上的安全连接状态。

此命令将重置受管设备的连接状态，且不可逆。

1. 登录至受管设备 CLI。
   - 登录到防火墙 CLI
   - 登录到日志收集器 CLI
   - 登录到 WildFire 设备 CLI
2. 重置安全连接状态。

```
admin> request sc3 reset
```

3. 重新启动受管设备上的管理服务器。

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

STEP 6 | 将受影响的受管设备添加回 Panorama。

- 添加防火墙作为受管设备
- 配置受管收集器
- 添加独立 WildFire 设备以使用 Panorama 进行管理

STEP 7 | 重新生成或重新导入所有证书以遵守 OpenSSL 安全级别 2。

在升级到 PAN-OS 11.1 时，要求所有证书满足以下最低要求：

- RSA 2048 位或以上，或 ECDSA 256 位或以上
- SHA256 或更高版本摘要

请参阅 PAN-OS 管理员指南或 Panorama 管理员指南，了解有关重新生成或重新导入证书的更多信息。

从 Panorama 11.1 降级

PAN-OS® 11.1 引入了针对零日攻击预防的高级威胁预防支持，它利用内联深度学习、简化 Panorama 和受管设备的软件升级和降级，以减少跨多个 PAN-OS 版本升级受管设备的操作负担，主动最佳使用 AIOps 的实践评估 (BPA) 进一步消除安全状态受损的风险，本地 Web 代理有助于在不牺牲安全性或效率的情况下过渡到云，防火墙支持有状态的 DHCPv6 客户端获取 IPv6 地址，增强用户的可见性云身份引擎 (CIE) 的用户上下文、对管理访问的 TLSv1.3 支持以及增强的 IoT 安全策略规则建议，以便更轻松地扩展和管理策略规则建议。在将运行 Panorama 11.1 版的日志收集器和 Panorama 降级到更早功能版本之前，应先使用以下工作流降级防火墙。此过程适用于管理本地日志收集器的 Panorama 以及管理一个或多个专用日志收集器的 Panorama。

要从 *PAN-OS 11.1* 降级到更早的 *PAN-OS* 版本，您必须下载并安装首选的 *PAN-OS 11.0* 或更高的 *PAN-OS 11.0* 版本，然后才能继续降级到目标 *PAN-OS* 版本。如果您尝试降级到 *PAN-OS 10.2* 或更早的 *PAN-OS* 版本，从 *PAN-OS 11.0* 降级失败。

查看 Palo Alto Networks 兼容性矩阵以确认您打算降级的防火墙和设备是否与您打算降级至的 *PAN-OS* 版本兼容。对于可以降级的防火墙和设备，您还应该查看 升级/降级注意事项 以确保您考虑到在降级后所有功能和配置设置将不同或不可用。

运行 *PAN-OS 11.1* 时生成的日志与 *PAN-OS 11.0* 及更早版本不兼容，并且在降级时会被删除。要保留运行 *PAN-OS 11.1.1* 或 *PAN-OS 11.1.0* 时生成的日志，必须先升级到 *PAN-OS 11.1.2*，然后再开始降级到目标 *PAN-OS* 版本。这是降级后成功恢复 *PAN-OS 11.1* 中生成的日志所必需的操作。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 保存 Panorama 和受管设备的配置备份。

1. **Export Panorama and device configuration snapshot**（导出 **Panorama** 和设备配置快照）（**Panorama** > **Setup**（设置） > **Operations**（操作））。
2. 将导出的 .tgz 文件保存到 Panorama、日志收集器和防火墙外部的位置。如果出现导致重新开始的问题，您可以使用此备份还原配置。

STEP 3 | 如果您已经针对专用日志收集器配置身份验证，且移除了 `admin` 管理员，请配置新的 `admin` 用户并推送到您的专用日志收集器。

专用日志收集器必须配置 `admin` 用户才可降级至 PAN-OS 9.1 和更早版本。

STEP 4 | 对于当前安装在 Panorama 上的所有插件，选择 **Panorama** > **Plugins**（插件）并 **Download**（下载）PAN-OS 11.0 上支持的插件版本。

有关 PAN-OS 11.0 和更早版本支持的 Panorama 插件版本，请参阅 Panorama 插件兼容性矩阵。

这是成功地将 Panorama 从 PAN-OS 11.1 降级到 PAN-OS 11.0 和更早版本所必需的。降级到 PAN-OS 11.0 期间，系统会自动安装所下载的插件版本。如果未下载支持的插件版本，将阻止降级到 PAN-OS 11.0。

（仅限 *ZTP* 插件）要成功地将 *Panorama* 降级到 *PAN-OS 11.0*，您必须在开始降级过程之前卸载 ZTP 插件。成功降级到 *PAN-OS 11.0* 后，您必须在 *Panorama* 上重新安装 *ZTP* 插件。

STEP 5 | 降级运行 PAN-OS 11.1 版本的每个防火墙。

要从 *PAN-OS 11.1* 降级到以前的功能版本，需要先降级到首选的 *PAN-OS 11.0* 版本或更高的 *PAN-OS 11.0* 版本。成功降级到首选 *PAN-OS 11.0* 或更高的 *PAN-OS 11.0* 版本后，您可以继续降级到目标 *PAN-OS* 版本。

如果要降级多个防火墙，请在开始降级前将各防火墙特定的 *PAN-OS 11.0* 映像下载到 *Panorama* 以简化流程。例如，要将 *PA-220* 防火墙降级到 *PAN-OS 11.0*，请下载 *`PanOS_220-11.0.0`* 或 *`PanOS_3000-11.0.0`* 映像。

Panorama 要求所有防火墙都运行相同或更早的 PAN-OS 版本。因此，在降级 Panorama 前，请根据您的环境按需使用并重复以下相应的任务来降级所有受管防火墙：

1. **Check Now**（立即检查）可用的映像（**Panorama** > **Device Deployment**（设备部署） > **Software**（软件））。

   （PAN-OS 11.1.3 及更高版本）默认情况下，显示首选版本和相应的基础版本。要仅查看首选版本，请禁用（清除）**Base Releases**（基础版本）复选框。同样地，要仅查看基础版本，请禁用（清除）**Preferred Releases**（首选版本）复选框。
2. 找到您打算降级的每个型号或系列防火墙的 PAN-OS 11.0 映像。如果尚未下载映像，请 **Download**（下载）。

非 **HA** 防火墙

Install（安装）（操作列）相应的 PAN-OS 11.0 版本，选择您打算降级的所有防火墙，接着选择 **Reboot device after install**（安装后重启设备），然后单击 **OK**（确定）。

主动/主动 **HA** 防火墙

1. 单击 **Install**（安装），禁用（清除）**Group HA Peers**（组高可用性对端设备），选择任意一个高可用性对端设备，选择 **Reboot device after install**（安装后重新启动设备），然后单击 **Ok**（确定）。等待防火墙完成重新启动之后再继续进行操作。
2. 单击 **Install**（安装），禁用（清除）**Group HA Peers**（组高可用性对端设备），选择在上一步中尚未更新的高可用性对端设备，选择 **Reboot device after install**（安装后重新启动设备），然后单击 **Ok**（确定）。

主动/被动 **HA** 防火墙

在本例中，主动防火墙的名称为 fw1，被动防火墙的名称为 fw2：

1. **Install**（安装）（“操作”列）相应更新，禁用（取消选中）**Group HA Peers**（组高可用性对等设备），选择 fw2，选择 **Reboot device after install**（安装后重新启动设备），然后单击 **OK**（确定）。
2. 在 fw2 完成重新启动后，核实 fw1（**Dashboard**（仪表板） > **High Availability**（高可用性）小部件）是否仍是主动对等设备，fw2 仍为被动对等设备（本地防火墙状态为 `active`，对等设备 fw2 为 `passive`）。
3. 访问 fw1 和 **Suspend local device**（挂起本地设备）（**Device**（设备） > **High Availability**（高可用性） > **Operational Commands**（操作命令））。

4. 访问 fw2（**Dashboard**（仪表板） > **High Availability**（高可用性）），并确认本地防火墙状态为`active`，对等设备防火墙 fw1 为 `suspended`。
5. 访问 Panorama，选择 **Panorama** > **Device Deployment**（设备部署） > **Software**（软件），**Install**（安装）（“操作”列）相应更新，禁用（取消选中）**Group HA Peers**（组高可用性对等设备），选择 fw1，选择 **Reboot device after install**（安装后重新启动设备），然后单击 **OK**（确定）。等待 fw1 完成重新启动之后再继续进行操作。
6. 访问 fw1（**Dashboard**（仪表板） > **High Availability**（高可用性）小部件）上，并核实本地防火墙状态为 `passive`，对等设备 fw2 为 `active`。

   如果您启用 *Election Settings*（选择设置）中的抢先（***Device***（设备） > ***High Availability***（高可用性） > ***General***（常规）），则 *fw1* 在重新启动后将恢复为主动对端设备。

STEP 6 | 降级运行 Panorama 11.0 的各日志收集器。

要从 *PAN-OS 11.1* 降级到以前的功能版本，需要先降级到首选的 *PAN-OS 11.0* 版本或更高的 *PAN-OS 11.0* 版本。成功降级到首选 *PAN-OS 11.0* 或更高的 *PAN-OS 11.0* 版本后，您可以继续降级到目标 *PAN-OS* 版本。

1. 登录到日志收集器 CLI 并删除所有 `esdata` 目录。

   ```
   admin> debug elasticsearch erase data
   ```

   对要降级的收集器组中的所有日志收集器重复此步骤。
2. **Check Now**（立即检查）可用的映像（**Panorama** > **Device Deployment**（设备部署） > **Software**（软件））。

   （PAN-OS 11.1.3 及更高版本）默认情况下，显示首选版本和相应的基础版本。要仅查看首选版本，请禁用（清除）**Base Releases**（基础版本）复选框。同样地，要仅查看基础版本，请禁用（清除）**Preferred Releases**（首选版本）复选框。
3. 找到 PAN-OS 11.0 映像。如果尚未下载映像，请 **Download**（下载）（Action（操作）列）。
4. 下载完成后，在运行 11.1 版本的各日志收集器上 **Install**（安装）映像。选择 **Reboot device after install**（安装后重新启动设备）在升级完成后自动重新启动设备。

STEP 7 | 降级 Panorama。

要从 *PAN-OS 11.1* 降级到以前的功能版本，需要先降级到首选的 *PAN-OS 11.0* 版本或更高的 *PAN-OS 11.0* 版本。成功降级到首选 *PAN-OS 11.0* 或更高的 *PAN-OS 11.0* 版本后，您可以继续降级到目标 *PAN-OS* 版本。

1. （仅限 Panorama 模式）登录到 Panorama CLI 并删除所有 `esdata` 目录。

   ```
   admin> debug elasticsearch erase data
   ```

2. 登录到 Panorama Web 界面并选择 **Panorama** > **Software**（软件），然后 **Check Now**（立即检查）可用的映像。

   （PAN-OS 11.1.3 及更高版本）默认情况下，显示首选版本和相应的基础版本。要仅查看首选版本，请禁用（清除）**Base Releases**（基础版本）复选框。同样地，要仅查看基础版本，请禁用（清除）**Preferred Releases**（首选版本）复选框。

3. 找到目标 PAN-OS 映像。如果尚未下载映像，请 **Download**（下载）。
4. 下载完成后，在 Panorama 上 **Install**（安装）映像。
5. 重新启动 Panorama，如下所示：
   - 如果提示重新启动，请单击是。如果系统显示 **CMS Login** 提示符，按 Enter 键，而不输入用户名或密码。当 Panorama 登录提示符出现后，输入在初始配置期间设置的用户名和密码。
   - 如果未提示重新启动，请选择 **Panorama** > **Setup**（设置） > **Operations**（操作），然后单击 **Reboot Panorama**（重新启动 **Panorama**）（设备操作）。

STEP 8 | （仅限 ZTP 插件）重新安装 ZTP 插件。

1. 登录到 Panorama Web 界面。
2. 安装 ZTP 插件。
3. 选择 **Panorama** > **Zero Touch Provisioning**（零接触配置） 并选中（启用）**ZTP**。

STEP 9 | （仅限企业 DLP） 编辑企业 DLP 数据过滤设置 以将 **Max File Size**（最大文件大小） 减小到 20MB 或更少。

从企业 DLP 4.0.1 或更高版本的 Panorama 插件降级时，需要执行此操作。企业 DLP 4.0.1 及更高版本支持大文件大小检查。

STEP 10 | （仅限企业 DLP）将 Panorama 上的企业 DLP 数据过滤配置文件与 DLP 云服务同步。

将 Panorama 从 PAN-OS 11.0.2 和企业 DLP 插件 4.0.1 降级到 PAN-OS 11.0.1 或更早的 11.1 版本以及企业 DLP 插件 4.0.0 时，需要执行此操作。

1. 登录到 Panorama 命令行界面。
2. 将企业 DLP 配置从 Panorama 推送到 DLP 云服务。

   ```
   admin> request plugins dlp push-dlp-config
   ```

3. 重置企业 DLP 插件。

   ```
   admin> request plugins dlp reset
   ```

4. 在 Panorama 上提交并推送到使用企业 DLP 的受管防火墙。
   1. 登录到 Panorama Web 界面。
   2. 选择 **Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**），然后 **Commit**（提交）。
   3. 选择 **Commit**（提交） > **Push to Devices**（推送到设备），然后 **Edit Selections**（编辑选择）。
   4. 选择 **Device Groups**（设备组），并选择 **Include Device and Network Templates**（包含设备和网络模板）。
   5. 单击 **OK**（确定）。
   6. 将您的配置更改 **Push**（推送）到使用企业 DLP 的受管防火墙。

STEP 11 | 登录到 Panorama CLI 并恢复在 PAN-OS 11.1 中生成的日志。

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

查看日志迁移状态：

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


Panorama 升级问题故障排除

要对 Panorama 插件升级进行故障排除，请使用下表查看可能的问题以及如何解决这些问题。

症状	解决方案
软件保修许可证已过期。	从 CLI 中删除过期的许可证密钥： 1. 输入 **delete license key <software license key>**。 2. 输入 **delete license key Software_Warranty<expiredate>.key**。
最新的 PAN OS 软件版本不可用。	您只能看到比当前安装版本高一个功能版本的软件版本。例如，如果您安装了 8.1 版本，则只有 9.0 版本可供您使用。要查看 9.1 版本，您必须先升级到 9.0。
（仅限旧版模式下的 Panorama 虚拟设备）升级版本无法预加载到软件管理器中。	当没有足够的可用资源时，会出现此问题。您可以增加虚拟机容量，也可以从旧版模式迁移到 Panorama 模式。

使用 Panorama 将更新部署到防火墙、日志收集器和 WildFire 设备

在其他受管设备上安装更新之前，可以通过将更新部署到一部分防火墙、专用日志收集器或 WildFire® 设备和设备群集来使用 Panorama™ 更新软件和内容。如果要计划定期更新内容，Panorama 要求建立直接互联网连接。当根据需求（非计划）部署软件或内容更新时，步骤可能会有所不同，具体取决于 Panorama 是否已连接上互联网。当计划更新流程已经启动或即将在五分钟之内启动时，如果您手动部署内容更新，Panorama 将会显示一条警告消息。

在部署更新时，Panorama 会通知受管设备（防火墙，日志收集器和 WildFire 设备）有更新可用，然后设备从 Panorama 检索更新包。默认情况下，受管设备通过 Panorama 上的管理 (MGT) 接口检索更新。但是，如果要通过使用设备的其他接口检索更新来减少 MGT 接口的流量负载，则可以配置 Panorama 以使用多个接口。

您可以使用 Panorama 快速将一个或多个防火墙的内容版本恢复为以前安装的内容版本。在防火墙上安装新的内容版本后，如果新安装的内容版本不稳定或以其他方式中断您的网络操作，则可以恢复为先前安装的版本。

默认情况下，您最多可以将每种类型的两项软件或内容更新下载到 *Panorama*。如果您启动超过该最大限制的任何下载，*Panorama* 将会删除选定类型的最早更新。要更改最大限制，请参阅管理用于软件和内容更新的 Panorama 存储。

- Panorama 可以向其他设备推送哪些更新？
- Panorama、日志收集器、防火墙和 WildFire 的版本兼容性
- 使用 Panorama 计划内容更新
- 当 Panorama 连接上互联网时升级防火墙
- 当 Panorama 未连接互联网时升级防火墙
- 当 Panorama 连接上互联网时升级日志收集器
- 当 Panorama 未连接互联网时升级日志收集器
- 在有互联网连接的情况下从 Panorama 升级 WildFire 集群
- 在没有互联网连接的情况下从 Panorama 升级 WildFire 集群
- 升级 ZTP 防火墙
- 安装 PAN-OS 软件补丁
- 从 Panorama 恢复内容更新

Panorama 可以向其他设备推送哪些更新？

您可以安装的软件和内容更新取决于每个防火墙、日志收集器、WildFire® 设备和设备群集上都有哪些激活的订阅：

设备类型	软件更新	内容更新
日志收集器	Panorama™	应用程序（日志收集器不需要威胁签名） 反病毒 WildFire®
防火墙	PAN-OS® GlobalProtect™ 代理/应用	应用程序 应用程序和威胁 反病毒 WildFire
WildFire	PAN-OS VM 映像	WildFire

使用 Panorama 计划内容更新

Panorama™ 需要建立直接互联网连接安排防火墙、日志收集器、WildFire® 设备和设备群集的支持的更新。否则，您只能执行按需更新。（若要为日志收集器计划防病毒软件、WildFire 或 BrightCloud URL 更新，则日志收集器必须运行 Panorama 7.0.3 或更高版本。)接收了更新的每个防火墙、日志收集器或 WildFire 设备或设备群集都会生成日志，以表明安装是成功（配置日志）还是失败（系统日志）。要在 Panorama 管理服务器上安排更新，请参阅使用互联网连接安装 Panorama 更新。

部署更新前，请参阅 Panorama、日志收集器、防火墙和 WildFire 的版本兼容性了解有关内容发布版本兼容性的重要详细信息。请参阅发布说明以了解您必须为 *Panorama* 发布产品安装的最低内容发布版本。

对于相同类型的更新，*Panorama* 一次只能下载一个更新。如果您计划在同一时间重复下载多个相同类型的更新，则只有第一次下载会成功。

如果您的防火墙直接连接至 *Palo Alto Networks®* 更新服务器，您也可以使用 *Panorama* 模板（***Device*** （设备） **> *Dynamic Updates*** （动态更新）将内容更新调度推送到防火墙。如果要在更新发布后延迟安装，您必须使用模板部署调度。内容更新基本很少包括错误；指定一个延迟时间，以便防火墙在 *Palo Alto Networks* 从更新服务器发现并移除此类更新后再安装更新。

应为要计划的每种更新类型执行以下步骤。

STEP 1 | 选择 **Panorama > Device Deployment**（设备部署） **> Dynamic Updates**（动态更新），单击 **Schedules**（计划），然后 **Add**（添加）计划。

STEP 2 | 指定 **Name**（名称）以识别计划、更新 **Type**（类型）和更新频率（**Recurrence**（重复周期））。频率选项取决于更新 **Type**（类型）。

PAN-OS® 使用 *Panorama* 时区执行更新计划。

如果您将 **Type**（类型）设置为 **App and Threat**（应用和威胁），日志收集器都只安装和需要应用程序内容，而不是威胁内容。防火墙同时使用应用程序和威胁内容。有关详细信息，请参阅 Panorama、日志收集器、防火墙和 WildFire 的版本兼容性。

STEP 3 | 选择以下一个调度操作，然后选择防火墙或日志收集器：

- **Download And Install**（下载并安装）（最佳做法）— 选择 **Devices**（设备）（防火墙）、**Log Collectors**（日志收集器）或 **WildFire Appliances and Clusters**（**WildFire** 设备和群集）。
- **Download Only**（仅下载）— Panorama 将下载更新但不安装更新。

STEP 4 | 单击 **OK**（确定）。

STEP 5 | 选择 **Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**），然后 **Commit**（提交）更改。

Panorama、日志收集器、防火墙和 WildFire 的版本兼容性

为获得最佳效果，请遵循以下 Panorama™ 兼容性准则：

- 同时在 Panorama 管理服务器和专用日志收集器上安装相同的 Panorama 版本。
- Panorama 必须运行与用于管理防火墙的版本相同或更高的 PAN-OS 版本。有关详细信息，请参阅 Panorama管理兼容性 。

  将防火墙升级至 PAN-OS 11.0 之前，必须先将 Panorama 升级至 11.0。
- 专用日志收集器必须运行与转发日志的托管防火墙相同或更高的 PAN-OS 版本。
- 运行 PAN-OS 11.1 的 Panorama 可以管理运行相同或更早 PAN-OS 版本的 WildFire® 设备和 WildFire 设备集群。有关详细信息，请参阅 Panorama管理兼容性 。

  建议 Panorama 管理服务器、Wildfire 设备和 Wildfire 设备群集运行相同的 PAN-OS 版本。
- Panorama 管理服务器上的内容发布版本必须与任何专用日志收集器或受管防火墙上的内容发布版本相同（或低于后者）。有关详细信息，请参阅 Panorama管理兼容性 。

Palo Alto Networks® 建议在 *Panorama* 上安装版本与在专用日志收集器和防火墙上所安装版本相同的应用程序数据库。

无论您的订阅是包括应用程序数据库，还是应用程序和威胁数据库，Panorama 都只安装应用程序数据库。Panorama 和专用日志收集器不会强制实施策略规则，所以不需要威胁数据库的威胁签名。应用程序数据库包括定义策略规则以推送到受管防火墙时或解读日志与报告中的威胁信息时在 Panorama 和专用日志收集器中使用的威胁元数据（例如威胁 ID 和名称）。但是，防火墙需要完整的应用程序和威胁数据库，将日志中记录的标识符与相应的威胁、URL 或应用程序名称进行匹配。请参阅发布说明以了解 Panorama 版本所需的最低内容发布版本。

当 Panorama 连接上互联网时升级日志收集器

有关您可以在日志收集器上安装的软件和内容更新列表，请参阅支持的更新。

如果从 *PAN-OS 8.1* 升级，*PAN-OS 9.0* 为本地和专用日志收集器引入了新的日志数据格式。在升级到 *PAN-OS 10.1* 的路径中，现有日志数据会在从 *PAN-OS 8.1* 升级到 *PAN-OS 9.0* 时自动迁移到新的日志数据格式。

同时，您必须在收集器组中更新所有日志收集器，以避免日志数据丢失。如果收集器组内的日志收集器并非全部都运行相同的 PAN-OS 版本，则不会转发日志或日志收集。此外，在所有日志收集器都运行相同的 PAN-OS 版本前，**ACC** 或 **Monitor**（监控）选项卡将不会显示用于收集器组内日志收集器的日志数据。例如，如果在收集器组内有三个日志收集器，且您更新其中的两个，则不会有日志转发到收集器组内任何日志收集器。

Palo Alto Networks 建议您在维护窗口期间升级日志收集器。因为日志格式的迁移，整个升级过程需要另外花费数小时，具体取决于本地和专用日志收集器上的日志数据量。

STEP 1 | 在升级日志收集器之前，请确保您在 Panorama 管理服务器上运行相应的 Panorama™ 软件版本。

Palo AltoNetworks® 强烈建议 *Panorama* 和日志收集器运行相同的软件发行版本，并且 *Panorama*、日志收集器和所有受管防火墙运行相同的内容发行版本。有关软件和内容兼容性的重要详细信息，请参阅 Panorama、日志收集器、防火墙和 WildFire 的版本兼容性。

Panorama 必须与日志收集器运行相同（或更高）的软件发行版本，但必须具有相同或更高的内容发行版本：

- 软件发行版本 — 如果 Panorama 管理服务器尚未运行与您打算将日志收集器更新到的版本相同或更高的软件发行版本，则在更新任何日志收集器之前，必须在 Panorama 上安装相同或更高的 Panorama 发行版本（请参阅 安装 Panorama 的内容更新和软件升级）。
- 内容发布版本 — 对于内容发布版本，您应该确保所有日志收集器都运行最新的内容发布版本，或者至少运行比在 Panorama 上运行的版本更高的版本；否则，在更新 Panorama 管理服务器的内容发布版本之前先 从 Panorama 中将防火墙升级到 PAN-OS 11.1，然后更新日志收集器。

检查软件和内容版本：

- **Panorama** 管理服务器 — 要确定 Panorama 管理服务器上正在运行的软件和内容版本，请登录到 Panorama Web 界面并转到 General Information（一般信息）设置（**Dashboard**（仪表盘））。
- 日志收集器 — 要确定在日志收集器上正在运行的软件和内容版本，请登录到每个日志收集器的 CLI 并运行 **`show system info`** 命令。

STEP 2 | 在您的网络上启用以下 TCP 端口。

必须在网络上启用这些 TCP 端口，才能允许日志收集器之间进行通信。

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

STEP 3 | 确定升级到 PAN-OS 11.1 的路径.

不能跳过从当前运行的 PAN-OS 版本升级到 PAN-OS 11.1.0 的路径中任何功能发行版本的安装。

对于您在升级路径中会经过的每个版本，查看发行说明和升级/降级注意事项中的PAN-OS 升级清单、已知问题以及默认行为更改。

STEP 4 | 安装最新的内容更新。

请参阅发布说明以了解 *Panorama* 软件版本所需的最低内容发布版本。

1. 登录到 Panorama Web 界面。
2. 选择 **Panorama** > **Device Deployment**（设备部署） > **Dynamic Updates**（动态更新），然后 **Check Now**（立即检查）最近更新。如果有更新可用，Action（操作）列会显示 **Download**（下载）链接。
3. 如果尚未安装，请 **Download**（下载）相应内容更新。成功下载后，Action（操作）列中的链接将从**Download**（下载）更改为**Install**（安装）。
4. 先 **Install**（安装）内容更新（应用程序和威胁更新），再安装任何其他更新。

   如果您的订阅同时包含应用程序和威胁内容，请先安装应用程序内容。这会自动安装应用程序和威胁内容。

   无论您的订阅是否同时包括应用程序和威胁内容，*Panorama* 都只安装和需要应用程序内容。有关详细信息，请参阅 Panorama、日志收集器、防火墙和 WildFire 的版本兼容性。
5. 根据需要对其他任何更新（防病毒、WildFire 或 URL 筛选）重复上述子步骤，一次针对一个更新，可随意选择更新顺序。

STEP 5 | 沿着升级到 PAN-OS 11.1 的路径，将日志收集器升级到 PAN-OS 发行版本。

如果升级多个日志收集器，请在开始下载映像之前通过确定打算升级的所有日志收集器的升级路径来简化该过程。

1. 在 Panorama 连接至互联网的情况下升级日志收集器到 PAN-OS 9.1。
2. 在 Panorama 连接至互联网的情况下升级日志收集器到 PAN-OS 10.0。
3. 在 Panorama 连接至互联网的情况下升级日志收集器到 PAN-OS 10.1。

   PAN-OS 11.1 引入了一种新的日志格式。从 PAN-OS 11.1 升级到 PAN-OS 10.1 时，您可以选择迁移在 PAN-OS 8.1 或更早版本中生成的日志。否则，在成功升级到 PAN-OS

10.1 时，系统会自动删除这些日志。在迁移期间，ACC 或监视选项卡中不会显示日志数据。在迁移过程中，日志数据会继续转发到相应的日志收集器，但是您可能会遇到一些性能影响。

4. 在 Panorama 连接至互联网的情况下升级日志收集器到 PAN-OS 10.2。
5. 在 Panorama 连接至互联网的情况下升级日志收集器到 PAN-OS 11.0。

STEP 6 | 将日志收集器升级到 PAN-OS 11.1。

1. 在 Panorama 上，**Check Now**（立即检查）（**Panorama** > **Device Deployment**（设备部署） > **Software**（软件））最新更新。如果有更新可用，“操作”列会显示 **Download**（下载）链接。
2. 为 PAN-OS 11.1 版本的发行版本 **Download**（下载）特定于型号的文件。例如，要将 M 系列设备升级到 Panorama 11.1.0，请下载 `Panorama_m-11.1.0` 映像。

   成功下载后，该映像的 Action（操作）列将从 **Download**（下载）更改为 **Install**（安装）。
3. **Install**（安装）PAN-OS 11.1 并选择适当的日志收集器。
4. 如果一个或多个选定的日志收集器包含在 PAN-OS 10.0 或更早版本中生成的日志，则会显示通知。

   在您第一次尝试 **Install**（安装）PAN-OS 11.1.2 或更高版本 11.1 时会显示此通知，关闭后不会再次显示该通知。它会警告您，系统检测到在运行 PAN-OS 10.0 或更早版本时由 Panorama 或托管设备生成的日志，并且将会在升级时删除这些日志。这意味着成功升级后无法查看或搜索受影响的日志。

   但您可以在升级后恢复这些受影响的日志。该通知还为您提供以下信息。如果选择了多个日志收集器，请单击 **Tasks**（任务）并查看每个日志收集器安装失败的作业详细信息，以便查看和复制所需的迁移命令。

   - 受影响的日志类型。
   - 每种日志类型受影响的时间范围。
   - 恢复每种日志类型受影响的日志所需的每个 `debug logdb migrate-lc` 命令。

     在 **Close**（关闭）通知之前复制所列的 `debug logdb migrate-lc` 命令。

   Close（关闭）通知。
5. 根据您的需要选择以下项之一：

   - **Upload only to device (do not install)**（仅上传到设备（不安装））。
   - **Reboot device after install**（在安装之后重新启动设备）。
6. 单击 **OK**（确定）开始安装（或上传）。

   在选定的日志收集器成功重启后继续下一步。

STEP 7 | 验证安装在日志收集器上的软件和内容更新版本。

输入**`show system info`**操作命令。输出将如下所示：

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


STEP 8 | （PAN-OS 11.1.2 及更高版本；仅限 Panorama 模式）对于每个受影响的日志收集器，登录到日志收集器 CLI，并使用上一步中列出的 `debug logdb migrate-lc` 命令恢复受影响的日志。

这些命令必须按顺序运行，不能同时运行。如果您没有从通知窗口复制 `debug logdb migrate-lc` 命令，请单击 **Tasks**（任务）并查看特定日志收集器的安装失败的作业详细信息。

STEP 9 | （仅限 FIPS-CC 模式） 在 FIPS-CC 模式下升级 Panorama 和受管设备。

如果您在专用日志收集器运行 PAN-OS 11.1 版本时将专用日志收集器添加到 Panorama 管理，则在 FIPS-CC 模式下升级专用日志收集器需要重置安全连接状态。

在专用日志收集器运行 PAN-OS 10.0 或更早版本时，您无需重新启动已添加到 Panorama 管理中的专用日志收集器。

STEP 10 | 重新生成或重新导入所有证书以遵守 OpenSSL 安全级别 2。

如果您从 PAN-OS 10.1 或更早版本升级到 PAN-OS 11.0，则需要执行此步骤。如果您从 PAN-OS 10.2 升级并且已经重新生成或重新导入了您的证书，请跳过此步骤。

所有证书都必须满足以下最低要求：

- RSA 2048 位或以上，或 ECDSA 256 位或以上
- SHA256 或更高版本的摘要

请参阅 PAN-OS 管理员指南或 Panorama 管理员指南，了解有关重新生成或重新导入证书的更多信息。

STEP 11 | （推荐用于 Panorama 虚拟设备）将 Panorama 虚拟设备的内存增加到 64GB。

在日志收集器模式下成功将 Panorama 虚拟设备升级到 PAN-OS 11.1 后，Palo Alto Networks 建议将 Panorama 虚拟设备的内存增加到 64GB 以满足增加的系统要求，从而避免与配置不足的 Panorama 虚拟设备相关的任何日志、管理和操作性能问题。

当 Panorama 未连接互联网时升级日志收集器

有关您可以在日志收集器上安装的软件和内容更新列表，请参阅支持的更新。

如果从 *PAN-OS 8.1* 升级，*PAN-OS 9.0* 为本地和专用日志收集器引入了新的日志数据格式。在升级到 *PAN-OS 10.1* 的路径中，现有日志数据会在从 *PAN-OS 8.1* 升级到 *PAN-OS 9.0* 时自动迁移到新格式。

同时，您必须在收集器组中更新所有日志收集器，以避免日志数据丢失。如果收集器组内的日志收集器并非全部都运行相同的 PAN-OS 版本，则不会转发日志或日志收集。此外，在所有日志收集器都运行相同的 PAN-OS 版本前，**ACC** 或 **Monitor**（监控）选项卡将不会显示用于收集器组内日志收集器的日志数据。例如，如果在收集器组内有三个日志收集器，且您更新其中的两个，则不会有日志转发到收集器组内任何日志收集器。

Palo Alto Networks 建议您在维护窗口期间升级日志收集器。因为日志格式的迁移，整个升级过程需要另外花费数小时，具体取决于本地和专用日志收集器上的日志数据量。

STEP 1 | 在升级日志收集器之前，请确保您在 Panorama 管理服务器上运行相应的 Panorama™ 软件版本。

Palo AltoNetworks® 强烈建议 *Panorama* 和日志收集器运行相同的软件发行版本，并且 *Panorama*、日志收集器和所有受管防火墙运行相同的内容发行版本。有关软件和内容兼容性的重要详细信息，请参阅 Panorama、日志收集器、防火墙和 WildFire 的版本兼容性。

Panorama 必须与日志收集器运行相同（或更高）的软件发行版本，但必须具有相同或更高的内容发行版本：

- 软件发布版本 — 如果 Panorama 管理服务器尚未运行与您打算更新日志收集器的版本相同或更高版本的软件版本，则在更新任何日志收集器之前必须在 Panorama 上安装相同或更高版本的 Panorama 版本（请参阅安装 Panorama 的内容和软件更新）。
- 内容发行版本 — 对于内容发行版本，您应该确保所有日志收集器都运行最新的内容发行版本，或者运行的版本至少高于您将安装的版本或 Panorama 上正在运行的版本；否则，在更新 Panorama 管理服务器的内容发行版本之前先 从 Panorama 中将防火墙升级到 PAN-OS 11.1，然后更新日志收集器（请参阅 安装 Panorama 的内容更新和软件升级）。

检查软件和内容版本：

- **Panorama** 管理服务器 — 要确定 Panorama 管理服务器上正在运行的软件和内容版本，请登录到 Panorama Web 界面并转到 General Information（一般信息）设置（**Dashboard**（仪表盘））。
- 日志收集器 — 要确定在日志收集器上正在运行的软件和内容版本，请登录到每个日志收集器的 CLI 并运行 **`show system info`** 命令。

STEP 2 | 确定升级到 PAN-OS 11.1 的路径.

对于您在升级路径中会经过的每个版本，查看发行说明和升级/降级注意事项中的PAN-OS 升级清单、已知问题以及默认行为更改。

如果升级多个日志收集器，请在开始下载映像之前通过确定打算升级的所有日志收集器的升级路径来简化该过程。

STEP 3 | 在您的网络上启用以下 TCP 端口。

必须在网络上启用这些 TCP 端口，才能允许日志收集器之间进行通信。

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

STEP 4 | 将最新内容和软件更新下载到可以通过 SCP 或 HTTPS 连接并将文件上传到 Panorama 的主机。

请参阅发布说明以了解 *Panorama* 软件版本所需的最低内容发布版本。

1. 使用能够访问互联网的主机，登录到 Palo Alto Networks 客户支持网站。
2. 下载最新的内容更新：
   1. 在 Resources（资源）部分中单击 **Dynamic Updates**（动态更新）。
   2. **Download**（下载）最新的内容更新，并将文件保存到主机。对您将更新的每种内容类型执行此步骤。
3. 下载软件更新：
   1. 返回到 Palo Alto Networks® 客户支持网站的主页，然后在资源部分中单击 **Software Updates**（软件更新）。
   2. 查看下载列以确定要安装的版本。M 系列设备的更新包文件名以“Panorama_m”开头，后跟版本号。例如，要将 M 系列设备升级到 Panorama 11.1.0，请下载 `Panorama_m-11.1.0` 映像。

      您可以通过从 ***Filter By***（筛选条件）下拉列表中选择 ***Panorama M Images***（***Panorama M*** 映像）（对于 *M* 系列设备）快速找到 *Panorama* 映像。
4. 单击相应的文件名并将文件保存到主机。

STEP 5 | 安装最新的内容更新。

如果您需要安装内容更新，则必须先安装软件更新。此外，在更新 *Panorama* 上的内容发布版本之前，先在防火墙上安装内容更新，然后在日志收集器上安装内容更新。

先安装应用程序或应用程序和威胁更新，然后根据需要一次性以任何顺序安装任何其他更新（防病毒软件、WildFire® 或 URL 筛选）。

无论您的订阅是否同时包括应用程序和威胁内容，*Panorama* 都只安装和需要应用程序内容。有关详细信息，请参阅 Panorama、日志收集器、防火墙和 WildFire 的版本兼容性。

1. 登录到 Panorama Web 界面。
2. 选择 **Panorama** > **Device Deployment**（设备部署） > **Dynamic Updates**（动态更新）。
3. 单击 **Upload**（上传），选择更新 **Type**（类型），**Browse**（浏览）至主机上的相应内容更新文件，然后单击 **OK**（确定）。
4. 单击 **Install From File**（从文件安装），选择更新 **Type**（类型），然后选择您刚上传的更新的 **File Name**（文件名）。
5. 选择日志收集器。
6. 单击 **OK**（确定）以开始安装。
7. 对于每个内容更新，请重复这些步骤。

STEP 6 | 沿着升级到 PAN-OS 11.1 的路径，将日志收集器升级到 PAN-OS 发行版本。

1. 在 Panorama 未连接到互联网的情况下升级日志收集器到 PAN-OS 9.1。
2. 在 Panorama 未连接到互联网的情况下升级日志收集器到 PAN-OS 10.0。
3. 在 Panorama 未连接到互联网的情况下升级日志收集器到 PAN-OS 10.1。

   PAN-OS 10.0 引入了一种新的日志格式。从 PAN-OS 10.0 升级到 PAN-OS 10.1 时，您可以选择迁移在 PAN-OS 8.1 或更早版本中生成的日志。否则，在成功升级到 PAN-OS 10.1 时，系统会自动删除这些日志。在迁移期间，ACC 或监视选项卡中不会显示日志数据。在迁移过程中，日志数据会继续转发到相应的日志收集器，但是您可能会遇到一些性能影响。
4. 在 Panorama 未连接到互联网的情况下升级日志收集器到 PAN-OS 10.2。
5. 在 Panorama 未连接到互联网的情况下升级日志收集器到 PAN-OS 11.0。

STEP 7 | 将日志收集器升级到 PAN-OS 11.1。

1. 选择 **Panorama** > **Device Deployment**（设备部署） > **Software**（软件）。
2. 单击 **Upload**（上传），**Browse**（浏览）至主机上的相应软件更新文件，然后单击 **OK**（确定）。
3. 单击您刚上传的更新版本的 Action（操作）列中的 **Install**（安装）。
4. **Install**（安装）PAN-OS 11.1 并选择适当的日志收集器。
5. 如果一个或多个选定的日志收集器包含在 PAN-OS 10.0 或更早版本中生成的日志，则会显示通知。

   在您第一次尝试 **Install**（安装）PAN-OS 11.1.2 或更高版本 11.1 时会显示此通知，关闭后不会再次显示该通知。它会警告您，系统检测到在运行 PAN-OS 10.0 或更早版本时由 Panorama 或托管设备生成的日志，并且将会在升级时删除这些日志。这意味着成功升级后无法查看或搜索受影响的日志。

   但您可以在升级后恢复这些受影响的日志。该通知还为您提供以下信息。如果选择了多个日志收集器，请单击 **Tasks**（任务）并查看每个日志收集器安装失败的作业详细信息，以便查看和复制所需的迁移命令。

   - 受影响的日志类型。
   - 每种日志类型受影响的时间范围。
   - 恢复每种日志类型受影响的日志所需的每个 `debug logdb migrate-lc` 命令。

     在 **Close**（关闭）通知之前复制所列的 `debug logdb migrate-lc` 命令。

   Close（关闭）通知。
6. 根据您的需要选择以下项之一：
   - **Upload only to device (do not install)**（仅上传到设备（不安装））。
   - **Reboot device after install**（在安装之后重新启动设备）。
7. 单击 **OK**（确定）开始安装（或上传）。

   在选定的日志收集器成功重启后继续下一步。

STEP 8 | 验证安装在每个日志收集器上的软件和内容版本。

登录到日志收集器 CLI，然后输入操作命令 **`show system info`**。输出将如下所示：

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

STEP 9 | （PAN-OS 11.1.2 及更高版本；仅限 Panorama 模式）对于每个受影响的日志收集器，登录到日志收集器 CLI，并使用上一步中列出的 `debug logdb migrate-lc` 命令恢复受影响的日志。

这些命令必须按顺序运行，不能同时运行。如果您没有从通知窗口复制 `debug logdb migrate-lc` 命令，请单击 **Tasks**（任务）并查看特定日志收集器的安装失败的作业详细信息。

STEP 10 | （仅限 FIPS-CC 模式） 在 FIPS-CC 模式下升级 Panorama 和受管设备。

如果您在专用日志收集器运行 PAN-OS 11.1 版本时将专用日志收集器添加到 Panorama 管理，则在 FIPS-CC 模式下升级专用日志收集器需要重置安全连接状态。

在专用日志收集器运行 PAN-OS 10.0 或更早版本时，您无需重新启动已添加到 Panorama 管理中的专用日志收集器。

STEP 11 | （PAN-OS 10.2 及更高版本）重新生成或重新导入所有证书以符合 OpenSSL 安全级别 2。

如果您从 PAN-OS 10.1 或更早版本升级到 PAN-OS 11.0，则需要执行此步骤。如果您从 PAN-OS 10.2 升级并且已经重新生成或重新导入了您的证书，请跳过此步骤。

所有证书都必须满足以下最低要求：

- RSA 2048 位或以上，或 ECDSA 256 位或以上
- SHA256 或更高版本的摘要

请参阅 PAN-OS 管理员指南或 Panorama 管理员指南，了解有关重新生成或重新导入证书的更多信息。

STEP 12 | （推荐用于 Panorama 虚拟设备）将 Panorama 虚拟设备的内存增加到 64GB。

在日志收集器模式下成功将 Panorama 虚拟设备升级到 PAN-OS 11.1 后，Palo Alto Networks 建议将 Panorama 虚拟设备的内存增加到 64GB 以满足增加的系统要求，从而避免与配置不足的 Panorama 虚拟设备相关的任何日志、管理和操作性能问题。

在有互联网连接的情况下从 Panorama 升级 WildFire 集群

集群内的 WildFire 设备受 Panorama 管理时，可并行升级。如果 Panorama 直接连接互联网，您可以检查并从 Panorama 直接下载新版本。

Panorama 可以管理运行相同或更早 *PAN-OS* 软件版本的 *WildFire* 设备和设备集群。

STEP 1 | 升级 Panorama 至与您想在 WildFire 集群上安装的目标软件版本相同或更新的版本。

有关升级 Panorama 的信息，请参阅安装 Panorama 的内容和软件更新。

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：
   1. 登录到 Panorama Web 界面。
   2. 选择 **Panorama > Managed WildFire Clusters**（受管理的 **WildFire** 集群）并 **View**（查看）集群分析环境 **Utilization**（使用率）。
   3. 验证 **Virtual Machine Usage**（虚拟机使用）不显示任何进行中的样本分析。

   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。

这些更新为设备带来了最新的威胁信息，以准确检测恶意软件。

在安装软件升级之前，必须安装内容更新。请参阅发布说明以了解您必须为 *Panorama* 发布产品安装的最低内容发布版本。

1. 下载 WildFire 内容更新：
   1. 选择 **Panorama > Device Deployment > Dynamic Updates**（**Panorama >** 设备部署 **>** 动态更新）。
   2. 选择 WildFire 内容升级版本包并单击 **Download**（下载）。
2. 单击 **Install**（安装）。
3. 选择您想要升级的 WildFire 集群或单独的设备。
4. 单击 **OK**（确定）以开始安装。

STEP 4 | 下载 PAN-OS 软件版本至 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 9.1 升级至 PAN-OS 11.0，您必须首先下载并安装 PAN-OS 10.0、PAN-OS 10.1 和 PAN-OS 10.2。

1. 下载 WildFire 软件升级：
   1. 选择 **Panorama > Device Deployment > Software**（**Panorama >** 设备部署 **>** 软件）。
   2. 单击 **Check Now**（现在检查）以获取版本更新列表。
   3. 选择要安装的 WildFire 版本，然后单击 **Downdload**（下载）。
   4. 单击 **Close**（关闭）退出 **Download Software**（下载软件）窗口
2. 单击 **Install**（安装）。
3. 选择您想要升级的 WildFire 集群。
4. 选择 Reboot device after install（在安装之后重新启动设备）：
5. 单击 **OK**（确定）以开始安装。
6. （可选）在 Panorama 上监控安装进度。

STEP 5 | （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 6 | 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 11.0.0：

   ```
   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
   ```

在没有互联网连接的情况下从 Panorama 升级 WildFire 集群

集群内的 WildFire 设备受 Panorama 管理时，可并行升级。如果 Panorama 未直接连接互联网，您必须从 Palo Alto Networks 支持网站下载软件和升级内容，然后在在内部服务器上托管，之后才能通过 Panorama 分配。

Panorama 可以管理运行相同或更早 *PAN-OS* 软件版本的 *WildFire* 设备和设备集群。

STEP 1 | 升级 Panorama 至与您想在 WildFire 集群上安装的目标软件版本相同或更新的版本。

有关升级 Panorama 的信息，请参阅安装 Panorama 的内容和软件更新。

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：
   1. 登录到 Panorama Web 界面。
   2. 选择 **Panorama > Managed WildFire Clusters**（受管理的 **WildFire** 集群）并 **View**（查看）集群分析环境 **Utilization**（使用率）。
   3. 验证 **Virtual Machine Usage**（虚拟机使用）不显示任何进行中的样本分析。

   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 | 将 WildFire 内容和软件更新下载到能够访问互联网的主机。Panorama 必须能够访问主机。

1. 使用能够访问互联网的主机，登录到 Palo Alto Networks 客户支持网站。
2. 下载内容更新：
   1. 在“Tools（工具）”部分中单击 **Dynamic Updates**（动态更新）。
   2. **Download**（下载）所需内容更新，然后将文件保存到主机。对您将更新的每种内容类型执行此步骤。
3. 下载软件更新：
   1. 返回到 Palo Alto Networks 客户支持网站的主页，然后在“Tools（工具）”部分中单击 **Software Updates**（软件更新）。
   2. 查看 Download（下载）列以确定要安装的版本。更新包文件名显示升级的型号和版本：WildFire_<release>。
   3. 单击文件名并将文件保存到主机。

STEP 4 | 安装最新的 WildFire 设备内容更新。

这些更新为设备带来了最新的威胁信息，以准确检测恶意软件。

在安装软件升级之前，必须安装内容更新。请参阅发布说明以了解您必须为 *Panorama* 发布产品安装的最低内容发布版本。

1. 下载 WildFire 内容更新：
   1. 选择 **Panorama > Device Deployment > Dynamic Updates**（**Panorama >** 设备部署 **>** 动态更新）。
   2. 单击 **Upload**（上传），选择内容 **Type**（类型），**Browse**（浏览）至 WildFire 内容更新文件，然后单击 **OK**（确定）。
   3. 单击 **Install From File**（从文件安装），选择文件包 **Type**（类型）、**File Name**（文件名），然后选择您想要升级的集群内 WildFire 设备，最后单击 **OK**（确定）。
2. 单击 **OK**（确定）以开始安装。

STEP 5 | 下载 PAN-OS 软件版本至 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 9.1 升级至 PAN-OS 11.0，您必须首先下载并安装 PAN-OS 10.0、PAN-OS 10.1 和 PAN-OS 10.2。

1. 下载 WildFire 软件升级：
   1. 选择 **Panorama > Device Deployment > Software**（**Panorama >** 设备部署 **>** 软件）。
   2. 单击 **Check Now**（现在检查）以获取版本更新列表。
   3. 选择要安装的 WildFire 版本，然后单击 **Downdload**（下载）。
   4. 单击 **Close**（关闭）退出 **Download Software**（下载软件）窗口
2. 单击 **Install**（安装）。
3. 选择您想要升级的 WildFire 集群。
4. 选择 Reboot device after install（在安装之后重新启动设备）：
5. 单击 **OK**（确定）以开始安装。
6. （可选）在 Panorama 上监控安装进度。

STEP 6 | （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 7 | 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 11.0.0：

```
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
```

当 Panorama 连接上互联网时升级防火墙

查看 PAN-OS 11.1 发行说明，然后遵循以下程序升级使用 Panorama 管理的防火墙。此程序适用于独立防火墙和部署在高可用性 (HA) 配置中的防火墙。

在多个功能 PAN-OS 版本上升级 HA 防火墙时，必须将升级路径上的每个 HA 对等设备升级到相同的功能 PAN-OS 版本，然后才能继续。例如，您正在将 HA 对等设备从 PAN-OS 10.2 升级到 PAN-OS 11.1。必须先将两个 HA 对等设备都升级到 PAN-OS 11.0，然后才能继续升级到目标 PAN-OS 11.1 版本。当 HA 对等设备相隔两个或更多功能版本时，安装了较旧版本的防火墙会进入暂停状态，并显示消息对端设备版本太旧。

如果 *Panorama* 无法直接连接到更新服务器，则遵循 当 Panorama 未连接互联网时升级防火墙 程序以手动将映像下载到 *Panorama*，并将其分发给防火墙。

当从 PAN-OS 11.1 上的 Panorama 设备升级到 PAN-OS 10.1 或更高版本上的防火墙时，新的跳过软件版本升级功能使您能够跳过最多三个版本。

更新 Panorama 的防火墙前，必须：

- 确保 Panorama 运行的 PAN-OS 版本与更新到的版本相同或，高于更新到的版本。在将托管防火墙升级到 11.1 版本之前，您必须将 Panorama 及其日志收集器升级到该版本。此外，在将日志收集器升级到 11.1 时，由于日志记录基础架构中的变化，您必须同时升级所有日志收集器。
- 确保防火墙已连接至可靠的电源。升级时断电可能导致防火墙无法使用。
- 如果 Panorama 虚拟设备在升级到 PAN-OS 11.1 时处于旧版模式，则决定是否保持处于旧版模式。运行 PAN OS 9.1 或更高版本的新 Panorama 虚拟设备部署不支持旧版模式。如果您将 Panorama 虚拟设备从 PAN-OS 9.0 或更早版本升级到 PAN-OS 11.1，Palo Alto Networks 建议查看 Panorama 虚拟设备的安装先决条件，并根据您的需要更改为 Panorama 模式或仅管理模式。

  如果要让 Panorama 虚拟设备保持处于旧版模式，请将分配给 Panorama 虚拟设备的 CPU 和内存增加到至少 16 个 CPU 和 32GB 内存，以成功升级到 PAN-OS 11.1。有关详细信息，请参阅 Panorama 虚拟设备的安装先决条件。

- （建议用于多 vsys 受管防火墙）将多 vsys 受管防火墙的所有 vsys 过渡到 Panorama。

  之所以这样建议是为了避免在多 vsys 受管防火墙上出现提交问题，并且使您能够利用 Panorama 经过优化的共享对象推送。

  适用于仅使用跳过软件版本升级从 PAN-OS 10.1 升级到 PAN-OS 11.1 的多 vsys 防火墙。

- （多 vsys 受管防火墙）删除或重命名与 Panorama **Shared**（共享）配置中的对象具有相同名称的任何本地配置 的**Shared**（共享）对象。否则，来自 Panorama 的配置推送在升级后会失败，并显示错误 `<object-name>` 已在使用中。

  适用于仅使用跳过软件版本升级从 PAN-OS 10.1 升级到 PAN-OS 11.1 的多 vsys 防火墙。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 已修改您的安全策略规则以允许 SSL 应用程序流量。

> 适用于仅使用跳过软件版本升级从 *PAN-OS 10.1* 升级到 *PAN-OS 11.1* 的防火墙。
>
> 升级到 *PAN-OS 11.1* 之后，如果使用 *Panorama App-ID* 控制 *Panorama* 与托管设备之间的流量，则必须采取此操作才能防止托管设备与 *Panorama* 断开连接。如果在升级之前不允许使用 *SSL* 应用程序，则托管设备将断开与 *Panorama* 的连接。

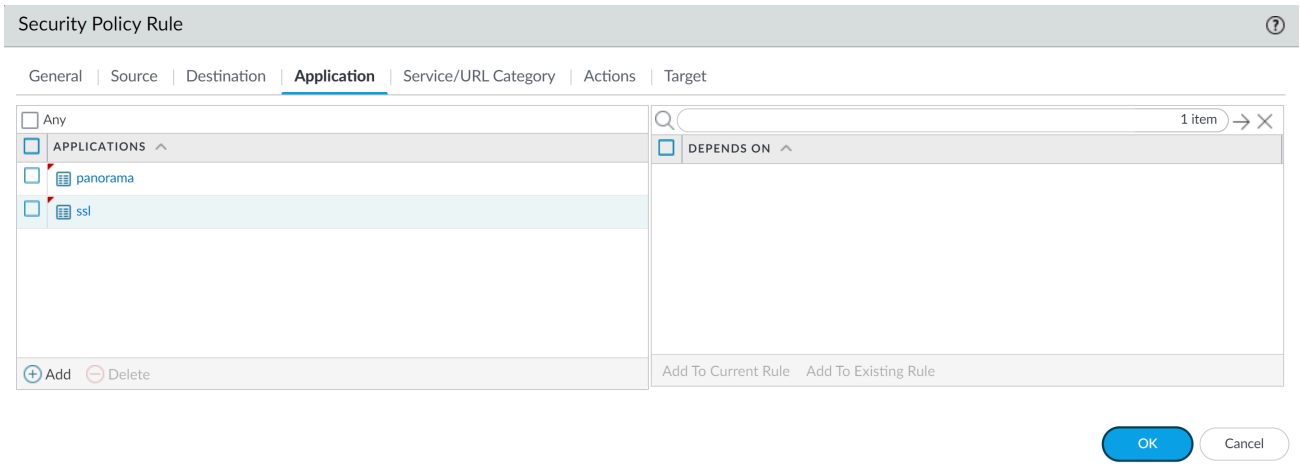
PAN-OS 11.1 使用 TLS 1.3 版本来加密服务证书以及 Panorama 和受管防火墙之间的握手消息。因此，从受管防火墙到 Panorama 的流量的 App-ID 将从 `Panorama` 重新分类为 SSL。要

继续在 Panorama 和托管设备之间进行通信，您必须修改控制 Panorama 和托管设备之间的流量的安全策略规则，以便同样允许使用 SSL 应用程序。

如果控制 Panorama 和托管设备之间的流量的安全策略规则允许使用 **Any**（任何）应用程序，或者您已经修改了控制 Panorama 和托管设备之间的流量的安全策略规则，请跳过此步骤。

1. 选择 **Policys**（策略） > **Security**（安全） > **Pre Rules**（前导规则）。
2. 选择包含控制 Panorama 和受管防火墙之间流量的安全策略规则的 **Device Group**（设备组）。
3. 选择安全策略规则。
4. 选择 **Application**（应用程序）并 **Add**（添加）SSL。

   请勿删除 *Panorama* 应用程序。这会导致在您推送更改后所有受管防火墙与 *Panorama* 断开连接。

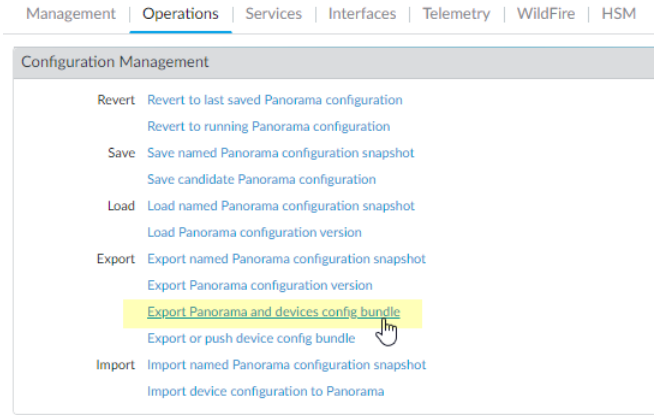


5. 单击 **OK**（确定）。
6. 选择 **Commit**（提交） > **Commit and Push**（提交并推送），然后 **Commit and Push**（提交并推送）您的配置更改。

STEP 3 | 将当前配置文件的备份保存在计划要升级的每个托管防火墙上。

尽管防火墙自动创建配置备份，但最佳做法是在升级之前创建备份并通过外部方式将其保存。

1. 选择 **Panorama > Setup**（设置） **> Operations**（操作）并单击**Export Panorama and devices config bundle**（导出 **Panorama** 和设备配置包）以生成和导出 Panorama 和每个受管设备的最新配置备份。

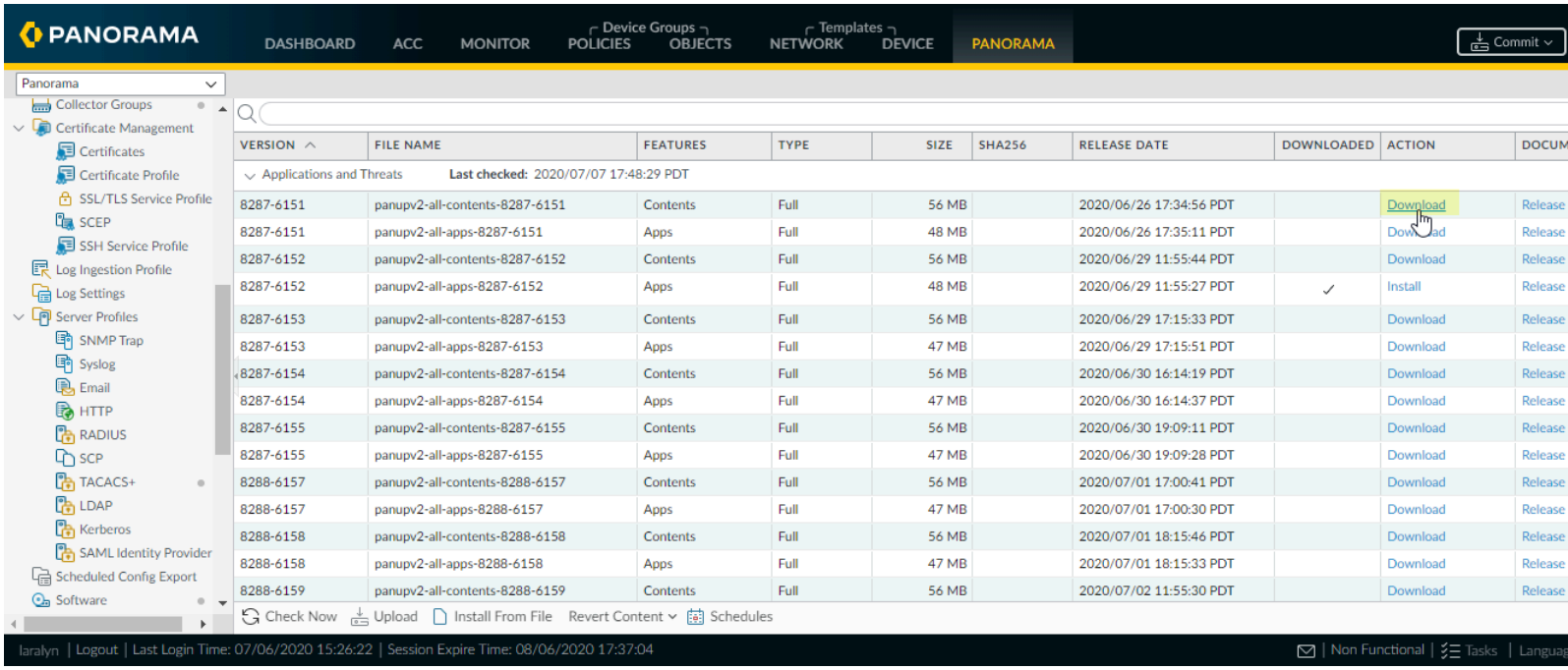


2. 将导出的文件保存到防火墙外部的位置。如果升级出现问题，您可以使用此备份还原配置。

STEP 4 | 安装最新的内容更新。

要了解 PAN-OS 11.1 所需的最低内容发行版本，请参阅发行说明。确保在将内容更新部署到 Panorama 和受管防火墙时遵循 应用程序和威胁内容更新的最佳实践。

1. 选择 **Panorama > Device Deployment**（设备部署） **> Dynamic Updates**（动态更新），然后 **Check Now**（立即检查）最近更新。如果有更新可用，“操作”列会显示 **Download**（下载）链接。



2. 单击 **Install**（安装）并选择要在其中安装更新的防火墙。如果更新 HA 防火墙，则必须更新两个对等的内容。
3. 单击 **OK**（确定）

STEP 5 | 确定升级到 PAN-OS 11.1 的路径.

对于您在升级路径中会经过的每个版本，了解发行说明中的 PAN-OS 升级清单、已知问题和默认行为更改，以及升级/降级注意事项。

如果升级多个防火墙，请在开始下载映像之前通过确定所有防火墙的升级路径来简化该过程。

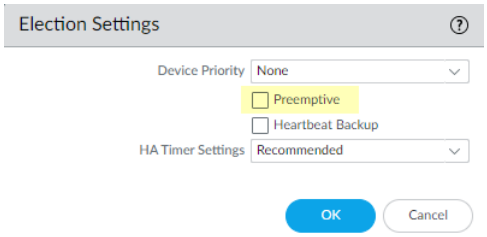
STEP 6 | （最佳实践）如果您使用 Cortex 数据湖 (CDL)，请安装设备证书。

在升级到 PAN-OS 11.1 时，防火墙会自动切换到使用设备证书向 CDL 摄取和查询端点进行身份验证。

如果您未在升级到 *PAN-OS 11.1* 之前安装设备证书，防火墙将继续使用现有的日志服务证书进行身份验证。

STEP 7 | （仅限 HA 防火墙更新）如果将要更新作为 HA 对组成部分的防火墙，请禁用抢先。您仅需要禁用每个 HA 对上每个防火墙的此设置。

1. 选择 **Device**（设备） > **High Availability**（高可用性），然后编辑 **Election Settings**（选择设置）。
2. 如果已启用，则禁用（取消选择）**Preemptive**（抢先）设置，然后单击 **OK**（确定）。



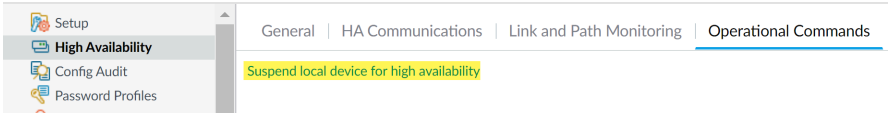
3. **Commit**（提交）更改。必须确保已成功提交，然后才能进行更新。

STEP 8 | （仅限 HA 防火墙升级）挂起主要 HA 对等设备以强制进行故障转移。

（主动/被动防火墙）对于主动/被动 HA 配置中的防火墙，请先暂停和升级主动 HA 对等设备。

（主动/主动防火墙）对于主动/主动 HA 配置中的防火墙，请先暂停和升级主动-主要 HA 对等设备。

1. 登录到主动主要防火墙 HA 对等设备的防火墙 Web 界面 。
2. 选择 **Device**（设备） > **High Availability**（高可用性） > **Operational Commands**（操作指令），并 挂起本地设备以实现高可用性。



3. 在右下角，验证状态是否已暂停。

   由此产生的故障转移应导致辅助被动 HA 对等设备转换为 主动 状态。

   生成的故障转移会在您升级之前验证 *HA* 故障转移是否正常运行。

STEP 9 | （可选） 将您的托管防火墙升级到 PAN-OS 10.1。

跳过软件版本升级功能支持运行 PAN-OS 10.1 或更高版本的托管防火墙。如果您的托管防火墙位于 PAN-OS 10.0 或更早版本上，请先升级到 PAN-OS 10.1 或更高版本。

STEP 10 | （可选）将文件 **Export**（导出） 到已配置的 SCP 服务器。

在 PAN-OS 11.1 中，在将升级部署到受管防火墙时，SCP 服务器可用作下载源。在下一步下载软件和内容映像之前导出文件。

STEP 11 | 验证并下载目标版本所需的软件和内容版本。

在此步骤中，您可以查看和下载升级到 PAN-OS 11.1 所需的中间软件和内容映像。

使用多映像下载来下载软件和内容映像是可选的。您仍然可以一次下载一个映像。

1. 单击 **Panorama** > **Device Deployment**（设备部署） > **Software**（软件） > **Action**（操作） > **Validate**（验证）
2. 查看您需要下载的中间软件和内容版本。
3. 选择要升级的防火墙，然后单击 **Deploy**（部署）。
4. 选择下载源并单击 **Download**（下载）。

STEP 12 | 在防火墙上安装 PAN-OS 11.1.0。

（仅限 *SD-WAN*）为了保持 *SD-WAN* 链接的准确状态，必须在升级分支防火墙之前将中心防火墙升级到 *PAN-OS 11.1*。先升级分支防火墙再升级中心防火墙可能导致错误的监视数据（***Panorama*** > ***SD-WAN*** > ***Monitoring***（监视）），且 *SD-WAN* 链接会错误地显示为 *down*。

1. 单击与想要更新的防火墙型号匹配的操作列中的 **Install**（安装）。例如，如果想升级 PA-440 防火墙，请单击与 PanOS_440-11.1.0 相对应的行中的 **Install**（安装）。
2. 在部署软件文件对话框，选择想要升级的所有防火墙。

   （仅限 HA 防火墙升级）要减少停机时间，请在每个 HA 对中只选择一个对端设备。对于主动/被动对，选择主动对等；对于主动/主动对，选择主动-辅助对等。
3. （仅限 HA 防火墙更新）请勿选择**Group HA Peers**（组高可用性对端设备）。
4. 选择**Reboot device after install**（在安装之后重新启动设备）。
5. 要开始更新，请单击 **OK**（确定）。
6. 安装成功完成后，请使用以下方法之一重新启动：
   - 如果提示重新启动，请单击 **Yes**（是）。
   - 如果未提示重启，请选择 **Device**（设备） > **Setup**（设置） > **Operations**（操作），然后单击 **Reboot Device**（重启设备）。
7. 防火墙完成重启后，请选择 **Panorama** > **Managed Devices**（托管设备），然后验证用于已升级的防火墙的软件版本是否为 11.1.0。此外，还检验已更新的任何被动防火墙的 HA 状态是否仍为被动。

STEP 13 | （仅限 HA 防火墙升级）将 HA 功能恢复到主要 HA 对等设备。

1. 登录到挂起的主防火墙 HA 对等设备的防火墙 Web 界面。
2. 选择 **Device**（设备） > **High Availability**（高可用性） > **Operational Commands**（操作指令），并 使本地设备正常运行以实现高可用性。
3. 在右下角，验证状态是否为 被动。对于处于主动/主动配置的防火墙，请验证其状态是否为 主动。
4. 等待 HA 对等设备运行配置同步。

   在 **Dashboard**（仪表板）中，监控 高可用性小部件中的运行配置状态。

STEP 14 | （仅限 HA 防火墙升级）暂停辅助 HA 对等设备以强制故障转移回主要 HA 对等设备。

1. 登录到主要辅助防火墙 HA 对等设备的防火墙 Web 界面 。
2. 选择 **Device**（设备） > **High Availability**（高可用性） > **Operational Commands**（操作指令），并 挂起本地设备以实现高可用性。
3. 在右下角，验证状态是否已暂停。

   由此产生的故障转移应导致主动被动 HA 对等设备转换为 主动 状态。

   生成的故障转移会在您升级之前验证 *HA* 故障转移是否正常运行。

STEP 15 | （仅限 HA 防火墙更新）更新每个 HA 对中的第二个 HA 对端设备。

1. 在 Panorama Web 界面中，选择 **Panorama** > **Device Deployment**（设备部署） > **Software**（软件）。
2. 单击与正在更新的 HA 对中防火墙型号匹配的操作列中的 **Install**（安装）。
3. 在部署软件文件对话框，选择想要升级的所有防火墙。此时，仅选择刚升级的 HA 防火墙的对等。
4. 请勿选择 **Group HA Peers**（组高可用性对等）。
5. 选择**Reboot device after install**（在安装之后重新启动设备）。
6. 要开始更新，请单击 **OK**（确定）。
7. 安装成功完成后，请使用以下方法之一重新启动：
   - 如果提示重新启动，请单击 **Yes**（是）。
   - 如果未提示重启，请选择 **Device**（设备） > **Setup**（设置） > **Operations**（操作）和 **Reboot Device**（重启设备）。

STEP 16 | （仅限 HA 防火墙升级）将 HA 功能恢复到辅助 HA 对等设备。

1. 登录挂起的辅助防火墙 HA 对等设备的防火墙 Web 界面 。
2. 选择 **Device**（设备） > **High Availability**（高可用性） > **Operational Commands**（操作指令），并 使本地设备正常运行以实现高可用性。
3. 在右下角，验证状态是否为 被动。对于处于主动/主动配置的防火墙，请验证其状态是否为 主动。
4. 等待 HA 对等设备运行配置同步。

   在 **Dashboard**（仪表板）中，监控 高可用性小部件中的运行配置状态。

STEP 17 | （仅限 FIPS-CC 模式） 在 FIPS-CC 模式下升级 Panorama 和受管设备。

如果在受管防火墙运行 PAN-OS 11.1 版本时将专用日志收集器添加到 Panorama 管理中，则在 FIPS-CC 模式下升级受管防火墙需要重置安全连接状态。

当托管防火墙运行 PAN OS 10.0 或更早版本时，您无需重新加入添加到 Panorama 管理的托管防火墙。

STEP 18 | 验证每个托管防火墙上运行的软件和内容发行版本。

1. 在 Panorama 上选择 **Panorama** > **Managed Devices**（托管设备）。
2. 找到防火墙并检查表格中的内容和软件版本。

   对于 HA 防火墙，您还可以验证每个对等的 HA 状态是否符合预期。

	DEVICE NAME	MODEL	IP Address IPV4	TEMPLATE	Status DEVICE STATE	Status HA STATUS	Status CERTIFICATE	Status L... M... D...	SOFTWARE VERSION	APPS AND THREAT	ANTIVIRUS
	DG-VM (5/5 Devices Connected): Shared > DG-VM										
	PA-VM-6	PA-VM		Stack-VM	Connected		pre-defined		8.1.0	8320-6307	3881-4345
	PA-VM-73	PA-VM		Stack-Test73	Connected		pre-defined		9.1.3	8320-6307	3873-4337
	PA-VM-95	PA-VM		Stack-VM	Connected		pre-defined		10.0.0	8320-6307	3881-4345
	PA-VM-96	PA-VM		Stack-VM	Connected	Passive	pre-defined		10.0.0	8299-6216	3881-4345
	PA-VM			Stack-Test92	Connected	Active	pre-defined		10.0.0	8299-6216	3881-4345

STEP 19 | （仅限 HA 防火墙升级）如果您在升级之前禁用其中一个 HA 防火墙的抢占，请编辑 **Election Settings**（选择设置）（**Device**（设备） > **High Availability**（高可用性）），并重新启用该防火墙的 **Preemptive**（抢占）设置，然后 **Commit**（提交）更改。

STEP 20 | 在 Panorama Web 界面上，将整个 Panorama 托管配置推送到您的托管防火墙。

此步骤需要启用选择性提交和推送设备组和模板堆栈配置更改从 Panorama 到您的托管防火墙。

在从 PAN-OS 10.1 或更早版本成功升级到 PAN-OS 11.1 后，这是成功将配置更改推送到由 Panorama 管理的多 vsys 防火墙所必需执行的操作。有关详细信息，请参阅 Panorama 管理的多 vsys 防火墙的共享配置对象的默认行为更改。

1. 选择 **Commit**（提交） > **Push to Devices**（推送到设备）。
2. **Push**（推送）。

STEP 21 | 重新生成或重新导入所有证书以遵守 OpenSSL 安全级别 2。

在升级到 PAN-OS 11.1 或更高版本时，要求所有证书满足以下最低要求。如果您从 PAN OS 10.2 升级并且已经重新生成或重新导入您的证书，请跳过此步骤。

- RSA 2048 位或以上，或 ECDSA 256 位或以上
- SHA256 或更高版本摘要

请参阅 PAN-OS 管理员指南或 Panorama 管理员指南，了解有关重新生成或重新导入证书的更多信息。

STEP 22 | 查看防火墙的软件升级历史。

1. 登录到 Panorama 界面。
2. 转到 **Panorama** > **Managed Devices**（受管设备） > **Summary**（摘要） 并单击 **Device History**（设备历史记录）。

当 Panorama 未连接互联网时升级防火墙

有关您可以在防火墙上安装的软件和内容更新列表，请参阅支持的更新。

当从 PAN-OS 11.1 上的 Panorama 设备升级到 PAN-OS 10.1 或更高版本上的防火墙时，新的跳过软件版本升级功能使您能够跳过最多三个版本。

更新 Panorama 的防火墙前，必须：

- 确保 Panorama 运行的 PAN-OS 版本与更新到的版本相同或，高于更新到的版本。在将托管防火墙升级到 11.1 版本之前，您必须将 Panorama 及其日志收集器升级到该版本。此外，在将日志收集器升级到 11.1 时，由于日志记录基础架构中的变化，您必须同时升级所有日志收集器。
- 确保防火墙已连接至可靠的电源。升级时断电可能导致防火墙无法使用。
- 如果 Panorama 虚拟设备在升级到 PAN-OS 11.1 时处于旧版模式，则决定是否保持处于旧版模式。运行 PAN OS 9.1 或更高版本的新 Panorama 虚拟设备部署不支持旧版模式。如果您将 Panorama 虚拟设备从 PAN-OS 9.0 或更早版本升级到 PAN-OS 11.1，Palo Alto Networks 建议查看 Panorama 虚拟设备的安装先决条件，并根据您的需要更改为 Panorama 模式或仅管理模式。

  如果要让 Panorama 虚拟设备保持处于旧版模式，请将分配给 Panorama 虚拟设备的 CPU 和内存增加到至少 16 个 CPU 和 32GB 内存，以成功升级到 PAN-OS 11.1。有关详细信息，请参阅 Panorama 虚拟设备的安装先决条件。
- （建议用于多 vsys 受管防火墙）将多 vsys 受管防火墙的所有 vsys 过渡到 Panorama。

  之所以这样建议是为了避免在多 vsys 受管防火墙上出现提交问题，并且使您能够利用 Panorama 经过优化的共享对象推送。

  适用于仅使用跳过软件版本升级从 PAN-OS 10.1 升级到 PAN-OS 11.1 的多 vsys 防火墙。
- （多 vsys 受管防火墙）删除或重命名与 Panorama **Shared**（共享）配置中的对象具有相同名称的任何本地配置 的**Shared**（共享）对象。否则，来自 Panorama 的配置推送在升级后会失败，并显示错误 `<object-name>` 已在使用中。

  适用于仅使用跳过软件版本升级从 PAN-OS 10.1 升级到 PAN-OS 11.1 的多 vsys 防火墙。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 已修改您的安全策略规则以允许 SSL 应用程序流量。

> 适用于仅使用跳过软件版本升级从 *PAN-OS 10.1* 升级到 *PAN-OS 11.1* 的防火墙。
>
> 升级到 *PAN-OS 11.1* 之后，如果使用 *Panorama App-ID* 控制 *Panorama* 与托管设备之间的流量，则必须采取此操作才能防止托管设备与 *Panorama* 断开连接。如果在升级之前不允许使用 *SSL* 应用程序，则托管设备将断开与 *Panorama* 的连接。

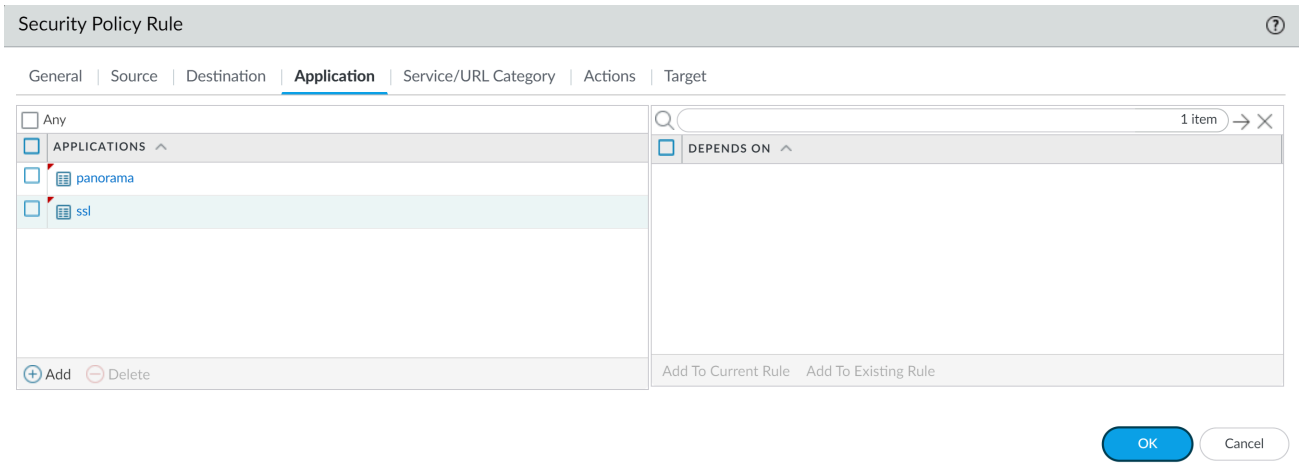
PAN-OS 11.1 使用 TLS 1.3 版本来加密服务证书以及 Panorama 和受管防火墙之间的握手消息。因此，从受管防火墙到 Panorama 的流量的 App-ID 将从 `Panorama` 重新分类为 SSL。要

继续在 Panorama 和托管设备之间进行通信，您必须修改控制 Panorama 和托管设备之间的流量的安全策略规则，以便同样允许使用 SSL 应用程序。

如果控制 Panorama 和托管设备之间的流量的安全策略规则允许使用 **Any**（任何）应用程序，或者您已经修改了控制 Panorama 和托管设备之间的流量的安全策略规则，请跳过此步骤。

1. 选择 **Policys**（策略） > **Security**（安全） > **Pre Rules**（前导规则）。
2. 选择包含控制 Panorama 和受管防火墙之间流量的安全策略规则的 **Device Group**（设备组）。
3. 选择安全策略规则。
4. 选择 **Application**（应用程序）并 **Add**（添加）SSL。

   请勿删除 *Panorama* 应用程序。这会导致在您推送更改后所有受管防火墙与 *Panorama* 断开连接。



5. 单击 **OK**（确定）。
6. 选择 **Commit**（提交） > **Commit and Push**（提交并推送），然后 **Commit and Push**（提交并推送）您的配置更改。

STEP 3 | 将当前配置文件的备份保存在计划要升级的每个托管防火墙上。

尽管防火墙自动创建配置备份，但最佳做法是在升级之前创建备份并通过外部方式将其保存。

1. **Export Panorama and devices config bundle**（导出 **Panorama** 和设备配置包）（**Panorama** > **Setup**（设置） > **Operations**（操作））用于生成和导出 Panorama 和每个受管设备的最新配置备份。
2. 将导出的文件保存到防火墙外部的位置。如果升级出现问题，您可以使用此备份还原配置。

STEP 4 | 确定您需要安装的内容更新。请参阅发布说明以了解您必须为 PAN-OS® 发布产品安装的最低内容发布版本。

Palo Alto Networks 强烈建议 *Panorama*，日志收集器和所有受管防火墙运行相同的内容发布版本。

对于每个内容更新，确定是否需要更新和在下一步中需要下载的内容更新。

确保 *Panorama* 运行的版本与受管防火墙和日志收集器上运行的内容发布版本相同，但不是更高版本。

STEP 5 | 对于打算更新到 Panorama 11.1 的防火墙，确定软件升级路径。

登录到 Panorama，选择 **Panorama** > **Managed Devices**（托管设备），然后记下您打算升级的防火墙的当前软件版本。

对于您在升级路径中会经过的每个版本，查看发行说明和升级/降级注意事项中的PAN-OS 升级清单、已知问题以及默认行为更改。

STEP 6 | （可选）将您的托管防火墙升级到 PAN-OS 10.1。

跳过软件版本升级功能支持运行 PAN-OS 10.1 或更高版本的托管防火墙。如果您的托管防火墙位于 PAN-OS 10.0 或更早版本上，请先升级到 PAN-OS 10.1 或更高版本。

STEP 7 | 执行版本的验证检查。

在此步骤中，您可以查看升级到 11.1 所需的中间软件和内容映像。

1. 选择 **Panorama** > **Device Deployment**（设备部署） > **Software**（软件） > **Action**（操作） > **Validate**（验证）。
2. 查看您需要下载的中间软件和内容版本。

STEP 8 | 将内容和软件更新下载到可以通过 SCP 或 HTTPS 连接并将文件上传到 Panorama 或配置的 SCP 服务器的主机。

默认情况下，您可以将最多两种软件或每种类型的内容更新上传到 Panorama 设备，并且如果您下载相同类型的第三个更新，Panorama 将删除该类型的最早版本的更新。如果您需要

上传两个以上的软件更新或单个类型的内容更新，请使用 **`set max-num-images count <number>`** CLI 命令增加 Panorama 可以存储的最大映像数量。

1. 使用能够访问互联网的主机，登录到 Palo Alto Networks 客户支持网站。
2. 下载内容更新：
   1. 在 Resources（资源）部分中单击 **Dynamic Updates**（动态更新）。
   2. **Download**（下载）最新的内容发布版本（或至少与将在 Panorama 管理服务器上安装或运行的版本相同或更高的版本）并将文件保存到主机；对于您需要更新的每个内容类型，请重复执行上述步骤。
3. 下载软件更新：
   1. 返回到 Palo Alto Networks 客户支持网站的主页，然后在 Resources（资源）部分中单击 **Software Updates**（软件更新）。
   2. 查看下载列以确定您需要安装的版本。更新包的文件名将指明型号。例如，要将 PA-440 和 PA-5430 防火墙升级到 PAN-OS 11.1.0，请下载 `Pan0S_440-11.1.0` 和 `Pan0S_5430-11.1.0` 映像。

      您可以通过从 ***Filter By***（筛选条件）下拉列表中选择 ***PAN-OS for the PA***（*PA* 的 ***PAN-OS***）*-<series/model>* 快速找到特定 *PAN-OS* 映像。
4. 单击相应的文件名并将文件保存到主机。

STEP 9 | 下载中间软件版本和最新的内容版本。

在 PAN OS 11.0 上，您可以使用多映像下载功能下载多个中间版本。

1. 选择要升级的防火墙（**Required Deployments**（所需部署） > **Deploy**（部署））。
2. 选择下载源并单击 **Download**（下载）。

STEP 10 | 在受管防火墙上安装内容更新。

在安装软件更新之前，必须安装内容更新。

先安装应用程序或应用程序和威胁更新，然后根据需要一次性以任何顺序安装任何其他更新（防病毒软件、WildFire® 或 URL 筛选）。

1. 选择 **Panorama** > **Device Deployment** > **Dynamic Updates**（Panorama > 设备部署 > 动态更新）。
2. 单击 **Upload**（上传），选择更新 **Type**（类型），**Browse**（浏览）至相应的内容更新文件，然后单击 **OK**（确定）。
3. 单击 **Install From File**（从文件安装），选择更新 **Type**（类型），然后选择您刚上传的内容更新的 **File Name**（文件名）。
4. 选择要安装更新的防火墙。
5. 单击 **OK**（确定）以开始安装。
6. 对于每个内容更新，请重复这些步骤。

STEP 11 | （仅限用作 GlobalProtect™ 门户的防火墙）在防火墙中上传并激活 GlobalProtect 代理/应用程序软件更新。

您在防火墙上激活了更新，因此用户将可以把更新下载到其端点（客户端系统）。

1. 使用能够访问互联网的主机登录到 Palo Alto Networks 客户支持网站。
2. 下载相应的 GlobalProtect 代理/应用程序软件更新。
3. 在 Panorama 上，选择 **Panorama** > **Device Deployment**（设备部署） > **GlobalProtect Client**（**GlobalProtect** 客户端）。
4. 单击 **Upload**（上传），**Browse**（浏览）到将文件下载到的主机上的相应 GlobalProtect 代理/应用程序软件更新，然后单击 **OK**（确定）。
5. 单击 **Activate From File**（从文件激活），然后选择您刚上传的 GlobalProtect 代理/应用程序软件更新的 **File Name**（文件名）。

   您一次只能激活一个版本的代理/应用程序软件更新。如果激活新版本，但某些代理需要以前的版本，则必须再次重新激活早期版本以便这些代理下载先前的更新。
6. 选择要激活更新的防火墙。
7. 单击 **OK**（确定）以激活。

STEP 12 | 安装 PAN-OS 11.1。

当您在高可用性 *(HA)* 防火墙上更新软件时，为了避免出现停机，一次只应更新一台高可用性对端设备。

对于主动/主动防火墙，无论您首先更新哪一个对端设备都没有关系。

对于主动/被动防火墙，您必须首先更新被动对端设备，挂起主动对端设备（故障转移），更新主动对端设备，然后再使主动对端设备恢复为运行状态（故障恢复）。

（仅限 *SD-WAN*）为了保持 *SD-WAN* 链接的准确状态，必须在升级分支防火墙之前将中心防火墙升级到 *PAN-OS 11.1*。先升级分支防火墙再升级中心防火墙可能导致错误的监视数据（***Panorama*** > ***SD-WAN*** > ***Monitoring***（监视）），且 *SD-WAN* 链接会错误地显示为 *down*。

1. 执行适用于防火墙配置的步骤以安装刚上传的 PAN-OS 软件更新。
   - 非高可用性防火墙 — 单击 Action（操作）列中的 **Install**（安装），选择您正在升级的所有防火墙，选择 **Reboot device after install**（安装后重新启动设备），然后单击 **OK**（确定）。
   - 主动/被动高可用性防火墙：
     1. 确认已在您打算升级的第一个对端设备上禁用抢先设置（**Device**（设备） > **High Availability**（高可用性） > Election Settings（选择设置））。如果启用，则编辑 **Election Settings**（选择设置），然后禁用（清除）**Preemptive**（抢先）设置并

Commit（提交）更改。您只需要在每个 HA 对中的一个防火墙上禁用此设置，但在继续之前确保提交成功。

2. 单击 **Install**（安装），禁用（清除）**Group HA Peers**（组高可用性对端设备），选择任意一个高可用性对端设备，选择 **Reboot device after install**（安装后重新启动设备），然后单击 **OK**（确定）。等待防火墙完成重新启动之后再继续进行操作。
3. 单击 **Install**（安装），禁用（清除）**Group HA Peers**（组高可用性对端设备），选择在上一步中尚未更新的高可用性对端设备，选择 **Reboot device after install**（安装后重新启动设备），然后单击 **OK**（确定）。

- 主动/被动高可用性防火墙 — 在本例中，主动防火墙的名称为 fw1，被动防火墙的名称为 fw2：
  1. 确认已在您打算升级的第一个对端设备上禁用抢先设置（**Device**（设备） > **High Availability**（高可用性） > Election Settings（选择设置））。如果启用，则编辑 **Election Settings**（选择设置），然后禁用（清除）**Preemptive**（抢先）设置并 **Commit**（提交）更改。您只需要在每个 HA 对中的一个防火墙上禁用此设置，但在继续之前确保提交成功。
  2. 单击相应更新的操作列中的 **Install**（安装），禁用（清除）**Group HA Peers**（组高可用性对端设备），选择 fw2，选择 **Reboot device after install**（安装后重新启动设备），然后单击 **OK**（确定）。等待 fw2 完成重新启动之后再继续进行操作。
  3. fw2 完成重新启动后，在 fw1（**Dashboard**（仪表板） > High Availability（高可用性））上核实 fw2 仍为被动对端设备（本地防火墙状态为 `active`，对端设备 (fw2) 为 `passive`）。
  4. 访问 fw1 和 **Suspend local device**（挂起本地设备）（**Device**（设备） > **High Availability**（高可用性） > **Operational Commands**（操作命令））。
  5. 访问 fw2（**Dashboard**（仪表板） > High Availability（高可用性）），并核实本地防火墙状态为 `active`，对端设备为 `suspended`。
  6. 访问 Panorama，选择 **Panorama** > **Device Deployment**（设备部署） > **Software**（软件），在相应版本的操作列中单击 **Install**（安装），禁用（清除）**Group HA Peers**（组高可用性对端设备），选择 fw1，选择 **Reboot device after install**（安装后重新启动设备），然后单击确定。等待 fw1 完成重新启动之后再继续进行操作。
  7. 访问 fw1（**Device**（设备） > **High Availability**（高可用性） > **Operational Commands**（高可用性）），单击 **Make local device functional**（使本地设备正常运行），然后等待两分钟后进行下一步。
  8. 在 fw1（**Dashboard**（仪表板） > High Availability（高可用性）） 上，核实本地防火墙状态为 `passive`，对端设备 (fw2) 为 `active`。

STEP 13 | （仅限 FIPS-CC 模式） 在 FIPS-CC 模式下升级 Panorama 和受管设备。

如果在受管防火墙运行 PAN-OS 11.1 版本时将专用日志收集器添加到 Panorama 管理中，则在 FIPS-CC 模式下升级受管防火墙需要重置安全连接状态。

当托管防火墙运行 PAN OS 10.0 或更早版本时，您无需重新加入添加到 Panorama 管理的托管防火墙。

STEP 14 | 验证安装在每个受管防火墙上的软件和内容版本。

1. 选择 **Panorama** > **Managed Devices**（受管设备）。
2. 找到防火墙，并查看 Software Version（软件版本）、Apps and Threat（应用程序和威胁）、Antivirus（防病毒软件）、URL Filtering（URL 筛选）和 GlobalProtect Client（GlobalProtect 客户端）列中的值。

STEP 15 | 如果您在升级之前禁用其中一个 HA 防火墙的抢先，请编辑 **Election Settings**（选择设置）（**Device**（设备） > **High Availability**（高可用性）），并重新启用该防火墙的 **Preemptive**（抢先）设置。

STEP 16 | 在 Panorama Web 界面上，将整个 Panorama 托管配置推送到您的托管防火墙。

此步骤需要启用选择性提交和推送设备组和模板堆栈配置更改从 Panorama 到您的托管防火墙。

在成功升级到 PAN-OS 11.1 后，这是成功地将配置更改推送到由 Panorama 管理的多 vsys 防火墙所必需的。有关详细信息，请参阅 Panorama 管理的多 vsys 防火墙的共享配置对象的默认行为更改。

1. 选择 **Commit**（提交） > **Push to Devices**（推送到设备）。
2. **Push**（推送）。

STEP 17 | 重新生成或重新导入所有证书以遵守 OpenSSL 安全级别 2。

在升级到 PAN-OS 11.1 时，要求所有证书满足以下最低要求：

- RSA 2048 位或以上，或 ECDSA 256 位或以上
- SHA256 或更高版本摘要

请参阅 PAN-OS 管理员指南或 Panorama 管理员指南，了解有关重新生成或重新导入证书的更多信息。

STEP 18 | 查看防火墙的软件升级历史。

1. 登录到 Panorama 界面。
2. 转到 **Panorama** > **Managed Devices**（受管设备） > **Summary**（摘要） 并单击 **Device History**（设备历史记录）。

升级 ZTP 防火墙

在您成功添加 ZTP 防火墙至 Panorama™ 管理服务器后，请配置 ZTP 防火墙的目标 PAN-OS 版本。当 ZTP 防火墙首次成功连接到 Panorama 后，Panorama 会检查 ZTP 防火墙上安装的 PAN-OS 版本是否大于或等于所配置的目标 PAN-OS 版本。如果 ZTP 防火墙上安装的 PAN-OS 版本低于目标 PAN-OS 版本，则 ZTP 防火墙将进入一个升级周期，直至安装目标 PAN-OS 版本。

STEP 1 | 以管理员身份登录到 Panorama Web 界面。

STEP 2 | 将 ZTP 防火墙添加到 Panorama。

STEP 3 | 选择 **Panorama** > **Device Deployment**（设备部署） > **Updates**（更新），然后 **Check Now**（立即检查）最新 PAN-OS 版本。

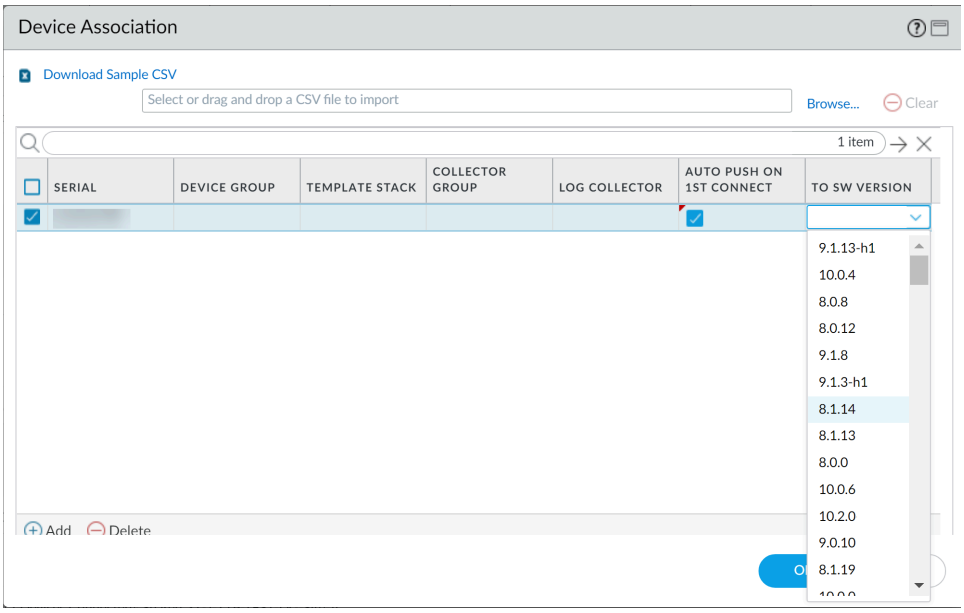
STEP 4 | 选择 **Panorama** > **Managed Devices**（受管设备） > **Summary**（摘要），然后选择一个或多个 ZTP 防火墙。

STEP 5 | **Reassociate**（重新关联）所选的 ZTP 防火墙。

STEP 6 | 检查（启用） 第一次连接时自动推送。

STEP 7 | 在 **To SW Version**（至 **SW** 版本）列中，选择 ZTP 防火墙的目标 PAN-OS 版本。

STEP 8 | 单击 **OK**（确定）保存您的配置更改。



STEP 9 | 选择 **Commit**（提交） 和 **Commit to Panorama**（提交到 **Panorama**）。

STEP 10 | 开启 ZTP 防火墙。

当 ZTP 防火墙首次连接到 Panorama 时，它会自动升级到您选择的 PAN-OS 版本。

- 运行 **PAN-OS 11.1.0** 的 **Panorama** — 如果您要跨 PAN-OS 主要版本或维护版本升级受管防火墙，则先安装升级路径上的中间 PAN-OS 版本，然后再安装目标 PAN-OS 版本。

  例如，您将受管防火墙的目标 **To SW Version**（到 **SW** 版本）配置为 PAN-OS 11.1.0，并且该防火墙运行的是 PAN-OS 10.2。第一次连接到 Panorama 时，先在受管防火墙上安装 PAN-OS 11.0.0。PAN-OS 11.0.0 成功安装后，防火墙会自动升级到目标 PAN-OS 11.1.0 版本。

- **Panorama** 运行 **PAN-OS 11.0.1** 及更高版本—如果您正在跨 PAN-OS 主要版本或维护版本升级托管防火墙，则先安装升级路径上的中间 PAN-OS 主要版本并下载基本 PAN-OS 主要版本，然后再安装目标 PAN OS 维护版本。

  例如，您将托管防火墙的目标 到 **SW** 版本 配置为 PAN-OS 11.0.1，并且防火墙正在运行 PAN-OS 10.0。在第一次连接到 Panorama 时，PAN-OS 10.1.0 和 PAN-OS 10.2.0 安装在托管防火墙上。托管防火墙重新启动后，将下载 PAN OS 11.0.0，然后防火墙自动安装到目标 PAN OS 11.0.1 版本。

STEP 11 | 验证 ZTP 防火墙是否升级。

1. 登录到 Panorama Web 界面。
2. 选择 **Panorama** > **Managed Devices**（受管设备） > **Summary**（摘要），然后导航至 ZTP 防火墙。
3. 验证 **Software Version**（软件版本）列是否显示正确的目标 PAN-OS 版本。

STEP 12 | 对于所有未来的 PAN-OS 升级，请参阅 从 Panorama 中将防火墙升级到 PAN-OS 11.1.

安装 PAN-OS 软件补丁

在何处可以使用？	需要提供什么？
• Panorama 管理的下一代防火墙 不支持 CN 系列防火墙 • Panorama 管理的 WildFire 设备	❑ 设备管理许可证 ❑ 支持许可证 ❑ PAN-OS 11.1.3 或更高的 11.1 版本 ❑ 出站互联网接入

查看 PAN-OS 11.1 发行说明，然后按照以下步骤安装 PAN-OS 软件补丁，以解决在 Panorama™ 管理服务器的托管设备上当前运行的 PAN-OS 版本中的错误以及公共漏洞和暴露 (CVE)。安装 PAN-OS 软件补丁可修复错误和 CVE，无需安排长期维护，并允许您立即加强安全态势，而不会引入任何新的已知问题或更改安装新 PAN-OS 版本时可能出现的默认行为。此外，您可以恢复当前安装的软件补丁，以卸载安装软件补丁时应用的错误和 CVE 修复程序。

安装或恢复 PAN-OS 软件补丁时会生成系统日志（**Monitor**（监视） > **Logs**（日志） > **System**（系统））。需要出站互联网连接才能从 Palo Alto Networks 客户支持门户下载 PAN-OS 软件补丁。对于气隙式托管设备，Panorama 仍然必须具有互联网接入才能下载 PAN-OS 软件补丁，但不需要出站互联网连接就可以安装补丁并将其应用于托管设备。

- 安装
- 恢复

安装

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 选择 **Panorama** > **Device Deployment**（设备部署） > **Software**（软件），然后 **Check Now**（立即检查）以从 Palo Alto Networks 更新服务器检索最新的 PAN-OS 软件补丁。

STEP 3 | 选中（启用）**Include Patch**（包含补丁），以显示所有可用的 PAN-OS 软件补丁。

STEP 4 | 找到当前安装在托管设备上的 PAN-OS 版本的软件补丁。

通过 **Version**（版本）名称旁边显示的 `Patch` 标签来表示软件补丁。

STEP 5 | 查看 **More Info**（更多信息），以查看软件补丁的详细信息，例如严重错误和 CVE 修复程序，以及是否需要重新启动托管设备才能应用修复程序。

STEP 6 | **Download**（下载）软件补丁。

（仅限 HA）选中（启用）同步到 HA 对等设备，然后选择 **Continue Download**（继续下载）以下载 PAN-OS 软件补丁。

成功下载软件补丁后单击 **Close**（关闭）。

STEP 7 | **Install**（安装）软件补丁。

成功安装软件补丁后，单击 **Close**（关闭）。

STEP 8 | 选择要安装 PAN-OS 软件补丁的托管设备，然后单击 **OK**（确定）。

（仅限 HA）如果要在高可用性 (HA) 配置中的一对托管设备上安装软件补丁，则必须在两个 HA 对等设备上选择并安装该软件补丁。

STEP 9 | **Apply**（应用）软件补丁。

当系统提示您确认要将已安装的 PAN-OS 软件补丁应用于托管设备时，单击 **Apply**（应用）。

将显示一个状态栏，显示 PAN-OS 软件补丁应用程序的当前进度。成功应用补丁后，单击 **Close**（关闭）。

此时，如果需要重新启动才能将 PAN-OS 软件补丁应用于托管设备，防火墙将自动重新启动。

恢复

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 选择 **Panorama** > **Device Deployment**（设备部署） > **Software**（软件），然后 **Check Now**（立即检查）以从 Palo Alto Networks 更新服务器检索最新的 PAN-OS 软件补丁。

STEP 3 | **Revert**（恢复）软件补丁。

STEP 4 | 选择要恢复 PAN-OS 软件补丁的托管设备，然后单击 **OK**（确定）。

仅显示符合条件的托管设备。

（仅限 HA）如果要在高可用性 (HA) 配置中的一对托管设备上安装软件补丁，则必须在两个 HA 对等设备上选择并安装该软件补丁。

STEP 5 | 当系统提示您确认要恢复所选托管设备上安装的 PAN-OS 软件补丁时，单击 **Revert**（恢复）。

将显示一个状态栏，显示 PAN-OS 软件补丁应用程序的当前进度。成功应用补丁后，单击 **Close**（关闭）。

此时，如果需要重新启动才能将 PAN-OS 软件补丁应用于 Panorama，防火墙将自动重新启动。

从 Panorama 恢复内容更新

Panorama™ 允许您直接从 Panorama 恢复一个或多个防火墙、日志收集器或 WildFire 设备上的应用程序、应用程序和威胁、防病毒软件、WildFire® 以及 WildFire 内容版本。使用 Panorama 恢复受管设备上的内容版本，以利用集中式工作流程，这有助于降低与内容更新中应用程序或新威胁签

名引入或修改相关的任何风险。Panorama 在恢复内容时为每个设备生成系统日志。确保在将内容更新部署到受管设备时使用应用程序和威胁内容更新的最佳实践。

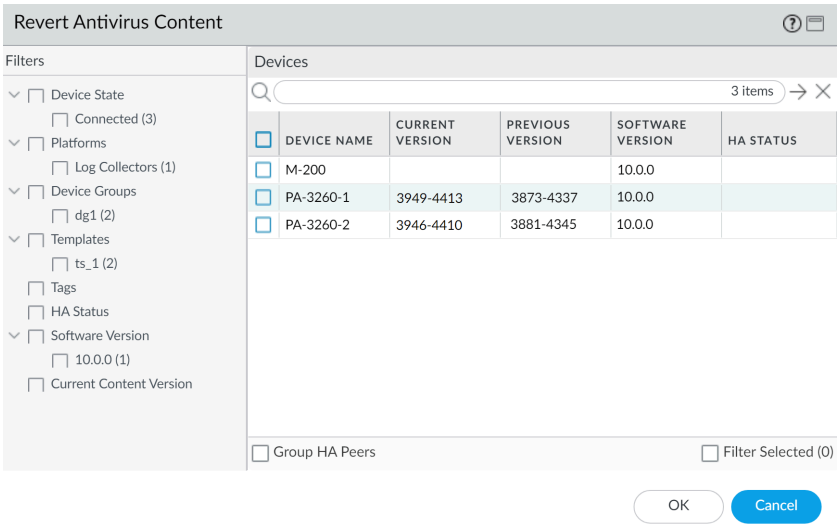
STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 选择 **Panorama** > **Device Deployment** > **Dynamic Updates**（动态更新），并 **Revert Content**（恢复内容）。

STEP 3 | 选择需要恢复的内容类型。

Antivirus
Apps
Applications and Threats
WildFire
WildFire-Content

STEP 4 | 选择要恢复内容的一个或多个防火墙，然后单击 **OK**（确定）。要恢复到的内容版本必须低于防火墙上当前安装的版本。



升级 PAN-OS

PAN-OS 升级清单

规划 PAN-OS 升级有助于确保 Panorama 或防火墙更平稳地过渡到更新版本的 PAN-OS。

- 确保设备已注册并已获得许可。
- 验证可用的磁盘空间。

  所需的磁盘空间因 PAN-OS 版本而异。选择 **Device**（设备） > **Software**（软件）并查看目标 PAN-OS 发行版本 **Size**（大小）以确定所需的磁盘空间。

  - 运行 **`show system disk-space`**
- 验证最低内容发行版本。
- 确定首选版本。

  - （PAN-OS 11.1.3 及更高版本）

    选择 **Device**（设备） > **Software**（软件）。默认情况下，Release Type（版本类型）列显示首选版本和基础版本。要仅查看首选版本，请禁用（清除）**Base Releases**（基础版本）复选框。
  - （PAN-OS 11.1.3 及更高版本）

    运行 **`request system software info preferred`**

  有关详细信息，请参阅 Palo Alto Networks 支持软件发行指南和生命周期终止摘要。此外，请查看目标 PAN-OS 版本的已知问题和已解决问题、升级和降级注意事项以及限制，以了解 PAN-OS 升级可能对您造成的影响。
- 确定升级路径。

  从一个 *PAN-OS* 功能发行版本升级到更高的功能发行版本时，不能跳过到达目标版本的路径中任何功能发行版本的安装。
- 查看升级路径中所有版本的升级/降级注意事项。
- （对于 GlobalProtect 为必需）验证最低 GlobalProtect™ 代理程序版本，以防止 GlobalProtect 用户丢失 VPN 连接。GlobalProtect 可以直接升级到最新版本。
- 对于已安装的任何插件，验证目标发行版本上的最低插件发行版本。
- 验证从管理界面到更新服务器的连接。

  - 选择 **Device**（设备） > **Troubleshooting**（故障排除）并测试 **Update Server Connectivity**（更新服务器连接）以检查 DNS 是否可以解析该地址。

    如果无法解析，请将 DNS 更改为 **`8.8.8.8`**（您需要使用公共 DNS 服务器而不是自己的 DNS 服务器），然后再次执行 ping 操作。

    如果此操作不能解决问题，请将更新服务器更改为 **`staticupdates.paloaltonetworks.com`** 并 **Commit**（提交）。
- （仅限 SD-WAN）确定要升级到 PAN-OS 11.1 的中心和分支防火墙。

  要保持 SD-WAN 链接的准确状态，必须在升级分支防火墙之前将中心防火墙升级到 PAN-OS 11.1。在中心防火墙之前升级分支防火墙可能导致错误的监视数据（**Panorama** > **SD-WAN** > **Monitoring**（监视）），且 SD-WAN 链接会错误地显示为 down（关闭）。

- 如果当前安装了任何插件，请在升级之前为当前安装在 Panorama（**Panorama > Plugins**（插件））或防火墙（**Device**（设备） > **Plugins**（插件））上的所有插件下载 PAN-OS 11.1 支持的插件版本。

  有关 PAN-OS 11.1 支持的 Panorama 插件版本，请参阅 Panorama 插件兼容性矩阵。

  这是成功将 Panorama 和防火墙升级到 PAN-OS 11.1 所必需执行的操作。升级到 PAN-OS 11.1 时会自动安装下载的插件版本。如果未下载支持的插件版本，将阻止升级到 PAN-OS 11.1。

升级/降级注意事项

下表列出了会受升级或降级影响的新功能。在升级到 PAN-OS 11.1 版本或从 PAN-OS 11.1 版本降级之前，请务必了解全部升级/降级注意事项。有关 PAN-OS 11.1 及更高版本的更多信息，请参阅 PAN-OS 发行说明。

功能	升级注意事项	降级注意事项
具有动态分配 IPv6 地址前缀的 NPTv6	无。	降级到 PAN-OS 11.1.5 之前的版本之前，请在具有动态分配的 IPv6 地址的接口上禁用 NPTv6 或删除配置。（在 PAN-OS 11.1.5 和 11.1.0 之间降级阻止功能不可用；因此，映像降级成功，但自动提交失败。）
重叠 IP 地址支持	无。	启用 Duplicate IP Address Support（重复 IP 地址支持）后，将阻止降级到 PAN-OS 11.1.4 之前的版本的尝试。尝试降级时会出现错误消息，表示降级失败。旧版本不支持重复的 IP 地址。请删除所有重复的 IP 地址配置，禁用 Duplicate IP Address Support（重复 IP 地址支持），提交，然后再继续降级。
高级路由引擎 (PAN-OS 11.2.0)	在 PAN-OS 11.2.0 中，启用 Advanced Routing（高级路由）时，不支持 IP 多播。即将推出的版本将提供对此功能的支持。已配置组播或计划部署组播路由的客户不应升级到 11.2.0。 此外，在 PAN-OS 11.2.0 中，当启用 Advanced Routing（高级路由）时，BGP 抑制配置不会应用于任何对等设备或对等组；该配置被保留，但对 BGP 没有影响。即使客户已将抑制配置文件应用于特定的一组对	无

功能	升级注意事项	降级注意事项
	等设备，他们仍然可以使用 BGP。该问题不会影响任何其他 BGP 功能。	
使用序列号和 IP 地址方法对 LSVPN 卫星进行身份验证 （PAN-OS 11.1.3 及更高版本）	PAN-OS 将配置更改存储在数据库内部。因此，当您升级到此功能时，将应用最新保存的配置。 从 PAN-OS 10.0 或更早版本升级到 PAN-OS 10.1 及更高版本（启用了用户名/密码和卫星 Cookie 身份验证方法）后，如果卫星 Cookie 过期，将导致登录失败。 在这种情况下，您应该输入用户名和密码才能成功进行身份验证。	• 如果您降级到 PAN-OS 10.1 及更高版本，则仅支持用户名/密码和卫星 Cookie 身份验证方法。 • 如果您下载并安装插件的次要版本，然后决定降级到同一版本的另一个次要版本，则降级前在次要版本上完成的配置将对同一版本降级后的次要版本生效。 PAN-OS 将配置更改存储在数据库内部。因此，当您从此功能降级时，将应用最新保存的配置。 例如，如果您已经安装了具有配置（配置 1）的 SD-WAN 插件 11.1.5，然后决定降级到同一版本的另一个次要版本，即具有不同配置（配置 2）的 11.1.4。这种情况下，降级前的次要版本配置，即配置 1，会对降级后的次要版本 11.1.4 生效。
	从 PAN-OS 10.0 或更早版本/PAN-OS 10.1 及更高版本升级到 PAN-OS 11.1.3 后，请考虑以下事项： • 如果您禁用了序列号和 IP 地址身份验证方法，并且卫星 Cookie 过期，则会导致登录失败。在这种情况下，管理员应该输入用户名和密码才能成功进行身份验证。 • 如果您启用了序列号和 IP 地址身份验证方法，在 GlobalProtect 门户中注册	• 如果降级到 PAN-OS 10.1 之前的版本，则仅支持序列号身份验证方法。 • 如果降级到高于 10.1 且早于 10.2.8 的 PAN-OS 版本，则支持用户名/密码和卫星 Cookie 身份验证方法。 • 如果降级到 PAN-OS 10.2.8 及更高的 10.2 版本，则支持“用户名/密码和卫星 Cookie 身份验

功能	升级注意事项	降级注意事项
	了卫星序列号，并且 IP 地址出现在 IP 允许列表中，则登录将成功。 • 如果您启用了序列号和 IP 地址身份验证方法，但未在 GlobalProtect 门户中注册卫星序列号，或者 IP 地址未出现在 IP 允许列表中，则登录失败。在这种情况下，防火墙不会回退到任何其他身份验证方法并导致身份验证失败。如果身份验证失败，卫星将等到配置的重试间隔过去后再尝试再次进行身份验证。确保在门户中正确注册了卫星序列号，并且卫星 IP 地址出现在 IP 允许列表中，以便成功进行身份验证。	证”以及“序列号和 IP 地址身份验证”方法。
每项策略的持久 DIPP	使用 Panorama 将防火墙从 PAN-OS 11.0.0 升级到 11.1.1 时，应将常规 DIPP NAT 规则转换为持久 DIPP NAT 规则，但是转换失败，规则仍然是常规 DIPP NAT 规则。	使用 Panorama 将防火墙从 PAN-OS 11.1.1 降级到 11.0 0 时，每项策略的持久 DIPP NAT 规则将转换为常规 DIPP NAT 规则。
GlobalProtect 的 TLSv1.3 支持	如果从较早的 PAN-OS 版本升级到 PAN-OS 11.1，且 SSL/TLS 服务配置文件中的 **Max Version**（最大版本）设置为 **Max**（最大），则升级后 TLS 版本将替换为 TLSv1.2。 如果从 PAN-OS 11.1 升级到更高的 PAN-OS 版本，并且在 SSL/TLS 服务配置文件中将 **Max Version**（最大版本）设置为 <TLS Version>，则升级后 TLS 版本将保留为配置的 <TLS Version>。由于版本已在 11.1.x 本身进行了配置，因此无需替换版本。	如果从具有 TLSv1.3 的 PAN-OS 11.1 降级到较早的 PAN-OS 版本，则降级后 TLSv1.3 将被替换为 TLSv1.2。降级将成功，但如果您在 PAN-OS 11.1 中选择了较早的 PAN-OS 版本不支持的 TLS v1.3 **aes-chacha20-poly1305** 密码，则自动提交将失败。您必须在降级后的版本中添加或替换相应的支持密码，然后手动提交更改。

功能	升级注意事项	降级注意事项
升级 VM-50 和 VM-50L	在将 VM-50 或 VM-50L 防火墙升级到 PAN-OS 11.1 之前，需要先安装最低插件版本，然后才能开始升级： • 从 **PAN-OS 10.2** 升级 — 所需的最低插件版本为 3.0.6 • 从 **PAN-OS 11.0** 升级 — 所需的最低插件版本为 4.0.3-h1。	无。
VM 系列防火墙	将 VM-Series 防火墙从 PAN-OS 版本 10.1.x 升级到 11.1.x 时，必须在执行升级之前将所有 10.1.x 防火墙上的 VM-Series 插件版本升级到 2.1.6 以上，以避免出现 HA 问题。	无。
收集器组	升级到 PAN-OS 11.1.1 时，运行 PAN-OS 10.0 或更早版本时生成的所有日志都将被删除。 要恢复在 PAN-OS 11.0 或更早版本中生成的日志，必须升级到 PAN-OS 11.1.2 或更高版本，在该版本中您可以使用 Palo Alto Networks 提供的 CLI 命令手动恢复所有受影响的日志。	不建议执行降级。如果选择从 11.1 降级，则在 PAN-OS 11.1 中生成的所有日志都将被删除，需要通过手动方式恢复。要恢复在 11.1 中生成的日志，您必须： 1. 升级到 PAN-OS 11.1.2 或更高的 11.1 版本。 这是成功恢复受影响的日志所必需执行的操作。 2. 登录到日志收集器 CLI 并删除所有 `esdata` 目录。 `admin>` **`debug elasticsearch erase data`** 3. 降级到您的目标 PAN-OS 版本。 4. 提交更改并将其推送到收集器组以及所有托管设备。

功能	升级注意事项	降级注意事项
		5. 登录到日志收集器 CLI 并恢复受影响的日志。 `admin> debug logdb migrate-lc start log-type all` 如果您已从 *PAN-OS 11.1* 降级，并且 *ElasticSearch* 陷入了重启循环，请联系 Palo Alto Networks 支持部门
	收集器组中的所有日志收集器必须同时升级。不支持在升级窗口期内升级收集器组中的部分（而非全部）日志收集器。	无。
	必须使用设备注册身份验证登录运行 PAN-OS 11.1 的日志收集器，以便进行日志收集器间的通信。 在升级到 PAN-OS 11.1 的过程中，运行 PAN-OS 9.1 或更早版本时添加到 Panorama 管理的日志收集器必须先升级到 PAN-OS 10.1 或更高版本，然后再 使用设备注册身份验证密钥将其重新加入 Panorama 管理。 如果检测到没有设备注册身份验证密钥的日志收集器加入 Panorama 管理，则会阻止升级到 PAN-OS 11.1。	无。
	如果您使用收集器组，则必须满足以下要求才能升级到 11.1.0。	无。

功能	升级注意事项	降级注意事项
	• 升级到 11.1 后，必须手动推送收集器组，才能升级托管的日志收集器。 *PAN-OS* 要求收集器组内的所有日志收集器都使用相同的版本。 • 您必须使用设备注册身份验证密钥向 Panorama 注册日志收集器。 如果设备注册身份验证密钥未正确初始化，则无法形成与对等节点的连接。	
	将日志收集器升级到 PAN-OS 11.1 后，现在需要以下 TCP 端口才能进行日志收集器间的通信，并且必须在网络上打开这些端口。 • TCP/9300 • TCP/9301 • TCP/9302	无。
Pan 服务代理	无。	如果启用了 Pan 服务代理，则将下一代防火墙从 PAN-OS 11.1 降级的操作将会失败。要成功降级，请在降级前禁用 Pan 服务代理。 下一代防火墙：选择 **Network**（网络） > **Proxy**（代理），单击代理启用的设置图标，选择 **None**（无），然后单击 **OK**（确定）。 Panorama：**Templates**（模板） > **Network**（网络）

功能	升级注意事项	降级注意事项
		> **Proxy**（代理），单击代理启用的设置图标，选择 **None**（无），然后单击 **OK**（确定）。
身份验证序列	当您升级到 PAN-OS 11.1.1 时，身份验证失败时退出序列选项将不再依赖于使用域确定身份验证配置文件选项。	如果选择身份验证失败时退出序列选项，则除非未选择身份验证失败时退出序列选项，或者除非同时选择身份验证失败时退出序列选项和使用域确定身份验证配置文件选择，否则从 PAN-OS 11.1.1 降级到之前版本的操作将会失败。
多 vsys 防火墙的 Panorama 管理 仅使用跳过软件版本升级从 PAN-OS 10.1 升级到 PAN-OS 11.1	在使用跳过软件版本升级将 Panorama 托管的多 vsys 防火墙升级到 PAN-OS 11.0 之前： • 删除或重命名任何本地配置的与 **Panorama Shared**（**Panorama** 共享）配置中的对象同名的防火墙 **Shared**（共享）对象。否则，来自 Panorama 的配置推送在升级后会失败，并显示错误 `<object-name>` 已在使用中。 • Palo Alto Networks 建议，如果多 vsys 防火墙由 Panorama 管理，则所有 vsys 配置都应由 Panorama 管理。 这样有助于避免托管的多 vsys 防火墙上的提交失败，并允许您利用 Panorama 经过优化的共享对象推送。	无。
	使用跳过软件版本升级成功将托管的多 vsys 防火墙升级到 PAN-OS 10.2 后，Panorama 上的防火墙将不同步，需要进行完整提交和推送。	

功能	升级注意事项	降级注意事项
	在 Panorama 上，选择提交并推送到设备，将整个 Panorama 管理配置提交并推送到多 vsys 防火墙，然后再提交并推送来自 Panorama 的任何配置更改。	
(PAN-OS 11.2) TLSv1.3 支持 HSM 与 SSL 入站检测的集成	无。	从 PAN-OS 11.2 降级到更早版本后，将不再支持在 HSM 上存储内部服务器的私钥时建立和解密 TLSv1.3 会话。即使客户端和服务器都支持 TLSv1.3，设备也会建立 TLSv1.2 连接。

将防火墙升级到 PAN-OS 11.1

您升级到 PAN-OS 11.1 的方式取决于您是拥有独立防火墙还是高可用性 (HA) 配置中的防火墙，以及对于这两种情况，您是否使用 Panorama 来管理防火墙。查看 PAN-OS 11.1 发行说明，然后按照特定于您的部署的过程进行操作：

- 确定升级到 PAN-OS 11.1 的路径
- 从 Panorama 中将防火墙升级到 PAN-OS 11.1
- 升级独立防火墙
- 升级 HA 防火墙对

升级您使用 *Panorama* 管理的防火墙或配置为将内容转发到 *WildFire* 设备的防火墙时，您必须先升级 Panorama 及其日志收集器，然后升级 WildFire 设备，再升级防火墙。

此外，不建议管理运行比 *Panorama* 更高的维护版本的防火墙，因为这可能导致功能无法正常使用。例如，若 *Panorama* 运行的是 *PAN-OS 10.1.0*，则不建议管理运行 *PAN-OS 10.1.1* 或更高维护版本的防火墙。

确定升级到 PAN-OS 11.1 的路径

从一个 PAN-OS 功能发行版本升级到更高的功能发行版本时，不能跳过到达目标版本的路径中任何功能发行版本的安装。此外，建议的升级路径包括在安装下一个功能发行版本的基本映像之前，在每个发行版本中安装最新的维护发行版本。为了最大限度地减少用户停机时间，请在非工作时间执行升级。

对于手动升级，*Palo Alto Networks* 建议在升级路径上为每个 *PAN OS* 版本安装和升级最新的维护版本。不要为功能版本安装 *PAN OS* 基础映像，除非它是您要升级到的目标版本。

按如下方式确定升级路径：

STEP 1 | 确定当前安装的版本。

- 从 Panorama 中，选择 **Panorama** > **Managed Devices**（受管设备），然后在计划升级的防火墙上检查软件版本。
- 从防火墙中，选择 **Device**（设备） > **Software**（软件），然后检查哪个版本在 Currently Installed（当前已安装）列中有复选标记。

STEP 2 | （PAN-OS 11.1.3 及更高版本）查看首选版本。

- 在 Panorama 中，单击 **Panorama** > **Software**（软件），然后禁用（清除）**Base Releases**（基础版本）复选框。
- 在防火墙中，单击 **Device**（设备） > **Software**（软件），然后禁用（清除）**Base Releases**（基础版本）复选框。

STEP 3 | 确定升级路径：

对于您在升级路径中会经过的每个版本，查看发行说明和升级/降级注意事项中的已知问题以及默认行为更改。

已安装的 PAN-OS 版本	升级到 PAN-OS 11.1 的推荐路径
11.0.x	• 如果您已经在运行 PAN-OS 11.0 版本，则可以直接升级到 PAN-OS 11.1
10.2.x	• 如果您已经在运行 PAN-OS 10.2 版本，则可以直接升级到 PAN-OS 11.1
10.1.x	从 PAN-OS 10.1 或更高版本升级设备时，您现在可以使用 Skip Software Version Upgrade（跳过软件版本升级）功能跳过软件版本。 • 如果您已经在运行 PAN-OS 10.1 版本，则可以直接升级到 PAN-OS 11.1。
10.0.x	• 下载并安装最新的首选 PAN-OS 10.0 维护版本，然后重新启动。 • 下载 PAN-OS 10.1.0 • 下载并安装最新的首选 PAN-OS 10.1 维护版本，然后重新启动。 从 PAN-OS 10.1 或更高版本升级设备时，您现在可以使用 Skip Software Version Upgrade（跳过软件版本升级）功能跳过软件版本。 • 继续将防火墙升级到 PAN-OS 11.1。
9.1.x	• 下载并安装最新的首选 PAN-OS 9.1 维护版本，然后重新启动。 • 下载 PAN-OS 10.0.0。 • 下载并安装最新的首选 PAN-OS 10.0 维护版本，然后重新启动。 • 下载 PAN-OS 10.1.0 • 下载并安装最新的首选 PAN-OS 10.1 维护版本，然后重新启动。 从 PAN-OS 10.1 或更高版本升级设备时，您现在可以使用 Skip Software Version Upgrade（跳过软件版本升级）功能跳过软件版本。 • 继续将防火墙升级到 PAN-OS 11.1。

已安装的 PAN-OS 版本	升级到 PAN-OS 11.1 的推荐路径
9.0.x	• 下载并安装最新的首选 PAN-OS 9.0 维护版本，然后重新启动。 在将任何日志收集器升级到最新的 *PAN-OS 9.0* 维护版本之前，请查看升级/降级注意事项。 • 下载 PAN-OS 9.1.0。 • 下载并安装最新的首选 PAN-OS 9.1 维护版本，然后重新启动。 • 下载 PAN-OS 10.0.0。 • 下载并安装最新的首选 PAN-OS 10.0 维护版本，然后重新启动。 • 下载 PAN-OS 10.1.0 • 下载并安装最新的首选 PAN-OS 10.1 维护版本，然后重新启动。 从 PAN-OS 10.1 或更高版本升级设备时，您现在可以使用 Skip Software Version Upgrade（跳过软件版本升级） 功能跳过软件版本。 • 继续将防火墙升级到 PAN-OS 11.1。
8.1.x	• 下载并安装最新的首选 PAN-OS 8.1 维护版本，然后重新启动。 • 下载 PAN-OS 9.0.0 • 下载并安装最新的首选 PAN-OS 9.0 维护版本，然后重新启动。 在将任何日志收集器升级到最新的 *PAN-OS 9.0* 维护版本之前，请查看升级/降级注意事项。 • 下载 PAN-OS 9.1.0。 • 下载并安装最新的首选 PAN-OS 9.1 维护版本，然后重新启动。 • 下载 PAN-OS 10.0.0。 • 下载并安装最新的首选 PAN-OS 10.0 维护版本，然后重新启动。 • 下载 PAN-OS 10.1.0

已安装的 PAN-OS 版本	升级到 PAN-OS 11.1 的推荐路径
	• 下载并安装最新的首选 PAN-OS 10.1 维护版本，然后重新启动。 从 PAN-OS 10.1 或更高版本升级设备时，您现在可以使用 Skip Software Version Upgrade（跳过软件版本升级） 功能跳过软件版本。 • 继续将防火墙升级到 PAN-OS 11.1。

升级独立防火墙

查看 PAN-OS 11.1 发行说明，然后使用以下步骤将不在 HA 配置中的防火墙升级到 PAN-OS 11.1。

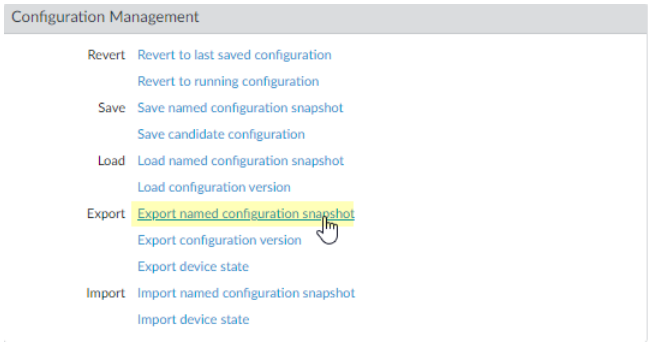
如果您的防火墙配置为将样本转发到 *WildFire* 设备以进行分析，则您必须先升级 WildFire 设备，然后再升级转发防火墙。

为避免影响流量，计划在中断时间段内进行升级。确保防火墙已连接至可靠的电源。升级时断电可能导致防火墙无法使用。

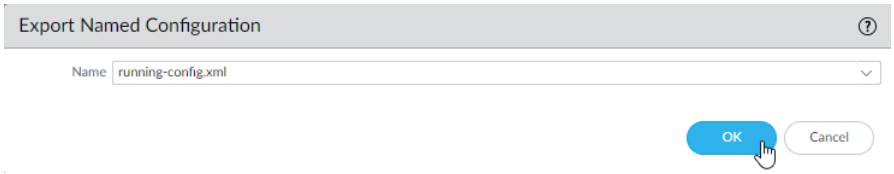
STEP 1 | 保存当前配置文件的备份。

尽管防火墙自动创建配置备份，但最佳做法是在升级之前创建备份并通过外部方式将其保存。

1. 选择 **Device**（设备） > **Setup**（设置） > **Operations**（操作），然后单击 **Export named configuration snapshot**（导出已命名的配置快照）。



2. 选择包含正在运行的配置（如 **running-config.xml**）的 XML 文件，并单击 **OK**（确定）导出配置文件。



3. 将导出的文件保存到防火墙外部的位置。如果升级出现问题，您可以使用此备份还原配置。

STEP 2 | （可选）如果您已启用 User-ID，则在升级后防火墙将清除当前 IP 地址到用户名和组映射，以便可以使用 User-ID 源中的属性重新填充这些映射。要估计环境重新填充映射所需的时间，请在防火墙上运行以下 CLI 命令。

- 对于 IP 地址到用户名映射：
  - **`show user user-id-agent state all`**
  - **`show user server-monitor state all`**
- 对于组映射：**`show user group-mapping statistics`**

STEP 3 | 确保防火墙运行最新的内容发行版本。

请参阅发行说明以了解您必须为 PAN-OS 11.1 版本安装的最低内容发行版本。请务必遵循应用程序和威胁内容更新的最佳实践。

1. 选择 **Device**（设备） > **Dynamic Updates**（动态更新），然后查看当前安装的 **Applications**（应用程序）或 **Applications and Threats**（应用程序和威胁）内容发行版本。

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

2. 如果防火墙未运行 PAN-OS 11.1 所需的最低内容发行版本或更高版本，请 **Check Now**（立即检查）以获取可用更新的列表。
3. 找到并 **Download**（下载）所需的内容发行版本。

   成功下载内容更新文件后，该内容发行版本的 Action（操作）列中的链接从 **Download**（下载）更改为 **Install**（安装）。
4. **Install**（安装）更新。

STEP 4 | 确定升级到 PAN-OS 11.1 的路径

对于您在升级路径中会经过的每个版本，查看发行说明和升级/降级注意事项中的PAN-OS 升级清单、已知问题以及默认行为更改。

STEP 5 | （最佳实践）如果您使用 Cortex 数据湖 (CDL)，请安装设备证书。

在升级到 PAN-OS 11.1 时，防火墙会自动切换到使用设备证书向 CDL 摄取和查询端点进行身份验证。

如果您未在升级到 *PAN-OS 11.1* 之前安装设备证书，防火墙将继续使用现有的日志服务证书进行身份验证。

STEP 6 | 升级到 PAN-OS 11.1。

如果防火墙无法从管理接口访问互联网，则您可以从 Palo Alto Networks 客户支持门户下载软件映像，然后手动将其 ***Upload***（上传）到防火墙。

1. 选择 **Device**（设备） > **Software**（软件），然后单击 **Check Now**（立即检查）以显示最新的 PAN-OS 更新。

   仅显示下一个可用 PAN-OS 发行版本的版本。例如，如果防火墙上安装了 PAN-OS 11.1，则仅显示 PAN-OS 11.1 版本。

   （PAN-OS 11.1.3 及更高版本）默认情况下，显示首选版本和相应的基础版本。要仅查看首选版本，请禁用（清除）**Base Releases**（基础版本）复选框。
2. 选择 **Panorama** > **Device Deployment**（设备部署） > **Software**（软件） > **Action**（操作） > **Validate**（验证）

   Panorama > **Device Deployment**（设备部署） > **Software**（软件） > **Action**（操作） > **Validate**（验证）以查看升级到 11.1.0 所需的所有中间软件和内容映像。
3. 下载中间软件和内容映像。
4. 在下载映像后（或者，对于手动升级，在上传映像后），请 **Install**（安装）映像。
5. 安装成功完成后，请使用以下方法之一重新启动：
   - 如果提示重新启动，请单击 **Yes**（是）。
   - 如果未提示重启，请选择 **Device**（设备） > **Setup**（设置） > **Operations**（操作），然后单击 **Reboot Device**（重启设备）。

   此时，防火墙将清除 *User-ID* 映射，然后连接到 *User-ID* 源以重新填充映射。
6. 如果您已启用 User-ID，请使用以下 CLI 命令在允许流量之前验证防火墙是否已重新填充 IP 地址到用户名和组映射。
   - **`show user ip-user-mapping all`**
   - **`show user group list`**

STEP 7 | 重新生成或重新导入所有证书以遵守 OpenSSL 安全级别 2。

在升级到 PAN-OS 11.1 时，要求所有证书满足以下最低要求：

- RSA 2048 位或以上，或 ECDSA 256 位或以上
- SHA256 或更高版本的摘要

请参阅 PAN-OS 管理员指南，了解有关重新生成或重新导入证书的更多信息。

STEP 8 | 验证防火墙是否正在传递流量。

选择 **Monitor**（监控） > **Session Browser**（会话浏览器），然后验证是否显示新的会话。

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

STEP 9 | 查看防火墙上的软件升级历史。

1. 登录到防火墙界面。
2. 转到 **Device**（设备） > **Summary**（摘要） > **Software**（软件），然后单击 **Device History**（设备历史记录）。

升级 HA 防火墙对

查看 PAN-OS 11.1 发行说明，然后使用以下步骤升级高可用性 (HA) 配置中的一对防火墙。此程序适用于主动/被动和主动/主动配置。

当您在高可用性 (HA) 配置中更新防火墙时，为了避免出现停机，一次只应更新一台高可用性对等：对于主动/主动防火墙，首先升级哪个对端设备并不重要（为简单起见，此程序介绍了首先如何升级主动-主要对端设备）。对于主动/被动防火墙，必须先暂停（故障转移）并升级主动（主要）对端设备。升级主要对端设备后，必须取消主要对端设备的暂停才能将其恢复到功能状态（被动）。接下来，必须暂停被动（辅助）对端设备以使主要对端设备再次处于主动状态。在主要对端设备处于主动状态且辅助对端设备暂停后，您可以继续升级。为了防止在升级 HA 对等期间发生故障转移，您必须确保在继续升级之前禁用抢占行为。您只需要禁用对中一个对等的抢占行为。

在多个功能 PAN-OS 版本上升级 HA 防火墙时，必须将升级路径上的每个 HA 对等设备升级到相同的功能 PAN-OS 版本，然后才能继续。例如，您正在将 HA 对等设备从 PAN-OS 10.2 升级到 PAN-OS 11.1。必须先将两个 HA 对等设备都升级到 PAN-OS 11.0，然后才能继续升级到目标 PAN-OS 11.1 版本。当 HA 对等设备相隔两个或更多功能版本时，安装了较旧版本的防火墙会进入暂停状态，并显示消息对端设备版本太旧。

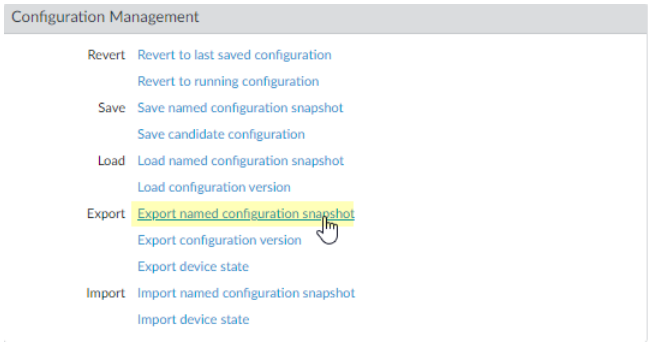
为避免影响流量，计划在中断时间段内进行升级。确保防火墙已连接至可靠的电源。升级时断电可能导致防火墙无法使用。

STEP 1 | 保存当前配置文件的备份。

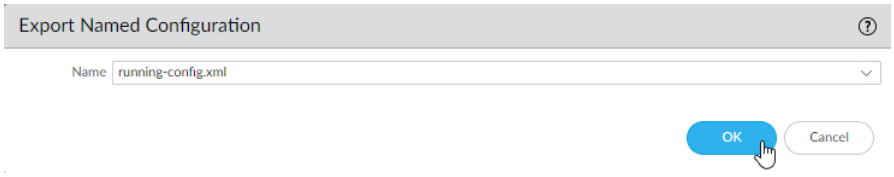
尽管防火墙自动创建配置备份，但最佳做法是在升级之前创建备份并通过外部方式将其保存。

对该对中的每个防火墙执行以下步骤：

1. 选择 **Device**（设备） > **Setup**（设置） > **Operations**（操作），然后单击 **Export named configuration snapshot**（导出已命名的配置快照）。



2. 选择包含正在运行的配置（如 **running-config.xml**）的 XML 文件，并单击 **OK**（确定）导出配置文件。



3. 将导出的文件保存到防火墙外部的位置。如果升级出现问题，您可以使用此备份还原配置。

STEP 2 | 选择 **Device**（设备） > **Support**（支持）并 **Generate Tech Support File**（生成技术支持文件）。

当提示生成技术支持文件时，单击 **Yes**（是）。

STEP 3 | 确保 HA 对中的每个防火墙都运行最新的内容发行版本。

请参阅发行说明以了解您必须为 PAN-OS 11.1 版本安装的最低内容发行版本。请务必遵循应用程序和威胁内容更新的最佳实践。

1. 选择 **Device**（设备） > **Dynamic Updates**（动态更新），然后选择 **Applications**（应用程序）或 **Applications and Threats**（应用程序和威胁）以确定当前安装的更新。

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

2. 如果防火墙未运行 PAN-OS 11.1 所需的最低内容发行版本或更高版本，请 **Check Now**（立即检查）以获取可用更新的列表。
3. 找到并 **Download**（下载）所需的内容发行版本。

   成功下载内容更新文件后，该内容发行版本的 Action（操作）列中的链接从 **Download**（下载）更改为 **Install**（安装）。
4. **Install**（安装）更新。您必须在两个对等上安装更新。

STEP 4 | 确定升级到 PAN-OS 11.1 的路径

在从当前运行的 PAN-OS 版本升级到 PAN-OS 11.1 的路径中，您无法跳过任何功能发行版本的安装。

对于您在升级路径中会经过的每个版本，查看发行说明和升级/降级注意事项中的PAN-OS 升级清单、已知问题以及默认行为更改。

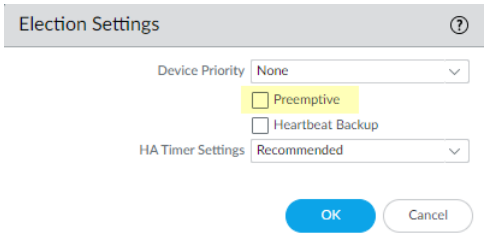
STEP 5 | （最佳实践）如果您使用 Cortex 数据湖 (CDL)，请在每个 HA 对等设备上安装设备证书。

在升级到 PAN-OS 11.1 时，防火墙会自动切换到使用设备证书向 CDL 摄取和查询端点进行身份验证。

如果您未在升级到 *PAN-OS 11.1* 之前安装设备证书，防火墙将继续使用现有的日志服务证书进行身份验证。

STEP 6 | 在每个对中的第一个对等上禁用抢占行为。您只需要在 HA 对中的一个防火墙上禁用此设置，但在继续升级之前确保提交成功。

1. 选择 **Device**（设备） > **High Availability**（高可用性），然后编辑 **Election Settings**（选择设置）。
2. 如果已启用，则禁用（取消选择）**Preemptive**（抢先）设置，然后单击 **OK**（确定）。



3. **Commit**（提交）更改。

STEP 7 | 挂起主要 HA 对等设备以执行故障转移。

（主动/被动防火墙）对于主动/被动 HA 配置中的防火墙，请先暂停和升级主动 HA 对等设备。

（主动/主动防火墙）对于主动/主动 HA 配置中的防火墙，请先暂停和升级主动-主要 HA 对等设备。

1. 选择 **Device**（设备） > **High Availability**（高可用性） > **Operational Commands**（操作指令），并 挂起本地设备以实现高可用性。
2. 在右下角，验证状态是否已暂停。

   由此产生的故障转移应导致辅助 HA 对等设备过渡到主动状态。

   在升级之前，生成的故障转移会验证 *HA* 故障转移是否正常运行。

STEP 8 | 在暂停的 HA 对等设备上安装 PAN-OS 11.1。

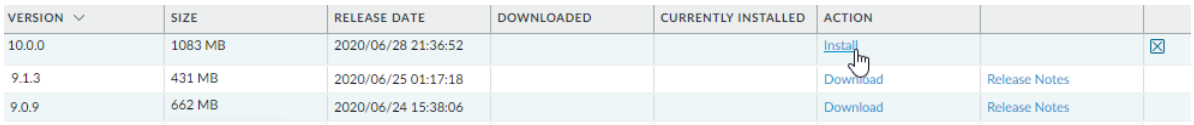
1. 在主要 HA 对等设备上，选择 **Device**（设备） > **Software**（软件），然后单击 **Check Now**（立即检查）以获取最新更新。

   仅显示下一个可用 PAN-OS 发行版本的版本。例如，如果防火墙上安装了 PAN-OS 11.1，则仅显示 PAN-OS 11.1 版本。

   （PAN-OS 11.1.3 及更高版本）默认情况下，显示首选版本和相应的基础版本。要仅查看首选版本，请禁用（清除）**Base Releases**（基础版本）复选框。
2. 找到并 **Download**（下载）PAN-OS 11.1.0。

   如果防火墙无法从管理接口访问 *Internet*，则您可以从 Palo Alto Networks 支持门户下载软件映像，然后手动将其 ***Upload***（上传）到防火墙。

   如果您的防火墙确实可以访问互联网，并且遇到文件下载错误，请再次单击 ***Check Now***（立即检查）以刷新 *PAN-OS* 映像列表。
3. 在下载映像后（或者，对于手动升级，在上传映像后），请 **Install**（安装）映像。



4. 安装成功完成后，请使用以下方法之一重新启动：
   - 如果提示重新启动，请单击 **Yes**（是）。
   - 如果未提示重启，请选择 **Device**（设备） > **Setup**（设置） > **Operations**（操作）和 **Reboot Device**（重启设备）。
5. 设备完成重启后，查看 **Dashboard**（仪表板）上的高可用性小部件，并验证您刚刚升级的设备是否与对端设备同步。

STEP 9 | 将 HA 功能恢复到主要 HA 对等设备。

1. 选择 **Device**（设备） > **High Availability**（高可用性） > **Operational Commands**（操作指令），并 使本地设备正常运行以实现高可用性。
2. 在右下角，验证状态是否为 被动。对于处于主动/主动配置的防火墙，请验证其状态是否为 主动。
3. 等待 HA 对等设备运行配置同步。

   在 **Dashboard**（仪表板）中，监控 高可用性小部件中的运行配置状态。

STEP 10 | 在辅助 HA 对等设备上，暂停 HA 对对端设备。

1. 选择 **Device**（设备） > **High Availability**（高可用性） > **Operational Commands**（操作指令），并 挂起本地设备以实现高可用性。
2. 在右下角，验证状态是否已暂停。

   由此产生的故障转移应导致主要 HA 对等设备转换为 主动 状态。

STEP 11 | 在辅助 HA 对等设备上安装 PAN-OS 11.1。

1. 在第二个对端设备上，选择 **Device**（设备） > **Software**（软件），然后单击 **Check Now**（立即检查）以获取最新更新。
2. 找到并 **Download**（下载）PAN-OS 11.1.0。
3. 下载映像后，请 **Install**（安装）。
4. 安装成功完成后，请使用以下方法之一重新启动：
   - 如果提示重新启动，请单击 **Yes**（是）。
   - 如果未提示重启，请选择 **Device**（设备） > **Setup**（设置） > **Operations**（操作）和 **Reboot Device**（重启设备）。

STEP 12 | 将 HA 功能恢复到辅助 HA 对等设备。

1. 选择 **Device**（设备） > **High Availability**（高可用性） > **Operational Commands**（操作指令），并 使本地设备正常运行以实现高可用性。
2. 在右下角，验证状态是否为 被动。对于处于主动/主动配置的防火墙，请验证其状态是否为 主动。
3. 等待 HA 对等设备运行配置同步。

   在 **Dasbhoard**（仪表板）中，监视运行配置状态高可用性小部件。

STEP 13 | 在上一步中禁用的 HA 对等设备上重新启用抢占。

1. 选择 **Device**（设备） > **High Availability**（高可用性），然后编辑 **Election Settings**（选择设置）。
2. 启用（选中） **Preemptive**（抢占）设置，然后单击 **OK**（确定）。
3. **Commit**（提交）更改。

STEP 14 | 重新生成或重新导入所有证书以遵守 OpenSSL 安全级别 2。

在升级到 PAN-OS 11.1 时，要求所有证书满足以下最低要求：

- RSA 2048 位或以上，或 ECDSA 256 位或以上
- SHA256 或更高版本摘要

请参阅 PAN-OS 管理员指南或 Panorama 管理员指南，了解有关重新生成或重新导入证书的更多信息。

STEP 15 | 验证两个对等是否按预期传递流量。

在主动/被动配置中，仅主动对等应传递流量；两个对等应在主动/主动配置中传递流量。

运行以下 CLI 命令以确认升级成功：

- （仅限主动对等）要验证主动对等是否正在传递流量，请运行 **show session all** 命令。
- 要验证会话同步，请运行 **show high-availability interface ha2** 命令，并确保 CPU 表中的硬件接口计数器按如下方式增加：
  - 在主动/被动配置中，只有主动对等显示传输的数据包；被动对等将仅显示接收的数据包。

    如果启用了 *HA2 keep-alive*，则被动对等上的硬件接口计数器将同时显示传输和接收的数据包。发生这种情况是因为 *HA2 keep-alive* 是双向的，这意味着两个对等都会发送 *HA2 keep-alive* 数据包。
  - 在主动/主动配置中，您会看到这两个对等上收到的数据包和传输的数据包。

从 Panorama 中将防火墙升级到 PAN-OS 11.1

从 Panorama™ 管理服务器中为受管防火墙部署内容更新和升级 PAN-OS。

- 当 Panorama 连接上互联网时升级防火墙
- 当 Panorama 未连接互联网时升级防火墙
- 升级 ZTP 防火墙

当 Panorama 连接上互联网时升级防火墙

查看 PAN-OS 11.1 发行说明，然后遵循以下程序升级使用 Panorama 管理的防火墙。此程序适用于独立防火墙和部署在高可用性 (HA) 配置中的防火墙。

在多个功能 PAN-OS 版本上升级 HA 防火墙时，必须将升级路径上的每个 HA 对等设备升级到相同的功能 PAN-OS 版本，然后才能继续。例如，您正在将 HA 对等设备从 PAN-OS 10.2 升级到 PAN-OS 11.1。必须先将两个 HA 对等设备都升级到 PAN-OS 11.0，然后才能继续升级到目标 PAN-OS 11.1 版本。当 HA 对等设备相隔两个或更多功能版本时，安装了较旧版本的防火墙会进入暂停状态，并显示消息对端设备版本太旧。

如果 *Panorama* 无法直接连接到更新服务器，则遵循 当 Panorama 未连接互联网时升级防火墙 程序以手动将映像下载到 *Panorama*，并将其分发给防火墙。

当从 PAN-OS 11.1 上的 Panorama 设备升级到 PAN-OS 10.1 或更高版本上的防火墙时，新的跳过软件版本升级功能使您能够跳过最多三个版本。

更新 Panorama 的防火墙前，必须：

- 确保 Panorama 运行的 PAN-OS 版本与更新到的版本相同或，高于更新到的版本。在将托管防火墙升级到 11.1 版本之前，您必须将 Panorama 及其日志收集器升级到该版本。此外，在将日志收集器升级到 11.1 时，由于日志记录基础架构中的变化，您必须同时升级所有日志收集器。
- 确保防火墙已连接至可靠的电源。升级时断电可能导致防火墙无法使用。
- 如果 Panorama 虚拟设备在升级到 PAN-OS 11.1 时处于旧版模式，则决定是否保持处于旧版模式。运行 PAN OS 9.1 或更高版本的新 Panorama 虚拟设备部署不支持旧版模式。如果您将 Panorama 虚拟设备从 PAN-OS 9.0 或更早版本升级到 PAN-OS 11.1，Palo Alto Networks 建议查看 Panorama 虚拟设备的安装先决条件，并根据您的需要更改为 Panorama 模式或仅管理模式。

  如果要让 Panorama 虚拟设备保持处于旧版模式，请将分配给 Panorama 虚拟设备的 CPU 和内存增加到至少 16 个 CPU 和 32GB 内存，以成功升级到 PAN-OS 11.1。有关详细信息，请参阅 Panorama 虚拟设备的安装先决条件。
- （建议用于多 vsys 受管防火墙）将多 vsys 受管防火墙的所有 vsys 过渡到 Panorama。

  之所以这样建议是为了避免在多 vsys 受管防火墙上出现提交问题，并且使您能够利用 Panorama 经过优化的共享对象推送。

  适用于仅使用跳过软件版本升级从 PAN-OS 10.1 升级到 PAN-OS 11.1 的多 vsys 防火墙。

- （多 vsys 受管防火墙）删除或重命名与 Panorama **Shared**（共享）配置中的对象具有相同名称的任何本地配置 的**Shared**（共享）对象。否则，来自 Panorama 的配置推送在升级后会失败，并显示错误 `<object-name>` 已在使用中。

  适用于仅使用跳过软件版本升级从 PAN-OS 10.1 升级到 PAN-OS 11.1 的多 vsys 防火墙。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 已修改您的安全策略规则以允许 SSL 应用程序流量。

适用于仅使用跳过软件版本升级从 *PAN-OS 10.1* 升级到 *PAN-OS 11.1* 的防火墙。

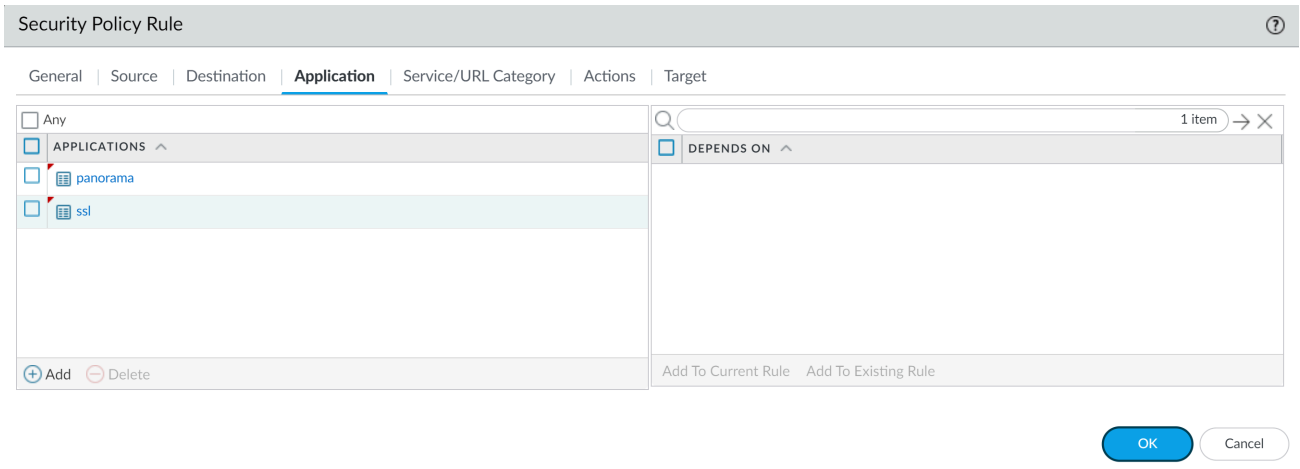
升级到 *PAN-OS 11.1* 之后，如果使用 *Panorama App-ID* 控制 *Panorama* 与托管设备之间的流量，则必须采取此操作才能防止托管设备与 *Panorama* 断开连接。如果在升级之前不允许使用 *SSL* 应用程序，则托管设备将断开与 *Panorama* 的连接。

PAN-OS 11.1 使用 TLS 1.3 版本来加密服务证书以及 Panorama 和受管防火墙之间的握手消息。因此，从受管防火墙到 Panorama 的流量的 App-ID 将从 `Panorama` 重新分类为 SSL。要继续在 Panorama 和托管设备之间进行通信，您必须修改控制 Panorama 和托管设备之间的流量的安全策略规则，以便同样允许使用 SSL 应用程序。

如果控制 Panorama 和托管设备之间的流量的安全策略规则允许使用 **Any**（任何）应用程序，或者您已经修改了控制 Panorama 和托管设备之间的流量的安全策略规则，请跳过此步骤。

1. 选择 **Policys**（策略） > **Security**（安全） > **Pre Rules**（前导规则）。
2. 选择包含控制 Panorama 和受管防火墙之间流量的安全策略规则的 **Device Group**（设备组）。
3. 选择安全策略规则。
4. 选择 **Application**（应用程序）并 **Add**（添加）SSL。

   请勿删除 *`Panorama`* 应用程序。这会导致在您推送更改后所有受管防火墙与 *Panorama* 断开连接。

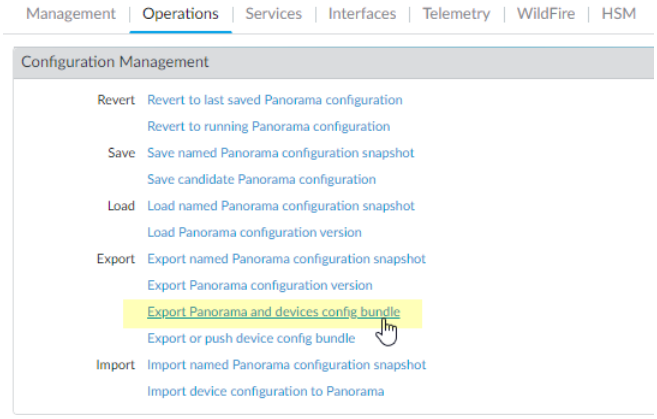


5. 单击 **OK**（确定）。
6. 选择 **Commit**（提交） > **Commit and Push**（提交并推送），然后 **Commit and Push**（提交并推送）您的配置更改。

STEP 3 | 将当前配置文件的备份保存在计划要升级的每个托管防火墙上。

尽管防火墙自动创建配置备份，但最佳做法是在升级之前创建备份并通过外部方式将其保存。

1. 选择 **Panorama > Setup**（设置） **> Operations**（操作）并单击**Export Panorama and devices config bundle**（导出 **Panorama** 和设备配置包）以生成和导出 Panorama 和每个受管设备的最新配置备份。

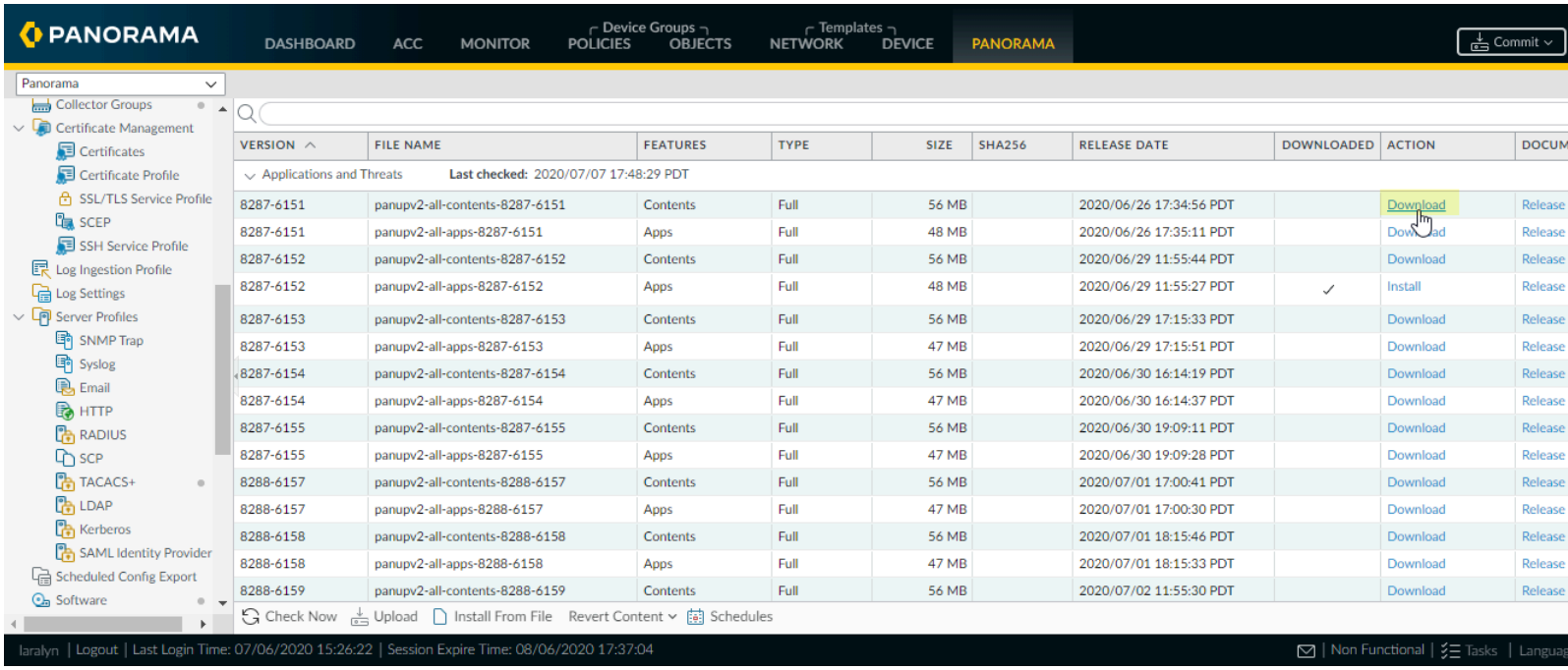


2. 将导出的文件保存到防火墙外部的位置。如果升级出现问题，您可以使用此备份还原配置。

STEP 4 | 安装最新的内容更新。

要了解 PAN-OS 11.1 所需的最低内容发行版本，请参阅发行说明。确保在将内容更新部署到 Panorama 和受管防火墙时遵循 应用程序和威胁内容更新的最佳实践。

1. 选择 **Panorama > Device Deployment**（设备部署） **> Dynamic Updates**（动态更新），然后 **Check Now**（立即检查）最近更新。如果有更新可用，“操作”列会显示 **Download**（下载）链接。



2. 单击 **Install**（安装）并选择要在其中安装更新的防火墙。如果更新 HA 防火墙，则必须更新两个对等的内容。
3. 单击 **OK**（确定）

STEP 5 | 确定升级到 PAN-OS 11.1 的路径.

对于您在升级路径中会经过的每个版本，了解发行说明中的 PAN-OS 升级清单、已知问题和默认行为更改，以及升级/降级注意事项。

如果升级多个防火墙，请在开始下载映像之前通过确定所有防火墙的升级路径来简化该过程。

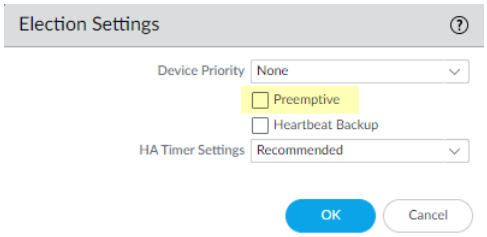
STEP 6 | （最佳实践）如果您使用 Cortex 数据湖 (CDL)，请安装设备证书。

在升级到 PAN-OS 11.1 时，防火墙会自动切换到使用设备证书向 CDL 摄取和查询端点进行身份验证。

如果您未在升级到 *PAN-OS 11.1* 之前安装设备证书，防火墙将继续使用现有的日志服务证书进行身份验证。

STEP 7 | （仅限 HA 防火墙更新）如果将要更新作为 HA 对组成部分的防火墙，请禁用抢先。您仅需要禁用每个 HA 对上每个防火墙的此设置。

1. 选择 **Device**（设备） > **High Availability**（高可用性），然后编辑 **Election Settings**（选择设置）。
2. 如果已启用，则禁用（取消选择）**Preemptive**（抢先）设置，然后单击 **OK**（确定）。



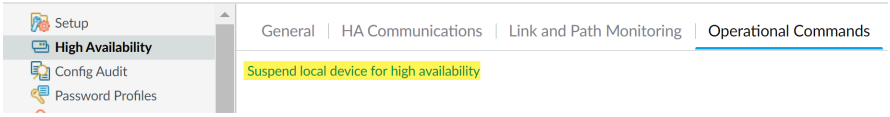
3. **Commit**（提交）更改。必须确保已成功提交，然后才能进行更新。

STEP 8 | （仅限 HA 防火墙升级）挂起主要 HA 对等设备以强制进行故障转移。

（主动/被动防火墙）对于主动/被动 HA 配置中的防火墙，请先暂停和升级主动 HA 对等设备。

（主动/主动防火墙）对于主动/主动 HA 配置中的防火墙，请先暂停和升级主动-主要 HA 对等设备。

1. 登录到主动主要防火墙 HA 对等设备的防火墙 Web 界面 。
2. 选择 **Device**（设备） > **High Availability**（高可用性） > **Operational Commands**（操作指令），并 挂起本地设备以实现高可用性。



3. 在右下角，验证状态是否已暂停。

   由此产生的故障转移应导致辅助被动 HA 对等设备转换为 主动 状态。

   生成的故障转移会在您升级之前验证 *HA* 故障转移是否正常运行。

STEP 9 | （可选） 将您的托管防火墙升级到 PAN-OS 10.1。

跳过软件版本升级功能支持运行 PAN-OS 10.1 或更高版本的托管防火墙。如果您的托管防火墙位于 PAN-OS 10.0 或更早版本上，请先升级到 PAN-OS 10.1 或更高版本。

STEP 10 | （可选）将文件 **Export**（导出） 到已配置的 SCP 服务器。

在 PAN-OS 11.1 中，在将升级部署到受管防火墙时，SCP 服务器可用作下载源。在下一步下载软件和内容映像之前导出文件。

STEP 11 | 验证并下载目标版本所需的软件和内容版本。

在此步骤中，您可以查看和下载升级到 PAN-OS 11.1 所需的中间软件和内容映像。

使用多映像下载来下载软件和内容映像是可选的。您仍然可以一次下载一个映像。

1. 单击 **Panorama** > **Device Deployment**（设备部署） > **Software**（软件） > **Action**（操作） > **Validate**（验证）
2. 查看您需要下载的中间软件和内容版本。
3. 选择要升级的防火墙，然后单击 **Deploy**（部署）。
4. 选择下载源并单击 **Download**（下载）。

STEP 12 | 在防火墙上安装 PAN-OS 11.1.0。

（仅限 *SD-WAN*）为了保持 *SD-WAN* 链接的准确状态，必须在升级分支防火墙之前将中心防火墙升级到 *PAN-OS 11.1*。先升级分支防火墙再升级中心防火墙可能导致错误的监视数据（***Panorama*** > ***SD-WAN*** > ***Monitoring***（监视）），且 *SD-WAN* 链接会错误地显示为 *down*。

1. 单击与想要更新的防火墙型号匹配的操作列中的 **Install**（安装）。例如，如果想升级 PA-440 防火墙，请单击与 PanOS_440-11.1.0 相对应的行中的 **Install**（安装）。
2. 在部署软件文件对话框，选择想要升级的所有防火墙。

   （仅限 HA 防火墙升级）要减少停机时间，请在每个 HA 对中只选择一个对端设备。对于主动/被动对，选择主动对等；对于主动/主动对，选择主动-辅助对等。
3. （仅限 HA 防火墙更新）请勿选择**Group HA Peers**（组高可用性对端设备）。
4. 选择**Reboot device after install**（在安装之后重新启动设备）。
5. 要开始更新，请单击 **OK**（确定）。
6. 安装成功完成后，请使用以下方法之一重新启动：
   - 如果提示重新启动，请单击 **Yes**（是）。
   - 如果未提示重启，请选择 **Device**（设备） > **Setup**（设置） > **Operations**（操作），然后单击 **Reboot Device**（重启设备）。
7. 防火墙完成重启后，请选择 **Panorama** > **Managed Devices**（托管设备），然后验证用于已升级的防火墙的软件版本是否为 11.1.0。此外，还检验已更新的任何被动防火墙的 HA 状态是否仍为被动。

STEP 13 | （仅限 HA 防火墙升级）将 HA 功能恢复到主要 HA 对等设备。

1. 登录到挂起的主防火墙 HA 对等设备的防火墙 Web 界面。
2. 选择 **Device**（设备） > **High Availability**（高可用性） > **Operational Commands**（操作指令），并 使本地设备正常运行以实现高可用性。
3. 在右下角，验证状态是否为 被动。对于处于主动/主动配置的防火墙，请验证其状态是否为 主动。
4. 等待 HA 对等设备运行配置同步。

   在 **Dashboard**（仪表板）中，监控 高可用性小部件中的运行配置状态。

STEP 14 | （仅限 HA 防火墙升级）暂停辅助 HA 对等设备以强制故障转移回主要 HA 对等设备。

1. 登录到主要辅助防火墙 HA 对等设备的防火墙 Web 界面 。
2. 选择 **Device**（设备） > **High Availability**（高可用性） > **Operational Commands**（操作指令），并 挂起本地设备以实现高可用性。
3. 在右下角，验证状态是否已暂停。

   由此产生的故障转移应导致主动被动 HA 对等设备转换为 主动 状态。

   生成的故障转移会在您升级之前验证 *HA* 故障转移是否正常运行。

STEP 15 | （仅限 HA 防火墙更新）更新每个 HA 对中的第二个 HA 对端设备。

1. 在 Panorama Web 界面中，选择 **Panorama** > **Device Deployment**（设备部署） > **Software**（软件）。
2. 单击与正在更新的 HA 对中防火墙型号匹配的操作列中的 **Install**（安装）。
3. 在部署软件文件对话框，选择想要升级的所有防火墙。此时，仅选择刚升级的 HA 防火墙的对等。
4. 请勿选择 **Group HA Peers**（组高可用性对等）。
5. 选择**Reboot device after install**（在安装之后重新启动设备）。
6. 要开始更新，请单击 **OK**（确定）。
7. 安装成功完成后，请使用以下方法之一重新启动：
   - 如果提示重新启动，请单击 **Yes**（是）。
   - 如果未提示重启，请选择 **Device**（设备） > **Setup**（设置） > **Operations**（操作）和 **Reboot Device**（重启设备）。

STEP 16 | （仅限 HA 防火墙升级）将 HA 功能恢复到辅助 HA 对等设备。

1. 登录挂起的辅助防火墙 HA 对等设备的防火墙 Web 界面 。
2. 选择 **Device**（设备） > **High Availability**（高可用性） > **Operational Commands**（操作指令），并 使本地设备正常运行以实现高可用性。
3. 在右下角，验证状态是否为 被动。对于处于主动/主动配置的防火墙，请验证其状态是否为 主动。
4. 等待 HA 对等设备运行配置同步。

   在 **Dashboard**（仪表板）中，监控 高可用性小部件中的运行配置状态。

STEP 17 | （仅限 FIPS-CC 模式） 在 FIPS-CC 模式下升级 Panorama 和受管设备。

如果在受管防火墙运行 PAN-OS 11.1 版本时将专用日志收集器添加到 Panorama 管理中，则在 FIPS-CC 模式下升级受管防火墙需要重置安全连接状态。

当托管防火墙运行 PAN OS 10.0 或更早版本时，您无需重新加入添加到 Panorama 管理的托管防火墙。

STEP 18 | 验证每个托管防火墙上运行的软件和内容发行版本。

1. 在 Panorama 上选择 **Panorama** > **Managed Devices**（托管设备）。
2. 找到防火墙并检查表格中的内容和软件版本。

   对于 HA 防火墙，您还可以验证每个对等的 HA 状态是否符合预期。

	DEVICE NAME	MODEL	IP Address IPV4	TEMPLATE	Status DEVICE STATE	Status HA STATUS	Status CERTIFICATE	Status L... M... D...	SOFTWARE VERSION	APPS AND THREAT	ANTIVIRUS
	DG-VM (5/5 Devices Connected): Shared > DG-VM										
	PA-VM-6	PA-VM		Stack-VM	Connected		pre-defined		8.1.0	8320-6307	3881-4345
	PA-VM-73	PA-VM		Stack-Test73	Connected		pre-defined		9.1.3	8320-6307	3873-4337
	PA-VM-95	PA-VM		Stack-VM	Connected		pre-defined		10.0.0	8320-6307	3881-4345
	PA-VM-96	PA-VM		Stack-VM	Connected	Passive	pre-defined		10.0.0	8299-6216	3881-4345
	PA-VM			Stack-Test92	Connected	Active	pre-defined		10.0.0	8299-6216	3881-4345

STEP 19 | （仅限 HA 防火墙升级）如果您在升级之前禁用其中一个 HA 防火墙的抢占，请编辑 **Election Settings**（选择设置）（**Device**（设备） > **High Availability**（高可用性）），并重新启用该防火墙的 **Preemptive**（抢占）设置，然后 **Commit**（提交）更改。

STEP 20 | 在 Panorama Web 界面上，将整个 Panorama 托管配置推送到您的托管防火墙。

此步骤需要启用选择性提交和推送设备组和模板堆栈配置更改从 Panorama 到您的托管防火墙。

在从 PAN-OS 10.1 或更早版本成功升级到 PAN-OS 11.1 后，这是成功将配置更改推送到由 Panorama 管理的多 vsys 防火墙所必需执行的操作。有关详细信息，请参阅 Panorama 管理的多 vsys 防火墙的共享配置对象的默认行为更改。

1. 选择 **Commit**（提交） > **Push to Devices**（推送到设备）。
2. **Push**（推送）。

STEP 21 | 重新生成或重新导入所有证书以遵守 OpenSSL 安全级别 2。

在升级到 PAN-OS 11.1 或更高版本时，要求所有证书满足以下最低要求。如果您从 PAN OS 10.2 升级并且已经重新生成或重新导入您的证书，请跳过此步骤。

- RSA 2048 位或以上，或 ECDSA 256 位或以上
- SHA256 或更高版本摘要

请参阅 PAN-OS 管理员指南或 Panorama 管理员指南，了解有关重新生成或重新导入证书的更多信息。

STEP 22 | 查看防火墙的软件升级历史。

1. 登录到 Panorama 界面。
2. 转到 **Panorama** > **Managed Devices**（受管设备） > **Summary**（摘要） 并单击 **Device History**（设备历史记录）。

当 Panorama 未连接互联网时升级防火墙

有关您可以在防火墙上安装的软件和内容更新列表，请参阅支持的更新。

当从 PAN-OS 11.1 上的 Panorama 设备升级到 PAN-OS 10.1 或更高版本上的防火墙时，新的跳过软件版本升级功能使您能够跳过最多三个版本。

更新 Panorama 的防火墙前，必须：

- 确保 Panorama 运行的 PAN-OS 版本与更新到的版本相同或，高于更新到的版本。在将托管防火墙升级到 11.1 版本之前，您必须将 Panorama 及其日志收集器升级到该版本。此外，在将日志收集器升级到 11.1 时，由于日志记录基础架构中的变化，您必须同时升级所有日志收集器。
- 确保防火墙已连接至可靠的电源。升级时断电可能导致防火墙无法使用。
- 如果 Panorama 虚拟设备在升级到 PAN-OS 11.1 时处于旧版模式，则决定是否保持处于旧版模式。运行 PAN OS 9.1 或更高版本的新 Panorama 虚拟设备部署不支持旧版模式。如果您将 Panorama 虚拟设备从 PAN-OS 9.0 或更早版本升级到 PAN-OS 11.1，Palo Alto Networks 建议查看 Panorama 虚拟设备的安装先决条件，并根据您的需要更改为 Panorama 模式或仅管理模式。

  如果要让 Panorama 虚拟设备保持处于旧版模式，请将分配给 Panorama 虚拟设备的 CPU 和内存增加到至少 16 个 CPU 和 32GB 内存，以成功升级到 PAN-OS 11.1。有关详细信息，请参阅 Panorama 虚拟设备的安装先决条件。
- （建议用于多 vsys 受管防火墙）将多 vsys 受管防火墙的所有 vsys 过渡到 Panorama。

  之所以这样建议是为了避免在多 vsys 受管防火墙上出现提交问题，并且使您能够利用 Panorama 经过优化的共享对象推送。

  适用于仅使用跳过软件版本升级从 PAN-OS 10.1 升级到 PAN-OS 11.1 的多 vsys 防火墙。
- （多 vsys 受管防火墙）删除或重命名与 Panorama **Shared**（共享）配置中的对象具有相同名称的任何本地配置 的**Shared**（共享）对象。否则，来自 Panorama 的配置推送在升级后会失败，并显示错误 `<object-name>` 已在使用中。

  适用于仅使用跳过软件版本升级从 PAN-OS 10.1 升级到 PAN-OS 11.1 的多 vsys 防火墙。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 已修改您的安全策略规则以允许 SSL 应用程序流量。

> 适用于仅使用跳过软件版本升级从 *PAN-OS 10.1* 升级到 *PAN-OS 11.1* 的防火墙。
>
> 升级到 *PAN-OS 11.1* 之后，如果使用 *Panorama App-ID* 控制 *Panorama* 与托管设备之间的流量，则必须采取此操作才能防止托管设备与 *Panorama* 断开连接。如果在升级之前不允许使用 *SSL* 应用程序，则托管设备将断开与 *Panorama* 的连接。

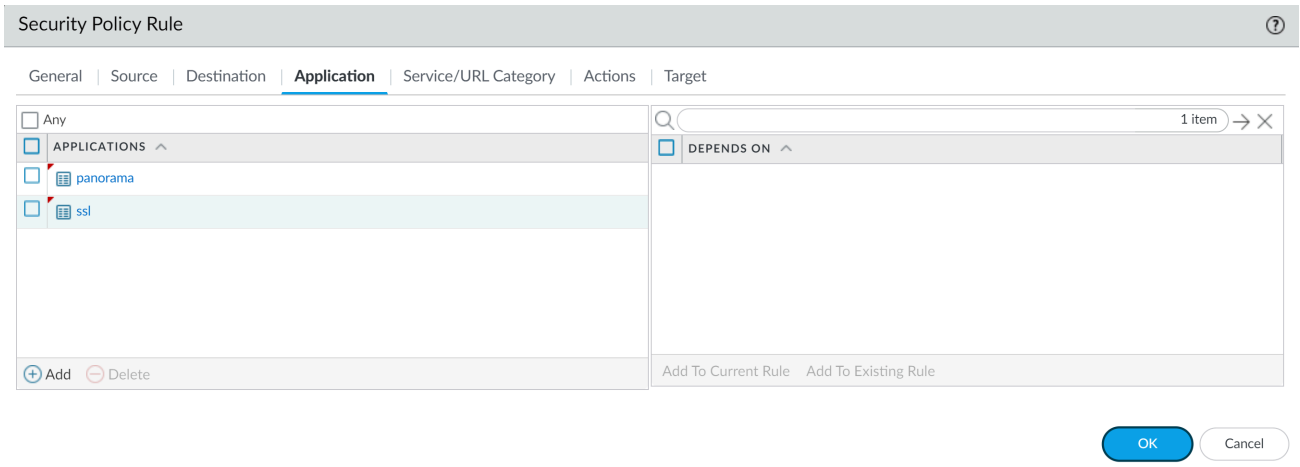
PAN-OS 11.1 使用 TLS 1.3 版本来加密服务证书以及 Panorama 和受管防火墙之间的握手消息。因此，从受管防火墙到 Panorama 的流量的 App-ID 将从 `Panorama` 重新分类为 SSL。要

继续在 Panorama 和托管设备之间进行通信，您必须修改控制 Panorama 和托管设备之间的流量的安全策略规则，以便同样允许使用 SSL 应用程序。

如果控制 Panorama 和托管设备之间的流量的安全策略规则允许使用 **Any**（任何）应用程序，或者您已经修改了控制 Panorama 和托管设备之间的流量的安全策略规则，请跳过此步骤。

1. 选择 **Policys**（策略） > **Security**（安全） > **Pre Rules**（前导规则）。
2. 选择包含控制 Panorama 和受管防火墙之间流量的安全策略规则的 **Device Group**（设备组）。
3. 选择安全策略规则。
4. 选择 **Application**（应用程序）并 **Add**（添加）SSL。

   请勿删除 *Panorama* 应用程序。这会导致在您推送更改后所有受管防火墙与 *Panorama* 断开连接。



5. 单击 **OK**（确定）。
6. 选择 **Commit**（提交） > **Commit and Push**（提交并推送），然后 **Commit and Push**（提交并推送）您的配置更改。

STEP 3 | 将当前配置文件的备份保存在计划要升级的每个托管防火墙上。

尽管防火墙自动创建配置备份，但最佳做法是在升级之前创建备份并通过外部方式将其保存。

1. **Export Panorama and devices config bundle**（导出 **Panorama** 和设备配置包）（**Panorama** > **Setup**（设置） > **Operations**（操作））用于生成和导出 Panorama 和每个受管设备的最新配置备份。
2. 将导出的文件保存到防火墙外部的位置。如果升级出现问题，您可以使用此备份还原配置。

STEP 4 | 确定您需要安装的内容更新。请参阅发布说明以了解您必须为 PAN-OS® 发布产品安装的最低内容发布版本。

Palo Alto Networks 强烈建议 *Panorama*，日志收集器和所有受管防火墙运行相同的内容发布版本。

对于每个内容更新，确定是否需要更新和在下一步中需要下载的内容更新。

确保 *Panorama* 运行的版本与受管防火墙和日志收集器上运行的内容发布版本相同，但不是更高版本。

STEP 5 | 对于打算更新到 Panorama 11.1 的防火墙，确定软件升级路径。

登录到 Panorama，选择 **Panorama** > **Managed Devices**（托管设备），然后记下您打算升级的防火墙的当前软件版本。

对于您在升级路径中会经过的每个版本，查看发行说明和升级/降级注意事项中的PAN-OS 升级清单、已知问题以及默认行为更改。

STEP 6 | （可选）将您的托管防火墙升级到 PAN-OS 10.1。

跳过软件版本升级功能支持运行 PAN-OS 10.1 或更高版本的托管防火墙。如果您的托管防火墙位于 PAN-OS 10.0 或更早版本上，请先升级到 PAN-OS 10.1 或更高版本。

STEP 7 | 执行版本的验证检查。

在此步骤中，您可以查看升级到 11.1 所需的中间软件和内容映像。

1. 选择 **Panorama** > **Device Deployment**（设备部署） > **Software**（软件） > **Action**（操作） > **Validate**（验证）。
2. 查看您需要下载的中间软件和内容版本。

STEP 8 | 将内容和软件更新下载到可以通过 SCP 或 HTTPS 连接并将文件上传到 Panorama 或配置的 SCP 服务器的主机。

默认情况下，您可以将最多两种软件或每种类型的内容更新上传到 Panorama 设备，并且如果您下载相同类型的第三个更新，Panorama 将删除该类型的最早版本的更新。如果您需要

上传两个以上的软件更新或单个类型的内容更新，请使用 **`set max-num-images count <number>`** CLI 命令增加 Panorama 可以存储的最大映像数量。

1. 使用能够访问互联网的主机，登录到 Palo Alto Networks 客户支持网站。
2. 下载内容更新：
   1. 在 Resources（资源）部分中单击 **Dynamic Updates**（动态更新）。
   2. **Download**（下载）最新的内容发布版本（或至少与将在 Panorama 管理服务器上安装或运行的版本相同或更高的版本）并将文件保存到主机；对于您需要更新的每个内容类型，请重复执行上述步骤。
3. 下载软件更新：
   1. 返回到 Palo Alto Networks 客户支持网站的主页，然后在 Resources（资源）部分中单击 **Software Updates**（软件更新）。
   2. 查看下载列以确定您需要安装的版本。更新包的文件名将指明型号。例如，要将 PA-440 和 PA-5430 防火墙升级到 PAN-OS 11.1.0，请下载 `Pan0S_440-11.1.0` 和 `Pan0S_5430-11.1.0` 映像。

      您可以通过从 ***Filter By***（筛选条件）下拉列表中选择 ***PAN-OS for the PA***（*PA* 的 ***PAN-OS***）*-<series/model>* 快速找到特定 *PAN-OS* 映像。
4. 单击相应的文件名并将文件保存到主机。

STEP 9 | 下载中间软件版本和最新的内容版本。

在 PAN OS 11.0 上，您可以使用多映像下载功能下载多个中间版本。

1. 选择要升级的防火墙（**Required Deployments**（所需部署） > **Deploy**（部署））。
2. 选择下载源并单击 **Download**（下载）。

STEP 10 | 在受管防火墙上安装内容更新。

在安装软件更新之前，必须安装内容更新。

先安装应用程序或应用程序和威胁更新，然后根据需要一次性以任何顺序安装任何其他更新（防病毒软件、WildFire® 或 URL 筛选）。

1. 选择 **Panorama** > **Device Deployment** > **Dynamic Updates**（Panorama > 设备部署 > 动态更新）。
2. 单击 **Upload**（上传），选择更新 **Type**（类型），**Browse**（浏览）至相应的内容更新文件，然后单击 **OK**（确定）。
3. 单击 **Install From File**（从文件安装），选择更新 **Type**（类型），然后选择您刚上传的内容更新的 **File Name**（文件名）。
4. 选择要安装更新的防火墙。
5. 单击 **OK**（确定）以开始安装。
6. 对于每个内容更新，请重复这些步骤。

STEP 11 | （仅限用作 GlobalProtect™ 门户的防火墙）在防火墙中上传并激活 GlobalProtect 代理/应用程序软件更新。

您在防火墙上激活了更新，因此用户将可以把更新下载到其端点（客户端系统）。

1. 使用能够访问互联网的主机登录到 Palo Alto Networks 客户支持网站。
2. 下载相应的 GlobalProtect 代理/应用程序软件更新。
3. 在 Panorama 上，选择 **Panorama** > **Device Deployment**（设备部署） > **GlobalProtect Client**（**GlobalProtect** 客户端）。
4. 单击 **Upload**（上传），**Browse**（浏览）到将文件下载到的主机上的相应 GlobalProtect 代理/应用程序软件更新，然后单击 **OK**（确定）。
5. 单击 **Activate From File**（从文件激活），然后选择您刚上传的 GlobalProtect 代理/应用程序软件更新的 **File Name**（文件名）。

   您一次只能激活一个版本的代理/应用程序软件更新。如果激活新版本，但某些代理需要以前的版本，则必须再次重新激活早期版本以便这些代理下载先前的更新。
6. 选择要激活更新的防火墙。
7. 单击 **OK**（确定）以激活。

STEP 12 | 安装 PAN-OS 11.1。

当您在高可用性 *(HA)* 防火墙上更新软件时，为了避免出现停机，一次只应更新一台高可用性对端设备。

对于主动/主动防火墙，无论您首先更新哪一个对端设备都没有关系。

对于主动/被动防火墙，您必须首先更新被动对端设备，挂起主动对端设备（故障转移），更新主动对端设备，然后再使主动对端设备恢复为运行状态（故障恢复）。

（仅限 *SD-WAN*）为了保持 *SD-WAN* 链接的准确状态，必须在升级分支防火墙之前将中心防火墙升级到 *PAN-OS 11.1*。先升级分支防火墙再升级中心防火墙可能导致错误的监视数据（***Panorama*** > ***SD-WAN*** > ***Monitoring***（监视）），且 *SD-WAN* 链接会错误地显示为 *down*。

1. 执行适用于防火墙配置的步骤以安装刚上传的 PAN-OS 软件更新。
   - 非高可用性防火墙 — 单击 Action（操作）列中的 **Install**（安装），选择您正在升级的所有防火墙，选择 **Reboot device after install**（安装后重新启动设备），然后单击 **OK**（确定）。
   - 主动/被动高可用性防火墙：
     1. 确认已在您打算升级的第一个对端设备上禁用抢先设置（**Device**（设备） > **High Availability**（高可用性） > Election Settings（选择设置））。如果启用，则编辑 **Election Settings**（选择设置），然后禁用（清除）**Preemptive**（抢先）设置并

Commit（提交）更改。您只需要在每个 HA 对中的一个防火墙上禁用此设置，但在继续之前确保提交成功。

2. 单击 **Install**（安装），禁用（清除）**Group HA Peers**（组高可用性对端设备），选择任意一个高可用性对端设备，选择 **Reboot device after install**（安装后重新启动设备），然后单击 **OK**（确定）。等待防火墙完成重新启动之后再继续进行操作。
3. 单击 **Install**（安装），禁用（清除）**Group HA Peers**（组高可用性对端设备），选择在上一步中尚未更新的高可用性对端设备，选择 **Reboot device after install**（安装后重新启动设备），然后单击 **OK**（确定）。

- 主动/被动高可用性防火墙 — 在本例中，主动防火墙的名称为 fw1，被动防火墙的名称为 fw2：
  1. 确认已在您打算升级的第一个对端设备上禁用抢先设置（**Device**（设备） > **High Availability**（高可用性） > Election Settings（选择设置））。如果启用，则编辑 **Election Settings**（选择设置），然后禁用（清除）**Preemptive**（抢先）设置并 **Commit**（提交）更改。您只需要在每个 HA 对中的一个防火墙上禁用此设置，但在继续之前确保提交成功。
  2. 单击相应更新的操作列中的 **Install**（安装），禁用（清除）**Group HA Peers**（组高可用性对端设备），选择 fw2，选择 **Reboot device after install**（安装后重新启动设备），然后单击 **OK**（确定）。等待 fw2 完成重新启动之后再继续进行操作。
  3. fw2 完成重新启动后，在 fw1（**Dashboard**（仪表板） > High Availability（高可用性））上核实 fw2 仍为被动对端设备（本地防火墙状态为 `active`，对端设备 (fw2) 为 `passive`）。
  4. 访问 fw1 和 **Suspend local device**（挂起本地设备）（**Device**（设备） > **High Availability**（高可用性） > **Operational Commands**（操作命令））。
  5. 访问 fw2（**Dashboard**（仪表板） > High Availability（高可用性）），并核实本地防火墙状态为 `active`，对端设备为 `suspended`。
  6. 访问 Panorama，选择 **Panorama** > **Device Deployment**（设备部署） > **Software**（软件），在相应版本的操作列中单击 **Install**（安装），禁用（清除）**Group HA Peers**（组高可用性对端设备），选择 fw1，选择 **Reboot device after install**（安装后重新启动设备），然后单击确定。等待 fw1 完成重新启动之后再继续进行操作。
  7. 访问 fw1（**Device**（设备） > **High Availability**（高可用性） > **Operational Commands**（高可用性）），单击 **Make local device functional**（使本地设备正常运行），然后等待两分钟后进行下一步。
  8. 在 fw1（**Dashboard**（仪表板） > High Availability（高可用性））上，核实本地防火墙状态为 `passive`，对端设备 (fw2) 为 `active`。

STEP 13 | （仅限 FIPS-CC 模式） 在 FIPS-CC 模式下升级 Panorama 和受管设备。

如果在受管防火墙运行 PAN-OS 11.1 版本时将专用日志收集器添加到 Panorama 管理中，则在 FIPS-CC 模式下升级受管防火墙需要重置安全连接状态。

当托管防火墙运行 PAN OS 10.0 或更早版本时，您无需重新加入添加到 Panorama 管理的托管防火墙。

STEP 14 | 验证安装在每个受管防火墙上的软件和内容版本。

1. 选择 **Panorama** > **Managed Devices**（受管设备）。
2. 找到防火墙，并查看 Software Version（软件版本）、Apps and Threat（应用程序和威胁）、Antivirus（防病毒软件）、URL Filtering（URL 筛选）和 GlobalProtect Client（GlobalProtect 客户端）列中的值。

STEP 15 | 如果您在升级之前禁用其中一个 HA 防火墙的抢先，请编辑 **Election Settings**（选择设置）（**Device**（设备） > **High Availability**（高可用性）），并重新启用该防火墙的 **Preemptive**（抢先）设置。

STEP 16 | 在 Panorama Web 界面上，将整个 Panorama 托管配置推送到您的托管防火墙。

此步骤需要启用选择性提交和推送设备组和模板堆栈配置更改从 Panorama 到您的托管防火墙。

在成功升级到 PAN-OS 11.1 后，这是成功地将配置更改推送到由 Panorama 管理的多 vsys 防火墙所必需的。有关详细信息，请参阅 Panorama 管理的多 vsys 防火墙的共享配置对象的默认行为更改。

1. 选择 **Commit**（提交） > **Push to Devices**（推送到设备）。
2. **Push**（推送）。

STEP 17 | 重新生成或重新导入所有证书以遵守 OpenSSL 安全级别 2。

在升级到 PAN-OS 11.1 时，要求所有证书满足以下最低要求：

- RSA 2048 位或以上，或 ECDSA 256 位或以上
- SHA256 或更高版本摘要

请参阅 PAN-OS 管理员指南或 Panorama 管理员指南，了解有关重新生成或重新导入证书的更多信息。

STEP 18 | 查看防火墙的软件升级历史。

1. 登录到 Panorama 界面。
2. 转到 **Panorama** > **Managed Devices**（受管设备） > **Summary**（摘要） 并单击 **Device History**（设备历史记录）。

升级 ZTP 防火墙

在您成功添加 ZTP 防火墙至 Panorama™ 管理服务器后，请配置 ZTP 防火墙的目标 PAN-OS 版本。当 ZTP 防火墙首次成功连接到 Panorama 后，Panorama 会检查 ZTP 防火墙上安装的 PAN-OS 版本是否大于或等于所配置的目标 PAN-OS 版本。如果 ZTP 防火墙上安装的 PAN-OS 版本低于目标 PAN-OS 版本，则 ZTP 防火墙将进入一个升级周期，直至安装目标 PAN-OS 版本。

STEP 1 | 以管理员身份登录到 Panorama Web 界面。

STEP 2 | 将 ZTP 防火墙添加到 Panorama。

STEP 3 | 选择 **Panorama** > **Device Deployment**（设备部署） > **Updates**（更新），然后 **Check Now**（立即检查）最新 PAN-OS 版本。

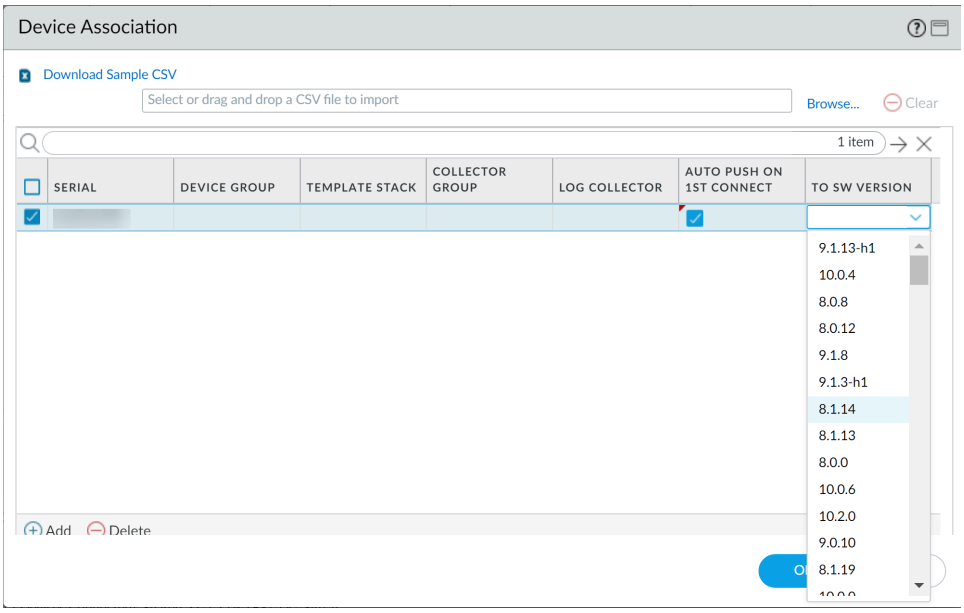
STEP 4 | 选择 **Panorama** > **Managed Devices**（受管设备） > **Summary**（摘要），然后选择一个或多个 ZTP 防火墙。

STEP 5 | **Reassociate**（重新关联）所选的 ZTP 防火墙。

STEP 6 | 检查（启用） 第一次连接时自动推送。

STEP 7 | 在 **To SW Version**（至 **SW** 版本）列中，选择 ZTP 防火墙的目标 PAN-OS 版本。

STEP 8 | 单击 **OK**（确定）保存您的配置更改。



STEP 9 | 选择 **Commit**（提交） 和 **Commit to Panorama**（提交到 **Panorama**）。

STEP 10 | 开启 ZTP 防火墙。

当 ZTP 防火墙首次连接到 Panorama 时，它会自动升级到您选择的 PAN-OS 版本。

- 运行 **PAN-OS 11.1.0** 的 **Panorama** — 如果您要跨 PAN-OS 主要版本或维护版本升级受管防火墙，则先安装升级路径上的中间 PAN-OS 版本，然后再安装目标 PAN-OS 版本。

  例如，您将受管防火墙的目标 **To SW Version**（到 **SW** 版本）配置为 PAN-OS 11.1.0，并且该防火墙运行的是 PAN-OS 10.2。第一次连接到 Panorama 时，先在受管防火墙上安装 PAN-OS 11.0.0。PAN-OS 11.0.0 成功安装后，防火墙会自动升级到目标 PAN-OS 11.1.0 版本。

- **Panorama** 运行 **PAN-OS 11.0.1** 及更高版本—如果您正在跨 PAN-OS 主要版本或维护版本升级托管防火墙，则先安装升级路径上的中间 PAN-OS 主要版本并下载基本 PAN-OS 主要版本，然后再安装目标 PAN OS 维护版本。

  例如，您将托管防火墙的目标 到 **SW** 版本 配置为 PAN-OS 11.0.1，并且防火墙正在运行 PAN-OS 10.0。在第一次连接到 Panorama 时，PAN-OS 10.1.0 和 PAN-OS 10.2.0 安装在托管防火墙上。托管防火墙重新启动后，将下载 PAN OS 11.0.0，然后防火墙自动安装到目标 PAN OS 11.0.1 版本。

STEP 11 | 验证 ZTP 防火墙是否升级。

1. 登录到 Panorama Web 界面。
2. 选择 **Panorama** > **Managed Devices**（受管设备） > **Summary**（摘要），然后导航至 ZTP 防火墙。
3. 验证 **Software Version**（软件版本）列是否显示正确的目标 PAN-OS 版本。

STEP 12 | 对于所有未来的 PAN-OS 升级，请参阅 从 Panorama 中将防火墙升级到 PAN-OS 11.1.

安装 PAN-OS 软件补丁

在何处可以使用？	需要提供什么？
• 下一代防火墙	❑ 支持许可证 ❑ PAN-OS 11.1.3 或更高的 11.1 版本 ❑ 出站互联网接入

查看 PAN-OS 11.1 发行说明，然后按照以下步骤安装 PAN-OS 软件补丁，以解决当前在下一代防火墙上运行的 PAN-OS 版本中的错误以及公共漏洞和暴露 (CVE)。安装 PAN-OS 软件补丁可修复错误和 CVE，无需安排长期维护，并允许您立即加强安全态势，而不会引入任何新的已知问题或更改安装新 PAN-OS 版本时可能出现的默认行为。此外，您可以恢复当前安装的软件补丁，以卸载安装软件补丁时应用的错误和 CVE 修复程序。

安装或恢复 PAN-OS 软件补丁时会生成系统日志（**Monitor**（监视） > **Logs**（日志） > **System**（系统））。需要出站互联网连接才能从 Palo Alto Networks 客户支持门户下载 PAN-OS 软件补丁。

- 安装
- 恢复

安装

STEP 1 | 登录到防火墙 Web 界面。

STEP 2 | 选择 **Device**（设备） > **Software**（软件），然后 **Check Now**（立即检查）以从 Palo Alto Networks 更新服务器检索最新的 PAN-OS 软件补丁。

STEP 3 | 选中（启用）**Include Patch**（包含补丁），以显示所有可用的 PAN-OS 软件补丁。

STEP 4 | 找到当前安装在下一代防火墙上的 PAN-OS 版本的软件补丁。

通过 **Version**（版本）名称旁边显示的 `Patch` 标签来表示软件补丁。

STEP 5 | 查看 **More Info**（更多信息），以查看软件补丁的详细信息，例如严重错误和 CVE 修复程序，以及是否需要重新启动下一代防火墙才能应用修复程序。

STEP 6 | **Download**（下载）软件补丁。

（仅限 HA）选中（启用）同步到 HA 对等设备，然后选择 **Continue Download**（继续下载）以下载 PAN-OS 软件补丁。

成功下载软件补丁后单击 **Close**（关闭）。

STEP 7 | **Install**（安装）软件补丁。

成功安装软件补丁后，单击 **Close**（关闭）。

STEP 8 | **Apply**（应用）软件补丁。

当系统提示您确认要将已安装的 PAN-OS 软件补丁应用于下一代防火墙时，单击 **Apply**（应用）。

将显示一个状态栏，显示 PAN-OS 软件补丁应用程序的当前进度。成功应用补丁后，单击 **Close**（关闭）。

此时，如果需要重新启动才能将 PAN-OS 软件补丁应用于下一代防火墙，防火墙将自动重新启动。

STEP 9 | （仅限 HA）在防火墙 HA 对等设备上安装 PAN-OS 软件补丁。

1. 登录到 HA 对等设备的防火墙 Web 界面。
2. 选择 **Device**（设备） > **Software**（软件）以及 **Check Now**（立即检查）。
3. **Install**（安装）软件补丁。
4. 如果需要，重新启动防火墙。

恢复

STEP 1 | 登录到防火墙 Web 界面。

STEP 2 | 选择 **Device**（设备） > **Software**（软件），并找到要恢复的 PAN-OS 软件补丁。

STEP 3 | **Revert**（恢复）软件补丁。

当系统提示您确认要恢复下一代防火墙上安装的 PAN-OS 软件补丁时，单击 **Revert**（恢复）。

将显示一个状态栏，显示 PAN-OS 软件补丁应用程序的当前进度。成功应用补丁后，单击 **Close**（关闭）。

此时，如果需要重新启动才能将 PAN-OS 软件补丁应用于下一代防火墙，防火墙将自动重新启动。

降级 PAN-OS

将防火墙从 PAN-OS 11.1 降级的方式取决于您是降级到以前的功能版本（PAN-OS 版本中的第一位或第二位数字更改，例如从 9.1.2 更改为 9.0.8 或从 9.0.3 更改为 8.1.14），还是降级到同一功能版本中的维护版本（发行版本中的第三位数字更改，例如从 8.1.2 更改为 8.1.0）。当您从一个功能版本降级到较早的功能版本时，可以将配置从更高版本迁移以适应新功能。要将 PAN-OS 11.1 配置迁移到较早的 PAN-OS 版本，请先恢复要降级到的功能版本的配置。在同一功能版本中从一个维护版本降级到另一个维护版本时，无需恢复配置。

- 将防火墙降级到以前的维护版本
- 将防火墙降级到以前的功能版本
- 降级 Windows 代理

始终降级为与软件版本匹配的配置。不匹配的软件版本和配置可能会导致降级失败或强制让系统进入维护模式。这仅适用于从一个功能版本降级到另一个功能版本（例如 *9.0.0* 到 *8.1.3*），不适用于同一功能发行版本内降级至维护版本（例如，*8.1.3* 至 *8.1.1*）。

如果在降级时遇到问题，则可能需要进入维护模式并将设备重置为出厂默认设置，然后从升级之前导出的原始配置文件中恢复配置。

将防火墙降级到以前的维护版本

由于维护版本不引入新功能，因此您可以在同一功能版本中降级到以前的维护版本，而无需恢复以前的配置。维护版本是发行版本中第三个数字发生变化的版本，例如，从 10.1.6 降级到 10.1.4 被视为维护版本降级，因为发行版本中只有第三位数字不同。

使用以下程序降级到同一功能版本中的旧版维护版本。

STEP 1 | 保存当前配置文件的备份。

尽管防火墙将自动创建配置的备份，但最佳做法是在降级之前创建备份并将它存储在外部。

1. **Export named configuration snapshot**（导出已命名的配置快照）（**Device**（设备） > **Setup**（设置） > **Operations**（操作））。
2. 选择包含正在运行的配置（如 **running-config.xml**）的 XML 文件，并单击 **OK**（确定）导出配置文件。
3. 将导出的文件保存到防火墙外部的位置。如果降级出现问题，您可以使用此备份还原配置。

STEP 2 | 安装旧版维护版本映像。

如果您的防火墙无法从管理端口访问互联网，则可以从 Palo Alto Networks 支持门户下载软件更新。然后，您可以手动将其 ***Upload***（上传）到防火墙。

1. **Check Now**（立即检查）（**Device**（设备） > **Software**（软件））可用的映像。

（PAN-OS 11.1.3 及更高版本）默认情况下，显示首选版本和相应的基础版本。要仅查看首选版本，请禁用（清除）**Base Releases**（基础版本）复选框。

2. 找到要降级到的版本。如果尚未下载映像，请 **Download**（下载）。
3. 下载完成后，请 **Install**（安装）映像。
4. 安装成功完成后，请使用以下方法之一重新启动：
   - 如果提示重新启动，请单击 **Yes**（是）。
   - 如果未提示重启，请转到 Device Operations（设备操作）（**Device**（设备） > **Setup**（设置） > **Operations**（操作）），然后选择 **Reboot Device**（重启设备）。

将防火墙降级到以前的功能版本

使用以下工作流程以还原在升级到其他功能版本之前正在运行的配置。自升级以来所做的任何更改都将丢失。因此，请务必备份当前配置，这样您可以在恢复到较新功能版本时还原这些更改。在将防火墙降级到以前的功能版本之前，请查看 升级/降级注意事项。

要从 *PAN-OS 11.1* 降级到更早的 *PAN-OS* 版本，您必须下载并安装 *PAN-OS 10.1.3* 或更高的 *PAN-OS 10.1* 版本，然后才能继续降级到目标 *PAN-OS* 版本。如果您尝试降级到 *PAN-OS 10.1.2* 或更早的 *PAN-OS 11.1* 版本，则从 *PAN-OS 11.1* 降级失败。

使用以下过程降级到以前的功能版本。

STEP 1 | 保存当前配置文件的备份。

尽管防火墙将自动创建配置文件的备份，但最佳做法是在升级和存储在外部设备之前创建备份。

1. **Export named configuration snapshot**（导出已命名的配置快照）（**Device**（设备） > **Setup**（设置） > **Operations**（操作））。
2. 选择包含正在运行的配置（如 **running-config.xml**）的 XML 文件，并单击 **OK**（确定）导出配置文件。
3. 将导出的文件保存到防火墙外部的位置。如果降级出现问题，您可以使用此备份还原配置。

STEP 2 | 安装上一功能版本映像。

升级到新版本时，将创建自动保存版本。

1. **Check Now**（立即检查）（**Device**（设备） > **Software**（软件））可用的映像。
2. 安装 PAN-OS 10.1。

   要从 PAN-OS 11.1 降级到以前的功能版本，需要先降级到 PAN-OS 10.1.3 或更高的 PAN-OS 10.1 版本。成功降级到 PAN-OS 10.1.3 或更高的 PAN-OS 10.1 版本后，您可以继续降级到目标 PAN-OS 版本。

   1. 找到并 **Download**（下载）PAN-OS 11.1 映像。
   2. **Install**（安装）PAN-OS 11.1 映像。
3. 找到要降级到的目标 PAN-OS 映像。如果尚未下载映像，请 **Download**（下载）。
4. 下载完成后，请 **Install**（安装）映像。
5. **Select a Config File for Downgrading**（选择用于降级的配置文件），防火墙将会在重启设备后加载该文件。在大多数情况下，您应选择在从现在正在降级的版本升级时自动保存的配置。例如，如果您正在运行 PAN-OS 11.1 并要降级到 PAN-OS 10.2.2，则应选择 `autosave-10.2.2`。
6. 安装成功完成后，请使用以下方法之一重新启动：
   - 如果提示重新启动，请单击 **Yes**（是）。
   - 如果未提示重启，请转到 Device Operations（设备操作）（**Device**（设备） > **Setup**（设置） > **Operations**（操作）），然后 **Reboot Device**（重启设备）。

降级 Windows 代理

卸载 PAN-OS 11.1 基于 Windows 的 User-ID 代理后，请在安装较早代理版本之前执行以下步骤。

STEP 1 | 打开 Windows 开始菜单并选择 **Administrative Tools**（管理工具）。

STEP 2 | 选择 **Computer Management**（计算机管理） > **Services and Applications**（服务和应用程序） > **Services**（服务），然后双击 **User-ID Agent**（**User-ID** 代理）。

STEP 3 | 选择 **Log On**（登录），选择 **This account**（此帐户），然后指定 User-ID 代理帐户的用户名。

STEP 4 | 输入 **Password**（密码）和 **Confirm Password**（确认密码）。

STEP 5 | 单击 **OK**（确定）保存更改。

PAN-OS 升级问题故障排除

要对 Panorama 插件升级进行故障排除，请使用下表查看可能的问题以及如何解决这些问题。

症状	解决方案
软件保修许可证已过期。	从 CLI 中删除过期的许可证密钥： 1. 输入 **delete license key <software license key>**。 2. 输入 **delete license key Software_Warranty<expiredate>.key**。
最新的 PAN OS 软件版本不可用。	您只能看到比当前安装版本高一个功能版本的软件版本。例如，如果您安装了 9.1 版本，则只有 10.0 版本可供您使用。要查看 11.1 版本，您必须先升级到 10.1。
检查动态更新失败。	此问题因网络连接错误而产生。请参阅知识库文章单击“立即检查”按钮后动态更新显示错误。
未找到有效的设备证书。	在 PAN-OS 9.1.3 及更高版本中，如果您使用的是 Palo Alto Networks 云服务，则必须安装设备证书。要安装设备证书，请执行以下操作： 1. 登录到客户支持门户。 2. 选择 **Generate OTP**（生成 **OTP**）（**Assets**（资产）> **Device Certificates**（设备证书））。 3. 在 **Device Type**（设备类型）中，选择 **Generate OTP for Next-Gen Firewalls**（为下一代防火墙生成 **OTP**）。 4. 选择您的 PAN OS 设备序列号。 5. **Generate OTP**（生成 **OTP**）并复制一次性密码。 6. 以管理员用户身份登录防火墙。 7. 选择 **Device Certificate**（设备证书）（**Device**（设备）> **Setup**（设置）> **Management**（管理）> **Device**（设备）> **Certificate**（证书）），然后选择 **Get Certificate**（获取证书）。 8. 粘贴 OTP 并单击 **OK**（确定）。

症状	解决方案
由于映像身份验证错误，软件映像文件无法加载到软件管理器中。	要更新软件映像列表，请单击 **Check Now**（立即检查）。这将建立到更新服务器的新连接。
VMware NSX 插件版本与新软件版本不兼容。	VMware NSX 插件是在升级到 8.0 时自动安装的。如果您不使用该插件，则可以将其卸载。
升级到 PAN OS 9.1 后，重启时间比预期的要长。	升级到应用程序和威胁内容发行版本 8221 或更高版本。有关最低软件和内容版本的更多信息，请参阅<xref to 11.1 Associated Software and Content Versions>。
即使许可证处于活动状态，该设备也没有支持。	在**Device**（设备）> **Software**（软件）中，单击 **Check Now**（立即检查）。 这通过与更新服务器建立新连接来更新防火墙上的许可信息。 如果这在 Web 界面中不起作用，请使用 **`request system software check`**。
防火墙没有 DHCP 服务器分配给它的 DHCP 地址。	配置安全策略规则，以允许从 ISP DHCP 服务器到内部网络的流量。
防火墙持续启动到维护模式。	在 CLI 中，Access the Maintenance Recovery Tool (MRT)（访问维护恢复工具 (MRT)）。在 MRT 窗口中，选择 **Continue**（继续）> **Disk Image**（磁盘映像）。选择 **Reinstall**（重新安装）**<current version>** 或 **Revert to**（恢复为）**<previous version>**。恢复或重新安装操作完成后，选择 **Reboot**（重新启动）。
在 HA 配置中，升级对等防火墙后，防火墙进入暂停状态，错误是防火墙太旧。	将一个防火墙升级到即将发布多个主要版本的版本将导致网络中断。在升级到下一个主要版本之前，两个防火墙中只有一个升级主要版本。 将对等防火墙降级到已暂停的防火墙停止的版本。

升级 VM 系列防火墙

升级 VM 系列 PAN-OS 软件（独立）

升级 VM 系列 PAN-OS 软件（HA 对）

使用 Panorama 升级 VM 系列 PAN-OS 软件

升级 PAN-OS 软件版本（适用于 NSX 的 VM 系列）

选择最适合您部署的升级方法。

- 在维护窗口期间升级 NSX 的 VM 系列 — 使用此选项可在维护窗口期间升级 VM 系列防火墙，而无需更改服务定义中的 OVF URL。
- 在不中断流量的情况下升级 NSX 的 VM 系列 — 使用此选项升级 VM 系列防火墙而不中断对来宾 VM 的服务或更改服务定义中的 OVF URL。

下图显示了目前支持的适用于 VMware NSX 的 Panorama 和 Panorama 插件组合，以及成功升级需要遵循的升级路径。

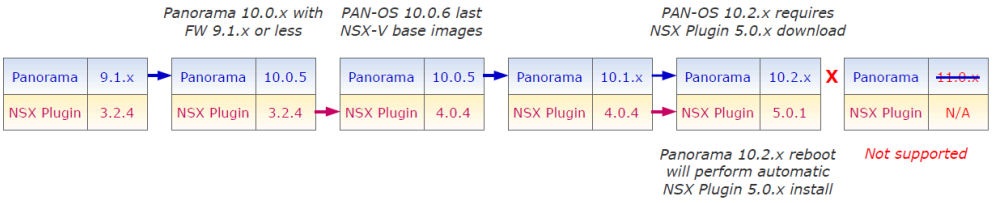
- 下面的每个方框都代表一个受支持的组合。
- 在 HA 对中升级适用于 NSX 的 Panorama 插件或 Panorama 时，请先升级被动 Panorama 对等，然后升级主动 HA 对等。

在升级用于 VMware NSX 部署的 VM 系列之前，请查看下面所示的升级路径以了解升级步骤，从而找到最适合您的环境的插件和 PAN-OS 组件。

Panorama and PAN NSX Plugin Upgrade Paths

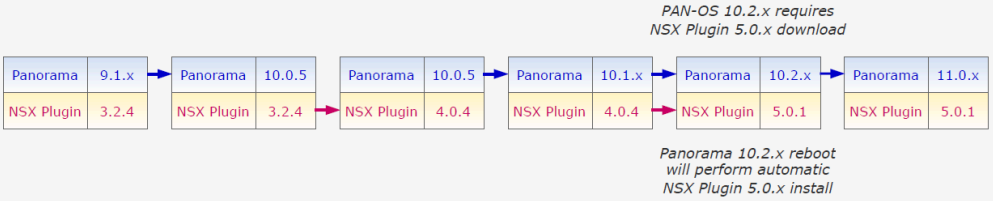
- For Panorama upgrades, first upgrade Panorama HA Passive, then Panorama HA Active
- For NSX Plugin upgrades, first upgrade Panorama HA Passive, then Panorama HA Active
- Best practice is always upgrade one at a time (either Panorama or NSX Plugin)

VM-Series for NSX-V



IMPORTANT! PAN-OS 10.0.6 are the last available base images for VM-Series for NSX-V.

VM-Series for NSX (formerly NSX-T)



IMPORTANT! VMware NSX-T has been renamed to VMware NSX as of version 4.0.x.

在维护窗口期间升级 NSX 的 VM 系列

在不中断流量的情况下升级 NSX 的 VM 系列

升级 VM 系列型号

VM 系列防火墙的许可过程会使用 UUID 和 CPU ID 生成每个 VM 系列防火墙的唯一序列号。因此，在生成许可证时，此许可证会映射到 VM 系列防火墙的特定实例中，并且不能修改。

如果处于以下情况，请使用本部分中的说明：

- 从评估许可证迁移到生产许可证。
- 升级型号以便获得更大的容量。例如，您想要从 VM-100 升级到 VM-300 型号。

- 升级容量可能会重新启动防火墙上的一些关键进程。建议使用 *HA* 配置以尽量减少服务中断；要升级 *HA* 对上的容量，请参阅升级 HA 对中的 VM 系列型号。
- 在私有云或公共云部署中，如果防火墙已获得 *BYOL* 选项的许可，则您必须在更改实例类型或 *VM* 类型之前停用您的 VM。升级型号或实例会更改 *UUID* 和 *CPU ID*，因此，在以下情况下，您必须应用许可证。

STEP 1 | 将额外的硬件资源分配给 VM 系列防火墙。

在启动容量升级之前，您必须验证是否有足够的硬件资源可用于 VM 系列防火墙以支持新容量。每个虚拟机监控程序上分配额外硬件资源的过程都不相同。

要检查新 VM 系列型号的硬件要求，请参阅 VM 系列型号。

虽然容量升级不需要重新启动 VM 系列防火墙，但需要关闭虚拟机以更改硬件分配。

STEP 2 | 从客户支持门户检索许可证 API 密钥。

1. 登录到客户支持门户。

   确保您使用的是您用于注册初始许可证的相同帐户。

2. 在左侧菜单中，选择 **Assets**（资产） > **API Key Management**（**API** 密钥管理）。
3. 复制 API 密钥。

tion Programming Interface (API) key is a unique identifier that authenticates a user or app calling Palo Alto Networks REST APIs. Each
ific Palo Alto Networks service. For example, Licensing API key work only with Licensing APIs, and Threat Vault API keys work only with

PI key Licensing API

ing APIs to manage firewall licenses (e.g., renew licenses, register auth codes, retrieve licenses attached to auth codes, deactivate licens

Licensing API key, click the Enable link below. You can also revoke an API key or regenerate an API key (which revokes the previous API

ate 12/06/2024

Extend Regenerate

STEP 3 | 在防火墙上，使用 CLI 安装上一步中复制的 API 密钥。

```
request license api-key set key <key>
```

STEP 4 | （如果可以访问 Internet）在 **Device**（设备） > **Setup**（设置） > **Service**（服务）上启用防火墙以 **Verify Update Server identity**（验证更新服务器标识）。

STEP 5 | **Commit**（提交）更改。确保防火墙上具有本地配置的用户。如果配置超过非许可的 PA-VM 对象限制，则在停用后 Panorama 推送的用户可能不可用。

STEP 6 | 升级容量。

选择 **Device**（设备） > **Licenses**（许可证） > **Upgrade VM Capacity**（升级 **VM** 容量），然后使用以下方式之一激活许可证及订阅：

- （访问 Internet）从许可证服务器检索许可证密钥 — 如果您已在客户支持门户上激活许可证，请使用此选项。
- （访问 Internet）使用授权代码 — 使用此选项升级为许可证使用授权代码的 VM 系列容量，该许可证之前在支持门户上为激活。系统提示时，输入 **Authorization Code**（授权代码），然后单击 **OK**（确定）。
- （无法访问 Internet）手动上传许可证密钥 — 如果防火墙无法通过 Internet 连接到客户支持门户，请使用此选项。从可以访问 Internet 的计算机登录 CSP，下载许可证密钥文件，将其传输到与防火墙处于同一网络的计算机，然后将其上传到防火墙。

STEP 7 | 验证防火墙已成功获得许可。

在 **Device**（设备） > **Licenses**（许可证）页面上，验证是否已成功激活许可证。

升级 HA 对中的 VM 系列型号

将 VM 系列防火墙降级到上一版本

升级 Panorama 插件

Panorama 插件升级/降级注意事项

下表列出了会受升级或降级影响的新功能。在升级到 PAN-OS 11.1 版本或从 PAN-OS 11.1 版本降级之前，请务必了解全部升级/降级注意事项。有关 PAN-OS 11.1 版本的更多信息，请参阅 PAN-OS 11.1 发行说明。

表 **1: Panorama** 插件升级**/**降级注意事项

功能	升级注意事项	降级注意事项
Panorama 插件 • AWS 插件 • Azure 插件 • Kubernetes 插件 • 软件防火墙许可插件 • SD-WAN 插件 • IPS 签名转换器插件 • ZTP 插件 • 企业 DLP 插件 • Openconfig 插件 • GCP 插件 • Cisco ACI 插件 • Nutanix 插件 • VCenter插件	在升级到 PAN-OS 11.1 之前，对于安装在 Panorama 上的所有插件，您必须下载 PAN-OS 11.1 支持的 Panorama 插件版本。这是成功升级到 PAN-OS 11.1 所必需执行的操作。有关详细信息，请参阅 兼容性矩阵。	要从 PAN-OS 11.0 降级，您必须下载 PAN-OS 10.2 和早期版本支持的 Panorama 插件版本，用于安装在 Panorama 上的所有插件。有关详细信息，请参阅 Panorama 插件兼容性矩阵 。
	（企业 DLP）将 Panorama 升级到 PAN-OS 10.2 后，您必须在运行 PAN-OS 11.1 或更早版本的所有受管防火墙上安装应用程序和威胁内容版本 8520。这是利用未升级到 PAN-OS 10.2 的企业 DLP 成功将配置更改推送到托管防火墙所必需的。	
	（企业 DLP） 加载包含共享企业 DLP 配置的 Panorama 配置备份 会删除扫描非基于文件的流量所需的共享应用程序排除过滤器。	
	(SD-WAN) PAN-OS 11.0 不支持 SD-WAN 2.2 和更早版本的 Panorama 插件。 在安装 SD-WAN 2.2 或更早版本的 Panorama 插件时，将 Panorama 管理服务器升级到 PAN-OS 11.1 会导致 SD-WAN 插件隐藏在 Panorama Web 界面中或导致 SD-WAN 配置被删除。在这两种情况下，您都无法安装新的 SD-WAN 插件版本或卸载 SD-WAN 插件。	

功能	升级注意事项	降级注意事项
SD-WAN	将 Panorama 成功升级到 PAN-OS 11.1 并将 Panorama 插件从 SD-WAN 2.0.0 版本升级到 SD-WAN 3.0 版本后，必须清除 Panorama 上现有 SD-WAN 部署的 SD-WAN 缓存。 清除 SD-WAN 缓存不会删除任何现有的 SD-WAN 配置，但会删除适用于 SD-WAN 3.0 版的 Panorama 插件中引入的新格式的 IP 地址、隧道和网关命名约定。 对于 SD-WAN 的新部署，如果升级到 PAN-OS 11.0 后在 Panorama 上安装了适用于 SD-WAN 3.0 版的 Panorama 插件，则无需清除 Panorama 上的 SD-WAN 缓存。 1. 登录到 Panorama 命令行界面。 2. 清除 Panorama 上的 SD-WAN 缓存。 `admin> debug plugins sd_wan drop-config-cache all`	无。

升级 Panorama 插件

使用以下步骤升级 Panorama 管理服务器上安装的大多数插件的版本。升级下面列出的插件之一时，请使用所提供链接中的步骤。要升级到最新的 VM-Series 插件，

- 升级企业 DLP 插件
- 升级 Panorama Interconnect 插件
- 升级 VMware NSX 的 Panorama 插件时，请参阅适用于 VMware NSX 的 VM-Series 文档。

STEP 1 | 请参阅兼容性矩阵，了解每个 Panorama 插件支持的最低 PAN-OS 版本。

STEP 2 | 查看 Panorama 插件发行说明，以确定您的目标插件版本。

STEP 3 | 查看Panorama 插件升级/降级注意事项。

STEP 4 | 下载插件。

1. 选择 **Panorama** > **Plugins**（插件）。
2. 选择**Check Now**（立即检查）以检索可用的更新列表。
3. 在操作列中选择 **Download**（下载）以下载插件。

STEP 5 | 安装插件。

选择上一步中下载的插件版本，单击 Action（操作）列中的 **Install**（安装）即可安装插件。安装完成后，Panorama 会提醒您。

在 *Panorama HA* 对中首次安装插件时，请在主动对等体之前将该插件安装到被动对等体上。在被动对等设备上安装插件时，将转换为非运行状态。然后，当您成功在主动对等体上安装插件后，被动对等体将恢复到运行状态。

STEP 6 | 可选 您可以使用以下 CLI 命令查看插件升级日志。

```
tail plugins-log ... tail mp-log plugin_install.log
```


升级企业 DLP 插件

在您的 Panorama™ 管理服务器上安装并配置企业数据丢失防护 (DLP) 插件。

请参阅 Palo Alto Networks Panorama 插件兼容性矩阵，查看目标企业 DLP 插件版本所需的最低 PAN-OS 版本。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 升级 Panorama 上的企业 DLP 插件版本。

如果 Panorama 为高可用性 (HA) 配置，则在 Panorama HA 对等设备上重复这个步骤。

1. 选择 **Panorama** > **Plugin**（插件）并 **Check Now**（立即检查）最新的 **dlp** 插件版本。
2. **Download**（下载）并 **Install**（安装）最新的企业 DLP 插件。
3. 成功安装新插件版本后，查看 Panorama **Dashboard**（仪表板）并在常规信息小部件中验证 `Plugin DLP`（插件 DLP） 版本是否显示您升级到的企业 DLP 插件版本。

STEP 3 | （仅升级到 4.0.0）编辑企业 DLP 数据筛选设置，将 **Max File Size**（最大文件大小减小）到 20MB 或更小。

从企业 DLP 3.0.3 或更高版本的 Panorama 插件升级到企业 DLP 4.0.0 时，这是必需的，因为此插件版本不支持 大文件大小检查。

升级 Panorama Interconnect 插件

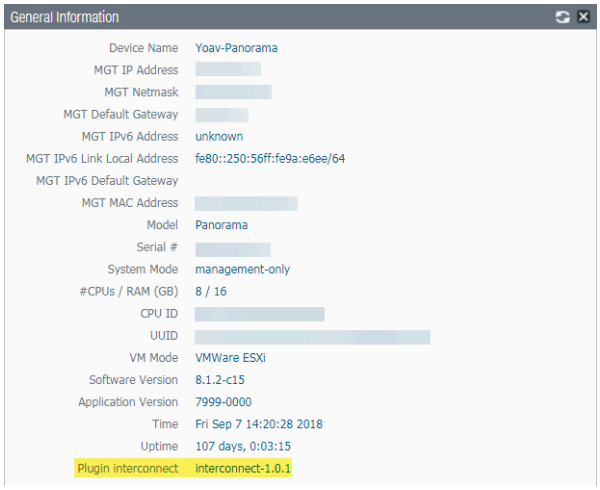
使用下列程序在 Panorama 控制器和 Panorama 节点上升级 Panorama™ Interconnect 插件。升级 Panorama Interconnect 插件时，必须先升级 Panorama 控制器，然后再将 Panorama 节点升级到与控制器相同的插件版本。在 Panorama 节点上下载并安装的新插件版本必须与您在 Panorama 控制器上安装的插件版本一致，确保 Panorama 控制器和所选 Panorama 节点上的插件版本保持同步。

如果这是您第一次安装插件，请参阅安装 Panorama Interconnect 插件。

STEP 1 | 对于 Panorama 控制器，请登录到 Panorama Web 界面。

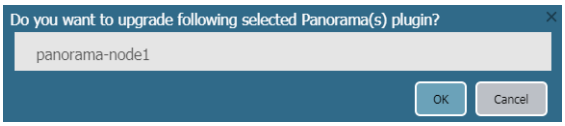
STEP 2 | 在 Panorama 控制器上升级 Panorama Interconnect 插件。

1. 选择 **Panorama** > **Plugins**（插件），然后搜索 **`Interconnect`**。
2. **Download**（下载）并 **Install**（安装）新的 Interconnect 插件版本。安装结束后，将出现一条通知提示。
3. 验证 **Dashboard**（仪表盘）是否显示新安装的 Interconnect 插件版本。

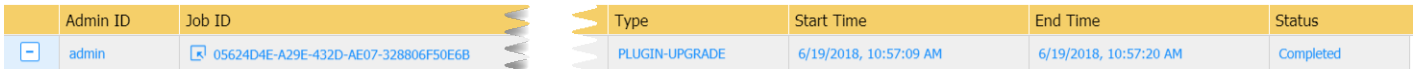


STEP 3 | 在 Panorama 节点上升级 Panorama Interconnect 插件。

1. 选择 **Panorama** > **Interconnect** > **Panorama Nodes**（**Panorama**节点），再选择一个或多个 Panorama 节点，然后 **Upgrade Plugin**（升级插件）。
2. 验证所选的 Panorama 节点，并单击 **OK**（确定）开始插件升级。



3. 等待插件升级工作完成（显示 `Completed`）。单击 **Panorama** > **Interconnect** > **Tasks**（任务）以查看工作进度。



4. 升级成功后，选择 **Panorama** > **Interconnect** > **Panorama Nodes**（**Panorama**节点）以验证 **Plugin**（插件）版本是否是适用于所选 Panorama 节点的正确版本。

安装/升级兼容 PAN-OS 版本的 SD-WAN 插件

在何处可以使用？	需要提供什么？
• PAN-OS • SD-WAN	❑ SD-WAN plugin license

必须确保现有的网络基础设施保持最新状态，并能够升级其功能以解锁新功能。SD-WAN 升级指南可帮助网络管理员升级与 SD-WAN 插件版本兼容的 Panorama 管理服务器和 Palo Alto Networks 防火墙。

在开始实际的升级或降级过程之前，必须制定适当的升级或降级计划，这一点很重要。请参阅当前安装的 SD-WAN 插件版本的有效升级和降级路径。

在继续执行升级过程之前，请确保满足以下条件：

- 备份每台设备上的所有配置。
- 请参阅 Panorama 插件兼容性矩阵，以查看适用于 SD-WAN 的 Panorama 插件的每个版本中引入的功能。
- 您具有对 Palo Alto Networks 设备的管理员访问权限。

先决条件

在升级 Panorama HA 对之前，请务必保存配置文件，创建技术支持文件并检查设备的兼容内容发布版本。

备份配置文件

备份当前的配置文件。建议备份当前的 Panorama 和防火墙配置：

- 在升级设备之前备份 Panorama 和防火墙配置。
- 保存并导出 Panorama 和防火墙配置以还原该备份。
- 保存并导出防火墙配置以恢复该备份。

如果升级时遇到问题，可以通过在 Panorama 管理服务器管理的防火墙上加载配置备份，使用这些备份来还原配置。

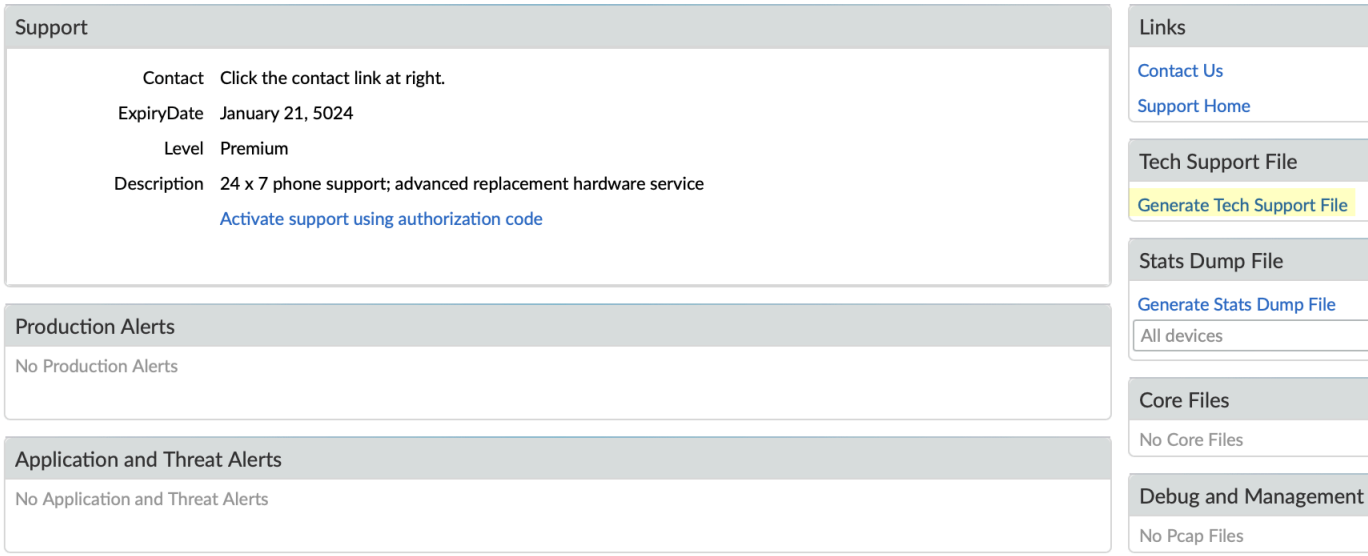
生成技术支持文件

生成用于调试目的的技术支持文件非常重要。

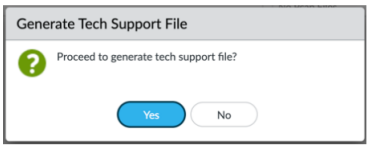
1. 选择 **Device**（设备） > **Support**（支持）并 **Generate Tech Support File**（生成技术支持文件）。

   必须在两个 HA 对上生成技术支持文件以用于调试目的。

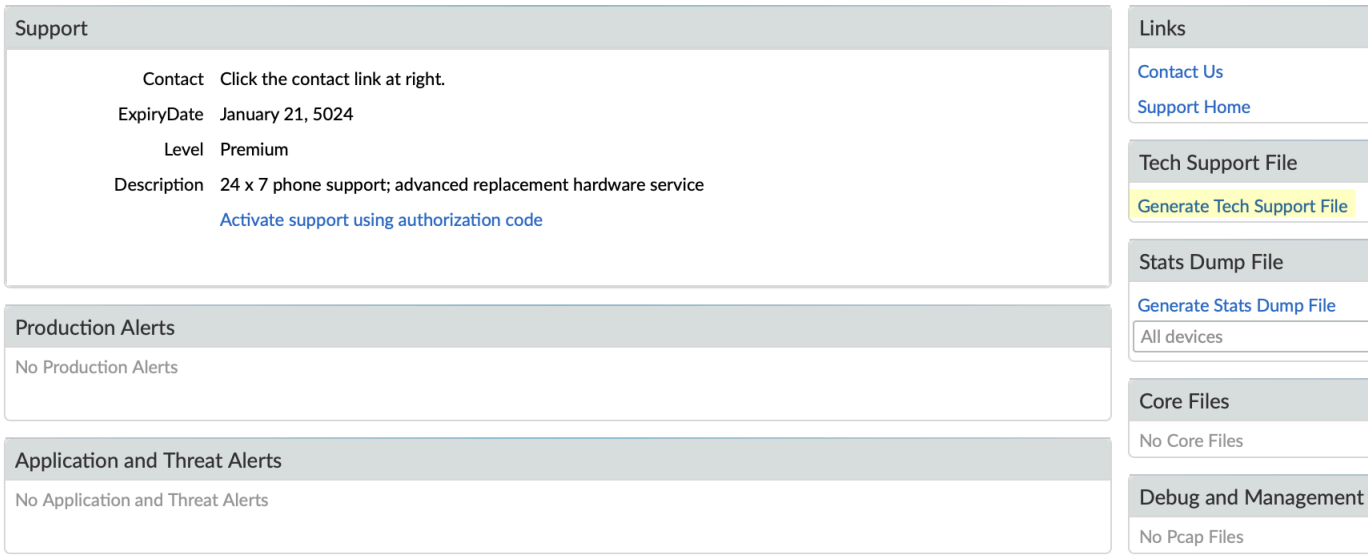
   生成技术支持文件可能需要几分钟时间，并且生成过程所需的具体时间也会有所不同。



2. 当提示生成技术支持文件时，单击 **Yes**（是）。



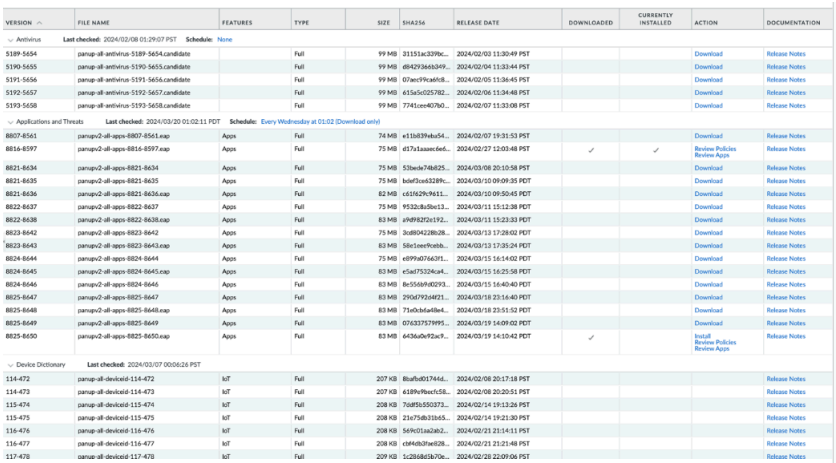
3. 单击 **Download Tech Support File**（下载技术支持文件）以将其保存在防火墙或 Panorama 中。



安装兼容的内容发布版本

确保每个防火墙和 Panorama HA 对都运行最新的内容发行（**Applications and Threats**（应用程序和威胁））版本。

所有防火墙和 *Panorama* 均必须下载并安装相同版本的 ***Applications and Threats***（应用程序和威胁），才能成功升级。



请参阅相应的发行说明，了解您必须为相应的 PAN-OS 版本安装的最低内容发行（例如 **Applications and Threats**（应用程序和威胁））版本。请务必遵循应用程序和威胁内容更新的最佳实践。

运行特定 PAN-OS 版本的防火墙和 Panorama 必须包含与 PAN-OS 版本兼容的最低内容发行（**Applications and Threats**（应用程序和威胁））版本。

使用以下工作流程下载并安装与 PAN-OS 版本兼容的内容发行版本：

1. 对于防火墙，选择 **Device**（设备） > **Dynamic Updates**（动态更新）；对于 Panorama，选择 **Panorama** > **Dynamic Updates**（动态更新），以查看 **Applications and Threats**（应用程序和威胁）的版本信息。
2. 选择 **Check Now**（立即检查）以检索可用的更新列表。
3. 找到并 **Download**（下载）相应的内容发行版本。成功下载内容更新文件后，该内容发行版本的 Action（操作）列中的链接从 **Download**（下载）更改为 **Install**（安装）。
4. 在 Palo Alto Networks 设备上 **Install**（安装）更新。

升级 Panorama 的重要注意事项

以下是在 Panorama 管理服务器上升级 SD-WAN 插件版本时的重要注意事项：

- （仅限 HA 部署）主动和被动 Panorama 必须具有相同的 Panorama 软件和 SD-WAN 插件版本。
- （仅限 HA 部署）在升级之后以及提交或提交全部之前，为 Panorama 和 Palo Alto Networks 下一代防火墙保持相同的 HA 状态，以便将配置更改降至最低。
- 始终确保 Panorama 软件版本高于 PAN-OS 版本。
- 有关 SD-WAN 插件版本的 MongoDB 同步状态，请参阅 MongoDB 与 SD-WAN 数据库集合的同步状态。

- （仅限 *HA* 部署）必须同时升级主动和被动 *Panorama HA* 对。
- 完成 *SD-WAN* 插件升级后，您必须在 *Palo Alto Networks* 设备上通过 *CLI* 命令执行强制提交（在配置模式下）。如果执行全部提交而不是强制提交，那么您将丢失该设备上的所有 *SD-WAN* 配置。

升级完成后，请注意升级后的变化。

SD-WAN 插件的升级和降级路径

在何处可以使用？	需要提供什么？
• PAN-OS • SD-WAN	❑ SD-WAN plugin license

在升级或降级 SD-WAN 插件之前，您必须知道可以从防火墙上当前安装的 SD-WAN 插件版本升级或降级哪些适当的插件版本。

升级和降级注意事项

- 如果您需要升级 ***SD-WAN*** 插件，请勿升级到我们在您当前安装的版本之前发布的版本。

  例如，我们不支持从 *SD-WAN* 插件版本 *3.0.7* 升级到 *SD-WAN* 插件版本 *3.2.0*，因为我们在 *SD-WAN* 插件 *3.0.7* 之前发布了 *SD-WAN* 插件版本 *3.2.0*。

  但是，您可以从任何维护版本升级到同一主要或次要版本内的另一个维护版本。例如，您可以从任何 *SD-WAN 2.2* 升级到任何其他 *SD-WAN 2.2* 插件版本。
- 如果您需要降级 ***SD-WAN*** 插件，请勿降级到我们在您当前安装的版本之后发布的版本。

  例如，我们不支持从 *SD-WAN* 插件版本 *3.2.0* 降级到 *SD-WAN* 插件版本 *3.0.7*，因为我们在 *SD-WAN* 插件 *3.2.0* 之后发布了 *SD-WAN* 插件版本 *3.0.7*。

因此，作为迁移计划的第一步，请始终参考当前安装的 *SD-WAN* 插件版本的有效升级和降级路径。

SD-WAN 插件的升级路径

升级表中的信息解释如下：

- 升级自 — 升级前的当前 SD-WAN 插件版本。
- 升级到的 **SD-WAN** 插件版本 — 您可以从当前的 SD-WAN 插件版本升级到的 SD-WAN 插件版本列表。
- 升级到的 **SD-WAN** 插件版本（推荐） — 我们建议您从当前的 SD-WAN 插件版本升级到的 SD-WAN 插件版本。

例如，您可以从 SD-WAN 插件版本 2.2.1 升级到 SD-WAN 插件版本 2.2.2、2.2.3、2.2.4、2.2.5、2.2.6 及更高的 2.2 版本。但是，在所有有效的 SD-WAN 插件版本（2.2.2、2.2.3、2.2.4、2.2.5、2.2.6 及更高的 2.2 版本）中，我们推荐使用版本 2.2.6。请注意，

如果您想从 SD-WAN 2.2.1 升级到 3.0.7，则不能直接升级。必须先将 SD-WAN 插件从 2.2.1 升级到 2.2.6（推荐版本），然后再升级到 3.0.7。

以下是 SD-WAN 插件版本的升级路径。当您执行 SD-WAN 升级时，目标插件版本会执行迁移过程。

从（当前安装的版本）升级	升级到允许使用的 **SD-WAN** 插件版本	升级到推荐使用的 **SD-WAN** 插件版本
SD-WAN 插件 **2.2** 版本		
2.2.1	2.2.2、2.2.3、2.2.4、2.2.5、2.2.6 及更高的 2.2 版本	2.2.6
2.2.2	2.2.3、2.2.4、2.2.5、2.2.6 及更高的 2.2 版本	2.2.6
2.2.3	2.2.4、2.2.5、2.2.6 及更高的 2.2 版本	2.2.6
2.2.4	2.2.5、2.2.6 及更高的 2.2 版本	2.2.6
2.2.5	2.2.6 及更高的 2.2 版本	2.2.6
2.2.6	• 3.0.7 及更高的 3.0 版本 • 3.1.3 及更高的 3.1 版本 • 3.2.1 及更高的 3.2 版本 • 3.3.0 及更高的 3.3 版本	2.2.6
SD-WAN 插件 **3.0** 版本		
3.0.0	3.0.5	—
3.0.1	3.0.5	—
3.0.2	3.0.5	—
3.0.3	3.0.5	—
3.0.4	3.0.5	—
3.0.5	• 3.0.6 • 3.0.7 及更高的 3.0 版本 • 3.1.0-hf	3.0.7-h2、3.1.3、3.2.1、3.3.0

从（当前安装的版本）升级	升级到允许使用的 **SD-WAN** 插件版本	升级到推荐使用的 **SD-WAN** 插件版本
	• 3.1.1、3.1.3 及更高的 3.1 版本 • 3.2.0 • 3.2.1 及更高的 3.2 版本 • 3.3.0 及更高的 3.3 版本	
3.0.6	• 3.0.7 及更高的 3.0 版本 • 3.1.3 及更高的 3.1 版本 • 3.2.0 • 3.2.1 及更高的 3.2 版本 • 3.3.0 及更高的 3.3 版本	3.0.7-h2、3.1.3、3.2.1、3.3.0
3.0.7	• 3.1.3 及更高的 3.1 版本 • 3.2.1 及更高的 3.2 版本 • 3.3.0 及更高的 3.3 版本	3.1.3、3.2.1、3.3.0
SD-WAN 插件 **3.1** 版本		
3.1.0	• 3.1.1 • 3.1.3 及更高的 3.1 版本 • 3.2.0 • 3.2.1 及更高的 3.2 版本 • 3.3.0 及更高的 3.3 版本	3.1.3、3.2.1、3.3.0
3.1.1	• 3.1.3 及更高的 3.1 版本 • 3.2.0 • 3.2.1 及更高的 3.2 版本 • 3.3.0 及更高的 3.3 版本	3.1.3、3.2.1、3.3.0
3.1.2	• 3.1.3 及更高的 3.1 版本 • 3.2.0 • 3.2.1 及更高的 3.2 版本 • 3.3.0 及更高的 3.3 版本	3.1.3、3.2.1、3.3.0
3.1.3	• 3.2.1 及更高的 3.2 版本 • 3.3.0 及更高的 3.3 版本	3.2.1 和 3.3.0
SD-WAN 插件 **3.2** 版本		

从（当前安装的版本）升级	升级到允许使用的 **SD-WAN** 插件版本	升级到推荐使用的 **SD-WAN** 插件版本
3.2.0	• 3.2.1 及更高的 3.2 版本 • 3.3.0 及更高的 3.3 版本	3.2.1 和 3.3.0
3.2.1	3.3.0 及更高的 3.3 版本	3.3.0

SD-WAN 插件的降级路径

降级表中的信息解释如下：

- 降级自 — 这是降级前的当前 SD-WAN 插件版本。
- 降级到的 **SD-WAN** 插件版本 — 这是您可以从当前的 SD-WAN 插件版本降级到的 SD-WAN 插件版本列表。
- 降级到的 **SD-WAN** 插件版本（推荐）— 这是我们建议您从当前的 SD-WAN 插件版本降级到的 SD-WAN 插件版本。

以下是 SD-WAN 插件版本的降级路径。当您执行 SD-WAN 降级时，当前插件版本会执行迁移过程。

从（当前安装的版本）降级	降级到允许使用的 **SD-WAN** 插件版本
2.2.2、2.2.3、2.2.4、2.2.5 和 2.2.6	2.2.1
2.2.3、2.2.4、2.2.5 和 2.2.6	2.2.2
2.2.4、2.2.5 和 2.2.6	2.2.3
2.2.5 和 2.2.6	2.2.4
2.2.6	2.2.5
3.0.7、3.1.3、3.2.1 和 3.3.0	2.2.6
3.0.5	3.0.0、3.0.1、3.0.2、3.0.3 和 3.0.4
3.0.6、3.0.7、3.1.0-hf、3.1.1、3.1.3、3.2.0、3.2.1 和 3.3.0	3.0.5
3.0.7、3.1.3、3.2.0、3.2.1 和 3.3.0	3.0.6
3.1.3、3.2.1 和 3.3.0	3.0.7
3.1.1、3.1.3、3.2.0、3.2.1 和 3.3.0	3.1.0
3.1.3、3.2.0、3.2.1 和 3.3.0	3.1.1

从（当前安装的版本）降级	降级到允许使用的 **SD-WAN** 插件版本
3.1.3、3.2.0、3.2.1 和 3.3.0	3.1.2
3.2.1 和 3.3.0	3.1.3 和 3.2.0

安装 SD-WAN 插件

在您的 Panorama™ 管理服务器和防火墙（使用 SD-WAN）上安装 SD-WAN 插件版本 。

请参阅 Palo Alto Networks Panorama 插件兼容性矩阵 ， 并查看目标 SD-WAN 插件版本所需的最低 PAN-OS 版本。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 在 Panorama 上安装 SD-WAN 插件版本。

如果 Panorama 为高可用性 (HA) 配置， 则在 Panorama HA 对等设备上重复这个步骤。

1. 选择 **Panorama** > **Plugin**（插件）并 **Check Now**（立即检查）最新的 **sd_wan** 插件版本。
2. **Download**（下载）并 **Install**（安装）最新的 SD-WAN 插件版本。

STEP 3 | 成功安装新插件版本后， 查看 Panorama **Dashboard**（仪表板）并在 General Information（常规信息）小部件中验证 SD-WAN 插件 版本是否显示您已安装的 SD-WAN 插件版本。

利用 SD-WAN 插件升级 Panorama 高可用性对（主动/被动）

在何处可以使用？	需要提供什么？
• PAN-OS • SD-WAN	❑ SD-WAN plugin license

根据 Panorama 管理服务器正在运行的 SD-WAN 插件版本遵循升级路径。

Panorama 运行的 **SD-WAN** 插件版本	按照步骤操作
1.0.x	Panorama HA 对：将 SD-WAN 插件 1.0.4 升级到 2.2.6 版本
2.1.x	Panorama HA 对：将 SD-WAN 插件 2.1.x 升级到 2.2.6 版本
2.2.6	Panorama HA 对：将 SD-WAN 插件 2.2.6 升级到 3.0.7 版本

Panorama HA 对：将 SD-WAN 插件 1.0.4 升级到 2.2.6 版本

当您的 Panorama 安装了 1.0.x 到 2.2.x 之间的任何 SD-WAN 插件版本时，如果要升级 SD-WAN 插件版本，则必须先升级到 SD-WAN 插件版本 2.2.6（而不是任何中间版本）。因为 SD-WAN 2.2.6 版本包含新功能、错误修复程序、性能改进和增强功能。

建议始终确保 Panorama 软件版本高于 PAN-OS 版本。例如，如果 Panorama 版本为 10.1.9，那么 PAN-OS 版本可以是更早的 PAN-OS 10.1.9 版本。

在开始升级过程之前，请阅读升级 Panorama 的重要注意事项。

按照相同的顺序使用以下工作流程升级具有 SD-WAN 2.2.6 插件版本的 Panorama HA 对。

STEP 1 | 升级 Panorama 管理服务器版本。

1. 从 Panorama 9.1.x 开始，在主动和被动 Panorama 上下载并安装 Panorama 10.0.7-h3。
2. 从 Panorama 10.0.7-h3 开始，在主动和被动 Panorama 上下载并安装最新的 Panorama 10.1 版本。
3. 将 Panorama 升级到最新的 10.1 版本后，检查主动 Panorama 是否保持为主动状态，被动 Panorama 是否保持为被动状态。如果 HA 状态没有变化，则升级成功。否则，您需要执行强制切换，以保持升级前的 HA 对状态。

   要执行强制切换，请按照相同的顺序从当前的主动 HA 对等设备执行以下 CLI 命令。

   ```
   admin > request high-availbility state suspend
   ```

   ```
   admin > request high-availbility state functional
   ```

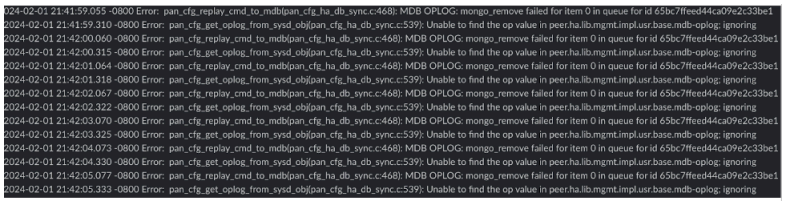
   ```
   admin@sdwan2-panorama-2(secondary-active)> request high-availability state suspend

   Successfully changed HA state to suspended
   admin@sdwan2-panorama-2(secondary-suspended)> request high-availability state functional

   Successfully changed HA state to functional
   admin@sdwan2-panorama-2(secondary-initial)>
   admin@sdwan2-panorama-2(secondary-passive)>
   admin@sdwan2-panorama-2(secondary-passive)>
   admin@sdwan2-panorama-2(secondary-passive)>
   ```


STEP 2 | 监视 *configd* 日志。

（在管理员模式下）在将 SD-WAN 插件升级到 2.2.6 之前，请开始监视两个 Panorama HA 对上的 *configd* 日志。

```
admin> tail follow yes mp-log configd.log
```

如果在执行 **tail follow yes mp-log configd.log** 命令时看到以下错误消息，则表示主动和被动 Panorama 的 Mongo DB 不同步。



要解决此问题：

1. （在管理员模式下）在主动和被动 Panorama 上删除整个数据库 *pan_oplog*。

   ```
   admin > debug mongo drop database pan_oplog instance mdb
   ```

2. （在管理员模式下）在主动和被动 Panorama 上重新启动 *configd*。

   ```
   admin > debug software restart process configd
   ```

重新启动 *configd* 后，刷新相应的 Web 界面和命令行界面。重新启动后，您将不会在任何提交过程中看到 *mongo pan_oplog* 错误。

我们建议您在整个升级过程中监视 *configd* 日志。

STEP 3 | 在主动和被动 Panorama 上下载并安装 SD-WAN 插件版本 2.2.6。

STEP 4 | （在管理员模式下）在主动和被动 Panorama 上删除 SD-WAN 集合。

```
admin > debug mongo drop database pl_sd_wan instance mdb
```

```
admin@sdwan-hw-panorama(secondary-passive)> debug mongo drop database pl_sd_wan instance mdb

No collection given, drop the whole database pl_sd_wan instead
MongoDB shell version v3.6.19
connecting to: mongodb://127.0.0.1:27017/pl_sd_wan?gssapiServiceName=mongodb
Implicit session: session { "id" : UUID("c6dcb502-4582-4a0f-90d7-19a0becf8773") }
MongoDB server version: 3.6.19
{ "dropped" : "pl_sd_wan", "ok" : 1 }
```

这是同步 SD-WAN Mongo DB 集合所必需执行的步骤。

STEP 5 | （在配置模式下）强制提交来自主动 Panorama 的更改。

```
Number of failed attempts since last successful login: 0


admin@sdwan2_panorama(primary-active)> configure
Entering configuration mode
[edit]
admin@sdwan2_panorama(primary-active)# commit force


Commit job 5307 is in progress. Use Ctrl+C to return to command prompt
...11%.77%.80%....91%.....100%
sd_wan plugin validation: Config valid
Configuration committed successfully
Disk 'A' on log collector 0007AQA994 in group lc-group1 has a size of zero bytes

[edit]
admin@sdwan2_panorama(primary-active)#
```

完成 SD-WAN 插件升级后，您必须在 Palo Alto Networks 设备上通过 CLI 命令执行强制提交（在配置模式下）。如果执行全部提交而不是强制提交，那么您将丢失该设备上的所有 SD-WAN 配置。

STEP 6 | 执行 Panorama HA 升级后检查以下内容。

1. 首先对分支设备执行选择性推送，然后对主动 Panorama 中的中心设备执行选择性推送。
2. 选择 **Panorama** > **Managed Devices**（托管设备） > **Summary**（摘要），并在设备摘要页面下验证主动和被动 Panorama 上的设备组和模板是否同步。
3. 验证 SD-WAN 配置（例如隧道、BGP、密钥 ID 和流量）是否符合预期。

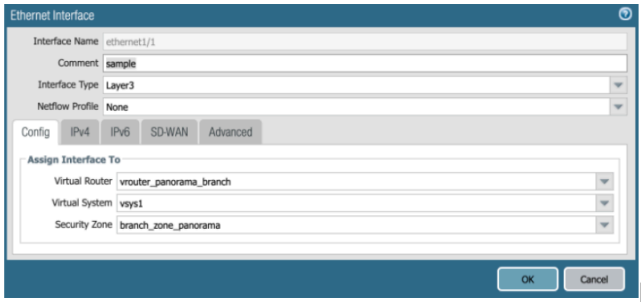
成功升级 *Panorama HA* 对后，密钥 *ID*、*PSK*、*IP* 缓存、*IPSec* 隧道缓存和子网缓存将被刷新，这不会影响 *SD-WAN* 的功能。

STEP 7 | （推荐）升级连接的防火墙。

Panorama HA 对升级成功后，可以逐一升级连接的中心和分支设备，先从分支防火墙开始升级，然后升级中心防火墙（分支和中心防火墙可以是独立防火墙或 HA 对）。

我们建议您在升级每个防火墙后检查 *SD-WAN* 配置和功能。

1. 通过修改或添加模板上接口的注释，对所有模板进行微小更改，然后 **Commit**（提交）提交并 **Push to Devices**（推送到设备）。这只是一个验证活动，旨在确保配置良好且升级正常。



2. 检查 SD-WAN 配置和功能。
3. 逐个升级分支防火墙，直至所有分支防火墙都升级完毕。
4. 请先按照以下步骤升级分支防火墙。
   1. 开始将一对分支 HA 或独立设备从 Panorama 版本 9.1.x 升级到 10.0.7-h3，然后升级到最新的 Panorama 10.1 版本。
   2. 从执行升级的主动 Panorama 中的特定防火墙模板对接口的注释进行微小更改，**Commit**（提交）并 **Push to Devices**（推送到设备）。完成 **Commit All**（全部提交）后，检查 SD-WAN 配置和功能。这只是一个验证活动，旨在确保配置良好且在防火墙升级后升级正常。
5. 按照以下步骤升级中心防火墙。先完成分支防火墙的升级，然后开始升级中心防火墙，这一点很重要。
   1. 开始将一对中心 HA 或独立设备从 Panorama 版本 9.1.x 升级到 10.0.7-h3，然后升级到最新的 Panorama 10.1 版本。
   2. 从执行升级的主动 Panorama 中的特定防火墙模板对接口的注释进行微小更改，**Commit**（提交）并 **Push to Devices**（推送到设备）。完成 **Commit All**（全部提交）后，检查 SD-WAN 配置和功能。

      这只是一个验证活动，旨在确保配置良好且在防火墙升级后升级正常。
6. 选择 **Panorama** > **Managed Devices**（托管设备） > **Summary**（摘要），并在设备摘要页面下验证主动和被动 Panorama 上的设备组和模板是否同步。
7. 升级完成后，请注意升级后的变化。

Panorama HA 对：将 SD-WAN 插件 2.1.x 升级到 2.2.6 版本

当您的 Panorama 安装了 SD-WAN 插件版本 2.1.x 时，如果要升级 SD-WAN 插件版本，则必须先升级到 SD-WAN 插件版本 2.2.6（而不是任何中间版本）。因为 SD-WAN 2.2.6 版本包含新功能、错误修复程序、性能改进和增强功能。

建议始终确保 Panorama 软件版本高于 PAN-OS 版本。例如，如果 Panorama 版本为 10.1.9，那么 PAN-OS 版本可以是更早的 PAN-OS 10.1.9 版本。

在开始升级过程之前，请阅读升级 Panorama 的重要注意事项。

按照相同的顺序使用以下工作流程升级具有 SD-WAN 2.2.6 插件版本的 Panorama HA 对。

STEP 1 | 升级 Panorama 管理服务器版本。

1. 在主动和被动 Panorama 上下载并安装最新的 Panorama 10.1 版本。
2. 将 Panorama 升级到最新的 10.1 版本后，检查主动 Panorama 是否保持为主动状态，被动 Panorama 是否保持为被动状态。如果 HA 状态没有变化，则升级成功。否则，您需要执行强制切换，以保持升级前的 HA 对状态。

   要执行强制切换，请按照相同的顺序从当前的主动 HA 对等设备执行以下 CLI 命令。

   ```
   admin > request high-availbility state suspend
   ```

   ```
   admin > request high-availbility state functional
   ```

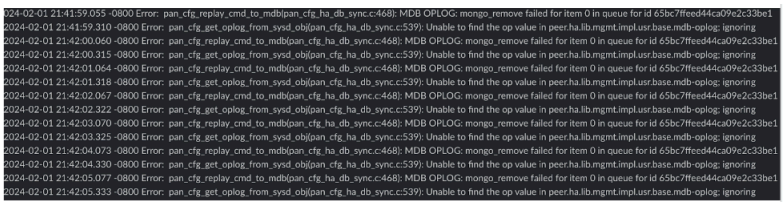
   ```
   admin@sdwan2-panorama-2(secondary-active)> request high-availability state suspend

   Successfully changed HA state to suspended
   admin@sdwan2-panorama-2(secondary-suspended)> request high-availability state functional

   Successfully changed HA state to functional
   admin@sdwan2-panorama-2(secondary-initial)>
   admin@sdwan2-panorama-2(secondary-passive)>
   admin@sdwan2-panorama-2(secondary-passive)>
   admin@sdwan2-panorama-2(secondary-passive)>
   ```


STEP 2 | 监视 *configd* 日志。

（在管理员模式下）在将 SD-WAN 插件升级到 2.2.6 之前，请开始监视两个 Panorama HA 对上的 *configd* 日志。

```
admin> tail follow yes mp-log configd.log
```

如果在执行 `admin > tail follow yes mp-log configd.log` 命令时看到以下错误消息，则表示主动和被动 Panorama 的 Mongo DB 不同步。



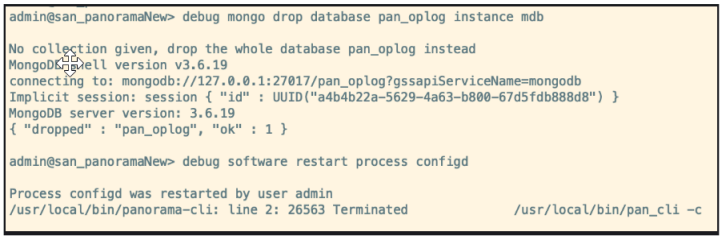
要解决此问题：

1. （在管理员模式下）在主动和被动 Panorama 上删除整个数据库 *pan_oplog*。

   ```
   admin > debug mongo drop database pan_oplog instance mdb
   ```

2. （在管理员模式下）在主动和被动 Panorama 上重新启动 *configd*。

   ```
   admin > debug software restart process configd
   ```



重新启动 *configd* 后，刷新相应的 Web 界面和命令行界面。重新启动后，您将不会在任何提交过程中看到 *mongo pan_oplog* 错误。

我们建议您在整个升级过程中监视 *configd* 日志。

STEP 3 | 在主动和被动 Panorama 上下载并安装 SD-WAN 插件版本 2.2.6。

STEP 4 | （在管理员模式下）在主动和被动 Panorama 上删除 SD-WAN 集合。

```
admin > debug mongo drop database pl_sd_wan instance mdb
```

```
admin@sdwan-hw-panorama(secondary-passive)> debug mongo drop database pl_sd_wan instance mdb

No collection given, drop the whole database pl_sd_wan instead
MongoDB shell version v3.6.19
connecting to: mongodb://127.0.0.1:27017/pl_sd_wan?gssapiServiceName=mongodb
Implicit session: session { "id" : UUID("c6dcb502-4582-4a0f-90d7-19a0becf8773") }
MongoDB server version: 3.6.19
{ "dropped" : "pl_sd_wan", "ok" : 1 }
```

这是同步 SD-WAN Mongo DB 集合所必需执行的步骤。

STEP 5 | （在配置模式下）强制提交来自主动 Panorama 的更改。

```
Number of failed attempts since last successful login: 0


admin@sdwan2_panorama(primary-active)> configure
Entering configuration mode
[edit]
admin@sdwan2_panorama(primary-active)# commit force


Commit job 5307 is in progress. Use Ctrl+C to return to command prompt
...11%.77%.80%....91%.....100%
sd_wan plugin validation: Config valid
Configuration committed successfully
Disk 'A' on log collector 0007AQA994 in group lc-group1 has a size of zero bytes

[edit]
admin@sdwan2_panorama(primary-active)#
```

完成 SD-WAN 插件升级后，您必须在 Palo Alto Networks 设备上通过 CLI 命令执行强制提交（在配置模式下）。如果执行全部提交而不是强制提交，那么您将丢失该设备上的所有 SD-WAN 配置。

STEP 6 | 执行 Panorama HA 升级后检查以下内容。

1. 首先对分支设备执行选择性推送，然后对主动 Panorama 中的中心设备执行选择性推送。
2. 选择 **Panorama** > **Managed Devices**（托管设备） > **Summary**（摘要），并在设备摘要页面下验证主动和被动 Panorama 上的设备组和模板是否同步。
3. 验证 SD-WAN 配置（例如隧道、BGP、密钥 ID 和流量）是否符合预期。

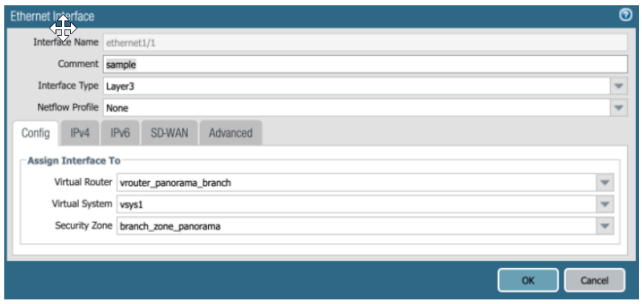
成功升级 *Panorama HA* 对后，密钥 *ID*、*PSK*、*IP* 缓存、*IPSec* 隧道缓存和子网缓存将被刷新，这不会影响 *SD-WAN* 的功能。

STEP 7 | （推荐）升级连接的防火墙。

Panorama HA 对升级成功后，可以逐一升级连接的中心和分支设备，先从分支防火墙开始升级，然后升级中心防火墙（分支和中心防火墙可以是独立防火墙或 HA 对）。

我们建议您在升级每个防火墙后检查 *SD-WAN* 配置和功能。

1. 通过修改或添加模板上接口的注释，对所有模板进行微小更改，然后 **Commit**（提交）提交并 **Push to Devices**（推送到设备）。这只是一个验证活动，旨在确保配置良好且升级正常。



2. 检查 SD-WAN 配置和功能。
3. 逐个升级分支防火墙，直至所有分支防火墙都升级完毕。
4. 请先按照以下步骤升级分支防火墙。
   1. 开始将一对分支 HA 或独立设备从 Panorama 版本 9.1.x 升级到 10.0.7-h3，然后升级到最新的 Panorama 10.1 版本。
   2. 从执行升级的主动 Panorama 中的特定防火墙模板对接口的注释进行微小更改，**Commit**（提交）并 **Push to Devices**（推送到设备）。完成 **Commit All**（全部提交）后，检查 SD-WAN 配置和功能。这只是一个验证活动，旨在确保配置良好且在防火墙升级后升级正常。
5. 按照以下步骤升级中心防火墙。先完成分支防火墙的升级，然后开始升级中心防火墙，这一点很重要。
   1. 开始将一对中心 HA 或独立设备从 Panorama 版本 9.1.x 升级到 10.0.7-h3，然后升级到最新的 Panorama 10.1 版本。
   2. 从执行升级的主动 Panorama 中的特定防火墙模板对接口的注释进行微小更改，**Commit**（提交）并**Push to Devices**（推送到设备）。完成 **Commit All**（全部提交）后，检查 SD-WAN 配置和功能。

      这只是一个验证活动，旨在确保配置良好且在防火墙升级后升级正常。
6. 选择 **Panorama** > **Managed Devices**（托管设备） > **Summary**（摘要），并在设备摘要页面下验证主动和被动 Panorama 上的设备组和模板是否同步。
7. 升级完成后，请注意升级后的变化。

Panorama HA 对：将 SD-WAN 插 2.2.6 升级到 3.0.7 版本

建议始终确保 Panorama 软件版本高于 PAN-OS 版本。例如，如果 Panorama 版本为 10.1.9，那么 PAN-OS 版本可以是更早的 PAN-OS 10.1.9 版本。

在开始升级过程之前，请阅读升级 Panorama 的重要注意事项。

STEP 1 | 下载 SD-WAN 插件 3.0.7，并删除 Panorama HA 对上下载的所有 3.0.x 插件（SD-WAN 插件版本 3.0.7 除外）。

STEP 2 | 将 Panorama 软件版本从最新的 10.1 版本升级到最新的 10.2 版本。成功升级到最新的 10.2 版本后，系统将自动安装 SD-WAN 插件 3.0.7。

要验证 Panorama 上是否安装了 SD-WAN 插件 3.0.7 版本，请在 Panorama **Dashboard**（仪表板）中查看 **General Information**（常规信息）。

STEP 3 | 升级完成后，检查 SD-WAN 配置及其功能是否符合预期。

STEP 4 | 在 Palo Alto Networks 设备上通过 CLI 命令执行强制提交（在配置模式下）。如果执行全部提交而不是强制提交，那么您将丢失该设备上的所有 SD-WAN 配置。

STEP 5 | （推荐）逐个升级连接的设备，先从分支对开始，然后升级中心对。

STEP 6 | 设备升级后，请检查 SD-WAN 配置及其功能。

STEP 7 | 升级完成后，请注意升级后的变化。

利用 SD-WAN 插件升级独立 Panorama

在何处可以使用？	需要提供什么？
• PAN-OS • SD-WAN	❑ SD-WAN plugin license

在继续升级过程之前，请先完成先决条件。

根据 Panorama 管理服务器正在运行的 SD-WAN 插件版本遵循升级路径。

Panorama 运行的 SD-WAN 插件版本	按照步骤操作
1.0.x	独立 Panorama：将 SD-WAN 插件 1.0.4 升级到 2.2.6 版本
2.1.x	独立 Panorama：将 SD-WAN 插件 2.1.x 升级到 2.2.6 版本
2.2.6	独立 Panorama：将 SD-WAN 插件 2.2.6 升级到 3.0.7 版本

独立 Panorama：将 SD-WAN 插件 1.0.4 升级到 2.2.6 版本

建议始终确保 Panorama 软件版本高于 PAN-OS 版本。例如，如果 Panorama 版本为 10.1.9，那么 PAN-OS 版本可以是更早的 PAN-OS 10.1.9 版本。

在开始升级过程之前，请阅读升级 Panorama 的重要注意事项。

STEP 1 | 下载并安装 Panorama 软件版本 10.0.7-h3。

STEP 2 | 从 Panorama 10.0.7-h3 下载并安装最新的 Panorama 10.1 版本。

STEP 3 | 在 Panorama 上下载并安装 SD-WAN 插件版本 2.2.6。

STEP 4 | （在配置模式下）强制提交来自主动 Panorama 的更改。

完成 SD-WAN 插件升级后，您必须在 Palo Alto Networks 设备上通过 CLI 执行强制提交（在配置模式下）。如果执行全部提交而不是强制提交，那么您将丢失该设备上的所有 SD-WAN 配置。

```
Number of failed attempts since last successful login: 0


admin@sdwan2_panorama(primary-active)> configure
Entering configuration mode
[edit]
admin@sdwan2_panorama(primary-active)# commit force


Commit job 5307 is in progress. Use Ctrl+C to return to command prompt
...11%.77%.80%....91%.....100%
sd_wan plugin validation: Config valid
Configuration committed successfully
Disk 'A' on log collector 0007AQA994 in group lc-group1 has a size of zero bytes

[edit]
admin@sdwan2_panorama(primary-active)#
```

STEP 5 | 升级独立 Panorama 后，请检查以下内容。

1. 从 Panorama 推送到设备。
2. 选择 **Panorama** > **Managed Devices**（托管设备） > **Summary**（摘要），并在设备摘要页面下验证主动和被动 Panorama 上的设备组和模板是否同步。

3. 验证 SD-WAN 配置（例如隧道、BGP、密钥 ID 和流量）是否符合预期。

成功升级 *Panorama HA* 对后，密钥 *ID*、*PSK*、*IP* 缓存、*IPSec* 隧道缓存和子网缓存将被刷新，这不会影响 *SD-WAN* 的功能。

STEP 6 | Panorama 升级成功后，如果需要，可以逐个升级所有连接的设备，先从分支对/独立设备开始，然后升级中心对/独立设备。建议在每次升级后检查 SD-WAN 配置和功能。

STEP 7 | 升级完成后，请注意升级后的变化。

独立 Panorama：将 SD-WAN 插件 2.1.x 升级到 2.2.6 版本

建议始终确保 Panorama 软件版本高于 PAN-OS 版本。例如，如果 Panorama 版本为 10.1.9，那么 PAN-OS 版本可以是更早的 PAN-OS 10.1.9 版本。

在开始升级过程之前，请阅读升级 Panorama 的重要注意事项。

STEP 1 | 下载并安装最新的 Panorama 10.1 版本。

STEP 2 | 在 Panorama 上下载并安装 SD-WAN 插件版本 2.2.6。

STEP 3 | （在配置模式下）强制提交来自主动 Panorama 的更改。

完成 SD-WAN 插件升级后，您必须在 Palo Alto Networks 设备上通过 CLI 执行强制提交（在配置模式下）。如果执行全部提交而不是强制提交，那么您将丢失该设备上的所有 SD-WAN 配置。

```
Number of failed attempts since last successful login: 0


admin@sdwan2_panorama(primary-active)> configure
Entering configuration mode
[edit]
admin@sdwan2_panorama(primary-active)# commit force


Commit job 5307 is in progress. Use Ctrl+C to return to command prompt
...11%.77%.80%....91%.....100%
sd_wan plugin validation: Config valid
Configuration committed successfully
Disk 'A' on log collector 0007AQA994 in group lc-group1 has a size of zero bytes

[edit]
admin@sdwan2_panorama(primary-active)#
```

STEP 4 | 升级独立 Panorama 后，请检查以下内容。

1. 从 Panorama 推送到设备。
2. 选择 **Panorama** > **Managed Devices**（托管设备） > **Summary**（摘要），并在设备摘要页面下验证主动和被动 Panorama 上的设备组和模板是否同步。

3. 验证 SD-WAN 配置（例如隧道、BGP、密钥 ID 和流量）是否符合预期。

成功升级 *Panorama HA* 对后，密钥 *ID*、*PSK*、*IP* 缓存、*IPSec* 隧道缓存和子网缓存将被刷新，这不会影响 *SD-WAN* 的功能。

STEP 5 | Panorama 升级成功后，如果需要，可以逐个升级所有连接的设备，先从分支对/独立设备开始，然后升级中心对/独立设备。建议在每次升级后检查 SD-WAN 配置和功能。

STEP 6 | 升级完成后，请注意升级后的变化。

独立 Panorama：将 SD-WAN 插 2.2.6 升级到 3.0.7 版本

建议始终确保 Panorama 软件版本高于 PAN-OS 版本。例如，如果 Panorama 版本为 10.1.9，那么 PAN-OS 版本可以是更早的 PAN-OS 10.1.9 版本。

在开始升级过程之前，请阅读升级 Panorama 的重要注意事项。

STEP 1 | 下载并安装最新的 Panorama 10.1 版本。

STEP 2 | 在 Panorama 上下载并安装 SD-WAN 插件版本 2.2.6。

STEP 3 | （在配置模式下）强制提交来自主动 Panorama 的更改。

完成 SD-WAN 插件升级后，您必须在 Palo Alto Networks 设备上通过 CLI 执行强制提交（在配置模式下）。如果执行全部提交而不是强制提交，那么您将丢失该设备上的所有 SD-WAN 配置。

```
Number of failed attempts since last successful login: 0


admin@sdwan2_panorama(primary-active)> configure
Entering configuration mode
[edit]
admin@sdwan2_panorama(primary-active)# commit force


Commit job 5307 is in progress. Use Ctrl+C to return to command prompt
...11%.77%.80%....91%.....100%
sd_wan plugin validation: Config valid
Configuration committed successfully
Disk 'A' on log collector 0007AQA994 in group lc-group1 has a size of zero bytes

[edit]
admin@sdwan2_panorama(primary-active)#
```

STEP 4 | 升级独立 Panorama 后，请检查以下内容。

1. 从 Panorama 推送到设备。
2. 选择 **Panorama** > **Managed Devices**（托管设备） > **Summary**（摘要），并在设备摘要页面下验证主动和被动 Panorama 上的设备组和模板是否同步。

3. 验证 SD-WAN 配置（例如隧道、BGP、密钥 ID 和流量）是否符合预期。

成功升级 *Panorama HA* 对后，密钥 *ID*、*PSK*、*IP* 缓存、*IPSec* 隧道缓存和子网缓存将被刷新，这不会影响 *SD-WAN* 的功能。

STEP 5 | Panorama 升级成功后，如果需要，可以逐个升级所有连接的设备，先从分支对/独立设备开始，然后升级中心对/独立设备。建议在每次升级后检查 SD-WAN 配置和功能。

STEP 6 | 升级完成后，请注意升级后的变化。

升级后需要注意的变化

在何处可以使用？	需要提供什么？
• PAN-OS • SD-WAN	❑ SD-WAN plugin license

升级后，必须先进行以下检查，然后再将更改提交给 *Panorama*：

- 验证 *VPN* 集群中的每个 *SD-WAN* 设备是否配置了 ***Router Name***（路由器名称）（***Panorama*** > ***SD-WAN*** > ***Devices***（设备））。*SD-WAN* 插件 *3.1.0* 及更高版本支持 ***Router Name***（路由器名称）配置。
- 验证 *VPN* 集群中的每个 *SD-WAN* 设备是否启用了 ***BGP***（***Panorama*** > ***SD-WAN*** > ***Devices***（设备））。确保启用了升级前配置的相同 *BGP* 地址系列（***IPv4 BGP*** 或 ***IPv6 BGP***）。*SD-WAN* 插件 *3.1.1* 及更高版本支持 *IPv6*。因此，只有当您从 *SD-WAN 3.1.1* 或更高版本升级时，升级后的插件才会包含 *IPv6* 选项。
- 验证是否启用了升级前配置的相同 *VPN* 身份验证类型（***Pre Shared Key***（预共享密钥）或 ***Certificate***（证书））（***Panorama*** > ***SD-WAN*** > ***Devices***（设备）> ***VPN Tunnel***（***VPN*** 隧道））。*SD-WAN* 插件 *3.2.0* 及更高版本支持证书身份验证类型。因此，只有当您从 *SD-WAN* 插件 *3.2.0* 或更高版本升级时，升级后的插件才会包含 *VPN* 身份验证类型（***Pre Shared Key***（预共享密钥）或 ***Certificate***（证书））。

（在 Panorama HA 对或独立 Panorama 上）升级后，可以看到以下变化：

- 对于已添加的 SD-WAN 设备，**Panorama** > **SD-WAN** > **Devices**（设备）中不会再显示区域选项卡。因此，您必须在现有区域和预定义区域（从区域到分支、从区域到中心、从区域到 Internet 以及从区域到内部）之间创建安全策略规则。
- 在全网状 VPN 集群中，序列号较低的分支将用作 IKE 发起方。如果是上游 NAT，NAT 设备上应同时存在入站和出站 NAT，不存在入站 NAT 时将会看到 PLUG-15276。

MongoDB 与 SD-WAN 数据库集合的同步状态

使用某些 SD-WAN 插件版本时，MongoDB 中的 SD-WAN 数据库集合可能不同步，这是一个已知问题。因此，从任何早期版本升级到 SD-WAN 插件版本 2.2.6 时，可能需要在升级过程中执行其他步骤。

下表列出了使用各 SD-WAN 插件版本（已经过测试）时 SD-WAN MongoDB 集合是否同步的状态。

序列号	使用 **SD-WAN** 插件版本的兼容 **PAN-OS** 软件版本	**SD-WAN** 插件版本	**Mongo** 端口	**Panorama HA** 上 **Mongo** 下的 **SD-WAN** 集合
1	10.1.6	2.1.2	31377	不同步
2	10.1.x	2.1.2	31377	不同步
3	10.1.x	2.2.6	27017	同步
4	10.2.7-h3	3.0.7	27017	同步

用于升级的 CLI 命令

- 使用 CLI 命令执行升级任务

使用 CLI 命令执行升级任务

使用以下 CLI 命令执行升级任务。

如果您要...	使用...
检查防火墙的当前版本	
• 检查防火墙软件和内容的当前版本。	**show system info**
访问可用的动态更新并升级防火墙的内容版本	
• 直接从 Palo Alto Networks 服务器检查动态更新的可用内容版本。	请求内容升级检查
• 直接从防火墙检查动态更新的可用内容版本。	请求内容升级信息
• 将内容版本直接下载到防火墙。	请求内容升级下载 **<content version>**
• 安装内容版本。	请求内容升级安装 **<content version>**

如果您要...	使用...
访问可用的软件版本并升级防火墙	
• 检查可供下载的可用软件版本。	请求系统软件信息
• 检查软件的首选版本。 （PAN-OS 11.1.3 及更高版本）	请求首选系统软件信息
• 检查软件的基础版本。 （PAN-OS 11.1.3 及更高版本）	请求基础系统软件信息
• 检查软件的首选版本和基础版本。 （PAN-OS 11.1.3 及更高版本）	请求首选基础系统软件信息
• 安装下载的软件。	请求系统软件安装版本 **10.1.0**
• 重新启动防火墙。	**request restart system**

访问防火墙的可用软件补丁：

补丁功能目前以预览模式提供。此功能不提供完全支持。

如果您要...	使用...
• 检查可供下载的可用软件版本。	请求系统补丁检查
• 检查当前安装的防火墙版本的可用补丁。	请求系统补丁信息
• 下载特定补丁版本。	请求系统补丁下载版本 **<version>**
• 查看特定补丁版本的更多详细信息。	请求系统补丁信息版本 **<version>**
• 安装下载的映像。	请求系统补丁安装版本 **<version>**
• 应用安装的补丁。	请求系统补丁应用

如果您要...	使用...

用于升级的 API

- 使用 API 执行升级任务

使用 API 执行升级任务

使用以下 CLI 命令执行升级任务。

如果您要...	使用...
检查防火墙的当前版本	
• 检查防火墙软件和内容的当前版本。	**https://firewall/api/?type=op&cmd=<request><system><software><chec check></software></system>**
访问可用的动态更新并升级防火墙的内容版本	
• 直接从 Palo Alto Networks 服务器检查动态更新的可用内容版本。	**https://firewall/api/?type=op&cmd=<request><content><upgrade><chec check></upgrade></content></request>**
• 直接从防火墙检查动态更新的可用内容版本。	**https://firewall/api/?type=op&cmd=<request><content><upgrade><info info></upgrade></content></request>**
• 将最新的内容版本直接下载到防火墙。	**https://firewall/api/?type=op&cmd=<request><content><upgrade><down latest></download></upgrade></content></request>**
• 将特定内容版本直接下载到防火墙。	**https://firewall/api/?type=op&cmd=<request><content><upgrade><down**此输入具体的文件名**<file></download></upgrade></content></request>**
• 安装内容版本。	**https://firewall/api/?type=op&cmd=<request><content><upgrade><inst <content version></version></install></upgrade></content></request>**
访问可用的软件版本并升级防火墙	
• 检查可供下载的可用软件版本。	**https://firewall/api/?type=op&cmd=<request><system><software><info**

如果您要...	使用...
	info></software></system></request>
• 检查防火墙上已加载的可用版本。	**https://firewall/api/?type=op&cmd=<request><system><software><chec check></software></system></request>**
• 下载软件的特定版本。	**https://firewall/api/?type=op&cmd=request><system><software><downl version></download></software></system></request>**
• 检查特定下载作业的状态。	**https://firewall/api/?type=op&cmd=<show><jobs></jobs></show>**
• 安装下载的软件。	**https://firewall/api/?type=op&cmd=<request><system><software><inst version></install></software></system></request>**
• 重新启动防火墙。	**https://firewall/api/?type=op&cmd=<request><restart><system></system></restart></request>**

