Panorama 管理员指南

Version 10.0 (EoL)

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

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

About the Documentation

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

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

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

Last Revised

December 4, 2020

Table of Contents

Panorama 概述 9
关于 Panorama 10
Panorama 型号 11
集中防火墙配置和更新管理 13
上下文切换 — 防火墙或 Panorama 13
Panorama 的总配置大小 13
模板和模板堆栈 14
设备组 15
¼¯ÖÐ日志记录和报告 19
受管收集器和收集器组 19
本地和分布式日志收集 20
具有多个日志收集器的收集器组的说明 20
日志转发选项 22
集中报告 23
使用 Panorama 重新分发数据 24
基于角色的访问控制 25
管理角色 25
身份验证配置文件和序列 26
访问域 26
管理身份验证 27
Panorama 提交、验证和预览操作 28
计划您的 Panorama 部署 29
部署 Panorama：任务概述 31

设置 Panorama 33
确定 Panorama 日志存储要求 34
设置 Panorama 虚拟设备 36
设置 Panorama 虚拟设备的前提条件 36
安装 Panorama 虚拟设备 38
执行 Panorama 虚拟设备的初始配置 64
设置 Panorama 虚拟设备为日志收集器 66
使用本地日志收集器设置 Panorama 虚拟设备 71
在 Panorama 模式下设置 Panorama 虚拟设备 75
在仅管理模式下设置 Panorama 虚拟设备 75
扩展 Panorama 虚拟设备上的日志存储容量 76
增加 Panorama 虚拟设备上的 CPU 和内存 93
增加 Panorama 虚拟设备上的系统磁盘 98
完成 Panorama 虚拟设备设置 103
设置 M 系列设备 104
M 系列设备接口 104
执行 M 系列设备的初始配置 105
M 系列设置概述 109
将 M 系列设备设为日志收集器 110
增加 M 系列设备上的存储容量 115
配置 Panorama 以使用多个接口 122
注册 Panorama 和安装许可证 127
注册 Panorama 127
激活 Panorama 支持许可证 128
在 Panorama 虚拟设备连接到互联网时激活/检索防火墙管理许可证 129

在 Panorama 虚拟设备未连接到互联网时激活/检索防火墙管理许可证 129
在 M 系列设备上激活/检索防火墙管理许可证 131
安装 Panorama 设备证书 133
安装 Panorama 的内容和软件更新 135
Panorama、日志收集器、防火墙和 WildFire 的版本兼容性 135
在高可用性配置中安装 Panorama 更新 135
使用互联网连接安装 Panorama 更新 136
未连接互联网时安装 Panorama 更新 140
不使用互联网连接自动安装 Panorama 更新 143
将 Panorama 日志迁移到新日志格式 147
过渡到另一 Panorama 型号 149
从 Panorama 虚拟设备迁移到 M 系列设备 149
从 Panorama 虚拟设备迁移到不同的管理程序 151
从 M 系列设备迁移到 Panorama 虚拟设备 154
从 M-100 设备迁移到 M-500 设备 158
访问和导航 Panorama 管理界面 161
登录到 Panorama Web 界面 161
导航 Panorama Web 界面 161
登录到 Panorama 命令行界面 162
设置 Panorama 的管理访问权限 164
配置管理角色配置文件 164
配置访问域 164
配置管理帐户和身份验证 165
使用自定义证书设置身份验证 175
SSL/TLS 连接如何进行相互身份验证？ 175
在 Panorama 上使用自定义证书配置身份验证 176
在受管设备上使用自定义证书配置身份验证 177
添加新客户端设备 179
更改证书 179

管理防火墙 183
添加防火墙作为受管设备 184
为受管防火墙安装设备证书 188
为一个受管防火墙安装设备证书 188
为多个受管防火墙安装设备证书 190
设置零接触配置 193
ZTP 概述 193
安装 ZTP 插件 194
配置 ZTP 安装程序管理员帐户 200
添加 ZTP 防火墙到 Panorama 200
使用 CLI 进行 ZTP 任务 204
卸载 ZTP 插件 206
管理设备组 207
添加设备组 207
创建设备组层次 208
创建要在共享或设备组策略中使用的对象 209
还原到继承对象值 210
管理未使用的共享对象 210
管理继承对象的优先级 211
将策略规则或对象移动或克隆到另一设备组 212
在 Panorama 上选择 URL 筛选服务供应商 213
将策略规则推送到防火墙的子集 216
管理规则层次结构 218

管理模板和模板堆栈 220
模板功能和例外 220
添加模板 220
配置模板堆栈 222
配置模板或模板堆栈变量 224
导入和覆盖现有模板堆栈变量 226
覆盖模板或模板堆栈值 228
禁用/删除模板设置 230
从 Panorama 管理主密钥 231
设置企业数据丢失防护 (DLP) 234
企业数据丢失防护 (DLP) 概述 234
企业数据丢失防护 (DLAP) 支持什么？ 235
预定义数据筛选配置文件 238
安装企业数据丢失防护 (DLP) 插件 238
创建数据模式 240
创建数据筛选配置文件 241
启用企业数据丢失防护 (DLP) 244
查看企业数据丢失防护 (DLP) 日志详情 246
启用现有数据模式和筛选配置文件 247
编辑企业数据丢失防护 (DLP) 设置 248
卸载企业数据丢失防护 (DLP) 插件 251
重新分发数据到受管防火墙 254
从防火墙过渡到 Panorama Management 256
计划向 Panorama 管理的过渡 256
从防火墙迁移到 Panorama 管理 257
从防火墙 HA 对迁移到 Panorama 管理 260
将部分防火墙配置加载到 Panorama 中 262
在 Panorama 上监控设备 265
监控设备运行状况 265
监控策略规则使用情况 266
用例：使用 Panorama 配置防火墙 271
本用例中的设备组 271
本用例中的模板 272
设置集中配置和策略 273

管理大规模防火墙部署 279
确定大规模防火墙部署最佳解决方案 280
提高 M-600 和 Panorama 虚拟设备的设备管理容量 281
提高设备管理容量要求 281
部署 Panorama 以提高设备管理容量 282
Panorama Interconnect 284
Panorama Interconnect 概述 284
Panorama Interconnect 要求 285
启动 Panorama 控制器和节点之间的身份验证 287
设置 Panorama Interconnect 插件 291
同步 Panorama Interconnect 293
采用 Panorama Interconnect 管理防火墙 295
升级 Panorama Interconnect 插件 303

管理日志收集 305
配置受管收集器 306
为专用日志收集器配置身份验证 309

为专用日志收集器配置管理员帐户 309
为专用日志收集器配置 RADIUS 身份验证 310
为专用日志收集器配置 TACACS+ 身份验证 312
为专用日志收集器配置 LDAP 身份验证 314
管理收集器组 318
配置收集器组 318
在日志收集器之间使用自定义证书配置身份验证 320
将日志收集器移动到另一收集器组 321
从收集器组删除防火墙 322
配置 Panorama 的日志转发 324
配置到外部目标的 Syslog 转发 327
转发日志至 Cortex 数据湖 330
验证 Panorama 的日志转发 331
修改日志转发和缓冲默认设置 332
配置从 Panorama 到外部目标的日志转发 334
日志收集部署 336
使用专用日志收集器部署 Panorama 336
使用本地日志收集器部署 Panorama M 系列设备 341
使用本地日志收集器部署 Panorama 虚拟设备 345
使用本地日志收集器在传统模式下部署 Panorama 虚拟设备 349

管理 Wildfire 设备 351
添加独立 WildFire 设备以使用 Panorama 进行管理 352
在 Panorama 上配置基本 WildFire 设备设置 355
为 WildFire 设备配置身份验证 355
在 WildFire 设备和集群上使用自定义证书设置身份验证 364
为 Panorama 管理的 WildFire 设备配置自定义证书 364
使用单个自定义证书为 WildFire 集群配置身份验证 366
在通过 Panorama 配置的 WildFire 设备上应用自定义证书 367
从 Panorama 管理中删除 WildFire 设备 369
管理 WildFire 集群 370
在 Panorama 上集中配置集群 370
通过 Panorama 查看 WildFire 集群状态 387
通过互联网连接在 Panorama 上集中升级集群 388
不通过互联网连接在 Panorama 上集中升级集群 390

管理许可证和更新 393
在防火墙上使用 Panorama 管理许可证 394
使用 Panorama 将更新部署到防火墙、日志收集器和 WildFire 设备 395
支持的更新 395
使用 Panorama 计划内容更新 396
当 Panorama 连接上互联网时升级日志收集器 397
当 Panorama 未连接互联网时升级日志收集器 399
当 Panorama 连接上互联网时升级防火墙 402
当 Panorama 未连接互联网时升级防火墙 406
升级 ZTP 防火墙 410
从 Panorama 恢复内容更新 411

监控网络活动 413
使用 Panorama 的可视化功能 414
使用 ACC 和 AppScope 监控网络 414

分析日志数据 415
生成、计划和用电子邮件发送报告 416
为已计划报告配置密钥限制 418
在 Panorama 上提取 Traps ESM 日志 421
用例：使用 Panorama 监控应用程序 423
用例：使用 Panorama 来响应事件 426
事件通知 426
查看 ACC 中的小部件 426
检查威胁日志 426
检查 WildFire 日志 427
检查数据筛选日志 427
更新安全规则 428

Panorama 高可用性 429
Panorama 高可用性前提条件 430
Panorama 高可用性的优先级和故障转移 432
故障转移触发 433
高可用性检测信号轮询和呼叫消息 433
高可用性路径监控 433
Panorama 高可用性的日志记录注意事项 434
在传统模式下 Panorama 虚拟设备的日志记录故障转移 434
在 Panorama 模式下 M 系列设备或 Panorama 虚拟设备的日志记录故障转移 434
Panorama 高可用性对端设备之间的同步 436
管理 Panorama 高可用性对 437
设置 Panorama 高可用性 437
在 HA 对端设备之间使用自定义证书设置身份验证 438
测试 Panorama 高可用性故障转移 439
在 Panorama 故障转移后切换优先级以恢复 NFS 日志记录 440
将主要 Panorama 还原至主动状态 441

管理 Panorama 443
预览、验证或提交配置更改 444
启用自动提交恢复 446
管理 Panorama 和防火墙配置备份 448
调度导出配置文件 448
保存并导出 Panorama 和防火墙配置 449
还原 Panorama 配置更改 451
配置 Panorama 上的配置备份最大数量 453
在受管防火墙上加载配置备份 453
比较 Panorama 配置的更改 454
管理配置更改限制锁 455
将自定义徽标添加到 Panorama 457
使用 Panorama 任务管理器 458
管理日志和报告的存储配额和过期期限 459
日志和报告存储 459
日志和报告过期期限 459
配置日志和报告的存储配额和过期期限 460
配置 Panorama 报告的运行时间 461
监视 Panorama 462
Panorama 系统和配置日志 462
使用 SNMP 监视 Panorama 和日志收集器统计信息 462
重新启动或关闭 Panorama 465

配置 Panorama 密码配置文件和复杂性 466

Panorama 插件 467
关于 Panorama 插件 468
安装 Panorama 插件 469
VM 系列插件和 Panorama 插件 471
在 Panorama 上安装 VM 系列插件 471

故障排除 473
Panorama 系统问题故障排除 474
生成 Panorama 诊断文件 474
诊断 Panorama 挂起状态 474
监视文件系统完成性检查 474
管理用于软件和内容更新的 Panorama 存储 475
从 Panorama 高可用性部署的脑裂恢复 475
日志存储和连接问题故障排除 477
验证 Panorama 端口使用情况 477
解决收集器组的零日志存储 478
在 M 系列设备上更换故障磁盘 479
替换 ESXi 服务器上的虚拟磁盘 479
替换 vCloud Air 上的虚拟磁盘 480
将日志迁移到日志收集器模式下的新 M 系列设备 480
将日志迁移到 Panorama 模式下的新 M 系列设备 485
将日志迁移到高可用性配置中 Panorama 模式下的新 M 系列设备型号 490
将日志迁移到高可用性的 Panorama 模式下的新 M 系列设备型号 496
非高可用性 Panorama 出现故障/RMA 时迁移日志收集器 502
重新生成 M 系列设备 RAID 对的元数据 504
查看日志查询作业 505
替换 RMA 防火墙 506
为防火墙生成局部设备状态 506
开始 RMA 防火墙替换之前 506
替换后还原防火墙配置 507
排除提交故障 510
排除注册或序列号错误 511
排除报告错误 512
排除设备管理许可证错误 513
排除自动恢复防火墙配置问题 514
在关闭 Panorama HA 对等设备时完成内容更新 516
查看任务成功或失败状态 518
测试受管设备的策略匹配和连接 519
排除策略规则流量匹配问题 519
排除网络资源连接问题 520
从 Panorama 10.0 降级 521

Panorama 概述

Panorama™ 管理服务器提供对多个 Palo Alto Networks 下一代防火墙以及 WildFire 设备和设备群集的集中监控和管理。它为您提供了一个独特的位置，您可以通过此位置监管遍及您网络的所有应用程序、用户和内容，然后利用获得的信息来创建保护和控制网络的应用程序启用策略。使用 Panorama 的集中策略和防火墙管理可提高管理和维护分布式网络防火墙的运营效率。将 Panorama 用于集中式 WildFire 设备和 WildFire 设备群集管理可增加单个网络支持的防火墙数量，为容错提供高可用性并提高管理效率。

- 关于 Panorama
- Panorama 型号
- 集中防火墙配置和更新管理
- ¼¯ÖÐ日志记录和报告
- 使用 Panorama 重新分发数据
- 基于角色的访问控制
- Panorama 提交、验证和预览操作
- 计划您的 Panorama 部署
- 部署 Panorama：任务概述

关于 Panorama

Panorama 能让您使用集中监督有效配置、管理和监控 Palo Alto Networks 防火墙。Panorama 的增值特点主要体现在三大主要方面，即：

- 集中配置和部署 — 要简化在网络上集中管理和快速部署防火墙和 WildFire 设备，可使用 Panorama 预先规划防火墙和 WildFire 设备部署。随后，您便可以将防火墙组合成组，创建模板应用基本网络和设备配置，并使用设备组来管理全局共享的本地策略规则。请参阅集中防火墙配置和更新管理。
- 聚合日志记录与集中监督进行分析和报告 — 收集有关网络中所有受管防火墙活动的信息，并集中分析、调查和报告相关数据。这是网络流量、用户活动和相关风险的综合性视图，使您能够利用丰富的策略组对潜在的威胁做出快速响应，从而在网络上安全地启用应用程序。请参阅集中日志和报告。
- 分布式管理 — 能让您委派或限制对全局及本地防火墙配置和策略的访问权限。关于为分布式管理委派适当的访问权限级别，请参阅基于角色的访问控制。

提供四种 Panorama 型号：PAN-OS 10.0 中支持 Panorama 虚拟设备、M-600 设备、M-500 设备和 M-200 设备。Panorama 集中管理说明如何在高可用性 (HA) 配置中部署 Panorama 以管理防火墙。

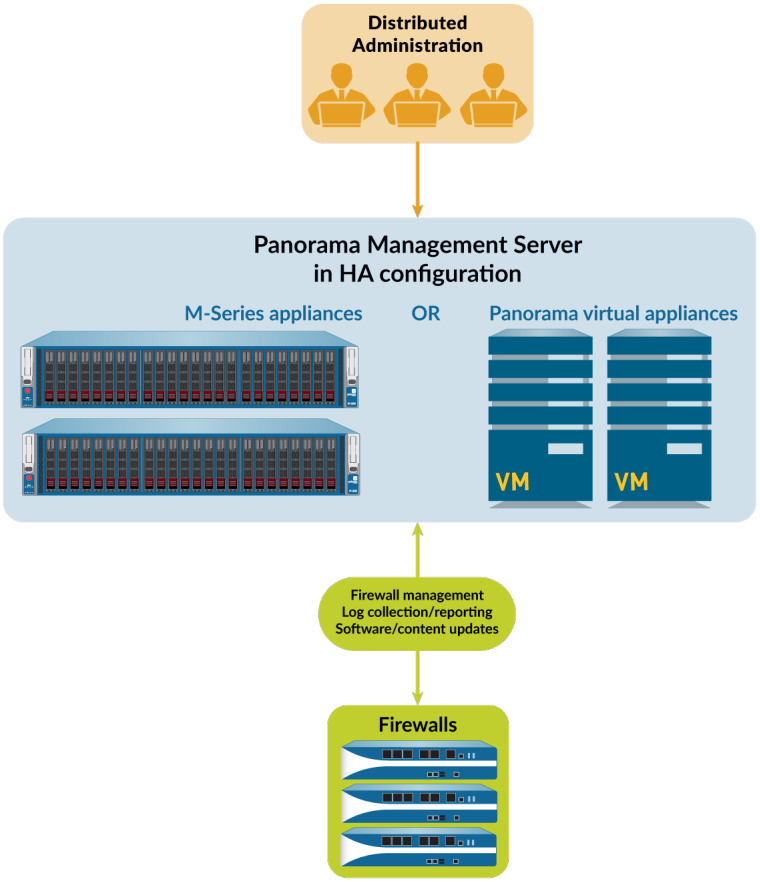


图 1: Panorama 集中管理

© 2019 Palo Alto Networks, Inc.

Panorama 型号

Panorama 可以用作以下虚拟或物理设备之一，其中每个设备均支持管理最多 25、100 或 1000 个防火墙的许可证。此外，M-600 设备以及具有类似资源的 Panorama 虚拟设备页支持最多可管理 5000 个防火墙的许可证：

- **Panorama** 虚拟设备 — 对于需要虚拟管理设备的站点，此型号可简化安装并促进服务器合并。您可以在 Amazon Web Services(AWS)、AWS GovCloud、Microsoft Azure、Google Cloud Platform (GCP)、KVM、Hyper-V、VMware ESXi 服务器或 VMware vCloud Air 上安装 Panorama。虚拟设备能够以最高达每秒 10,000 条日志的速率本地收集防火墙日志，并且可以管理专用日志收集器以获得更高日志记录速率。虚拟设备可用作专用管理服务器、具有本地日志收集功能的 Panorama 管理服务器，或是专用日志收集器。对于受支持的接口、日志存储容量和最大日志收集速率，请参阅设置 Panorama 虚拟设备的前提条件。您可以通过以下模式部署虚拟设备：
  - **Panorama** 模式 — 在此模式下，Panorama 虚拟设备支持具有 1 到 12 个虚拟日志记录磁盘的本地日志收集器（请参阅使用本地日志收集器部署 Panorama 虚拟设备）。每个日志记录磁盘具有 2TB 的存储容量，单个虚拟设备的最大总存储容量为 24 TB，高可用性 (HA) 对的最大总存储容量为 48TB。只有 Panorama 模式能让您添加多个虚拟日志记录磁盘，而不会丢失现有磁盘上的记录。Panorama 模式还可让您更快地生成报告。在 Panorama 模式下，虚拟设备不支持 NFS 存储。

    作为最佳做法，请在 *Panorama* 模式下部署虚拟设备以优化日志存储和报告生成。
  - “传统”模式（仅限 ESXi 和 vCloud Air）— 在此模式下，Panorama 虚拟设备接收并存储防火墙日志，而不使用本地日志收集器（请参阅使用本地日志收集在传统模式下部署 Panorama 虚拟设备）。默认情况下，传统模式下的 Panorama 虚拟设备使用一个磁盘分区存储所有数据。已经分配分区的大约 11GB 用于存储日志。如果您需要多个本地日志存储，可以在 ESXi 5.5 和更高版本或 vCloud Air 上添加容量达 8TB 的虚拟磁盘。更低版本的 ESXi 可支持一个容量达 2TB 的虚拟磁盘。如果您需要 8TB 以上的磁盘空间，您可以在传统模式下将虚拟设备安装到 NFS 数据存储上，但仅限于后者位于 ESXi 服务器而不是 vCloud Air 上时。只有当 Panorama 虚拟设备在“传统”模式下升级到 PAN-OS 10.0 时，此模式才可用。在升级到 PAN-OS 9.0 及更高版本时，如果您更改为任何其他模式，就再也无法使用“传统”模式。如果您将 Panorama 虚拟设备从传统模式更改为其中一种可用模式，则再也不能更改回传统模式。

    虽然“传统”模式受支持，但不建议在生产环境中使用，可仍用于实验室或演示环境中。
  - “仅管理”模式 — 在此模式下，Panorama 虚拟设备是用于受管设备的专用管理设备，也是专用日志收集器，并且在此模式下，具有适当资源的 Panorama 虚拟设备可以管理最多 5,000 个防火墙。除配置和系统日志外，Panorama 虚拟设备不再具有日志收集功能，且需要一个专用日志收集器来存储这些日志。默认情况下，处于“仅管理”模式的虚拟设备对所有数据只有一个磁盘分区，所以，所有在“仅管理”下转发到 Panorama 虚拟设备的日志将被全部丢弃。因此，如要存储受管设备的日志数据，您必须配置日志转发才能存储来自受管设备的日志数据。有关详细信息，请参阅提高设备管理容量要求。
  - 日志收集器模式—Panorama 虚拟设备充当专用日志收集器。如果多个防火墙转发大量日志数据，则“日志收集器”模式下的 Panorama 虚拟设备可提供规模和性能提升。在这种模式下，设备没有 Web 界面进行管理访问；只有命令行界面 (CLI)。但是，您可以使用 Panorama 管理服务器的 Web 界面管理设备。只有在初始设置过程中和调试过程中，才需要通过 CLI 访问日志收集器模式下的 Panorama 虚拟设备。有关配置详细信息，请参阅使用专用日志收集器部署 Panorama。
- **M-Series** 设备 — M-200、M-500 和 M-600 设备是设计用于大规模部署的专用硬件设备。在具有高日志记录速率（超过 10,000 条日志/秒）和日志保留要求的环境中，这些设备让您能够扩展您的日志收集基础架构。对于受支持的接口、日志存储容量和最大日志收集速率，请参阅M 系列设备接口。所有 M 系列型号共享以下属性：
  - RAID 驱动器用于存储防火墙日志，RAID 1 镜像用于防范磁盘故障
  - SSD 用于存储 Panorama 和日志收集器生成的日志

© 2019 Palo Alto Networks, Inc.

- 支持 1Gbps 吞吐量的 MGT、Eth1、Eth2 和 Eth3 接口
- 冗余热插拔电源
- 从前向后空气流通

M-600 和 M-500 设备具有以下附加属性，使其更适合数据中心：

- 支持 10Gbps 吞吐量的 Eth4 和 Eth5 接口

此外，下列属性使 M-600 设备更适合大规模防火墙部署：

- “仅管理”模式下的 M-600 设备最多可管理 5000 个防火墙。

您可以通过以下模式部署 M 系列设备：

- **Panorama** 模式 — 设备用作 Panorama 管理服务器来管理防火墙和专用日志收集器。设备还支持本地日志收集器聚合防火墙日志。Panorama 模式是默认模式。有关配置详细信息，请参阅使用本地日志收集器部署 Panorama M 系列设备。
- 仅管理模式— Panorama 设备是一个用于受管设备的专用管理设备，也是一个专用日志收集器。除配置和系统日志外，Panorama 设备不再具有日志收集功能，且您的部署需要一个专用日志收集器来存储这些日志。默认情况下，处于“仅管理”模式的 Panorama 设备对所有数据只有一个磁盘分区，所以，所有在“仅管理”下转发到 Panorama 虚拟设备的日志将被全部丢弃。因此，如要存储受管设备的日志数据，您必须配置日志转发才能存储来自受管设备的日志数据。
- 日志收集器模式 — 设备用作专用日志收集器。如果多个防火墙转发大量的日志数据，则日志收集器模式下 M 系列设备的规模和性能都将提升。在这种模式下，设备没有 Web 界面进行管理访问；只有命令行界面 (CLI)。但是，您可以使用 Panorama 管理服务器的 Web 界面管理设备。只有在初始设置过程中和调试过程中，才需要通过 CLI 访问日志收集器模式下的 M 系列设备。有关配置详细信息，请参阅使用专用日志收集器部署 Panorama。

有关 M 系列设备的更多详细信息和规格，请参阅《M 系列设备硬件参考指南》。

© 2019 Palo Alto Networks, Inc.

集中防火墙配置和更新管理

Panorama™ 使用设备组和模板将设备分成需要类似配置的逻辑设备组。您可以使用设备组和模板来集中地管理受管防火墙上的所有配置元素、策略和对象。Panorama 还使您能够集中地管理许可证、软件（PAN-OS® 软件、SSL-VPN 客户端软件、GlobalProtect™ 代理/应用软件）和内容更新（应用程序、威胁、WildFire® 和防病毒软件）。

- 上下文切换 — 防火墙或 Panorama
- Panorama 的总配置大小
- 模板和模板堆栈
- 设备组

上下文切换 — 防火墙或 Panorama

Panorama™ Web 界面让您能够通过使用位于各选项卡左上角的 **Context**（上下文）下拉列表来切换以 Panorama 为中心的视图与以防火墙为中心的视图。将 **Context**（上下文）设置为 **Panorama** 以集中地管理防火墙，或者将上下文切换至特定防火墙的 Web 界面以在本地对其加以配置。Panorama 和防火墙 Web 界面的相似性使您能够无缝地切换两者，以便监控和管理防火墙。

Context（上下文）下拉列表只显示已与 Panorama 连接的防火墙。对于设备组和模板管理员，此下拉列表只显示处于分配给该管理员的访问域内的已连接防火墙。若要搜索较长列表，可使用下拉列表中的筛选器。

对于在高可用性 (HA) 配置中的防火墙，图标采用了彩色背景以表明高可用性状态（如下所示）。知晓高可用性状态对于选择防火墙上下文而言很有帮助。例如，您通常会在主动防火墙上作出特定的防火墙配置更改。

- 绿色 — 激活。
- 黄色）— 被动或防火墙正在启动（启动状态会在开机后持续长达 60 秒）。
- 红色 — 防火墙处于非运行（错误状态）、已挂起（管理员已禁用防火墙）或暂定状态（对于主动/主动高可用性配置中的链路或路径监控事件）。

Panorama 的总配置大小

在确定需要在 Panorama 虚拟设备上分配哪个 M-Series 设备或最小数量的虚拟资源以确保满足安全要求时，Panorama™ M-Series 和虚拟设备的总配置文件大小是性能指标的重要部分。执行配置更改、提交和推送到受管防火墙时，超过 Panorama 管理服务器支持的总配置文件大小会导致性能降低。

对于所有模板、设备组和 Panorama 特定配置，处于 Panorama 模式下的 Panorama 管理服务器支持 80MB 的 总配置文件大小。处于“仅管理”模式下的 Panorama 最多支持 120MB 或 150MB 的总配置文件大小，具体取决于 Panorama 型号或您分配给 Panorama 虚拟设备的资源。请参阅以下表格，了解基于 Panorama M-Series 设备型号或分配给 Panorama 虚拟设备的资源建议的最大配置文件大小。

Panorama 型号	所需虚拟资源	建议的 Panorama 最大配置文件大小
M-200	N/A	120MB
M-500		120MB
M-600		150MB
Panorama 虚拟设备	• 16 vCPU • 128GB 内存	120MB

© 2019 Palo Alto Networks, Inc.

Panorama 型号	所需虚拟资源	建议的 Panorama 最大配置文件大小
请参阅 设置 Panorama 虚拟设备的前提条件 获取更多设置信息。	• 56 vCPU • 256GB 内存	150MB

模板和模板堆栈

您可以使用模板和模板堆栈来配置使防火墙能够在网络上运作的设置。模板是您用于在 Panorama™ 上配置 **Network**（网络）和 **Device**（设备）选项卡的基本构建块。您可以使用模板定义接口和区域配置、管理用于日志记录和 syslog 访问的服务器配置文件，或定义 VPN 配置。您可以通过模板堆栈对多个模板进行分层，并创建组合配置。因为模板堆栈允许您定义附加到模板堆栈的所有服务通用基本配置，并让您能够对多个模板进行分层以创建组合配置，因此模板堆栈可以简化管理。为此，您可以定义带特定位置或特定功能设置的模板，然后按优先级降序对模板进行堆栈处理，以便防火墙根据堆栈中模板的顺序继承设置。

模板和模板堆栈均支持变量。您可以根据您的配置需求通过变量创建带模板或模板堆栈中指定值的占位符对象。创建模板或模板堆栈变量，以替换 IP 地址、组 ID、以及您的配置中的接口。模板变量由模板堆栈继承，可以覆盖，以创建模板堆栈变量。但是，模板无法继承模板堆栈中定义的变量。当变量在模板或模板堆栈中定义，且推送给防火墙时，为变量定义的值将显示在防火墙上。

要适应具有唯一设置的防火墙时，您可以使用模板覆盖模板堆栈配置。或者，您也可以推送更广泛的通用基本配置，然后在单个防火墙中使用防火墙特定值覆盖某些推送的设置。当您覆盖防火墙上的设置时，防火墙会将该设置保存到其本地配置；Panorama 则不再管理该设置。要在覆盖后恢复模板值，应使用 Panorama 将模板或模板堆栈配置强制推送到防火墙上。例如，在模板中定义通用 NTP 服务器并在防火墙上覆盖 NTP 服务器配置以适应其本地时区之后，您可以在以后恢复在模板中定义的 NTP 服务器。

在定义模板堆栈时，应考虑分配属于相同硬件型号，且要求获得类似网络资源（例如网关和 syslog 服务器）访问权限的防火墙。这样便让您避免了向每一个模板堆栈添加每一个设置的重复操作。下图所示为一例典型配置，在此配置中，您把亚太 (APAC) 地区内的数据中心防火墙分配到一个拥有三个模板的堆栈；在这三个模板之中，一个具有全局设置，一个具有亚太地区特定设置，一个具有数据中心特定设置。若要管理亚太地区分支机构办事处内的防火墙，那么您可以通过将它们添加到另一个包含了带分支机构特定设置的堆栈来重新利用全局模板和亚太地区特定模板。堆栈中的模板具有可确保 Panorama 对任何重复设置只推送一个值的可配置优先级次序。Panorama 会自上而下地评估堆栈配置中所列的模板，而模板排位越高，其优先级也越高。下图所示为一个数据中心堆栈，其中数据中心模板的优先级高于全局模板的优先级：Panorama 推送来自数据中心模板的空闲超时值，而忽略来自全局模板的值。

© 2019 Palo Alto Networks, Inc.

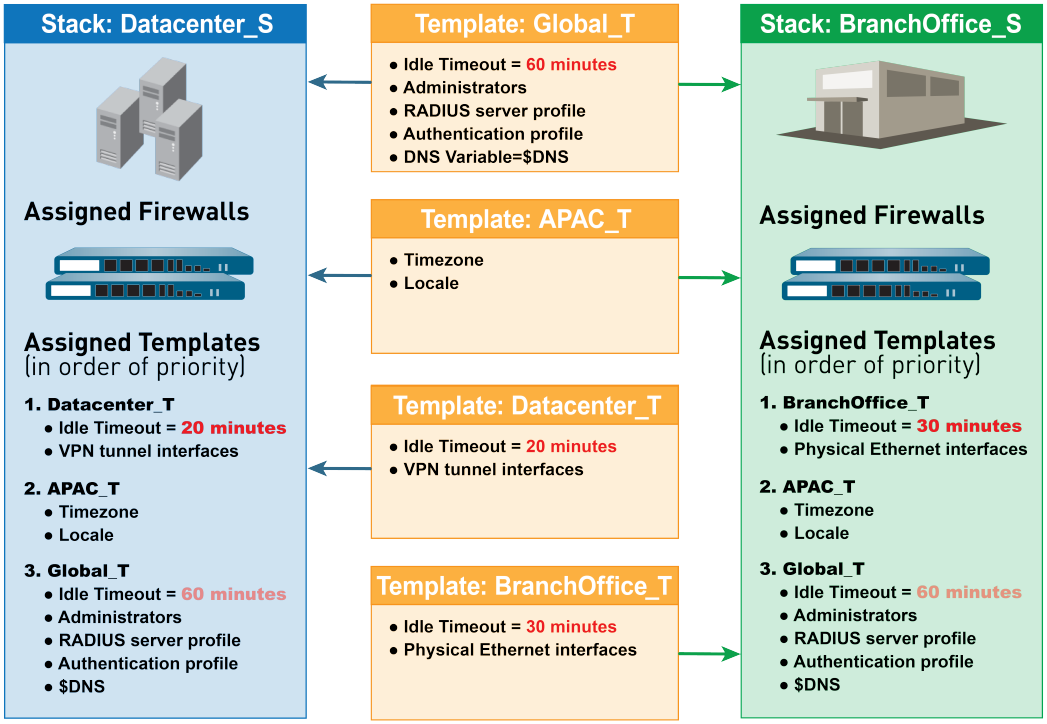


图 **2:** 模板堆栈

您无法使用模板或模板堆栈来设置以下防火墙模式：虚拟专用网络 (VPN) 模式、多虚拟系统模式（multi-vsys 模式）、操作模式（正常或 FIPS-CC 模式）。有关详细信息，请参阅模板功能和例外。但是，您可以将具有不匹配模式的多个防火墙分配到同一模板或堆栈。在这类情况下，Panorama 会将节点特定设置仅仅推送到支持这些模式的防火墙。例外情况是，您可以配置 Panorama 来将模板中默认虚拟系统的设置推送到不支持虚拟系统的或没有任何已配置虚拟系统的防火墙。

有关相应的程序，请参阅管理模板和模板堆栈。

设备组

要有效使用 Panorama，您必须将网络中的防火墙分组成逻辑单元，称为设备组。您可以根据网络分段、地理位置、组织功能或要求类似策略配置的防火墙的任何其他共同点来划分设备组。您可以使用设备组来配置它们引用的策略规则和对象。您可以分层次地组织设备组，使共享规则和对象处于顶部层级，设备组特定规则和对象处于各后继层级。这样做使您能够为那些强制执行防火墙处理流量方式的规则创建一个层次。例如，您可以将一组共享规则定义为企业可接受的使用策略。然后，为了只允许区域办事处访问点对点流量（如 BitTorrent），您可以定义 Panorama 仅向区域办事处推送的设备组规则（或者定义共享安全规则，并将区域办事处确定为其推送目的地）。有关相应的程序，请参阅 管理设备组：以下主题更为详细地介绍了设备组概念及组件：

- 设备组层次结构
- 设备组策略
- 设备组对象

设备组层次结构

您可以创建设备组层次，将设置组嵌套至最多含有 4 个层级的树形层次中，其中较低层级设备组将继承较高层级组的设置（策略规则和对象）。在底部层级，设备组可以具有父级、祖父级和曾祖父级设备组（祖先）。在顶部层级，设备组可以具有子级、孙级、曾孙级设备组（后代）。所有设备组都继承来自 *Shared* 位置的设置 — 对于通用于所有设备组的配置而言，Shared 是一个处于层次顶部的容器。

© 2019 Palo Alto Networks, Inc.

创建设备组层次让您可以根据通用策略要求来组织防火墙，而无需进行重复配置。例如，您可以配置通用于所有防火墙的共享设置，将具有功能特定设置的设备组配置在第一层级，并将具有位置特定设置的设备组配置在较低层级。如果没有层次，您就必须为 Shared 之下单个层级中的每一个设备组配置功能特定及位置特定设置。

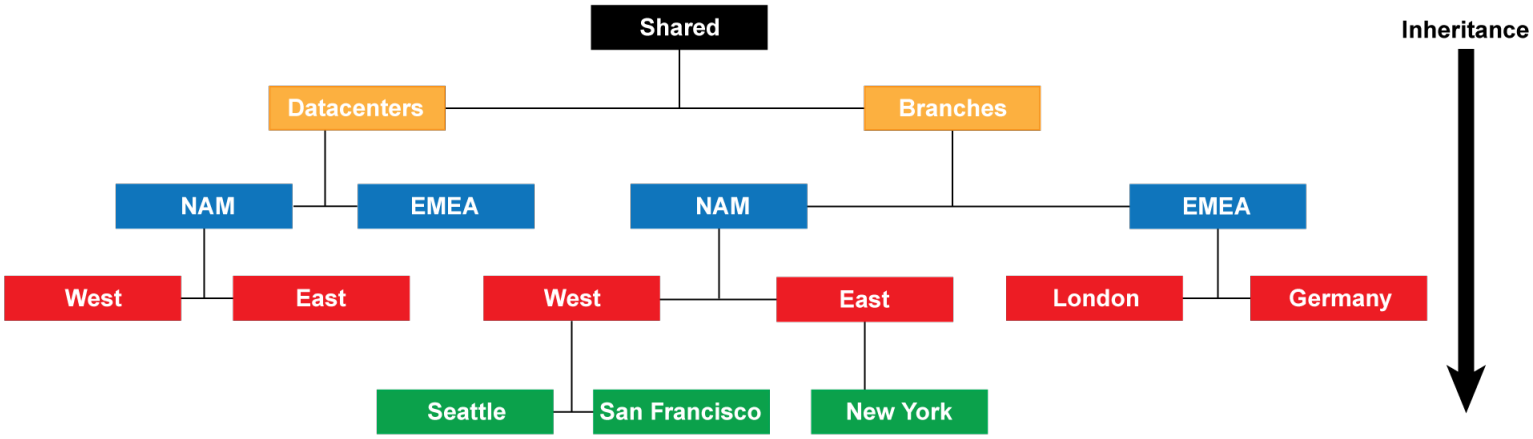
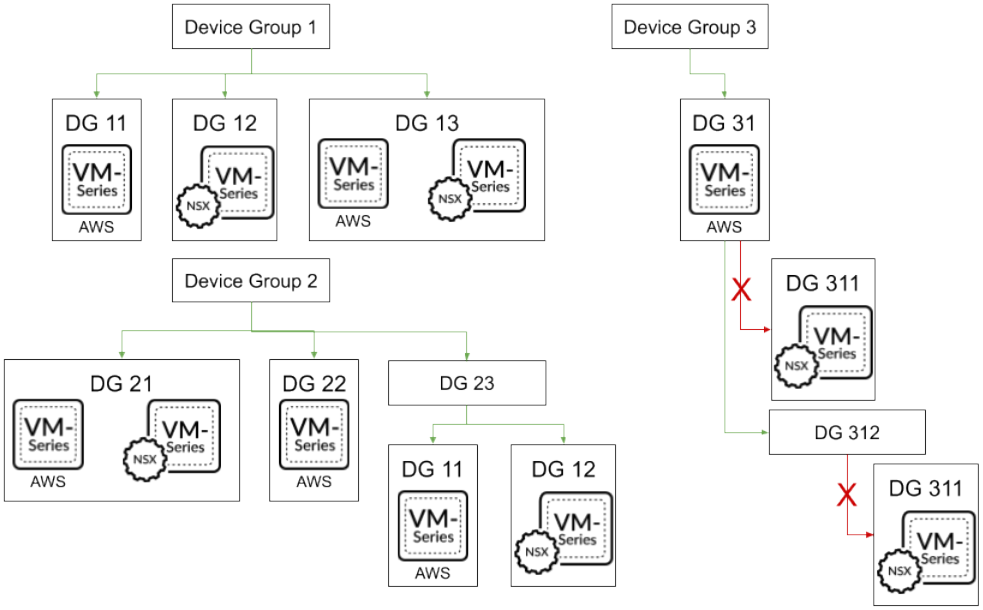


图 3: 设备组层次结构

有关设备组层次中防火墙评估策略规则所采用的次序的详细信息，请参阅设备组策略。有关覆盖设备组从祖先设备组所继承的对象的值的详细信息，请参阅设备组对象。

在一个要执行的多 Panorama 插件部署中，包含部署在特定管理程序中的防火墙的设备组不能是包含部署在其他管理程序中的防火墙的设备组的子级或父级。例如，如果 Panorama 从 VMware NSX-V 和 AWS 接收 IP 地址更新，您不能创建作为 AWS VM-Series 防火墙设备组子级的 NSX-V VM-Series 防火墙设备组。

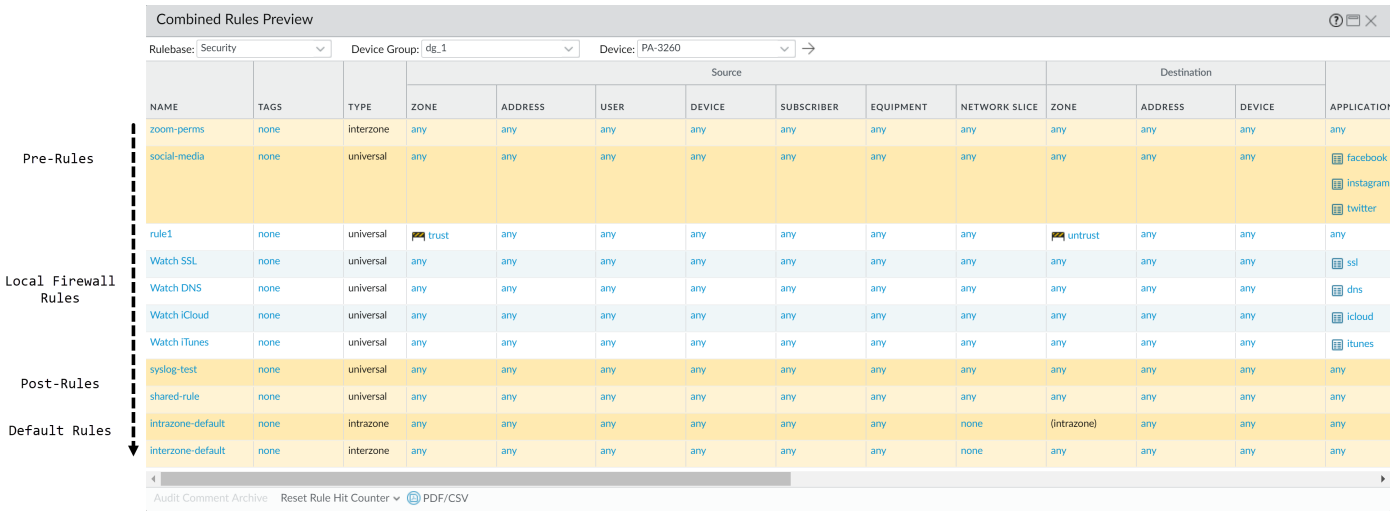


设备组策略

设备组提供了一种方式，可用来实现管理整个受管防火墙网络的策略的分层方法。防火墙将按层级（共享、设备组和本地）和按类型（前导规则、后继规则和默认规则）地以如下次序从上到下地评估策略规则。当防火墙收到流量时，它将执行在匹配该流量的第一个已评估规则中所定义的操作，并忽略所有的后继规则。若要对特定层级、类型和规则库（例如共享安全前导规则）内的规则更改评估次序，请参阅管理规则层次结构。

© 2019 Palo Alto Networks, Inc.

不论您是在防火墙上查看规则还是在 Panorama 中查看规则，Web 界面都会按照评估次序显示它们。防火墙从 Panorama 继承的所有共享、设备组和默认规则都显示为橙色。本地防火墙规则显示在前导规则和后继规则之间。



评估次序	规则范围和说明	管理设备
共享前导规则 设备组前导规则	Panorama 将共享前导规则推送到所有设备组中的所有防火墙。Panorama 将设备组特定前导规则推送到特定设备组及其后代设备组的所有防火墙。 如果防火墙继承了来自设备组层次中多个层级上设备组的规则，它将按照从最高级到最低级的次序评估前导规则。这意味着，防火墙会最先评估共享规则，而最后评估无后代设备组的规则。 您可以使用前导规则来强制执行组织的可接受使用策略。例如，前导规则可能会阻止访问特定 URL 类别，或者允许所有用户访问域名系统 (DNS) 流量。	虽然您可以在防火墙上看到这些规则，但您只能在 Panorama 中管理它们。
本地防火墙规则	本地规则只适用于单个防火墙或虚拟系统 (vsys)。	本地防火墙管理员或切换到本地防火墙上下文的 Panorama 管理员可以编辑本地防火墙规则。
设备组后续规则 共享后续规则	Panorama 将共享后继规则推送到所有设备组中的所有防火墙。Panorama 将设备组特定后继规则推送到特定设备组及其后代设备组的所有防火墙。 如果防火墙继承了来自设备组层次中多个层级上设备组的规则，它将按照从最低级到最高级的次序评估后继规则。这意味着，防火墙会最先评估无后代设备组的规则，而最后评估共享规则。	虽然您可以在防火墙上看到这些规则，但您只能在 Panorama 中管理它们。

© 2019 Palo Alto Networks, Inc.

评估次序	规则范围和说明	管理设备
	后继规则通常包括根据 App-ID™ 签名、User-ID™ 信息（用户或用户组）或服务而拒绝访问流量的规则。	
区域内默认 区域间默认	默认规则只适用于与安全规则库，且在 Panorama（处于 Shared 层级）和防火墙（在每个 vsys 中）上被预先加以定义。这些规则指定了 PAN-OS 如何处理不匹配任何其他规则的流量。 区域内默认规则允许区域内的所有流量。区域间默认规则拒绝区域间的所有流量。 如果您覆盖默认规则，它们的优先次序将变为从最低上下文到最高上下文：处于防火墙层级的已覆盖设置将优先于处于设备组层级的设置，而后者则优先于处于 Shared 层级的设置。	默认规则从一开始就处于只读状态，原因在于它们是预定义配置的一部分，或者是 Panorama 早已将它们推送到防火墙。但是，对于标记、操作、记录和安全配置文件，您可以覆盖这些设置。上下文决定了您可以在哪一个层级覆盖默认规则： • Panorama — 在 Shared 或设备组层级，您可以覆盖构成预定义配置一部分的默认规则。 • 防火墙 — 您可以覆盖构成防火墙或 vsys 上预定义配置一部分的默认规则，或者覆盖 Panorama 从 Shared 位置或设备组推送的默认规则。

设备组对象

对象是策略规则引用的配置元素，例如：IP 地址、URL 类别、安全配置文件、用户、服务和应用程序。任何类型的规则（前导规则、后继规则、默认规则以及以本地方式在防火墙上定义的规则）和任何规则库（安全、NAT、QoS、基于策略的转发、解密、应用程序覆盖、强制网络门户以及 DoS 保护）都可以引用对象。您可以在与设备组层次中对象有着相同范围的任意数量的规则中反复使用同一个对象。例如，如果您将一个对象添加到 Shared 位置，由于所有设备组均从 Shared 继承对象，因此层次中的所有规则都可以引用该共享对象。如果您将对象添加到某一特定设备组，则只有该设备组及其后代设备组中的规则可以引用该设备组对象。如果设备组中的对象值必须不同于那些从祖先设备组继承的值，您可以覆盖继承的对象值（请参阅步骤覆盖继承的对象值）。您还可随时还原到继承对象值。一旦您创建要在共享或设备组策略中使用的对象并多次使用它们，您便可以减少管理开销并确保防火墙策略之间的一致性。

您可以配置 Panorama 处理系统范围内对象的方式：

- 推送未使用的对象 — 默认情况下，Panorama 会向防火墙推送所有对象，而不论任何共享或设备组策略规则是否引用这些对象。或者，您也可以将 Panorama 配置为仅推送引用的对象。有关详细信息，请参阅管理未使用的共享对象。
- 祖先和后代对象的优先级 — 默认情况下，当层次中多层级上的设备组具有一个名称相同但值不同（例如因覆盖所致）的对象时，后代设备组中的策略规则将使用该后代内的对象值，而不是从祖先设备组或 Shared 继承的对象值。或者，您也可以颠倒此优先级顺序，将值从 Shared 或包含了对象的最高级祖先推送到所有后代设备组。有关详细信息，请参阅管理继承对象的优先级。

© 2019 Palo Alto Networks, Inc.

¼¯ÖÐ日志记录和报告

Panorama 可聚合所有受管防火墙的日志，并显示网络中所有流量的信息。此外，它还提供了所有策略修改的审核记录和对受管防火墙所作的配置更改。除了聚合日志外，Panorama 还可以将它们作为 SNMP 陷阱、电子邮件通知、syslog 消息和 HTTP 有效负载转发到外部服务器。

对于集中日志记录和报告，您也可以选择使用基于云的 Cortex 数据湖以便在架构上与 Panorama 无缝工作。Cortex 数据湖允许受管防火墙将日志转发到 Cortex 数据湖基础架构（而非 Panorama 或受管日志收集器），这样您就可以增强现有分布式日志收集设置或扩展当前日志记录基础架构，而无需自己投入时间和精力。

Panorama 上的应用程序命令中心 (ACC) 可为遍及所有防火墙的统一报告提供一个单独的窗格。它使您能够集中地监控网络活动以分析、调查和报告流量及安全事件。在 Panorama 中，您可以通过转发给 Cortex 数据湖、Panorama 或受管日志收集器（若已配置）的日志查看日志并生成报告，或者可以直接查询受管防火墙。例如，您可以根据存储在 Panorama（和受管收集器）中的日志或通过访问本地存储在受管防火墙或 Cortex 数据湖中的日志生成有关受管网络中流量、威胁和/或用户活动的报告。

如果您未配置将日志转发到 Panorama或 Cortex 数据湖，则可以安排要在每个受管防火墙上运行的报告并将结果转发到 Panorama，以生成用户活动和网络流量组合视图。尽管这些报告没有提供有关特定信息和活动的更精细的深入分析，但它们仍然提供了统一的监控方法。

- 受管收集器和收集器组
- 本地和分布式日志收集
- 具有多个日志收集器的收集器组的说明
- 日志转发选项
- 集中报告

受管收集器和收集器组

Panorama 使用日志收集器从受管防火墙聚合日志。在生成报告时，Panorama 会向日志收集器查询日志信息，让您看到防火墙监控的所有网络活动。由于您是使用 Panorama 来配置和管理日志收集器，因此它们也称为受管收集器。Panorama 可以管理两种类型的日志收集器：

- 本地日志收集器 — 此类型的日志收集器在 Panorama 管理服务器上本地运行。仅 Panorama 模式下的 M-600、M-500 、 M-200、M-100 设备或 Panorama 虚拟设备支持本地日志收集器。

  如果您将日志转发到传统模式下的 *Panorama* 虚拟设备，则它会在没有日志收集器的情况下在本地存储日志。
- 专用日志收集器 — 这是日志收集器模式下的 M-600、 M-500、M-200、 M-100 设备或 Panorama 虚拟设备。您可以使用 Panorama 模式下的 M 系列设备或 Panorama 或传统模式（ESXi 和 vCloud Air）下的 Panorama 虚拟设备管理专用日志收集器。要使用 Panorama Web 界面管理专用日志收集器，您必须将后者添加为受管收集器。否则，只能使用预定义管理用户 (*admin*) 帐户通过其 CLI 访问专用日志收集器。专用日志收集器不支持其他管理用户帐户。

您可以使用其中一种或两种类型的日志收集器为您的环境实现最佳的日志记录解决方案（请参阅本地和分布式日志收集）。

收集器组是作为单个逻辑日志收集单元而运作的 1 至 16 个受管收集器。如果收集器组包含专用日志收集器，则 Panorama 会在每个日志收集器的所有磁盘中和收集器组的所有日志收集器中均匀分布日志。此分布可优化可用存储空间。要启用日志收集器以接收日志，您必须将其添加到收集器组。如果您通过将多个日志收集器分配到同一个日志收集器组的方式启用日志冗余，请参阅具有多个日志收集器的收集器组的警告。收集器组配置指定了可以将日志发送到收集器组中日志收集器的受管防火墙。

要配置日志收集器和收集器组，请参阅管理日志收集。

© 2019 Palo Alto Networks, Inc.

本地和分布式日志收集

在您配置日志转发到 Panorama 前，您必须决定是使用本地日志收集器，专用日志收集器还是两者。

本地日志收集器易于部署，因为它不需要额外的硬件或虚拟机实例。在高可用性 (HA) 配置中，可以将日志发送到两个 Panorama 对端设备上的本地日志收集器；被动 Panorama 不会等待故障转移以开始收集日志。

对于本地日志收集，您还可以在传统模式下将日志转发到 *Panorama* 虚拟设备以存储日志，而不使用日志收集器作为逻辑容器。

专用日志收集器是指日志收集器模式下的 M-600、M-500、M-200 或 Panorama 虚拟设备。因为它们只执行日志收集而不是防火墙管理，所以专用日志收集器允许比本地日志收集器更强大的环境。专用日志收集器提供以下好处：

- 启用 Panorama 管理服务器使用更多管理功能资源而不是日志记录。
- 提供专用硬件设备的高容量日志存储。
- 启用更高日志记录速率。
- 为 RAID 1 存储设备提供水平可扩展性和冗余。
- 优化网络带宽资源，与远程 Panorama 管理服务器相比，为防火墙提供更多带宽向邻近日志收集器发送日志。
- 让您能够满足区域监管要求（例如，不允许日志离开特定区域的规定）。

分布式日志收集说明具有高可用性配置的 Panorama 对端设备管理防火墙和专用日志收集器的部署和配置的拓扑。

您可以在高可用性配置中部署 *Panorama* 管理服务器，但不是专用日志收集器。

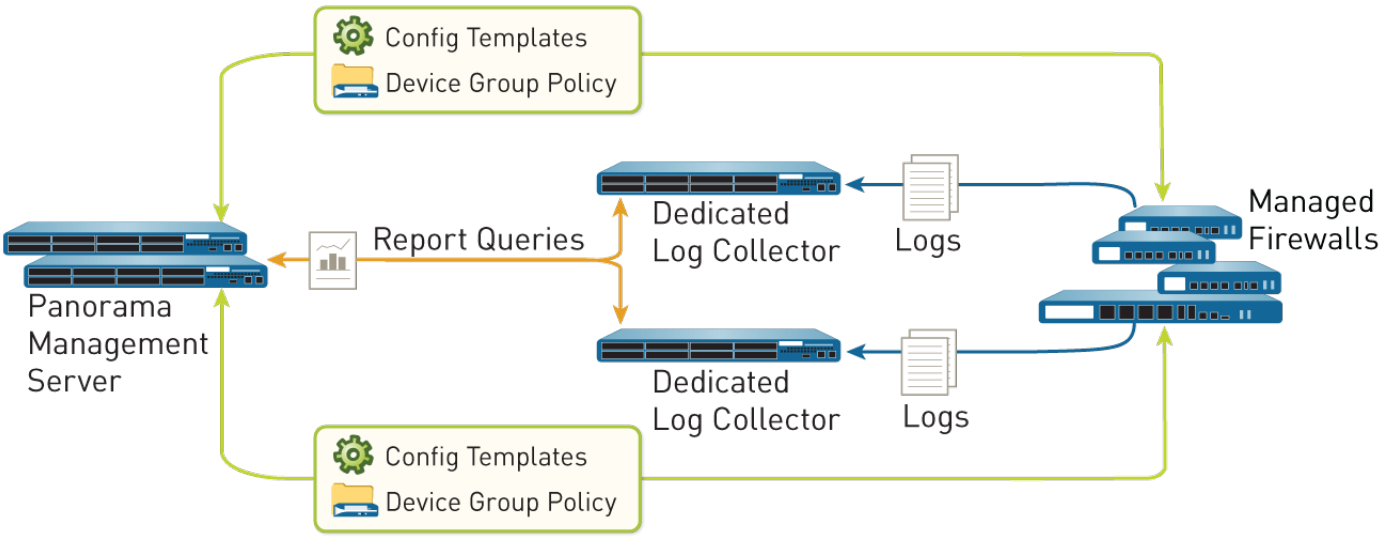


图 4: 分布式日志收集

具有多个日志收集器的收集器组的说明

您可以将收集器组配置为具有多个日志收集器（最多 16 个），从而确保日志冗余，提高日志保存期并适应超过单个日志收集器容量的日志记录速率（请参阅 Panorama 型号了解容量信息）。在任何单个收集器组中，所有日志收集器均必须在相同的 Panorama 型号上运行：均为 M-600 设备、均为 M-500 设备、均为 M-200 设备或均为 Panorama 虚拟设备。例如，如果单个受管防火墙生成 48TB 的日志，则接收这些日志的

© 2019 Palo Alto Networks, Inc.

收集器组将需要至少六个本身就是 M-200 设备的日志收集器或两个本身就是 M-500 设备或 Panorama 虚拟设备的日志收集器。

具有多个日志收集器的收集器组会将可用存储空间用作一个逻辑单元，并均匀地在其所有日志收集器之间分布日志。日志分发基于日志收集器的磁盘容量（请参阅Panorama 型号），并且哈希算法可动态确定拥有日志并将其写入磁盘的日志收集器。虽然 Panorama 使用首选项列表优先处理可以转发日志的受管防火墙的日志收集器列表，但并不一定需要将日志写入在首选项列表中指定的第一个日志收集器。例如，需要考虑以下首选项列表：

受管防火墙	在收集器组中定义的日志转发首选项列表
FW1	L1,L2,L3
FW2	L4,L5,L6

使用此列表，只要主日志收集器可用，FW1 就会将日志转发到 L1。但是，根据哈希算法，Panorama 可能会选择 L2 作为将日志写入其磁盘的所有者。如果 L2 变得不可访问或发生机箱故障，FW1 将由于它仍然可以连接到 L1 而无法知道其故障。

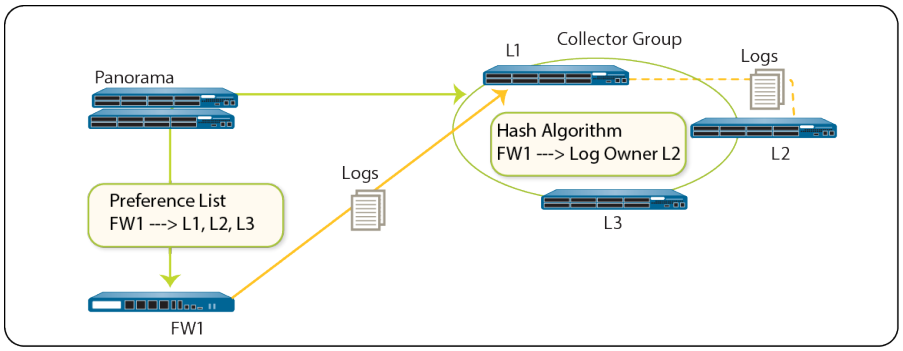


图 5: 示例 - 典型日志收集器组设置

在收集器组只有一个日志收集器且日志收集器出现故障的情况下，防火墙会将日志存储到其 HDD/SSD（可用存储空间因 防火墙型号而有所不同）。只要将连接恢复到日志收集器，防火墙就会在发生故障前继续转发停止的日志。

在收集器组具有多个日志收集器的情况下，如果只有一个日志收集器停机，则防火墙不会将日志缓存到其本地存储器。在 L2 关闭的示例场景中，FW1 继续向 L1 发送日志，L1 会缓存无法重新分发给 L2 的日志。一旦完成 L2 备份，L1 将不再存储前往 L2 的日志数据，而分发将按预期恢复。如果收集器组内某个日志收集器停机，写入停机日志收集器的日志会被重新分发到首选项列表中的下一个日志收集器。

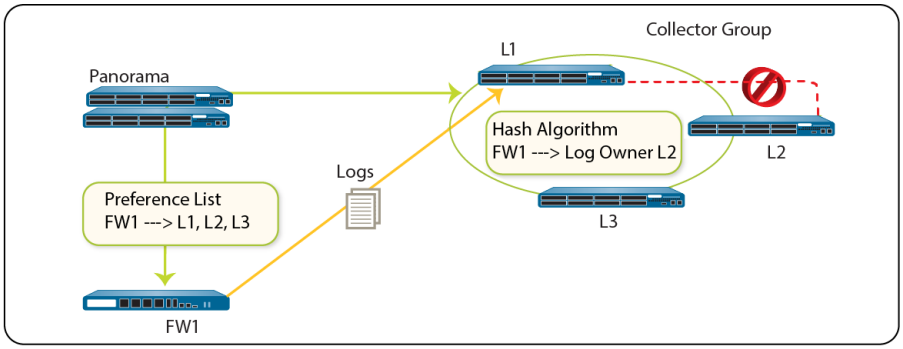


图 6: 示例 - 日志收集器失败时

© 2019 Palo Alto Networks, Inc.

如果在收集器组中使用多个日志收集器，Palo Alto Networks 建议您执行以下迁移：

- 当您配置收集器组时，启用日志冗余。这样做可以确保，当收集器组中的任何一个日志收集器变得无法使用时，所有日志都不会丢失。每个日志都将具有两个副本，而且每个副本都将都驻留在不同的日志收集器上。日志冗余只有在每个日志收集器拥有相同数量的日志记录磁盘时才可用。

  由于启用冗余会创建更多日志，因此该配置需要更多存储容量。当收集器组用完容量空间后，将会删除较早的日志。

  启用冗余会将收集器组中的日志处理通信增加一倍，从而将其最大日志记录速率降低一半，因为每个日志收集器均必须分发其收到的每个日志的副本。
- 获取现场备份 (OSS) 以在日志收集器发生故障时提示更换。
- 除了将日志转发到 Panorama，配置向外部服务转发为备份存储。外部服务可以是 syslog 服务器、电子邮件服务器、SNMP 陷阱服务器或 HTTP 服务器。

日志转发选项

默认情况下，每个防火墙都会将其日志存储在本地。要使用 Panorama 来集中地监控日志和生成报告，您必须配置 Panorama 的日志转发。Panorama 支持将日志转发给日志收集器、Cortex 数据湖，或并行转发给两者。您还可以通过将日志转发到直接来自防火墙或来自 Panorama 的服务，使用外部服务进行存档、通知或分析。外部服务包括 syslog 服务器、电子邮件服务器、SNMP 陷阱服务器或基于 HTTP 的服务。除了转发防火墙日志外，您还可以转发 Panorama 管理服务器和日志收集器生成的日志。Panorama 管理服务器、日志收集器或转发日志的防火墙会将它们转换为适合目标（syslog 消息、电子邮件通知、SNMP 陷阱或 HTTP 负载）的格式。

Palo Alto Networks 防火墙和 Panorama 支持以下日志转发选项。在选择选项之前，请考虑您的 Panorama 型号日志记录容量，并确定 Panorama 日志存储要求。

- 将日志从防火墙转发到 Panorama 和从 Panorama 转发到外部服务 — 此配置最适合用于防火墙和外部服务之间连接的没有足够带宽来以维持日志记录速率这一情况下的部署（在远程连接条件下，带宽往往不足）。此配置通过减轻 Panorama 的一部分处理负载来提高防火墙性能。

  您可以将每个收集器组都配置为向不同目标转发日志。

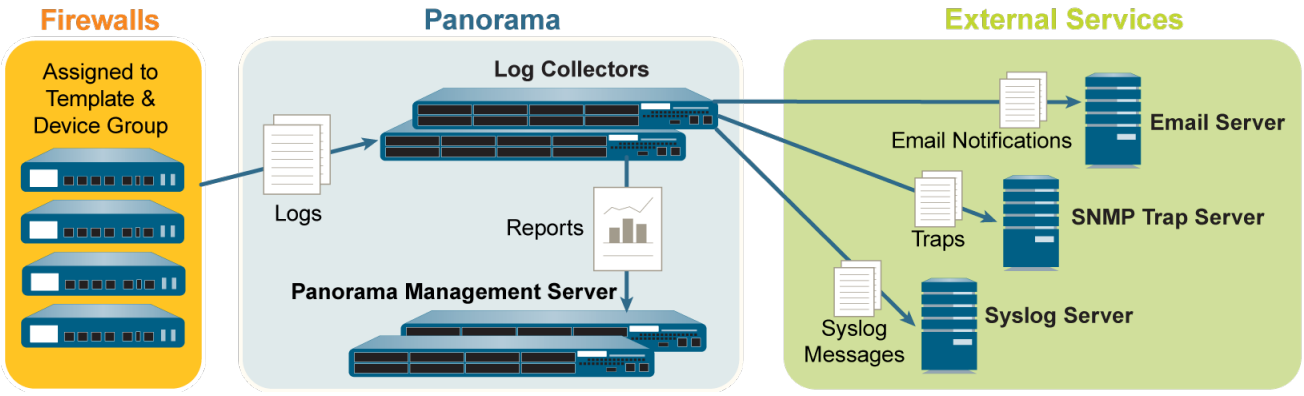


图 7: 将日志转发到 **Panorama** 后再转发到外部服务

- 同时将日志从防火墙转发到 Panorama 和外部服务 — 在此配置中，Panorama 和外部服务都是单独的日志转发流程的端点；防火墙不依赖 Panorama 将日志转发到外部服务。此配置最适合用于防火墙和外部服务之间连接的拥有充足带宽来以维持日志记录速率这一情况下的部署（在本地连接条件下，带宽往往充足）。

© 2019 Palo Alto Networks, Inc.

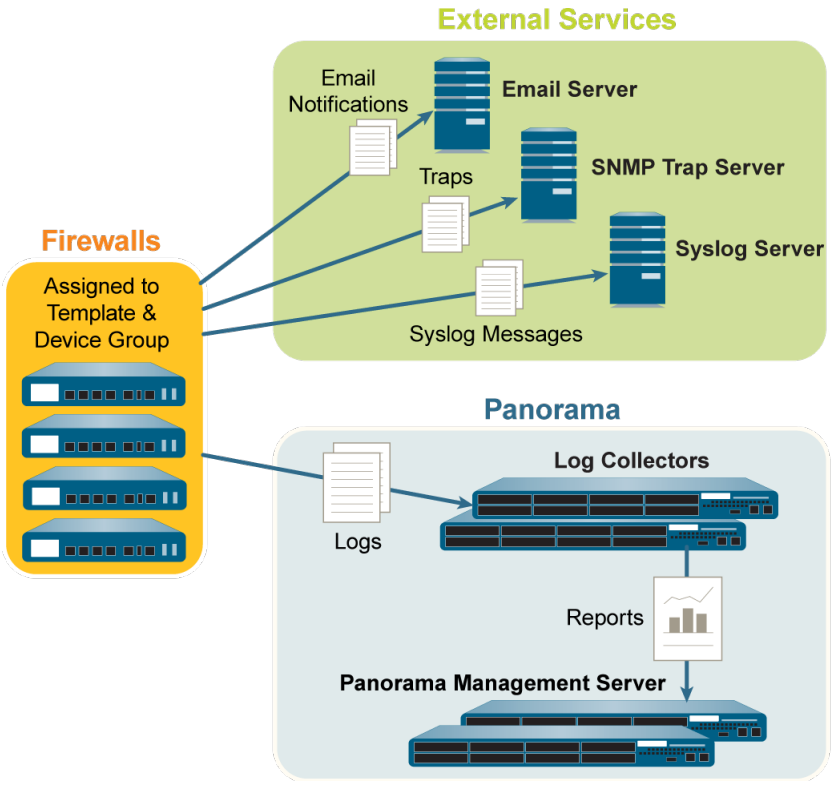


图 **8:** 同时将日志转发到外部服务和 **Panorama**

集中报告

Panorama 可聚合所有受管防火墙的日志并启用有关聚合数据的报告，生成整个网络的应用程序使用情况、用户活动和流量模式的全局视图。只要将防火墙添加到 Panorama，应用程序命令中心就可以显示遍历网络的所有流量。在启用日志记录后，单击应用程序命令中心中的日志条目，以提供直接访问有关应用程序的更精细的详细信息。

要生成报告，Panorama 使用两个来源：本地 Panorama 数据库及其管理的远程防火墙。Panorama 数据库是指在 Panorama 中分配用于存储摘要日志和一部分详细日志的本地存储设备。如果您拥有分布式日志收集部署，则 Panorama 数据库将包括 Panorama 的本地存储设备和所有受管日志收集器。Panorama 将按照每 15 分钟的时间间隔，汇总从受管防火墙收集的流量、应用程序和威胁的相关信息。使用本地 Panorama 数据库可以加快响应时间，但如果您不希望将日志转发到 Panorama，则 Panorama 可直接访问远程防火墙并运行本地存储在受管防火墙上的数据报告。

Panorama 提供了可以按原样使用的 40 多个预定义报告，或者可以通过结合其他报告的元素自定义这些报告，生成可以保存的自定义报告和报告组。可以按照需求和重复计划生成报告，并计划通过电子邮件交付这些报告。这些报告提供了有关用户和上下文的信息，便于您关联事件，以及识别模式、趋势和感兴趣的潜在区域。使用日志记录和报告的集成方法，应用程序命令中心可通过与同一事件关联的多个日志启用条目的相关性。

有关详细信息，请参阅监控网络活动。

© 2019 Palo Alto Networks, Inc.

使用 Panorama 重新分发数据

使用数据重新分发，您只需配置每个源一次，然后就可根据需要将多种数据类型重新分发到任意数量的客户端。这有助于您扩展网络，以便您可以根据网络需求的变化轻松添加或移除源和客户端。

而且，通过仅将信息类型重新分发给您指定的防火墙或 Panorama 管理系统，数据重新分发还提供了精细控制。您可以使用子网、范围和区域来进一步减少网络流量并最大化设备容量。

Palo Alto Networks 防火墙的主要优点之一是可以执行策略并根据用户名和标记（而非 IP 地址）生成报告。大规模网络面临的挑战是确保每个执行策略和生成报告的防火墙都具有应用于所有策略规则的映射和标记。此外，每个防火墙执行身份验证策略需要您的用户群的一组完整的相同身份验证时间戳。无论用户何时进行身份验证以访问服务和应用程序，单个防火墙都会记录相关的时间戳，但不会自动与其他防火墙共享以确保一致性。数据重新分发通过使您能够重新分发必要数据来解决大规模网络面临的这些挑战。但是，您无需建立额外连接来在防火墙之间重新分发数据，而是可以利用 Panorama 基础架构来 重新分发数据到受管防火墙。该基础架构具有现有连接，使您能够分层从防火墙重新分发数据到 Panorama。然后，Panorama 可以将信息重新分发到防火墙，从而执行策略并生成报告。

每个防火墙或 Panorama 管理服务器均可从最多 100 个重新分发点接收数据。重新分发点可以是其他防火墙或 Panorama 管理服务器。但是，您也可以使用基于 Windows 的 User-ID 代理执行映射并将信息重新分发给防火墙。当用户流量与身份验证策略规则匹配时，只有防火墙才会记录身份验证时间戳。

© 2019 Palo Alto Networks, Inc.

基于角色的访问控制

基于角色的访问控制 (RBAC) 可让您定义管理用户（管理员）的特权和责任。每一个管理员都必须具有一个指定了角色和身份验证方法的用户帐户。管理角色定义了对 Panorama 和防火墙上下文内特定配置设置、日志和报告的访问权限。对于设备组和模板管理员，您可以将角色映射到访问域，后者定义了对特定设备组、模板和防火墙的访问权限（通过上下文切换）。一旦将每个访问域与一个角色相结合，您便可以在您组织的功能性或地区性区域之间强制执行信息分离。例如，您可以限制管理员为数据中心防火墙监控活动，但允许该管理员为测试实验室防火墙设置策略。默认情况下，每一台 Panorama 设备（虚拟设备或 M 系列设备）都具有一个预定义管理帐户 (admin)，该帐户提供了对所有功能性区域和所有设备组、面板及防火墙的完全读写访问权限（超级访问权限）。对于每一个管理员，您可以定义确定 Panorama 如何验证用户访问凭据的身份验证配置文件。



作为最佳做法，您应为需要访问 *Panorama* 上管理或报告功能的每位用户创建一个单独的管理帐户，而不是将默认帐户用于所有管理员。这样可以更好地防范未经授权的配置更改，并使 *Panorama* 能够记录和识别每个管理员的操作。

- 管理角色
- 身份验证配置文件和序列
- 访问域
- 管理身份验证

管理角色

您可以根据贵组织、网络使用的任何现有身份验证服务以及所需管理角色的安全要求来配置管理员帐户。角色定义了管理员可用系统访问权限的类型。您可以根据需要广泛地或细致地定义和限制访问权限，具体取决于您组织的安全需求。例如，您可以决定数据中心管理员有权访问所有设备和联网配置，但安全管理员只可以控制安全策略定义，而其他重要的可以具有有限的 CLI 或 XML API 访问权限。角色类型包括：

- 动态角色 — 这些是内置角色，可提供对 Panorama 和受管防火墙的访问权限。添加新功能时，Panorama 会自动更新动态角色的定义；您不需要手动更新这些角色。下表列出了与动态角色相关的访问权限。

动态角色	权限
超级用户	对 Panorama 的完全读写访问权限
超级用户（只读）	对 Panorama 的只读访问权限
Panorama 管理员	对 Panorama 的完全访问权限，但以下操作除外： • 创建、修改或删除 Panorama 或防火墙管理员及角色。 • 在 **Device** > **Setup** > **Operations**（设备 > 设置 > 操作）页面上导出、验证、恢复、保存、加载或导入配置。 • 在 **Panorama** 选项卡中配置 **Scheduled Config Export**（已调度配置导出）功能。

- 管理员角色配置文件 — 要对 Web 界面、CLI 和 XML API 的功能区域提供更精细的访问权限控制，您可以创建自定义角色。将新功能添加到产品时，您必须使用相应的权限更新角色：Panorama 不会自动将新功能添加到自定义角色定义。当您配置管理角色配置文件时，应选择以下配置文件类型之一。

© 2019 Palo Alto Networks, Inc.

管理角色配置文件	说明
Panorama	对于这些角色，您可以将读写访问权限、只读访问权限分配给可供超级用户动态角色使用的所有 Panorama 功能，也可以不分配任何访问权限，但管理 Panorama 管理员和 Panorama 角色的功能除外。对于后两者，您可以分配只读访问权限或者不分配任何访问权限，但不能分配读写访问权限。 安全管理员需要对 Panorama 上的安全策略定义、日志和报告进行访问就是使用 Panorama 角色的一个例子。

设备组和模板	对于这些角色，您可以分配对设备组、模板和防火墙上下文内特定功能性区域的读写访问权限或只读访问权限，或不分配任何访问权限。一旦将这些角色与访问域相结合，您便可以在您组织的功能性或地区性区域之间强制执行信息分离。设备组和模板角色具有以下限制：
	• 没有对 CLI 或 XML API 的访问权限
	• 没有对配置或系统日志的访问权限
	• 没有对 VM 信息源的访问权限
	• 在 **Panorama** 选项卡中，访问权限仅适用于：
	  • 设备部署功能（读写、只读或无权访问）
	  • 管理员帐户中指定的设备组（读写、只读或无权访问）
	  • 管理员帐户中指定的模板和受管防火墙（读写、只读或无权访问）
	此角色的一个例子是，您的操作人员中的管理员需要访问特定设备组和/或模板的 Web 界面的设备和网络配置区域。

身份验证配置文件和序列

身份验证配置文件定义在管理员访问 Panorama 时对其登录凭据进行验证的身份验证服务。该服务可以是本地身份验证或外部身份验证服务。一些服务（SAML、TACACS+ 和 RADIUS）提供了在外部服务器（而非 Panorama）上管理管理帐户的身份验证和授权的选项。除了身份验证服务外，身份验证配置文件还定义了诸如 Kerberos 单点登录 (SSO) 和 SAML 单点登出 (SSO) 等选项。

一些网络具有多个数据库（例如 TACACS+ 和 LDAP）以用于不同用户和用户组。要在这种情况下对管理员进行身份验证，请配置身份验证序列 — 登录时 Panorama 与管理员匹配的身份验证配置文件的排列次序。Panorama 依次检查每个配置文件，直到成功验证管理员的身份。只有序列中所有配置文件的身份验证都失败时，才会拒绝管理员访问。

访问域

访问域控制对特定设备组和模板的管理访问，并且还控制将上下文切换到受管防火墙的 Web 界面的能力。访问域只适用于具有设备组和模板角色的管理员。将管理角色映射到访问域，能让您非常精细地控制管理员在 Panorama 上访问的信息。例如，假定您配置了一个访问域，其数据中心包含防火墙的所有设备组，您将此访问域分配给一个可监控数据中心流量，但不能配置防火墙的管理员。在这种情况下，您将访问域映射到特定角色，此角色拥有所有监控权限，但没有对设备组设置的访问权限。此外，设备组和模板管理员可以在其访问域中为受管防火墙执行管理任务，例如查看配置和系统日志、执行配置审计、查看挂起的任务以及直接访问防火墙操作（如重新启动、生成技术支持文件、执行统计数据转储和导出核心文件）。

您可以在本地 Panorama 配置中配置访问域，然后将它们分配给管理帐户和角色。您可以在本地执行分配或使用外部 SAML、TACACS+ 或 RADIUS 服务器进行分配。使用外部服务器能您通过目录服务快速重新分配访问域，而无需在 Panorama 上重新配置设置。要使用外部服务器，您必须定义使 Panorama 能够访问服务器的服务器配置文件。您还必须在 RADIUS 或 TACACS+ 服务器上定义供应商特定属性 (VSA)，或在 SAML IdP 服务器上定义 SAML 属性。

© 2019 Palo Alto Networks, Inc.

例如，如果您使用 RADIUS 服务器，则需要为每个管理员定义一个 VSA 编号和值。定义的值必须与 Panorama 上配置的访问域匹配。管理员尝试登录 Panorama 时，Panorama 将向 RADIUS 服务器查询管理员的访问域和属性号。根据 RADIUS 服务器的响应，管理员将获得访问授权，并被限制为只能访问已分配到访问域中的防火墙、虚拟系统、设备组和模板。

有关相应的程序，请参阅：

- 配置访问域。
- 为 Panorama 管理员配置 RADIUS 身份验证。
- 为 Panorama 管理员配置 TACACS+ 身份验证。
- 为 Panorama 管理员配置 SAML 身份验证。

管理身份验证

您可以为防火墙管理员配置以下类型的身份验证和授权（管理角色和访问域）：

身份验证方法	身份验证方法	说明
本地	本地	管理帐户凭据和身份验证机制对 Panorama 而言均属于本地。您可以使用 Panorama 将管理角色和访问域分配给帐户。若要进一步保护帐户，应创建定义密码有效期并设定 Panorama 范围内密码复杂性设置的密码配置文件。有关详细信息，请参阅为 Panorama 管理员配置本地或外部身份验证。
SSH 密钥	本地	管理帐号对 Panorama 而言属于本地，但对 CLI 的身份验证却基于 SSH 密钥。您可以使用 Panorama 将管理角色和访问域分配给帐户。有关详细信息，请参阅针对命令行界面为管理员配置基于 SSH 密钥的身份验证。
证书	本地	管理帐号对 Panorama 而言属于本地，但对 Web 界面的身份验证却基于客户端证书。您可以使用 Panorama 将管理角色和访问域分配给帐户。有关详细信息，请参阅针对 Web 界面为 Panorama 管理员配置基于证书的身份验证。
外部服务	本地	Panorama 本地定义的管理帐户作为外部多重因素身份验证、SAML、Kerberos、TACACS+、RADIUS 或 LDAP 服务器上的定义帐户引用。外部服务器执行身份验证。您可以使用 Panorama 将管理角色和访问域分配给帐户。有关详细信息，请参阅为 Panorama 管理员配置本地或外部身份验证。
外部	外部服务	管理帐户仅在外部 SAML、TACACS+ 或 RADIUS 服务器上定义。服务器执行身份验证和授权。对于授权，您可以在 TACACS+ 或 RADIUS 服务器上定义供应商特定属性 (VSA)，或在 SAML 服务器上定义 SAML 属性。Panorama 将这些属性映射到您在 Panorama 上定义的管理员角色和访问域。有关详细信息，请参阅： • 为 Panorama 管理员配置 SAML 身份验证 • 为 Panorama 管理员配置 TACACS+ 身份验证 • 为 Panorama 管理员配置 RADIUS 身份验证

© 2019 Palo Alto Networks, Inc.

Panorama 提交、验证和预览操作

当您准备激活对 Panorama 上的候选配置所作的更改或将更改推送到 Panorama 管理的设备（防火墙、日志收集器、WildFire 设备和设备群集）时，您可以预览、验证或提交配置更改。例如，如果您向 Panorama 配置添加日志收集器，防火墙不能向此日志收集器发送日志，直到您向 Panorama 提交更改，然后将更改推送到包含此日志收集器的收集器组。

您可以按管理员或位置筛选更改，然后仅提交、推送、验证或预览这些更改。位置可以是特定设备组、模板、收集器组、日志收集器、共享设置或 Panorama 管理服务器。

在提交更改后，这些更改成为正在运行的配置的一部分。未提交的更改是待选配置的一部分。Panorama 会将提交请求整理成队列，以便您可在之前的提交操作处于进行状态时，启动新的提交操作。Panorama 按提交启动顺序执行提交，但会优先执行 Panorama 启动的自动提交（如 FQDN 刷新）。但是，如果队列中管理员启动的提交已达到最大数量 (10)，则必须等待 Panorama 完成暂挂提交的处理后，才能启动新提交。您可以使用 Panorama 任务管理器 (Tasks) 取消暂挂提交或查看暂挂、进行中、已完成或失败提交的详细信息。要检查提交将激活的更改，可运行提交预览。

启动提交时，Panorama 会检查更改是否有效后再激活。验证输出将显示阻止提交（出错），或须知的重要事项（警告）的条件。例如，验证可能指出一个需要修复才能提交成功的无效路径目标。验证过程能让您在提交之前查找和修复错误（不会对正在运行的配置进行任何更改）。如果您拥有固定提交窗口，并且希望确保提交将成功而没有出现错误，这将非常有用。

默认情况下启用自动提交恢复，这就允许受管防火墙在本地测试从 Panorama 推送的配置，以验证新更改不会中断 Panorama 与受管防火墙之间的连接。如果提交的配置会中断 Panorama 与受管防火墙之间的连接，则防火墙会自动使提交失败并且配置会恢复到先前运行的配置，而且共享策略或模板状态（**Panorama** > **Managed Devices**（受管设备）> **Summary**（摘要））根据推送的配置对象退出同步。此外，受管防火墙每隔 60 分钟会测试一次它与 Panorama 的连接，而且，如果受管防火墙检测到它再也无法成功连接到 Panorama，就会将配置恢复为先前运行的配置。



有关待选和运行配置的详细信息，请参阅管理 Panorama 和防火墙配置备份。

要阻止多个管理员在当前会话期间对配置进行更改，请查阅 管理配置更改限制锁。

将配置推送到受管防火墙时，*Panorama* 会推送运行的配置。因此，在您首次将更改提交到 *Panorama* 之前，*Panorama* 不会让您将更改推送到受管防火墙。

© 2019 Palo Alto Networks, Inc.

计划您的 Panorama 部署

- 确定管理方法。您是否计划使用 Panorama 在网络的受管防火墙之间集中配置和管理策略，集中管理软件、内容和许可证更新和/或进行集中日志记录和报告？

  如果您已经在网络中部署和配置 Palo Alto Networks 防火墙，可确定是否将防火墙过渡至集中管理。该流程需要将所有配置和策略从防火墙迁移至 Panorama。有关详细信息，请参阅从防火墙过渡到 Panorama 管理。
- 验证 Panorama 和防火墙的软件版本。Panorama 可管理 PAN-OS 运行版本与 Panorama 版本匹配或低于 Panorama 版本的的防火墙。例如，Panorama 8.0 不能管理运行 PAN-OS 8.1 的防火墙。此外，Panorama 8.1 无法管理运行 PAN-OS 6.0.0 - 6.0.3 的防火墙，且无法管理运行高于 Panorama 版本的 PAN-OS 版本的防火墙。
- 计划在所有受管防火墙之间使用相同的 URL 筛选数据库（BrightCloud 或 PAN-DB）。如果某些防火墙使用 BrightCloud 数据库，而其他防火墙使用 PAN-DB，则 Panorama 只能管理其中一种数据库或其他 URL 筛选数据库的安全规则。必须在使用该数据库的防火墙本地管理其他数据库的 URL 筛选规则。
- 确定 Panorama 与其受管设备和高可用性对端设备之间的身份验证方法。默认情况下，Panorama 使用预定义证书对用于管理和设备间通信的 SSL 连接进行身份验证。但是，您可以配置自定义的基于证书的身份验证以增强 Panorama、防火墙和日志收集器之间的 SSL 连接的安全性。通过使用自定义证书，您可以建立唯一的信任链，以确保 Panorama 与其管理的设备之间的相互身份验证。您可以从企业公钥基础结构 (PKI) 导入证书或在 Panorama 上生成证书。
- 计划在高可用性配置中使用 Panorama；将其设置为主动/被动高可用性对。请参阅 Panorama 高可用性。
- 计划如何在大规模部署中适应网络分段和安全需求。默认情况下，在 M 系设备上运行的 Panorama 使用管理 (MGT) 接口管理 Panorama 的访问权限并管理设备（防火墙、日志收集器、WildFire 设备和设备群集），收集日志，与收集器组通信以及将软件和内容更新部署到设备。但是，为了提高安全性并启用网络分段，您可以为管理访问权限预留 MGT 接口并为其他服务使用专用M 系列设备接口（Eth1、Eth2、Eth3、Eth4 和 Eth5）。
- 如需网络活动的有意义的报告，应计划日志记录解决方案：
  - 检验 AWS 或 Azure 上以日志收集器模式部署的 Panorama 虚拟设备的资源分配。如果调整其大小，则 Panorama 虚拟设备不会保留日志收集器模式。这就会导致日志数据丢失。
  - 估计您的网络需要的日志存储容量，以满足安全性和合规性要求。需要考虑您的 Panorama 型号的日志记录容量等因素，例如网络拓扑接口、发送日志的防火墙数量、日志流量类型（例如，URL 筛选和威胁日志与流量日志）、防火墙生成日志的速率，以及您希望在 Panorama 上存储日志的天数。有关详细信息，请参阅确定 Panorama 日志存储要求。
  - 除 Panorama 外，您是否需要将日志转发到外部服务（如 syslog 服务器）？请参阅日志转发选项。
  - 是想拥有或管理自己的本地日志存储，还是想利用 Palo Alto Networks 提供的 Cortex 数据湖？
  - 如果您需要长期存储解决方案，您是否拥有转发日志所需的安全信息和事件管理 (SIEM) 解决方案（如 Splunk 或 ArcSight）？
  - 您是否需要日志记录冗余？

    如果配置具有多个日志收集器的收集器组，则可以启用冗余以确保在任何一个日志收集器不可用时都不会丢失日志（请参阅具有多个日志收集器的收集器组的说明）。

    如果您在 HA 配置中以传统模式部署 Panorama 虚拟设备，则受管防火墙可以将日志发送到两个 HA 对端设备，以便每个对端设备都驻留有每个日志的副本。此冗余选项默认启动（请参阅修改日志转发和缓冲默认设置）。
  - 您将记录到网络文件系统 (NFS) 吗？如果 Panorama 虚拟设备处于传统模式且不管理专用日志收集器，则 NFS 存储是将日志存储容量增加到 8TB 以上的唯一选择。仅当 Panorama 在 ESXi 服务器上运行时 NFS 存储仅才可用。如果使用 NFS 存储，请记住受管防火墙只能将日志发送到高可用性对中的主要对端设备；只能将主要对端设备安装到 NFS 且可以写入。
- 确定管理员访问受管防火墙和 Panorama 所需的基于角色的访问权限。请参阅设置 Panorama 的管理访问权限。

© 2019 Palo Alto Networks, Inc.

- 计划所需的设备组。考虑是根据功能、安全策略、地理位置还是网络分段来对防火墙进行分组。将研发团队使用的所有防火墙分为一组就是基于功能的设备组的一个例子。考虑是根据共性创建较小的设备组，或是创建扩展更为轻松的较大设备组，还是创建可简化复杂管理层级的设备组层次。
- 计划管理策略的分层策略。考虑防火墙如何继承和评估设备组层次内的策略规则，并考虑如何最佳地实施共享规则、设备组规则和防火墙特定规则以满足您的网络需求。对于可见性和集中策略管理，即使您需要共享或设备组规则的防火墙特定例外，也可以考虑使用 Panorama 来管理规则。必要时，可将策略规则推送到防火墙的子集（一个设备组内）。
- 根据防火墙继承来自模板和模板堆栈的网络配置设置的方式，计划防火墙的组织。例如，根据硬件型号、地理接近性和对时区、DNS 服务器及接口设置的相似网络需求，考虑将防火墙分配到模板。

© 2019 Palo Alto Networks, Inc.

部署 Panorama：任务概述

下面的任务列表总结了开始使用 Panorama 的步骤。有关如何使用 Panorama 进行集中式管理的示例，请参阅用例：使用 Panorama 配置防火墙。

STEP 1 | （仅限 M 系列设备）将设备安装到机架上。

STEP 2 | 执行初始配置，启用 Panorama 的网络访问。请参阅 设置 Panorama 虚拟设备或设置 M 系列设备。

STEP 3 | 注册 Panorama 和安装许可证。

STEP 4 | 安装 Panorama 的内容和软件更新。

STEP 5 | （推荐）在高可用性配置中设置 Panorama。请参阅Panorama 高可用性。

STEP 6 | 添加防火墙作为受管设备。

STEP 7 | 添加设备组 或创建设备组层次、添加模板以及（如适用）配置模板堆栈。

STEP 8 | （可选）配置将日志转发到 Panorama 和/或外部服务。请参阅管理日志收集。

STEP 9 | 监控网络活动使用 Panorama 上的可见性和报告工具。

© 2019 Palo Alto Networks, Inc.

设置 *Panorama*

为了实现跨网络上所有防火墙的集中式报告和连贯策略管理，您可以部署 Panorama™ 管理服务器作为虚拟设备或硬件设备（M-200、M-500 或 M-600 设备）。

以下主题介绍如何在您的网络上设置 Panorama：

> 确定 Panorama 日志存储要求
> 设置 Panorama 虚拟设备
> 设置 M 系列设备
> 注册 Panorama 和安装许可证
> 安装 Panorama 设备证书
> 安装 Panorama 的内容和软件更新
> 过渡到另一 Panorama 型号
> 访问和导航 Panorama 管理界面
> 设置 Panorama 的管理访问权限
> 使用自定义证书设置身份验证

确定 Panorama 日志存储要求

当您计划 Panorama 部署时，应估计 Panorama 型号需要多大日志存储容量，以确定要部署哪些、是否在这些型号上将存储器扩展至超过它们的默认容量、是否部署专用日志收集器以及是否配置从 Panorama 到外部目标的日志转发。当日志存储达到最大容量时，Panorama 会自动地删除较早的日志来为新日志创造空间。

执行以下步骤确定 Panorama 需要的大约日志存储容量。有关详细信息和用例，请参阅 Panorama 规格和设计指南。

STEP 1 | 确定您组织的日志保留要求。

影响保留要求的因素包括：

- 您组织的 IT 策略
- 日志冗余性 — 如果您在配置收集器组时启用日志冗余性，每个日志将有两个副本，这会使所需日志存储容量翻倍。
- 监管要求，例如支付卡行业数据安全标准 (PCI DSS)、萨班斯-奥克斯利法案及美国健康保险携带和责任法案 (HIPAA) 的规定。



如果您的组织要求在一定时间之后删除日志，则您可以为每种日志类型设置过期期限。如果您需要按类型划定日志保留优先次序，您也可以将每种日志类型的存储配额设置为总空间的百分比。有关详细信息，请参阅管理日志和报告的存储配额和过期期限。

STEP 2 | 确定平均每日日志记录速率。

每天在高峰期和非高峰期多次执行此操作，以估计平均值。您采样速率越频繁，您的估计就越准确。

1. 以每秒条数为单位显示当前的日志生成速率：
   - 如果 Panorama 目前尚未收集日志，则访问每个防火墙的 CLI，运行以下命令，然后计算所有防火墙的总速率。此命令可显示上一秒内接收的日志数。

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

   - 如果 Panorama 已经在手机日志，则在接收日志的每个设备（Panorama 管理服务器或专用日志收集器）的 CLI 中运行以下命令，然后计算总速率。此命令可给出上五分钟的平均日志记录速率。

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



您还可以使用 *SNMP* 管理器来确定日志收集器的日志记录速率（请参阅 *panLogCollector MIB*，*OID 1.3.6.1.4.1.25461.1.1.6*）和防火墙（请参阅 *panDeviceLogging, OID 1.3.6.1.4.1.25461.2.1.2.7*）。

2. 计算取样速率的平均值。
3. 将平均每秒日志数乘以 86,400，计算每日日志记录速率。

STEP 3 | 估计所需的存储容量。



此公式提供的只是一个估计值；所需存储的精确容量将与公式结果有所差异。

使用公式：

<required_storage_duration> x <average_log_size> x <average_logging_rate>

平均日志大小会随日志类型而呈现明显差异。但是，您可以使用 500 字节作为近似的平均日志大小。

© 2019 Palo Alto Networks, Inc.

例如，如果 Panorama 必须将日志存储 30 天且所有防火墙的平均总日志记录速率为每天 21,254,400 条日志，则所需的日志存储容量为：30 x 500 x 21,254,400 = 318,816,000,000 字节（大约为 318GB）。

STEP 4 | 后续步骤...

如果您确定 Panorama 需要更多日志存储容量：

- 扩展 Panorama 虚拟设备上的日志存储容量。
- 增加 M 系列设备上的存储容量。

© 2019 Palo Alto Networks, Inc.

设置 Panorama 虚拟设备

Panorama 虚拟设备使您能够使用现有 Vmware 虚拟基础架构集中管理和监控 Palo Alto Networks 防火墙和专用日志收集器。您可以在 ESXi 服务器、Amazon Web Services(AWS)、AWS GovCloud、Microsoft Azure、Google Cloud Platform(GCP)、KVM、Hyper-V 或 vCloud Air 上安装虚拟设备。除了部署专用日志收集器之外或代替部署专用日志收集器，您可以将防火墙日志直接转发到 Panorama 虚拟设备。为了获得更大的日志存储容量和更快的报告，您可以选择将虚拟设备从传统模式切换到 Panorama 模式并配置本地日志收集器。有关 Panorama 虚拟设备及其模式的更多详细信息，请参阅 Panorama 型号。

以下主题都假设您熟悉创建虚拟设备所需的公共和专有管理程序产品且不涉及任何相关概念或术语。

- 设置 Panorama 虚拟设备的前提条件
- 安装 Panorama 虚拟设备
- 执行 Panorama 虚拟设备的初始配置
- 设置 Panorama 虚拟设备为日志收集器
- 使用本地日志收集器设置 Panorama 虚拟设备
- 在 Panorama 模式下设置 Panorama 虚拟设备
- 在仅管理模式下设置 Panorama 虚拟设备
- 扩展 Panorama 虚拟设备上的日志存储容量
- 增加 Panorama 虚拟设备上的 CPU 和内存
- 增加 Panorama 虚拟设备上的系统磁盘
- 完成 Panorama 虚拟设备设置

设置 Panorama 虚拟设备的前提条件

安装 Panorama 虚拟设备前，完成下列任务：

- 使用浏览器访问 Palo Alto Networks 客户支持网站，然后注册 Panorama。您将需要使用在订单执行电子邮件中收到的 Panorama 序列号。注册 Panorama 之后，您便可以访问 Panorama 软件下载页面。
- 查看受支持的 Panorama 管理程序，以检验此管理程序是否满足部署 Panorama 的最低版本要求。
- 如要在 VMware ESXi 服务器上安装 Panorama，请验证该服务器是否满足Panorama 虚拟设备系统要求中所列的最低要求。这些要求适用于 Panorama 5.1 及更高版本。这些要求取决于您是以 Panorama 模式还是“仅管理”模式运行虚拟设备。有关模式的详细信息，请参阅 Panorama 型号。

  如果在 *VMware vCloud Air* 上安装 *Panorama*，则可以在安装期间设置系统设置。

查看在 Amazon Web Services (AWS)、AWS GovCloud、 Microsoft Azure、 Google Cloud Platform (GCP)、Hyper-V、 KVM 和 VMware ESXi 上部署 Panorama 虚拟设备的最低资源要求，确保虚拟机满足所需模式的最低所需资源（Panorama、仅管理或日志收集器）。Panorama 虚拟设备的最低资源需求旨在帮助您在 Panorama 和“日志收集器”模式下达到每秒日志数最大值 (LPS)。如果您添加或删除虚拟日志记录磁盘而导致配置不满足或超过推荐的虚拟日志记录磁盘数（如下所示），则您的 LPS 将减少。

如果在安装 Panorama 虚拟设备时不满足 Panorama 模式下的最低资源要求，对于所有受支持的公共（AWS、AWS GovCloud、Azure 和 GCP）和专有（Hyper-V、KVM 和 VMware ESXi）管理程序，Panorama 默认为“仅管理”模式。如果不满足“仅管理”模式下的最低资源要求，对于所有受支持的公共管理程序、Hyper-V 和 KVM，Panorama 默认为“维护”模式。如果在在 VMware 上安装 Panorama时不满足“仅管理”模式下的最低资源要求，Panorama 默认为“传统”模式。

© 2019 Palo Alto Networks, Inc.

建议在 *Panorama* 模式下部署 *Panorama* 管理服务器，以获取设备管理和日志收集功能。虽然“传统”模式仍受支持，但不建议在生产环境中使用。此外，您再也无法将 *Panorama* 切换到“传统”模式。有关受支持模式更多的详细信息，请参阅Panorama 型号。

表 **1: Panorama** 虚拟设备系统要求

要求	仅管理模式下的 Panorama 虚拟设备	Panorama 模式下的 Panorama 虚拟设备	日志收集器模式下的 Panorama 虚拟设备
虚拟硬件版本	• **VMware ESXi** 和 **vCloud Air** — 基于 64 位内核的 VMware ESXi 5.5、6.0、6.5 或 6.7。ESXi 服务器支持的虚拟硬件家族类型版本（也称 Vmware 虚拟硬件版本）为 vmx-10 • **Hyper-V** — 带 Hyper-V 角色或 Hyper-V 2016 的 Windows Server 2016 • **KVM** — Ubuntu 16.04 版或 CentOS7 在 Panorama 模式下，运行在任何 ESXi 版本上的虚拟设备最多可支持 12 个虚拟日志记录磁盘，每个虚拟日志记录磁盘的日志存储容量为 2Tb，最大总存储容量为 24TB。 （仅限 VMware ESXi 和 vCloud Air）在“传统”模式下，虚拟设备支持一个虚拟日志记录磁盘。ESXi 5.5 及更高版本可支持一个容量达 8TB 的磁盘。更低版本的 ESXi 可支持一个容量达 2TB 的磁盘。		
（仅限 ESXi 和 vCloud Air） 客户端计算机	要安装 Panorama 虚拟设备并管理其资源，您必须安装与 ESXi 服务器兼容的 VMware vSphere Client 或 VMware Infrastructure Client。		
系统磁盘	• **Default**（默认）— 81GB • **Upgraded**（已升级）— 224GB	• **Default**（默认）— 81GB • **Upgraded**（已升级）— 224GB（SD-WAN 所需） 对于日志存储，Panorama 使用虚拟日志记录磁盘而不是系统磁盘或 NFS 数据存储。	81GB 对于日志存储，Panorama 使用虚拟日志记录磁盘而不是系统磁盘或 NFS 数据存储。

CPU、内存和日志记录磁盘	• 管理最多 500 台受管设备
	  • 16 个 CPU
	  • 32GB 内存
	  • 本地日志存储不受支持
	• 管理最多 1,000 台受管设备
	  • 32 个 CPU
	  • 128GB 内存
	  • 本地日志存储不受支持
	• 如要管理 1,000 个以上防火墙，请参阅提高设备管理容量要求。
		• 最多 10,000 条日志/秒：
		  • 16 个 CPU
		  • 32GB 内存
		  • 4 个 2TB 日志记录磁盘
		  • 管理最多 500 台受管设备
		• 最多 20,000 条日志/秒
		  • 32 个 CPU
		  • 128GB 内存
		  • 8 个 2TB 日志记录磁盘
		  • 管理最多 1,000 台受管设备
			• 最多 15,000 条日志/秒
			  • 16 个 CPU
			  • 32GB 内存
			  • 4 个 2TB 日志记录磁盘
			• 最多 25,000 条日志/秒
			  • 32 个 CPU
			  • 128GB 内存
			  • 8 个 2TB 日志记录磁盘

© 2019 Palo Alto Networks, Inc.

要求	仅管理模式下的 Panorama 虚拟设备	Panorama 模式下的 Panorama 虚拟设备	日志收集器模式下的 Panorama 虚拟设备
日志存储容量	仅管理模式下的 Panorama 要求将日志转发到专用日志收集器。	2TB 至 24TB	2TB 至 24TB

支持的接口

接口可用于设备管理、日志收集、收集器组通信、许可和软件更新。

功能	Amazon Web Services (AWS) 和 AWS GovCloud	Microsoft Azure	Google Cloud Platform (GCP)	KVM	Hyper-V	VMware（ESXi Air）
设备管理	支持的任何接口					
设备日志收集	支持的任何接口					
收集器组通信	支持的任何接口					
许可和软件更新	仅限 MGT 接口	仅限 MGT 接口	仅限 MGT 接口	仅限 MGT 接口	支持的任何接口	支持的任何接口	支持的任何接口

安装 Panorama 虚拟设备

安装前，请决定是否在 Panorama 模式、仅管理模式、日志收集器模式、或传统模式（仅限 VMware）下运行虚拟设备。每种模式均有不同的资源要求，详情请见 设置 Panorama 虚拟设备的前提条件。在开始安装前，您必须完成先决条件。



作为最佳做法，请在 *Panorama* 模式下安装虚拟设备以优化日志存储和报告生成。有关 *Panorama* 和传统模式的详细信息，请参阅 Panorama 型号。

- 在 VMware 上安装 Panorama
- 在 AWS 上安装 Panorama
- 在 AWS GovCloud 上安装 Panorama
- 在 Azure 上安装 Panorama
- 在 Google Cloud Platform 上安装 Panorama
- 在 KVM 上安装 Panorama
- 在 Hyper-V 上安装 Panorama

在 *VMware* 上安装 *Panorama*

您可以在 ESXi 和 vCloud Air Vmware 平台上安装 Panorama 虚拟设备。

- 在 ESXi 服务器上安装 Panorama
- 在 vCloud Air 中安装 Panorama
- Panorama 虚拟设备上的 VMware 工具支持

© 2019 Palo Alto Networks, Inc.

在 ESXi 服务器上安装 Panorama

使用以下说明，在 VMware ESXi 服务器上安装新 Panorama 虚拟设备。对于升级到现有的 Panorama 虚拟设备，请跳转到安装 Panorama 的内容和软件更新。

STEP 1 | 下载 Panorama 10.0 基本映像开放虚拟设备 (OVA) 文件。

1. 访问 Palo Alto Networks 软件下载站点。（如果不能登录，请转到 Palo Alto Networks 客户支持站点获取援助。）
2. 在 Panorama Base Images（Panorama 基本映像）部分的 Download（下载）列中，下载 Panorama 最新版 OVA 文件 (`Panorama-ESX-10.0.0.ova`)。

STEP 2 | 安装 Panorama。

1. 启动 VMware vSphere Client 并连接到 VMware 服务器。
2. 选择 **File** > **Deploy OVF Template**（文件 > 部署 OVF 模板）。
3. **Browse**（浏览）以选择 Panorama OVA 文件，然后单击 **Next**（下一步）。
4. 确认产品名称和说明与下载版本匹配，然后单击 **Next**（下一步）。
5. 为 Panorama 虚拟设备输入一个描述性名称，然后单击 **Next**（下一步）。
6. 选择要安装 Panorama 映像的数据存储位置（系统磁盘）。请参阅 设置 Panorama 虚拟设备的前提条件 了解受支持的系统磁盘大小。选择数据存储后，单击 **Next**（下一步）。
7. 选择 **Thick Provision Lazy Zeroed**（密集配置延迟置零）作为磁盘格式，然后单击 **Next**（下一步）。
8. 指定库存中用于 Panorama 虚拟设备的网络，然后单击 **Next**（下一步）。
9. 确认所选选项，然后单击 **Finish**（完成）以启动安装过程，并在完成后单击 **Close**（关闭）。请勿开启 Panorama 虚拟设备。

STEP 3 | 在 Panorama 虚拟设备上配置资源。

1. 右击 Panorama 虚拟设备，然后选择 **Edit Settings**（编辑设置）。
2. 在 **Hardware**（硬件）设置中，根据需要分配 CPU 和内存。

   如果分配足够的 *CPU* 和 *Memory*（内存）并添加虚拟日志记录磁盘（稍后在此过程中），则虚拟设备在 *Panorama* 模式下启动。否则，设备将以“仅管理”模式启动。有关模式的详细信息，请参阅 Panorama 型号。
3. 将 **SCSI Controller**（**SCSI** 控制器）设置为 **LSI Logic Parallel**（**LSI** 逻辑并行）。
4. 添加虚拟日志记录磁盘。

   下列场景需要此步骤：

   - 在 *Panorama* 模式下将日志存储在专用日志记录磁盘上。
   - 在“仅管理”模式下管理您的 *SD-WAN* 部署。

   1. **Add**（添加）磁盘，选择 **Hard Disk**（硬盘）作为硬件类型，然后单击 **Next**（下一步）。
   2. **Create a new virtual disk**（创建新虚拟磁盘），单击 **Next**（下一步）。
   3. 将 **Disk Size**（磁盘大小）精确设置为 2TB。

      在 *Panorama* 模式下，您可以稍后 add additional logging disks（添加额外日志记录磁盘）（总共 *12* 个），每个日志记录磁盘的存储容量均为 *2TB*。已经添加到 *Panorama* 的日志记录磁盘不支持扩展大小。
   4. 选择您的首选 **Disk Provisioning**（磁盘配置）磁盘格式。

      当您选择磁盘配置格式时请考虑您的业务需求。有关磁盘配置性能考虑的更多信息，请参阅 VMware 厚盘与薄盘和所有闪存阵列文档，或其他 VMware 文档。

      在添加多个日志记录磁盘时，最佳实践是为所有磁盘选择相同的 *Disk Provisioning*（磁盘配置）格式，以避免可能出现的任何意外性能问题。

© 2019 Palo Alto Networks, Inc.

5. 选择 **Specify a datastore or datastore structure**（指定数据存储或数据存储结构）作为地点，**Browse**（浏览）到具有足够存储空间的数据存储区，单击 **OK**（确定），然后单击 **Next**（下一步）。
6. 选择 SCSI **Virtual Device Node**（虚拟设备节点）（您可使用默认选择），单击 **Next**（下一步）。

   如果选择 *SCSI* 以外的格式，*Panorama* 将无法启动。

7. 验证设置是否正确，然后单击 **Finish**（完成）。

5. 单击 **OK**（确定）保存更改。

STEP 4 | 开启 Panorama 虚拟设备。

1. 在 vSphere Client 中，右击 Panorama 虚拟设备，然后选择 **Power** > **Power On**（电源 > 开启电源）。等待 Panorama 启动后再继续。
2. 验证虚拟设备是否以正确的模式运行：
   1. 右击 Panorama 虚拟设备，然后选择 **Open Console**（打开控制台）。
   2. 输入您的用户名和密码（两者的默认设置均为 **admin**）以登录。
   3. 通过运行以下命令显示模式：

      ```
      > show system info
      ```

      在输出中，`system-mode`（系统模式）表示 `panorama` 或 `management-only`（仅管理）模式。

STEP 5 | 增加 ESXi 服务器上 Panorama 的系统磁盘 如果您打算在以下情况中使用 Panorama 虚拟设备：

- 在 Panorama 模式下管理您的 SD-WAN 部署。
- 在管理大规模防火墙部署时，需要额外存储空间进行动态更新。

现在可以执行 Panorama 虚拟设备的初始配置。

在 vCloud Air 中安装 Panorama

使用以下说明，在 VMware vCloud Air 中安装新 Panorama 虚拟设备。如果您正在升级部署在 vCloud Air 中的 Panorama 虚拟设备，请跳转到安装 Panorama 的内容和软件更新。

STEP 1 | 下载 Panorama 10.0 基本映像开放虚拟设备 (OVA) 文件。

1. 访问 Palo Alto Networks 软件下载站点。（如果不能登录，请转到 Palo Alto Networks 客户支持站点获取援助。）
2. 在 Panorama 基本映像部分的 Download（下载）列中，下载 Panorama 10.0 版本的 OVA 文件 (`Panorama-ESX-10.0.0.ova`)。

STEP 2 | 将 Panorama 映像导入到 vCloud Air 目录。

有关这些步骤的详细信息，请参阅《OVF 工具用户指南》。

1. 在您的客户端系统上安装 OVF 工具。
2. 访问客户端系统 CLI。
3. 导航到 OVF 工具目录（例如 C:\Program Files\VMware\VMware OVF Tool）。
4. 将 OVA 文件转换为 OVF 数据包：

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

5. 使用浏览器访问 vCloud Air Web 控制台，选择您的 **Virtual Private Cloud OnDemand**（按需虚拟私有云）区域，记录浏览器 URL。您将使用此 URL 信息完成下一步。URL 格

© 2019 Palo Alto Networks, Inc.

式为：**https://<*virtual-cloud-location*>.vchs.vmware.com/compute/cloud/org/<*vCloud-account-number*>/#/catalogVAppTemplateList?catalog=<*catalog-ID*>**。

6. 导入 OVF 数据包，使用 vCloud Air URL 中的信息填写 <virtual-cloud-location>、<vCloud-account-number> 和 <catalog-ID> 变量。其他变量是您的 vCloud Air 用户名和域 <user>@<domain>、虚拟数据中心 <datacenter> 和 vCloud Air 模板 <template>。

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

STEP 3 | 安装 Panorama。

1. 访问 vCloud Air Web 控制台，然后选择您的 **Virtual Private Cloud OnDemand**（按需虚拟私有云）区域。
2. 创建 Panorama 虚拟机。有关操作步骤，请在 vCloud Air 文档中心中参阅从模板添加虚拟机。配置 **CPU**、**Memory**（内存）和 **Storage**（存储器），如下所示：
   - 基于虚拟设备模式设置 **CPU** 和 **Memory**（内存）：请参阅 设置 Panorama 虚拟设备的前提条件。
   - 设置 **Storage**（存储空间）以配置 Panorama 虚拟设备系统磁盘。基于 Panorama 虚拟设备模式，参阅 设置 Panorama 虚拟设备的前提条件 了解受支持的磁盘大小。为了获得更好的日志记录及报告性能，请选择 **SSD-Accelerated**（**SSD** 加速）选项。

     要增加日志存储容量，您必须向 vCloud Air 中的 Panorama 添加虚拟磁盘。在 Panorama 模式下，虚拟设备不使用系统磁盘进行日志存储；您必须添加虚拟日志记录磁盘。

STEP 4 | 在网关上创建 vCloud Air NAT 规则，以允许流量流入和留出 Panorama 虚拟设备。

请在 vCloud Air 文档中心中参阅添加 NAT 规则以了解详细的说明：

1. 添加既允许 Panorama 接收来自防火墙的流量，又允许管理员访问 Panorama 的 NAT 规则。
2. 添加允许 Panorama 检索来自 Palo Alto Networks 更新服务器的更新并访问防火墙的 NAT 规则。

STEP 5 | 创建 vCloud Air 防火墙规则以允许流量流入 Panorama 虚拟设备。

默认情况下，允许流量留出。

请在 vCloud Air 文档中心中参阅添加防火墙规则以了解详细的说明：

STEP 6 | 如果 Panorama 虚拟设备的电源尚未开启，则将其开启。

在 vCloud Air Web 控制台中，选择 **Virtual Machines**（虚拟机）选项卡，选择 Panorama 虚拟机，然后单击 **Power On**（打开电源）。

现在可以执行 Panorama 虚拟设备的初始配置。

Panorama 虚拟设备上的 VMware 工具支持

VMware 工具与 Panorama 虚拟设备的软件映像 (ovf) 绑定。VMware 工具支持允许您使用 vSphere 环境（vCloud Director 和 vCenter 服务器）进行下列操作：

- 查看分配至 Panorama 管理接口的 IP 地址。
- 查看硬盘、内存和 CPU 的资源利用指标。您可使用这些指标启用 vCenter 服务器或 vCloud Director 上的警报或操作。
- 使用 vCenter 服务器或 vCloud Director 上的关机功能正常关闭和重启 Panorama。
- 启用 vCenter 服务器和 Panorama 之间的检测信号机制，验证 Panorama 是否在工作，或者防火墙/Panorama 是否重新启动。如果防火墙进入维护模式，检测信号被禁用，这样 vCenter 服务器不会关闭防火墙。防火墙无法向 vCenter 服务器发送检测信号时，禁用检测信号允许防火墙以维护模式保持工作。

© 2019 Palo Alto Networks, Inc.

在 *AWS* 上安装 *Panorama*

现在，您可以在 Amazon Web Services (AWS) 上部署 Panorama™ 和专用日志收集器。AWS 上部署的 Panorama 是自带许可 (BYOL)，支持所有部署模式（Panorama、日志收集器和仅管理），并与 M 系列硬件设备共享相同的流程和功能。更多有关 Panorama 模式的详细信息，请参阅 Panorama 型号。

STEP 1 | 登录到 AWS Web Service 控制台，然后选择 EC2 仪表盘。

- Amazon Web Service 控制台
- AWS GovCloud Web Service 控制台

STEP 2 | 设置网络需要的 VPC。

无论是在现有 VPC 中启动 Panorama 虚拟设备，还是创建新的 VPC，Panorama 虚拟设备必须能够接收来自 EC2 实例的流量，并在 VPC 和互联网之间执行入站和出站通信。

有关创建 VPC 和设置进行访问的说明，请参阅 AWS VPC 文档。

1. 创建新的 VPC 或使用现有的 VPC。请参阅《AWS 入门指南》文档。
2. 验证是否已适当定义网络和安全组件。
   - 启用与互联网的通信。默认 VPC 包括互联网网关，如果在默认子网中安装 Panorama 虚拟设备，则该 VPC 可以访问互联网。
   - 创建子网。子网是分配给可以在其中启动 EC2 实例的 VPC 的 IP 地址范围的分段。Panorama 虚拟设备必须属于公共子网，这样可以配置它以访问互联网。
   - 根据需要创建安全组管理来自 EC2 实例或子网的入站和出站流量。
   - 将路由添加到专用子网的路由表，以确保您可以通过 VPC 中的子网和安全组路由流量（如适用）。

STEP 3 | 在 Amazon Web Services 上部署 Panorama。

1. 在 EC2 仪表盘上，单击 **Instances**（实例）> **Launch Instance**（启动实例）。
2. 选择 **AWS Marketplace**，搜索 **`Palo Alto Networks Panorama`**，然后 **Select**（选择）Panorama AMI 并 **Continue**（继续）。
3. 对于 Panorama 虚拟设备所需的资源分配，请选择 **EC2 instance type**（**EC2** 实例类型），然后单击 **Next**（下一步）：**Configure Instance Details**（配置实例详细信息）。有关最小资源要求，请查看设置 Panorama 虚拟设备的前提条件。

   如果您打算将 *Panorama* 虚拟设备用作专用日志收集器，必须在初始部署时配置具备所需资源的设备。如果在部署虚拟机后调整其大小，则 *Panorama* 虚拟设备可能不会保留在日志收集器模式下，从而导致日志数据丢失。
4. 配置实例详细信息。
   1. 选择 **Next**（下一步）：**Configure Instance Details**（配置实例详细信息）。
   2. 选择您在上一步中创建的 **Network**（网络）或者使用 AWS 提供的默认 VPC。如果
   3. 选择您在上一步中创建的 **Subnet**（子网）或者使用 AWS 提供的默认子网。
   4. 要 **Auto-assign Public IP**（自动分配公共 **IP**），请选择 **Enable**（启用）。

      您计划使用 Panorama 管理的防火墙应能访问此 IP。这可让您获取 Panorama 虚拟设备管理接口的可访问公共 IP 地址。稍后，您可以将弹性 IP 地址附加到管理接口。不同于在终止实例时与虚拟设备解除关联的公共 IP 地址，弹性 IP 地址可提供持久性并且在 Panorama 虚拟设备实例关闭时可以重新附加到 Panorama 虚拟设备的新（或更换）实例，而不需要重新配置 IP 地址。
   5. 根据需要配置任何额外实例详细信息。
5. 配置 Panorama 虚拟设备存储区。
   1. 选择 **Next**（下一步）：添加存储区。
   2. 查看根系统磁盘大小，并确定是否需要扩展到 224GB 系统磁盘。需要时，请将系统磁盘 **Size**（大小）扩展到 224GB。

© 2019 Palo Alto Networks, Inc.

如要支持大型数据集，则需要 224GB 系统磁盘 管理大规模防火墙部署，以确保动态更新等活动有充足磁盘空间。

（仅限 SD-WAN）如果您打算在 Panorama 模式下使用 Panorama 虚拟设备来管理 SD-WAN 部署，则 224GB 系统磁盘可扩展存储空间来监控和报告受管防火墙运行状况数据。



如果您使用 *224GB* 系统磁盘来部署 *Panorama* 虚拟设备实例，则您以后无法迁移至更小的系统磁盘。

3. **Add New Volume**（添加新卷）以添加额外日志存储。

   （仅限 SD-WAN）如果您计划在“仅管理”模式下管理您的 SD-WAN 部署，则您必须添加一个 2TB 日志记录磁盘。

   如果您打算在 Panorama 模式下使用 Panorama 虚拟设备，或将 Panorama 虚拟设备用作专用日志收集器，则在初始部署时添加虚拟日志记录磁盘。默认情况下，当您满足 Panorama 模式资源要求，且已添加至少一个虚拟日志记录磁盘，则 Panorama 虚拟设备将处于 Panorama 模式，以进行初始部署。否则， Panorama 虚拟设备将默认为处于仅管理模式。如果您只想管理设备和专用日志收集器，并不想本地收集日志，则将 Panorama 虚拟设备更改为仅管理模式。

   AWS 上的 Panorama 虚拟设备仅支持 2TB 日志记录磁盘，最多支持共计 24TB 的日志存储。您不能添加小于 2TB 的日志记录磁盘，也不能添加不能被 2TB 日志记录磁盘要求整除的日志记录磁盘。Panorama 虚拟设备将大于 2TB 的日志记录磁盘分成一个一个的 2TB 分区。

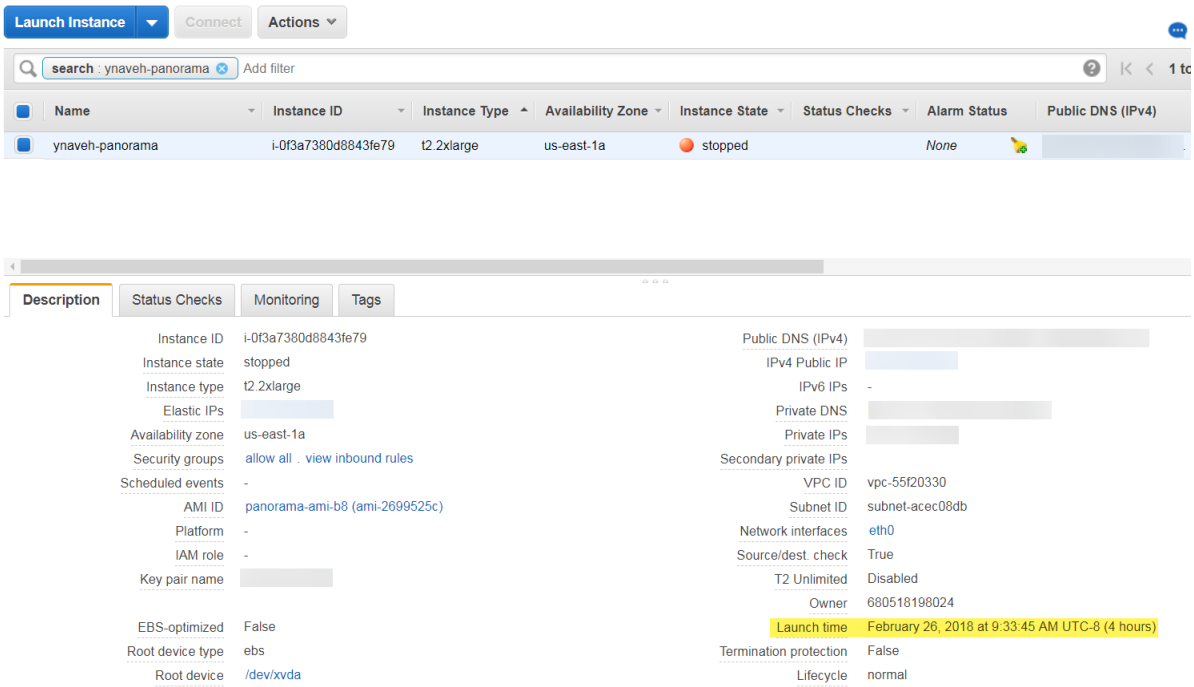
6. （可选）选择 **Next**（下一步）：添加标签，然后添加一个或多个标记作为元数据，以帮助您标识并分组 Panorama 虚拟设备。例如，添加一个带**Value**（值）的**Name**（名称）标记，以帮助您标识 Panorama 虚拟设备管理的防火墙。
7. 配置实例安全组。
   1. 选择 **Next**（下一步）：配置安全组。
   2. 创建一个新的 **Security Group**（安全组），或至少选择一个 HTTP 和 SSH 已启用的现有安全组。此安全组用于限制访问管理接口。
8. **Review and Launch**（查看并启动）Panorama 虚拟设备以验证 **Launch**（启动）前您的选择是否正确。
9. 选择现有的密钥对或创建新的密钥对，并确认免责声明。



如果您从 *AMS* 创建新密钥，请下载该密钥并将其保存在一个安全位置。此文件扩展名为 `.pem`。您必须将公共密钥加载至 PuTTYgen 并保存为 `.ppk` 格式。如果丢失，则将无法重新生成此密钥。

在 AWS 上启动后，将需要花费约 30 分钟的时间来完成 Panorama 虚拟设备的部署。Panorama 虚拟设备的部署时间可能更长，这取决于附加到实例的磁盘数量和大小。通过选择 Panorama 虚拟设备实例（**Instances**（实例））查看启动时间。

© 2019 Palo Alto Networks, Inc.



如果您打算将 *Panorama* 虚拟设备用作专用日志收集器，必须用于具备所需资源的设备。如果在部署虚拟机后调整其大小，则 *Panorama* 虚拟设备可能不会保留在日志收集器模式下，从而导致日志数据丢失。

STEP 4 | 关闭 Panorama 虚拟设备。

1. 在 EC2 仪表盘上，选择 **Instances**（实例）。
2. 选择 Panorama 虚拟设备，然后单击**Actions**（操作）> **Instance State**（实例状态）> **Stop**（停止）。

STEP 5 | 创建或分配弹性 IP(EIP) 地址给管理接口。

1. 在 AWS 控制台上，选择 **Elastic Ips**（弹性 **IP**），并 **Allocate New Address**（分配新地址）。
2. 单击 **Allocate**（分配）以生成新的 EIP 地址，单击 **Actions**（操作）然后 **Associate address**（关联地址）。
3. 选择 **Instance**（实例），选择分配 EIP 地址的 Panorama 虚拟设备实例，然后输入与管理接口关联的 **Private IP address**（专用 **IP** 地址）并单击 **Associate**（关联）。

STEP 6 | 开启 Panorama 虚拟设备。

1. 在 EC2 仪表盘上，选择 **Instance**（实例）。
2. 从列表中选择 Panorama 虚拟设备，然后单击 **Actions**（操作）> **Instance State**（实例状态）> **Start**（启动）。

STEP 7 | 配置 Panorama 虚拟设备的新管理密码。

您必须先配置唯一的管理密码，然后才能访问 Panorama 虚拟设备的 Web 界面。要访问 CLI，需要用于启动 Panorama 虚拟设备的私钥。

- 如果您的计算机上已安装 SSH 服务：

1. 输入以下命令以登录 Panorama 虚拟设备：

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


© 2019 Palo Alto Networks, Inc.

2. 使用以下命令并按照屏幕上的提示配置新密码：

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

3. 如果需要激活 BYOL，请设置 DNS 服务器 IP 地址，以使 Panorama 虚拟设备可以访问 Palo Alto Networks 许可服务器。输入以下命令，设置 DNS 服务器的 IP 地址：

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

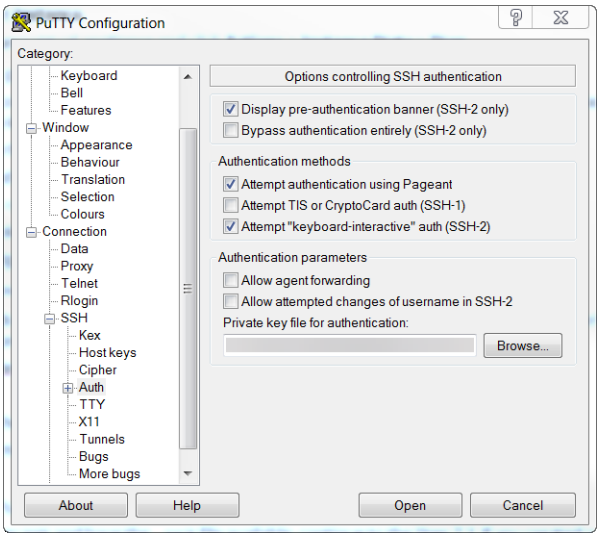
4. 使用以下命令提交您所做的更改：

```
admin# commit
```

5. 终止 SSH 会话。

- 如果使用 PuTTY 将 SSH 连接到 Panorama 虚拟设备：

1. 如果您使用现有密钥对，并拥有可用的 `.ppk`文件，可继续步骤 7.3。如果已创建新的密钥对，或仅拥有现有密钥对的 `.pem`文件，请打开 PuTTYgen，并 **Load**（加载）`.pem`文件。
2. **Save the private key**（保存私钥）至本地可访问目标。
3. 打开 PuTTY 并选择 **SSH** > **Auth**（身份验证）然后 **Browse**（浏览）至您在上一步保存的 `.ppk`文件。



4. 选择 **Sessions**（会话），然后输入 Panorama 虚拟设备的公共 IP 地址。单击 **Open**（打开），并在出现安全提示时单击 **Yes**（是）。
5. 看到提示时以管理员身份登录。
6. 使用以下命令并按照屏幕上的提示配置新密码：

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

7. 设置 DNS 服务器 IP 地址，以使 Panorama 虚拟设备可以访问 Palo Alto Networks 许可服务器。输入以下命令，设置 DNS 服务器的 IP 地址：

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

8. 使用以下命令提交您所做的更改：

© 2019 Palo Alto Networks, Inc.

```
admin# commit
```

9. 终止 SSH 会话。

STEP 8 | 激活 Panorama 虚拟设备上的设备管理许可证和支持许可证。

- 在 Panorama 虚拟设备连接到互联网时激活/检索防火墙管理许可证
- 在 Panorama 虚拟设备未连接到互联网时激活/检索防火墙管理许可证
- 激活 Panorama 支持许可证

STEP 9 | 完成配置 Panorama 虚拟设备，以满足您的部署需求。

- （仅管理模式）在仅管理模式下设置 Panorama 虚拟设备。
- （日志收集器模式）开始步骤 6 以从 Panorama 模式切换到日志收集器模式。

  在将日志收集器添加为 *Panorama* 管理服务器的受管收集器时，请输入专有日志收集器的公共 *IP* 地址。您无法指定 *IP Address*（*IP* 地址）、*Netmask*（子网掩码）或 *Gateway*（网关）。
- （Panorama 和仅管理模式）配置受管收集器以添加专用日志收集器至 Panorama 虚拟设备。仅管理模式不支持本地日志收集，需要专用日志收集器存储受管设备的日志。

在 *AWS GovCloud* 上安装 *Panorama*

现在，您可以在 Amazon Web Services (AWS) GovCloud 上部署 Panorama™ 和专用日志收集器。AWS GovCloud 是一种独立的 AWS 区域，该区域符合美国政府机构和客户在法规符合性方面的要求。AWS GovCloud 上部署的 Panorama 是自带许可(BYOL)，支持所有部署模式（Panorama、日志收集器和仅管理）。更多有关 Panorama 模式的详细信息，请参阅Panorama 型号。

为保护 AWS GovCloud（美国）区域中含各类受控非密信息 (CUI) 数据及可公用政府主导数据的工作负载，Panorama 虚拟设备在 AWS GovCloud 的标准 AWS 公共云上提供同样强大的安全功能。AWS GovCloud 上的 Panorama 虚拟设备和标准 AWS 公共云均支持相同的功能和能力。

查看设置 Panorama 虚拟设备的前提条件以查看受支持的 EC2 实例类型。准备就绪后，请参阅在 AWS 上安装 Panorama以在 AWS GovCloud 上安装 Panorama 虚拟设备。

要添加其他日志记录存储到 Panorama 虚拟设备，或是增加已分配的 CPU 内核和内存，请参阅以下步骤。

- 向 AWS 中的 Panorama 添加虚拟磁盘
- 增加 AWS 上的 Panorama 的 CPU 和内存

在 *Azure* 上安装 *Panorama*

现在，您可以在 Microsoft Azure 上部署 Panorama™ 和专用日志收集器。Azure 上部署的 Panorama 是自带许可 (BYOL)，支持所有部署模式（Panorama、日志收集器和仅管理），并与 M 系列硬件设备共享相同的流程和功能。更多有关 Panorama 模式的详细信息，请参阅 Panorama 型号。

STEP 1 | 登录到 Microsoft Azure 门户。

STEP 2 | 部署 Panorama 虚拟设备。

1. 在 Azure 仪表盘上，选择 **Virtual machines**（虚拟机），并 **Add**（添加）新的虚拟机。
2. 搜索 Palo Alto Networks 并选择最新的 Panorama 虚拟设备映像。
3. **Create**（创建） Panorama 虚拟设备。

STEP 3 | 配置 Panorama 虚拟设备。

1. 选择所需的 Azure **Subscription**（订阅）。

© 2019 Palo Alto Networks, Inc.

2. 选择 Azure **Resource Group**（资源组）以包含您所有的 Azure 实例资源。
3. 输入 Panorama 虚拟设备的 **Virtual machine name**（虚拟机名称）。
4. 选择 Panorama 虚拟设备要部署的 **Region**（区域）。
5. （可选）选择 **Availability options**（可用性选项）。更多信息，请参阅 如何使用可用性集。
6. 选择用于部署 Panorama 管理服务器的 **Image**（映像）。浏览所有公共和私有映像，以在 Azure Marketplace 上从 Panorama 映像部署 Panorama 管理服务器。
7. 配置 Panorama 虚拟设备大小。有关大小要求，请查看设置 Panorama 虚拟设备的前提条件。

   如果您打算将 *Panorama* 虚拟设备用作专用日志收集器，必须在初始部署时配置具备所需资源的设备。如果在部署虚拟机后调整其大小，则 *Panorama* 虚拟设备可能不会保留在日志收集器模式下，从而导致日志数据丢失。
8. 输入 Panorama 虚拟设备管理员的 **Name**（名称）。要保证您的用户名的安全，管理员不是一个有效的条目。
9. 输入 **Password**（密码）或复制粘贴 **SSH public key**（**SSH** 公钥）以确保对 Panorama 虚拟设备进行管理访问的安全。

   如果计划在 *FIPS-CC* 操作模式下使用 *Panorama* 虚拟设备的此实例，则必须启用 *SSH* 密钥身份验证。尽管您可以使用用户名和密码部署 *Panorama* 虚拟设备，但是，一旦将操作模式更改为 *FIPS-CC*，就无法使用用户名和密码进行身份验证。重置为 *FIPS-CC* 模式后，必须使用 *SSH* 密钥登录，然后才可以配置随后将用于登录到 *Panorama Web* 界面的用户名和密码。有关创建 *SSH* 密钥的详情，请参阅 Azure 文档。
10. 配置 Panorama 虚拟设备实例 **Networking**（联网）
    1. 选择现有 **Virtual network**（虚拟网络）或创建新虚拟网络。
    2. 配置 **Subnet**（子网）。此子网取决于您在上一步选择或创建的虚拟网络。如果选择现有虚拟网络，则可以为已选中的虚拟网络选择其中一个子网。
    3. 选择现有 **Public IP address**（公共 **IP** 地址）或创建新的公共 IP 地址。这将创建用于访问您的 Panorama 虚拟设备的管理界面。
    4. 选择现有 **NIC Network security group**（**NIC** 网络安全组）或 create a new security group（创建新安全组）。网络安全组控制流向虚拟机的流量。入站规则必须允许 HTTPS 和 SSH。
11. 配置实例 **Management**（管理）设置。
    1. 选择是否启用 **Auto-shutdown**（自动关闭）。自动关闭允许您配置每日自动关闭虚拟机的时间，当 Panorama 虚拟设备关闭时，禁用自动关闭以避免如下可能：新公共 IP 地址被分配到虚拟机、日志被丢弃、日志非您的防火墙相关日志或您无法管理您的防火墙。
    2. 选择是否启用启动 **Monitoring**（监控）。如果启用，请选择诊断存储账户。自动监控，将启动诊断日志发送到您的诊断存储账户。有关详细信息，请参阅 Microsoft Azure 中监控概述。
    3. 根据需要配置任何其他设置。
12. 查看摘要，接受使用条款和隐私政策，然后 **Create**（创建）以 Panorama 虚拟设备。

STEP 4 | 验证 Panorama 虚拟设备是否已成功部署。

1. 选择 **Dashboard**（仪表盘）> **Resource Groups**（资源组），然后选择包含 Panorama 虚拟设备的资源组。
2. 在设置中选择用于虚拟机部署状态的 **Deployments**（部署）。

   需要花费约 *30* 分钟的时间来完成 *Panorama* 虚拟设备的部署。启动 *Panorama* 虚拟设备需要更长的时间，这取决于虚拟机配置的资源。*Microsoft Azure* 不允许使用 *ICMP* 协议测试其是否已成功部署。

   如果您打算将 *Panorama* 虚拟设备用作专用日志收集器，必须正确配置设备所需资源。如果在部署虚拟机后调整其大小，则 *Panorama* 虚拟设备可能不会保留在日志收集器模式下，从而导致日志数据丢失。

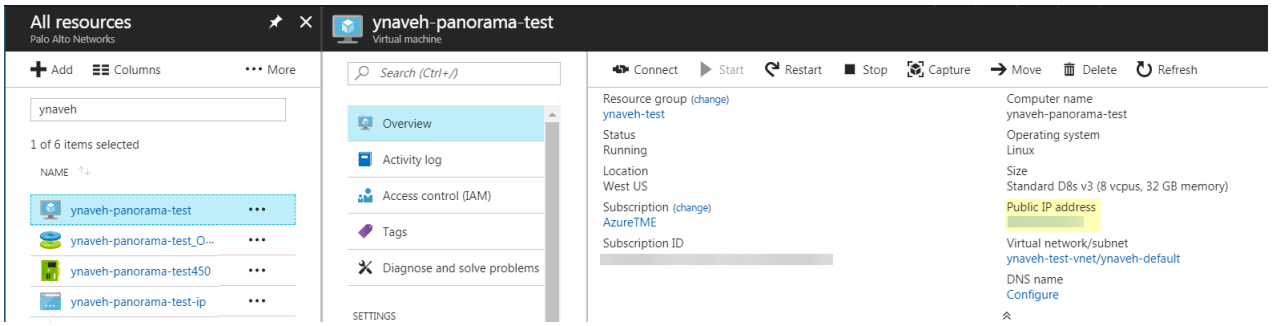
© 2019 Palo Alto Networks, Inc.

STEP 5 | 配置静态公共 IP 地址。

1. 在 Azure 门户上，选择 **Virtual machines**（虚拟机），然后选择 Panorama 虚拟机。
2. 选择 **Overview**（概述），然后单击 **Public IP address**（公共 **IP** 地址）。
3. 在分配中选择 **Static**（静态），并**Save**（保留）新的 IP 地址配置。

STEP 6 | 登录 Panorama 虚拟设备的 Web 界面。

1. 在 Azure 门户的 **All Resources**（所有资源）中，选择 Panorama 虚拟设备并在概述部分查看公共 IP 地址。



2. 使用您的 Web 浏览器中的安全 (https) 连接以通过公共 IP 地址登录到 Panorama 虚拟设备。
3. 输入 Panorama 虚拟设备的用户名和密码。提示您证书警告。接收证书警告，并继续浏览页面。

STEP 7 | 激活 Panorama 虚拟设备上的设备管理许可证和支持许可证。

- 在 Panorama 虚拟设备连接到互联网时激活/检索防火墙管理许可证
- 在 Panorama 虚拟设备未连接到互联网时激活/检索防火墙管理许可证
- 激活 Panorama 支持许可证

STEP 8 | 完成配置 Panorama 虚拟设备，以满足您的部署需求。

（仅限 SD-WAN）如果您计划在“仅管理”模式下管理您的 SD-WAN 部署，则您必须添加一个 2TB 日志记录磁盘。

1. 向 Azure 中的 Panorama 添加虚拟磁盘。默认情况下，在初始部署期间，会自动创建 81GB 系统磁盘。

   在您将 Panorama 虚拟设备更改为 Panorama 模式或日志收集器模式之前，必须添加虚拟日志记录磁盘。

   默认情况下，Azure 上的 Panorama 虚拟设备在仅管理模式下进行初始部署。如果您打算在 Panorama 模式下使用 Panorama 虚拟设备，或将 Panorama 虚拟设备用作专用日志收集器，则在 Azure 上成功部署 Panorama 后添加虚拟日志记录磁盘。

   Azure 上的 Panorama 虚拟设备仅支持 2TB 日志记录磁盘，最多支持共计 24TB 的日志存储。您不能添加小于 2TB 的日志记录磁盘，也不能添加不能被 2TB 日志记录磁盘要求整除的日志记录磁盘。Panorama 虚拟设备将大于 2TB 的日志记录磁盘分成一个一个的 2TB 分区。
2. 更改 Panorama 虚拟设备模式。

   默认情况下，Azure 上的 Panorama 虚拟设备在仅管理模式下部署。要更改为 Panorama 模式或日志收集器模式，您必须在初始部署后至少添加一个日志记录磁盘。如果您只想管理设备和专用日志收集器，并不想本地收集日志，则将 Panorama 虚拟设备集保持为仅管理模式。

   - 在 Panorama 模式下设置 Panorama 虚拟设备。
   - （日志收集器模式）开始步骤 6 以从 Panorama 模式切换到日志收集器模式。

© 2019 Palo Alto Networks, Inc.

在将日志收集器添加为 *Panorama* 管理服务器的受管收集器时，请输入专有日志收集器的公共 *IP* 地址。您无法指定 *IP Address*（*IP* 地址）、*Netmask*（子网掩码）或 *Gateway*（网关）。

3. （Panorama 和仅管理模式）配置受管收集器，以添加专用日志收集器至 Panorama 虚拟设备。仅管理模式不支持本地日志收集，需要专用日志收集器存储受管设备的日志。

在 Google Cloud Platform 上安装 Panorama

现在，您可以在 Google Cloud Platform (GCP) 上部署 Panorama™ 和专用日志收集器。GCP 上部署的 Panorama 是自带许可 (BYOL)，支持所有部署模式（Panorama、日志收集器和仅管理），并与 M 系列硬件设备共享相同的流程和功能。更多有关 Panorama 模式的详细信息，请参阅 Panorama 型号。

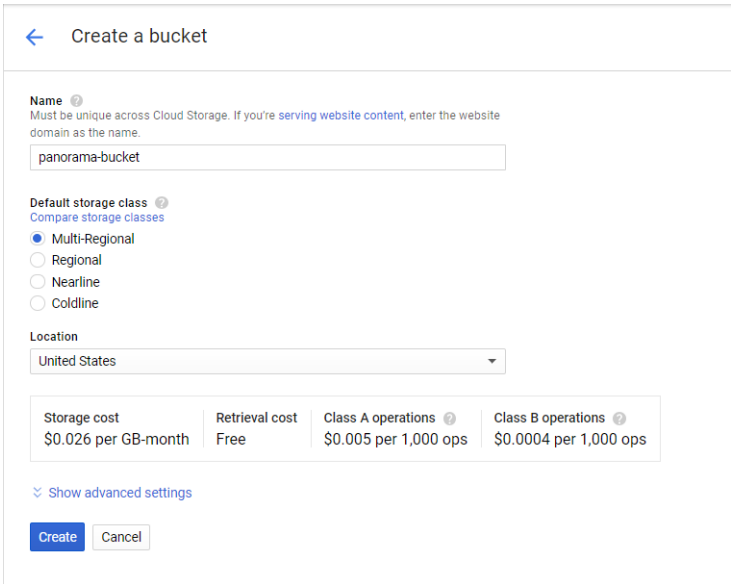
要在 GCP 上部署 Panorama 虚拟设备，则需要构建自定义映像。要开始此过程，必须从 Palo Alto Networks客户支持门户下载 Panorama `tar.gz`，然后将其上传到 GCP 存储桶。然后，您可以创建自定义映像，并使用该映像在 GCP 上部署 Panorama 虚拟设备。

STEP 1 | 下载 Panorama 虚拟设备映像。

1. 登录到 Palo Alto Networks 支持门户。
2. 选择 **Updates**（更新）> **Software Updates**（软件更新），然后按 **Panorama Base Images**（**Panorama** 基本映像）进行筛选。
3. 在 GCP `tar.gz` 映像上下载最新版的 Panorama。

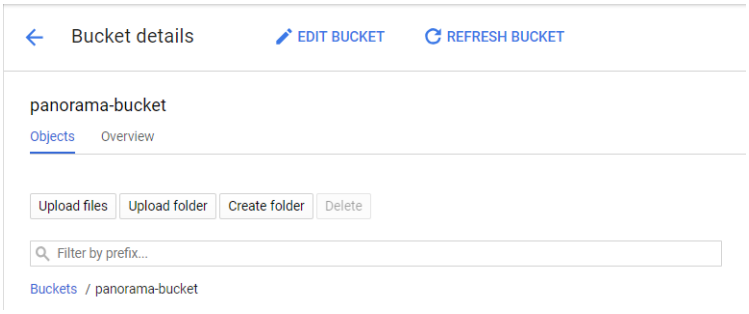
STEP 2 | 上传 Panorama 虚拟设备映像到 Google Cloud Platform。

1. 登录到 Google Cloud 控制台。
2. 从 **Products and Services**（产品和服务）菜单中选择 **Storage**（存储）。
3. 单击 **Create Bucket**（创建桶），配置新的存储桶，然后单击 **Create**（创建）。

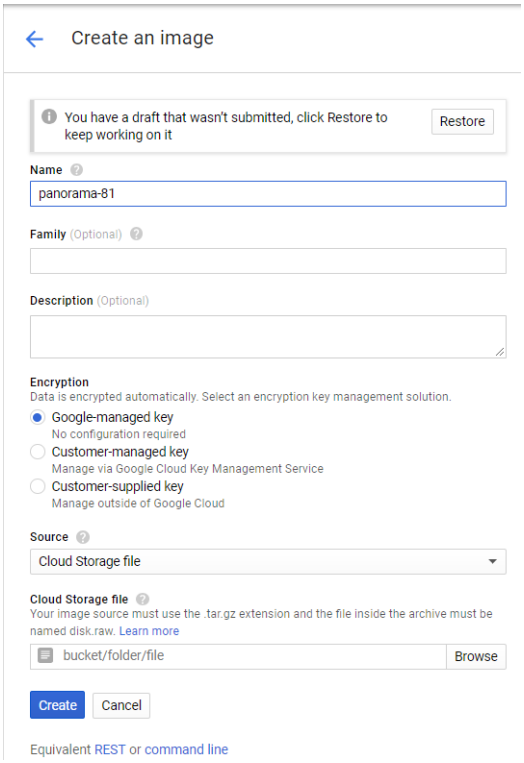


4. 选择在上一步中创建的存储桶，单击 **Upload files**（上传文件），然后选择已下载的 Panorama 虚拟设备映像。

© 2019 Palo Alto Networks, Inc.



5. 从 **Products and Services**（产品和服务）菜单中选择 **Compute Engine** > **Images**（映像）。
6. 单击 **Create Image**（创建映像），然后创建 Panorama 虚拟设备映像：
   1. 设定 Panorama 虚拟设备映像的 **Name**（名称）。
   2. 在 **Source**（源）字段中，从下拉菜单中选择 **Cloud Storage file**（云存储文件）。
   3. 单击 **Browse**（浏览）并导航至已上传 Panorama 虚拟设备映像的存储桶，然后 **Select**（选择）上传映像。
   4. **Create**（创建）Panorama 虚拟设备映像。



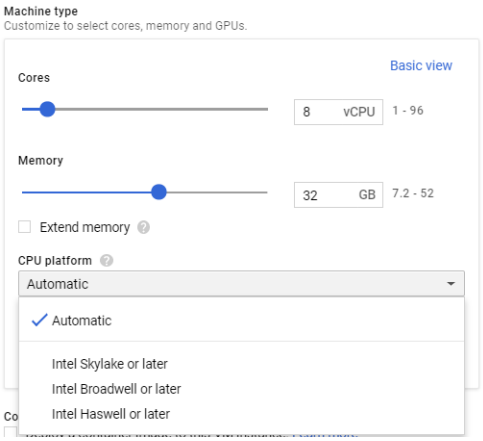
STEP 3 | 配置 Panorama 虚拟设备。

1. 从 **Products and Services**（产品和服务）菜单中选择 **Compute Engine**。
2. 单击 **Create Instance**（创建实例）以开始部署 Panorama 虚拟设备。
3. 添加描述性 **Name**（名称），以便轻松标识 Panorama 虚拟设备。
4. 选择您要部署 Panorama 虚拟设备的 **Region**（地区）和 **Zone**（区域）。
5. 分配 **Machine Type**（机器类型），并 **Customize**（自定义）CPU 内核、内存和 CPU 平台。有关最小资源要求，请查看设置 Panorama 虚拟设备的前提条件。

© 2019 Palo Alto Networks, Inc.

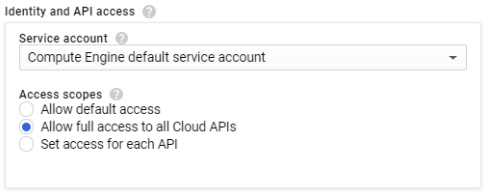
如果您打算将 *Panorama* 虚拟设备用作专用日志收集器，必须在初始部署时配置具备所需资源的设备。如果在部署虚拟机后调整其大小，则 *Panorama* 虚拟设备可能不会保留在日志收集器模式下，从而导致日志数据丢失。

选择 *GCP* 区域可确定可用的 *CPU* 平台。有关更多信息，请参阅地区和区域。

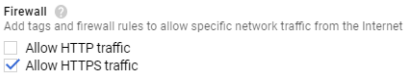


6. 配置 Panorama 启动磁盘。
   1. 对于 **Boot Disk**（启动磁盘），单击 **Change**（更改）> **Custom image**（自定义映像），然后选择在步骤 2 中上传的 Panorama 映像文件
   2. 配置启动磁盘大小。默认情况下，系统磁盘是 81GB，但是您可以将系统磁盘大小增至 224GB。

      （仅限 SD-WAN）如果您计划使用此 Panorama 虚拟设备在 Panorama 模式下管理您的 SD-WAN 部署，则您必须将系统磁盘大小增至 224GB。如果您计划在“仅管理”模式下管理您的 SD-WAN 部署，则您必须添加一个 2TB 日志记录磁盘。
   3. 单击 **Select**（选择）以保存您的配置。
7. 在 **Identity and API access**（身份识别和 **API** 访问）中选择 **Allow full access to all Cloud APIs**（允许完全访问 **Cloud API**）。



8. 在 **Firewall**（防火墙）中选择 **Allow HTTPS traffic**（允许 **HTTPS** 流量）。



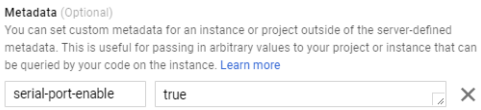
STEP 4 | 展开 **Management, security, disks, networking, sole tenancy**（管理、安全、磁盘、网络、独家租赁）Management, security, disks, networking, sole tenancy。

STEP 5 | 启用对串行端口的访问，以便您可以管理 Panorama 虚拟设备。

1. 选择 **Management**（管理）。
2. 输入以下名称-值对作为元数据：

   `serial-port-enable true`

© 2019 Palo Alto Networks, Inc.



STEP 6 | 保留管理接口的静态 IP 地址。

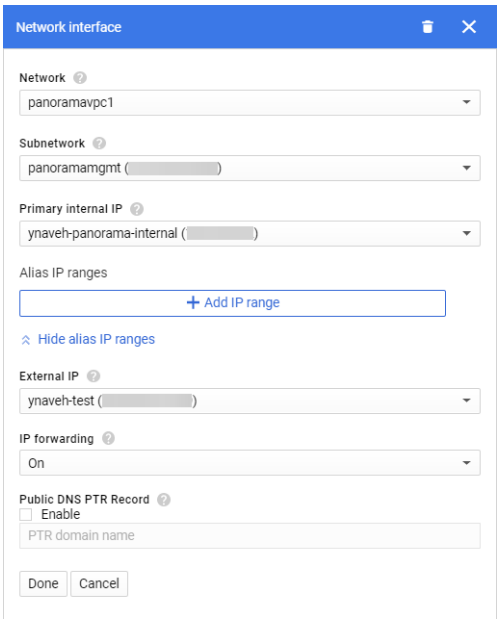
如果 Panorama 虚拟设备已重启，则保留管理接口的内部和外部静态 IP 地址。当重新分配 IP 地址时，受管设备不会丢失与 Panorama 虚拟设备的连接。

更多关于如何保留 IP 地址的信息，请参阅保留静态内部 IP 地址和 保留静态外部 IP 地址。

1. 选择 **Networking**（联网）。
2. **Edit**（编辑）网络接口。



3. 选择 Panorama 虚拟设备 **Network**（网络）。
4. 选择 Panorama 虚拟设备 **Subnetwork**（子网）。同一子网中的实例将通过其内部 IP 地址进行相互通信。
5. 设置 **Primary internal IP**（主要内部 **IP**）地址。
   - **Ephemeral (Automatic)**（临时（自动））— 自动分配主要内部 IP 地址。
   - **Ephemeral (Custom)**（临时（自定义））— 分配 GCP 用于分配主要内部 IP 地址的自定义 IP 范围。
   - **Reserve a static internal IP address**（保留静态内部 **IP** 地址）— 手动分配静态主要内部 IP 地址。
6. 设置 **External IP**（外部 **IP**）地址。
   - **Ephemeral**（临时）—自动从共享 IP 池中分配外部 IP 地址。
   - 选择现有已保留的外部 IP 地址。
   - **Create IP address**（创建 **IP** 地址）—保留外部 IP 地址。
7. 设置 **IP forwarding**（**IP** 转发）为**On**（打开），允许 Panorama 虚拟设备接收来自不匹配目标地址或源 IP 地址的数据包。

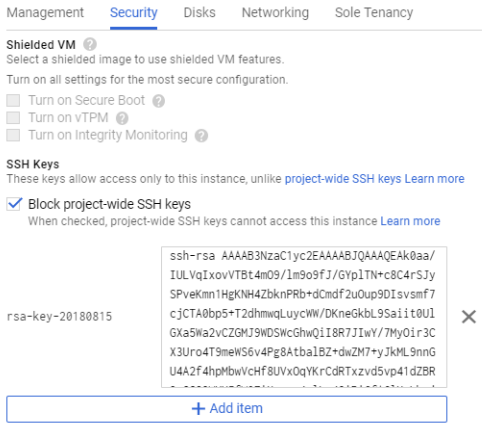


STEP 7 | 配置 SSH 密钥。初始部署后，您需要 SSH 密钥访问 Panorama 虚拟设备 CLI，以配置管理用户密码。

© 2019 Palo Alto Networks, Inc.

1. 选择 **Security**（安全）。
2. 选择 **Block project-wide SSH keys**（阻止项目范围内 **SSH** 密钥）框。初始部署后，目前仅实例密钥支持登录到 Panorama 虚拟设备。
3. 将 SSH 密钥粘贴到注释框中。有关 SSH 密钥正确格式以及如何生成 GCP 的 SSH 密钥等信息，请参阅在元数据中管理 SSH 密钥。

> 生成 *SSH* 密钥时，采用 *.ppk* 格式保留私钥。初始部署后，需要私钥才能登陆到 *Panoram* 虚拟设备，之后才能配置管理密码。

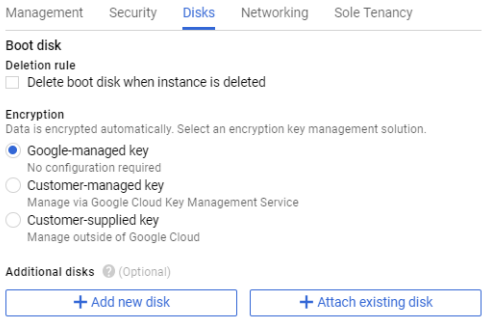


STEP 8 | （Panorama 和日志收集器模式）添加用于日志收集的额外存储。必要时重复该步骤，以添加额外的虚拟日志记录磁盘。

如果您打算在 Panorama 模式下使用 Panorama 虚拟设备，或将 Panorama 虚拟设备用作专用日志收集器，则在初始部署时添加虚拟日志记录磁盘。默认情况下，当您满足 Panorama 模式资源要求，且已添加至少一个虚拟日志记录磁盘，则 Panorama 虚拟设备将处于 Panorama 模式，以进行初始部署。否则，Panorama 虚拟设备默认为仅管理模式，您可以在其中管理设备和专用日志收集器，但无法在本地收集日志。

GCP 上的 Panorama 虚拟设备仅支持 2TB 日志记录磁盘，最多支持共计 24TB 的日志存储。您不能添加小于 2TB 的日志记录磁盘，也不能添加不能被 2TB 日志记录磁盘要求整除的日志记录磁盘。Panorama 虚拟设备将大于 2TB 的日志记录磁盘分成一个一个的 2TB 分区。

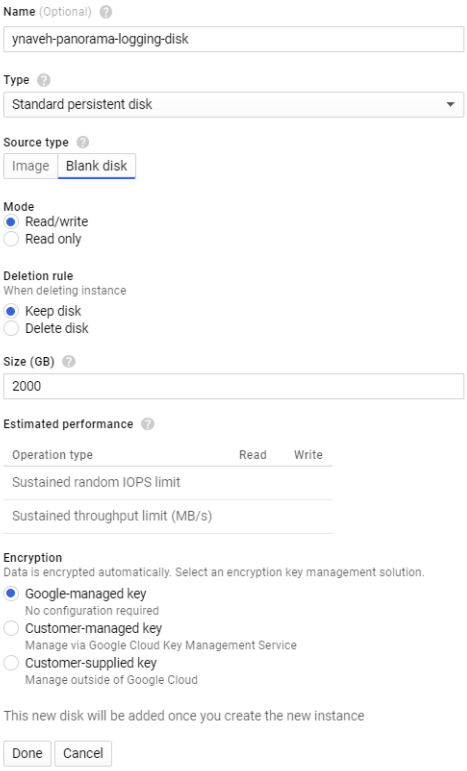
1. 选择 **Disks**（磁盘）> **Add new disk**（添加新磁盘）。



2. 输入**Name**（名称）。
3. 展开 **Type**（类型）下拉菜单，然后选择所需类别。
4. 对于 **Source type**（源类型），选择 **Blank disk**（空磁盘）。
5. 对于 **Mode**（模式），选择 **Read/write**（读取/写入）。
6. 选择 **Deletion rule**（删除规则），以配置是否在删除 Panorama 虚拟设备实例时删除虚拟日志记录磁盘。到

© 2019 Palo Alto Networks, Inc.

7. 设置虚拟日志记录磁盘的 **Size (GB)**（大小**(GB)**）。
8. 设置适用于虚拟日志记录磁盘上数据的首选 **Encryption**（加密）解决方案。
9. 单击 **Done**（完成）。



STEP 9 | **Create**（创建）Panorama 虚拟设备。初始部署后，启动 Panorama 虚拟设备可能需要约 10 分钟。

STEP 10 | 配置 Panorama 虚拟设备的新管理密码。

您必须先配置唯一的管理密码，然后才能访问 Panorama 虚拟设备的 Web 界面。要访问 CLI，请使用用于启动 Panorama 虚拟设备的私钥。

- 如果您的计算机上已安装 SSH 服务：

1. 输入以下命令以登录 Panorama 虚拟设备：

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

2. 使用以下命令并按照屏幕上的提示配置新密码：

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

3. 如果拥有所需 BYOL，请设置 DNS 服务器 IP 地址，以使 Panorama 虚拟设备可以访问 Palo Alto Networks 许可服务器。输入以下命令，设置 DNS 服务器的 IP 地址：

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

4. 提交更改：

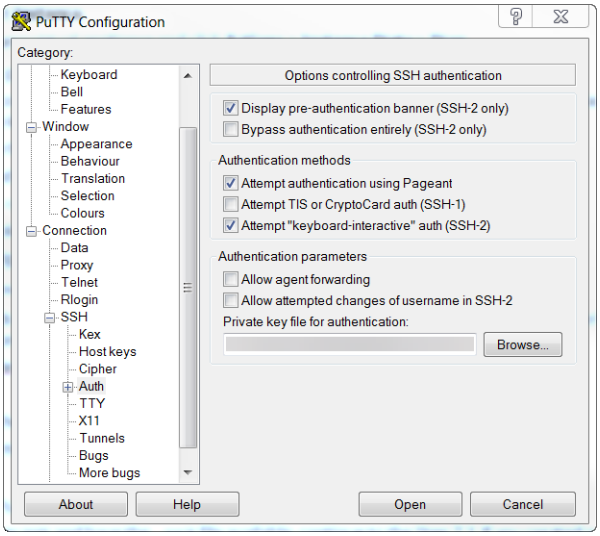
© 2019 Palo Alto Networks, Inc.

```
admin# commit
```

5. 终止 SSH 会话。

- 如果使用 PuTTY 将 SSH 连接到 Panorama 虚拟设备：

1. 如果您使用现有密钥对，并拥有可用的 `.ppk` 文件，可继续步骤 11.3。如果已创建新的密钥对，或仅拥有现有密钥对的 `.pem`文件，请打开 PuTTYgen，并 **Load**（加载）`.pem`文件。
2. **Save the private key**（保存私钥）至本地可访问目标。
3. 打开 PuTTY 并选择 **SSH** > **Auth**（身份验证）然后 **Browse**（浏览）至上一步保存的 `.ppk`文件。



4. 选择 **Sessions**（会话），然后输入 Panorama 虚拟设备的公共 IP 地址。然后 **Open**（打开），并在出现安全提示时单击 **Yes**（是）。
5. 提示时以管理员身份登录。
6. 使用以下命令并按照屏幕上的提示配置新密码：

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

7. 设置 DNS 服务器 IP 地址，以使 Panorama 虚拟设备可以访问 Palo Alto Networks 许可服务器。输入以下命令，设置 DNS 服务器的 IP 地址：

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

8. 使用以下命令提交您所做的更改：

```
admin# commit
```

9. 终止 SSH 会话。

STEP 11 | 激活 Panorama 虚拟设备上的设备管理许可证和支持许可证。

- 在 Panorama 虚拟设备连接到互联网时激活/检索防火墙管理许可证
- 在 Panorama 虚拟设备未连接到互联网时激活/检索防火墙管理许可证
- 激活 Panorama 支持许可证

STEP 12 | 完成配置 Panorama 虚拟设备，以满足您的部署需求。

- （仅管理模式）在仅管理模式下设置 Panorama 虚拟设备。

© 2019 Palo Alto Networks, Inc.

- （日志收集器模式）开始步骤 6 以从 Panorama 模式切换到日志收集器模式。

  在将日志收集器添加为 *Panorama* 管理服务器的受管收集器时，请输入专有日志收集器的公共 *IP* 地址。您无法指定 *IP Address*（*IP* 地址）、*Netmask*（子网掩码）或 *Gateway*（网关）。
- （Panorama 和仅管理模式）配置受管收集器以添加专用日志收集器至 Panorama 虚拟设备。仅管理模式不支持本地日志收集，需要专用日志收集器存储受管设备的日志。

在 *KVM* 上安装 *Panorama*

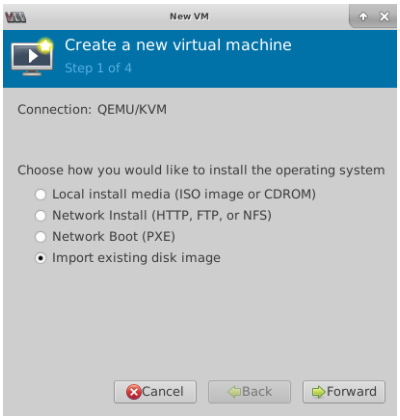
现在，您可以在 KVM 上部署 Panorama™ 和专用日志收集器。KVM 上部署的 Panorama 是自带许可 (BYOL)，支持所有部署模式（Panorama、日志收集器和仅管理），并与 M 系列硬件设备共享相同的流程和功能。更多有关 Panorama 模式的详细信息，请参阅 Panorama 型号。

STEP 1 | 下载用于 KVM 的 Panorama 虚拟设备映像。

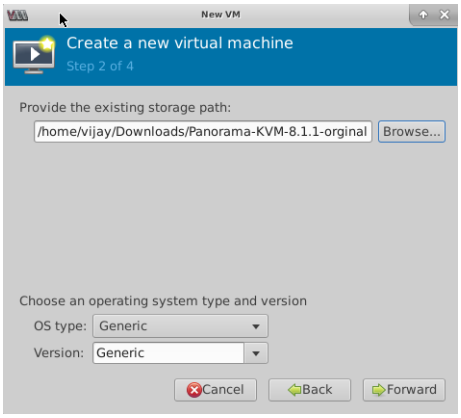
1. 登录到 Palo Alto Networks 支持门户。
2. 选择 **Software Updates**（软件更新），查找用于 KVM 基本映像的 Panorama。
3. 下载最新可用的Panorama .qcow2 文件。

STEP 2 | 创建新的虚拟机，并将用于 KVM 的 Panorama 虚拟设备映像添加到虚拟机管理器。

1. 在虚拟机管理器上，选择 **Create a new virtual machine**（创建新虚拟机）。
2. 选择 **Import Existing disk image**（导入现有磁盘映像），然后单击 **Forward**（转发）。



3. **Browse**（浏览），选择 Panorama 虚拟设备映像卷，然后 **Choose volume**（选择卷）。
4. 单击 **Forward**（转发）。



STEP 3 | 配置内存和 CPU 设置。

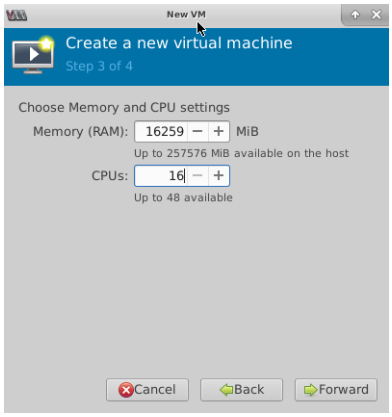
© 2019 Palo Alto Networks, Inc.

有关最小资源要求，请查看设置 Panorama 虚拟设备的前提条件。

如果您打算将 *Panorama* 虚拟设备用作专用日志收集器，必须在初始部署时配置具备所需资源的设备。如果在部署虚拟机后调整其大小，则 *Panorama* 虚拟设备可能不会保留在日志收集器模式下，从而导致日志数据丢失。

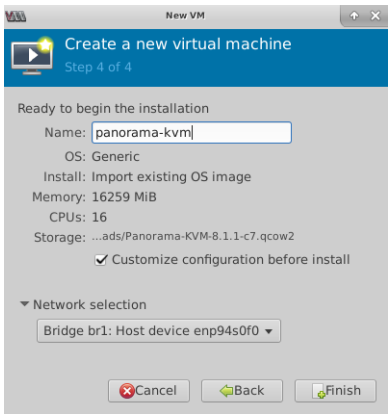
1. 根据所需操作模式的要求配置 **Memory**（内存）。

   根据您正在运行的版本，虚拟机管理器可以使用 *MiB(mebibyte)* 分配内存。如果使用 *MiB*，请根据 *Panorama* 虚拟设备的配置将您所需的内存进行正确分配。
2. 根据所需操作模式的要求配置 **CPU**。
3. 单击 **Forward**（转发）。



STEP 4 | 命名 Panorama 虚拟设备，启用配置自定义，然后选择管理接口网桥。

1. 输入 Panorama 虚拟设备的描述性 **Name**（名称）。
2. **Customize configuration before install**（在安装之前自定义配置）。
3. 进行 **Network selection**（网络选择）—选择管理接口的网桥，并接受默认设置。
4. 单击 **Finish**（完成）。

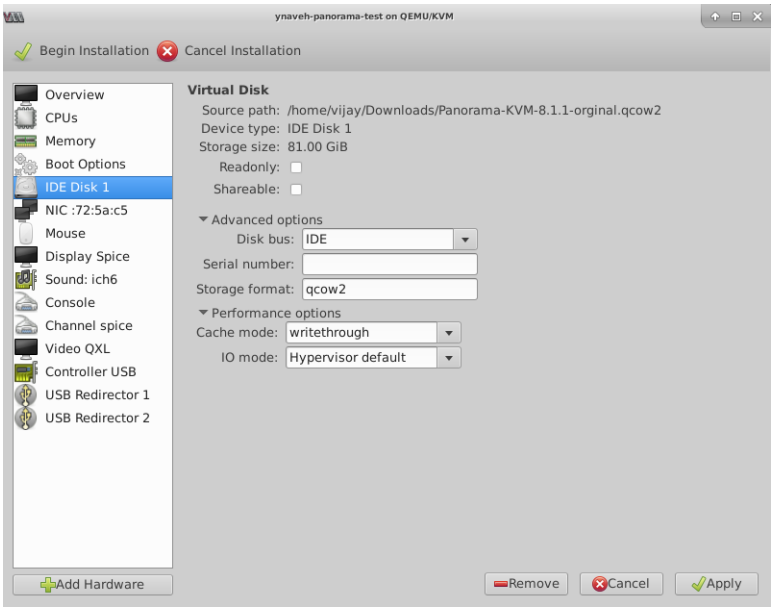


STEP 5 | 配置虚拟系统磁盘设置。

1. 选择 **IDE Disk 1**（**IDE** 磁盘 **1**），转到 **Advanced options**（高级选项），然后选择以下选项：
   - **Disk Bus**（磁盘总线）—**VirtIO** 或 **IDE**，这视您的配置而定。
   - **Storage format**（存储格式）—**qcow2**
2. 转到 **Performance options**（性能选项），并将 **Cache mode**（缓存模式）设置为 **writethrough**。此设置缩短了安装时间和提高了在 Panorama 虚拟设备上执行的速度。

© 2019 Palo Alto Networks, Inc.

3. 单击应用。

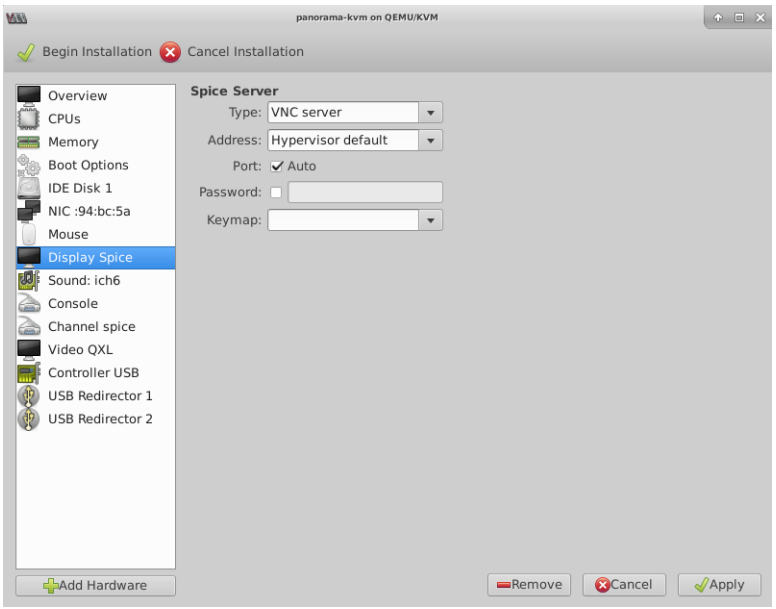


STEP 6 | 配置虚拟机控制台 显示，以使用 VNC 服务器与虚拟机进行交互。

1. 选择 **Display Spice**（显示 **Spice**）。

   因为虚拟机已配置为使用 *VNC* 服务器进行显示，因此，如果在硬件列表中列出 *Display VNC*（显示 *VNC*），则继续下一步。

2. 在 **Type**（类型）下拉列表中，选择 **VNC server**（**VNC** 服务器）。
3. 单击应用。



STEP 7 | （Panorama 和日志收集器模式）添加用于日志收集的额外存储。必要时重复该步骤，以添加额外的虚拟日志记录磁盘。

如果您打算在 Panorama 模式下使用 Panorama 虚拟设备，或将 Panorama 虚拟设备用作专用日志收集器，则在初始部署时添加虚拟日志记录磁盘。默认情况下，当您满足 Panorama 模式资源要求，且已添加至少一个虚拟日志记录磁盘，则 Panorama 虚拟设备将处于 Panorama 模式，以进行初始部署。否则，

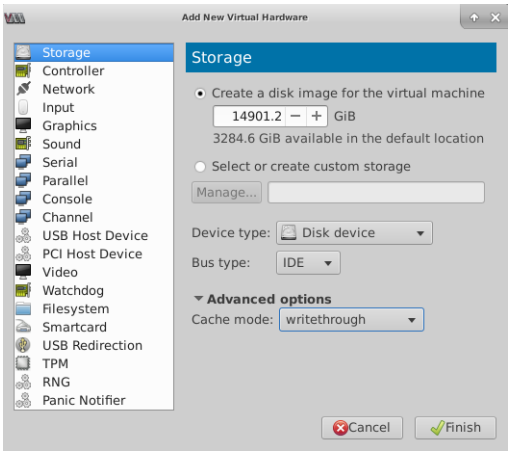
© 2019 Palo Alto Networks, Inc.

Panorama 虚拟设备将默认为处于仅管理模式。如果您只想管理设备和专用日志收集器，并不想本地收集日志，则将 Panorama 虚拟设备更改为仅管理模式。

KVM 上的 Panorama 虚拟设备仅支持 2TB 日志记录磁盘，最多支持共计 24TB 的日志存储。您不能添加小于 2TB 的日志记录磁盘，也不能添加不能被 2TB 日志记录磁盘要求整除的日志记录磁盘。Panorama 虚拟设备将大于 2TB 的日志记录磁盘分成一个一个的 2TB 分区。

1. **Add Hardware**（添加硬件）。
2. 配置新的 **Storage**（存储）磁盘：
   1. **Create a disk image for a virtual machine**（创建虚拟机磁盘映像），并将虚拟磁盘存储容量配置为 14901.2 GiB（这等于 2TB）。

      根据您正在运行的版本，虚拟机管理器可以使用 *GiB (gibibyte)* 分配内存。如果使用 *GiB*，必须正确转换所需存储容量，避免配置虚拟日志记录磁盘，并发送 *Panorama* 虚拟设备至维护模式。
   2. 设置 **Device type**（设备类型）为 **Disk**（磁盘）设备。
   3. 根据您的配置，将 **Bus type**（总线类型）设置为 **VirtIO** 或 **IDE**。
   4. 转到 **Advanced options**（高级选项），并将 **Cache mode**（缓存模式）设置为 **writethrough**。
3. 单击 **Finish**（完成）。



STEP 8 | **Begin Installatio**（开始安装）（Begin Installation）。启动 Panorama 虚拟设备可能需要约 10 分钟。

STEP 9 | 配置管理接口的网络访问设置。

1. 打开与控制台的连接。
2. 使用默认用户名和密码 (admin/admin) 登录到防火墙。
3. 通过运行以下命令进入配置模式：

```
admin> configure
```

4. 使用以下命令配置并启动访问管理接口：

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

其中 *<Panorama-IP>* 是您想要分配给管理接口的 IP 地址，*<netmask>* 是子网掩码，*<gateway-IP>* 是网关的 IP 地址，*<DNS-IP>* 是 DNS 服务器的 IP 地址。

© 2019 Palo Alto Networks, Inc.

```
admin# commit
```

STEP 10 | 激活 Panorama 虚拟设备上的设备管理许可证和支持许可证。

- 在 Panorama 虚拟设备连接到互联网时激活/检索防火墙管理许可证
- 在 Panorama 虚拟设备未连接到互联网时激活/检索防火墙管理许可证
- 激活 Panorama 支持许可证

STEP 11 | 完成配置 Panorama 虚拟设备，以满足您的部署需求。

- （仅管理模式）在仅管理模式下设置 Panorama 虚拟设备。
- （日志收集器模式）开始步骤 6 以从 Panorama 模式切换到日志收集器模式。

  在将日志收集器添加为 *Panorama* 管理服务器的受管收集器时，请输入专有日志收集器的公共 *IP* 地址。您无法指定 *IP Address*（*IP* 地址）、*Netmask*（子网掩码）或 *Gateway*（网关）。
- （Panorama 和仅管理模式）配置受管收集器以添加专用日志收集器至 Panorama 虚拟设备。仅管理模式不支持本地日志收集，需要专用日志收集器存储受管设备的日志。

在 *Hyper-V* 上安装 *Panorama*

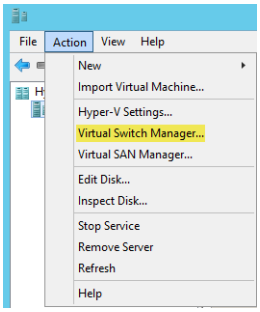
现在，您可以在 Hyper-V 上部署 Panorama™ 和专用日志收集器。现在，您可以在 Hyper-V 上部署的 Panorama™ 和专用日志收集器。Hyper-V 上部署的 Panorama 是自带许可 (BYOL)，支持所有部署模式（Panorama、日志收集器和仅管理），并与 M 系列硬件设备共享相同的流程和功能。更多有关 Panorama 模式的详细信息，请参阅 Panorama 型号。Hyper-V 上的 Panorama 虚拟设备和虚拟专用日志收集器仅适用于 PAN-OS 8.1.3 或更高版本。

STEP 1 | 下载 VHDX 文件。

1. 登录到 Palo Alto Networks 支持门户。
2. 选择 **Updates**（更新）> **Software Updates**（软件更新），并按 **Panorama Base Images**（**Panorama** 基本映像）进行筛选，然后下载 VHDX 文件。

STEP 2 | 设置所需的任何 vSwitch。有关更多信息，请查看虚拟交换机类型。

1. 在 Hyper-V 管理器中，选择主机，然后选择 **Action**（操作）> **Virtual Switch Manager**（虚拟交换机管理器），以打开虚拟交换机管理器窗口。

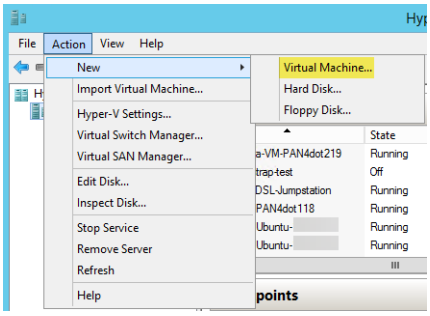


2. 在 **Create virtual switch**（创建虚拟交换机）中，选择 vSwitch 类型进行创建，然后单击 **Create Virtual Switch**（创建虚拟交换机）。

STEP 3 | 安装 Panorama 虚拟设备。

1. 在 Hyper-V 管理器中，选择主机，然后选择 **Action**（操作）> **New**（新建）> **Virtual Machine**（虚拟机）。在新建虚拟机向导中配置以下设置：

© 2019 Palo Alto Networks, Inc.



1. 为 Panorama 虚拟设备选择一个 **Name**（名称）和 **Location**（位置）。Panorama 虚拟设备会在指定位置存储 VHDX 文件。
2. 选择 **Generation 1**（第 **1** 代）。该选项为默认选项，也是唯一支持的版本。
3. 对于 **Startup Memory**（启动内存），根据预期的系统模式分配内存。有关每个模式的内存要求，请参阅 设置 Panorama 虚拟设备的前提条件 。

   切勿启用动态内存；*Panorama* 虚拟设备需要静态内存分配。
4. 配置 **Networking**（联网）。选择一个外部 vSwitch，以连接防火墙上的管理接口。
5. 若要连接 **Virtual Hard Disk**（虚拟硬盘），选择 **Use an existing virtual hard disk**（使用现有虚拟硬盘），并浏览到您之前下载的 VHDX 文件。
6. 检查摘要，然后单击 **Finish**（完成）。

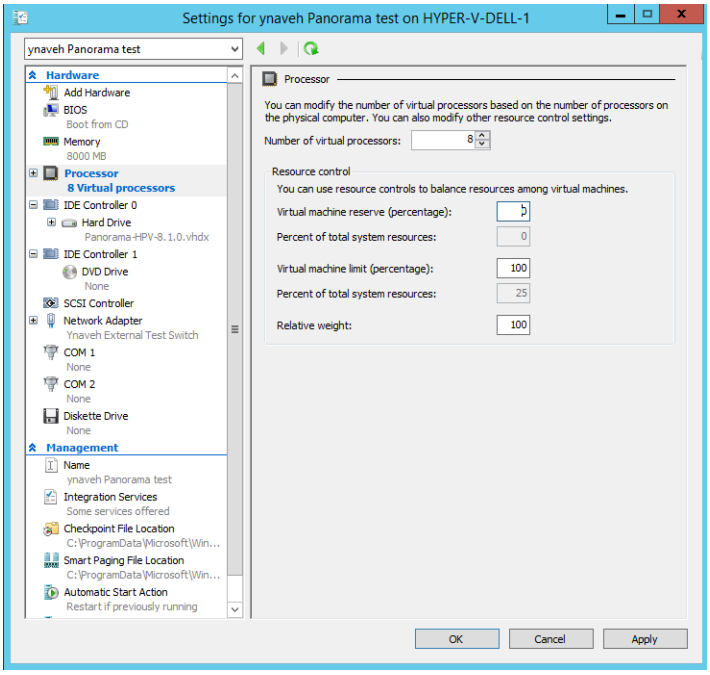
STEP 4 | 分配 Panorama 虚拟设备 CPU 内核。

有关最小资源要求，请查看设置 Panorama 虚拟设备的前提条件。

如果您打算将 *Panorama* 虚拟设备用作专用日志收集器，必须在初始部署时配置具备所需资源的设备。如果在部署虚拟机后调整其大小，则 *Panorama* 虚拟设备可能不会保留在日志收集器模式下，从而导致日志数据丢失。

1. 在 **Hardware**（硬件）列表中，选择 **Processor**（处理器）。
2. 编辑当前已分配的 **Number of virtual processors**（虚拟处理器数量）。

© 2019 Palo Alto Networks, Inc.



STEP 5 | 对于防火墙上的数据面板接口，至少连接一个网络适配器。请重复此步骤以在 Panorama 虚拟设备上创建其他网络接口。

1. 选择 **Settings**（设置）> **Hardware**（硬件）> **Add Hardware**（添加硬件），然后选择网络适配器的 **Hardware type**（硬件类型）。

   不支持传统网络适配器和 *SR-IOV*。若选择这两种适配器，防火墙将会以维护模式启动。

2. 单击 **OK**（确定）。

STEP 6 | （Panorama 和日志收集器模式）添加用于日志收集的额外存储。必要时重复该步骤，以添加额外的虚拟日志记录磁盘。如果打算在仅管理模式下部署 Panorama 虚拟设备，则继续步骤 6。

如果您打算在 Panorama 模式下使用 Panorama 虚拟设备，或将 Panorama 虚拟设备用作专用日志收集器，则在初始部署时添加虚拟日志记录磁盘。默认情况下，当您满足 Panorama 模式资源要求，且已添加至少一个虚拟日志记录磁盘，则 Panorama 虚拟设备将处于 Panorama 模式，以进行初始部署。否则，Panorama 虚拟设备将默认为处于仅管理模式。如果您只想管理设备和专用日志收集器，并不想本地收集日志，则将 Panorama 虚拟设备更改为仅管理模式。

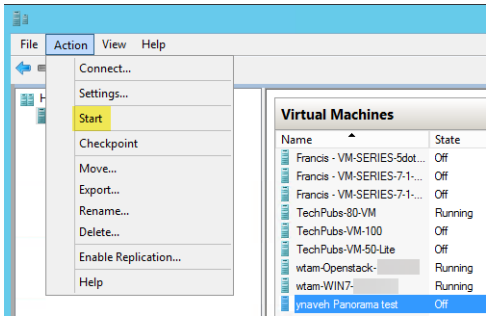
Hyper-V 上的 Panorama 虚拟设备仅支持 2TB 日志记录磁盘，最多支持共计 24TB 的日志存储。您不能添加小于 2TB 的日志记录磁盘，也不能添加不能被 2TB 日志记录磁盘要求整除的日志记录磁盘。Panorama 虚拟设备将大于 2TB 的日志记录磁盘分成一个一个的 2TB 分区。

1. 在 Hyper-V 管理器中，选择主机，然后选择 **Action**（操作）> **New**（新建）> **Hard Disk**（硬盘）。
2. 如果看到开始之前提示，则单击 **Next**（下一步）以开始添加虚拟日志记录磁盘。
3. 对于磁盘格式，请选择 **VHDX**。单击 **Next**（下一步）以继续。
4. 对于磁盘类型，根据需要选择 **Fixed Size**（固定大小）或 **Dynamically Expanding**（动态扩展）。单击 **Next**（下一步）以继续。
5. 指定虚拟日志记录磁盘文件的 **Name**（名称）和 **Location**（位置）。单击 **Next**（下一步）以继续。
6. 要配置磁盘，请选择 **Create a new virtual hard disk**（创建新虚拟硬盘），然后输入磁盘大小。单击 **Next**（下一步）以继续。
7. 查看摘要，**Finish**（完成）添加虚拟硬盘日志记录。

© 2019 Palo Alto Networks, Inc.

STEP 7 | 开启 Panorama 虚拟设备。

1. 从 **Virtual Machines(虚拟机)**列表中选择 Panorama 虚拟设备实例。
2. 选择 **Action**（操作）> **Start**（开始）以启动 Panorama 虚拟设备。



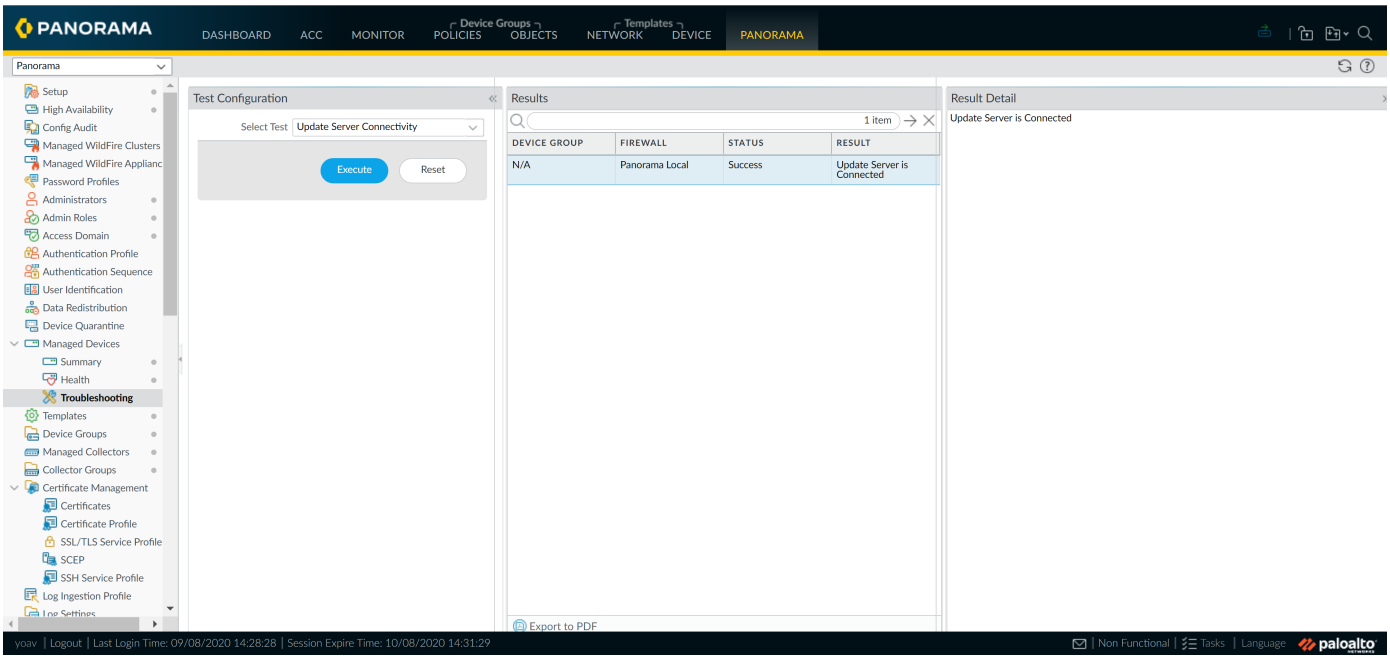
STEP 8 | 配置管理接口 IP 地址。

如果已在虚拟交换机网络上启用 DHCP 服务，则可跳过此步骤。

1. 在 **Virtual Machines**（虚拟机）列表中选择 Panorama 虚拟设备。
2. 选择 **Actions**（操作）> **Connect**（连接），然后输入您的用户名和密码（两者的默认设置均为 admin）以登录。
3. 输入以下命令，其中 *<Panorama-IP>* 是您希望分配给 Panorama 管理接口的 IP 地址，*<netmask>* 是子网掩码，*<gateway-IP>* 是网关的 IP 地址，*<DNS-IP>* 是 DNS 服务器的 IP 地址。

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

4. 排除网络资源连接问题验证防火墙管理所需的对默认网关、DNS 服务器和 Palo Alto Networks 更新服务器等外部服务的网络访问，如下所示：



STEP 9 | 激活 Panorama 虚拟设备上的设备管理许可证和支持许可证。

© 2019 Palo Alto Networks, Inc.

- 在 Panorama 虚拟设备连接到互联网时激活/检索防火墙管理许可证
- 在 Panorama 虚拟设备未连接到互联网时激活/检索防火墙管理许可证
- 激活 Panorama 支持许可证

STEP 10 | 完成配置 Panorama 虚拟设备，以满足您的部署需求。

- （仅管理模式）在仅管理模式下设置 Panorama 虚拟设备。
- （日志收集器模式）开始步骤 6 以从 Panorama 模式切换到日志收集器模式。



在将日志收集器添加为 *Panorama* 管理服务器的受管收集器时，请输入专有日志收集器的公共 *IP* 地址。您无法指定 *IP Address*（*IP* 地址）、*Netmask*（子网掩码）或 *Gateway*（网关）。

- （Panorama 和仅管理模式）配置受管收集器以添加专用日志收集器至 Panorama 虚拟设备。仅管理模式不支持本地日志收集，需要专用日志收集器存储受管设备的日志。

执行 Panorama 虚拟设备的初始配置

根据 Panorama 型号，使用AWS、Azure 或 GCP Web 界面，KVM 虚拟机管理器，Hyper-V 管理器，VMware vSphere Client 或 vCloud Air Web 控制台以设置 Panorama 虚拟设备的网络访问权限。默认情况下，Panorama 虚拟设备在仅管理模式下部署。为了确保统一的报告，应考虑在 Panorama 和所有受管防火墙和日志收集器之间将格林威治标准时间 (GMT) 或协调世界时间 (UTC) 用作统一时区。

STEP 1 | 从网络管理员处收集必要的信息。

收集管理 (MGT) 接口的以下信息：

- 管理 (MGT) 接口的 IP 地址
- 子网掩码
- 默认网关
- DNS 服务器 IP 地址



要完成 *MGT* 接口的配置，您必须指定 *IP* 地址、网络掩码（对于 *IPv4*）或前缀长度（对于 *IPv6*）以及默认网关。如果忽略某些设置（如默认网关）的值，则以后更改配置时只能通过控制台端口访问 *Panorama*。作为最佳做法，始终提交完整的 *MGT* 接口配置。

STEP 2 | 访问 Panorama 虚拟设备的控制台。

1. 访问该控制台。

   在 ESXi 服务器上：

   1. 启动 VMware vSphere Client。
   2. 选择 Panorama 虚拟设备的 **Console**（控制台）选项卡，然后按下 Enter 键进入登录屏幕。

   在 vCloud Air 上：

   1. 访问 vCloud Air Web 控制台，然后选择您的 **Virtual Private Cloud OnDemand**（按需虚拟私有云）区域。
   2. 选择 **Virtual Machines**（虚拟机）选项卡，右击 Panorama 虚拟机，然后选择 **Open In Console**（在控制台中打开）。
2. 输入您的用户名和密码（两者的默认设置均为 admin）以登录。

   在 AWS、Azure、GCP、KVM 和 Hyper-V 上：

   - 登录到 Panorama 命令行界面。

STEP 3 | 更改默认的管理员密码。

© 2019 Palo Alto Networks, Inc.

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

请务必使用密码强度最佳实践来确保密码强度，并查看密码复杂性设置。

为了确保管理接口仍然安全无虞，请配置最小密码复杂性（*Panorama* > *Setup*（设置）> *Management*（管理））。

1. 在 Web 界面页脚的左侧，单击 **admin**（管理员）链接。
2. 输入 **Old Password**（旧密码）和 **New Password**（新密码），然后将新密码记录在安全位置。
3. 单击 **OK**（确定）。

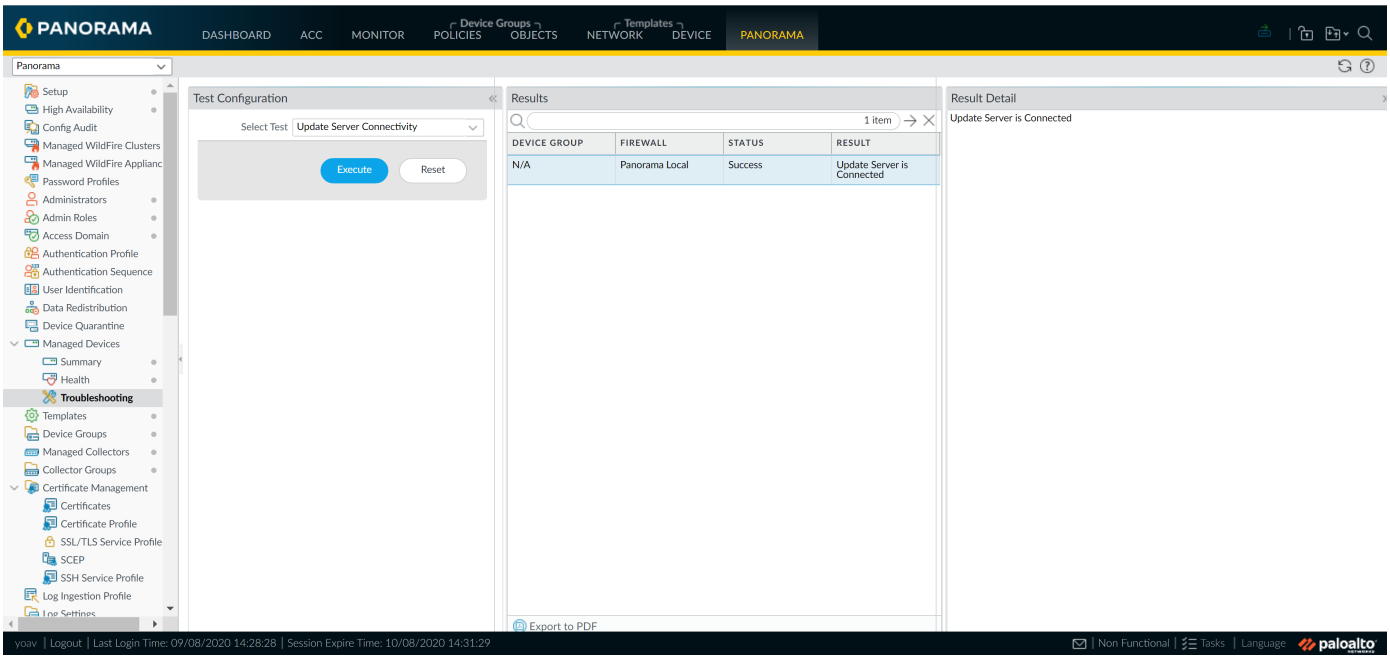
STEP 4 | 配置管理接口的网络访问设置。

Panorama 将 MGT 接口用于管理流量、高可用性同步、日志收集以及收集器组内部通信。

1. 输入以下命令，其中 *<Panorama-IP>* 是您希望分配给 Panorama 管理接口的 IP 地址，*<netmask>* 是子网掩码，*<gateway-IP>* 是网关的 IP 地址，*<DNS-IP>* 是 DNS 服务器的 IP 地址。

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

2. 排除网络资源连接问题验证防火墙管理所需的对默认网关、DNS 服务器和 Palo Alto Networks 更新服务器等外部服务的网络访问，如下所示：



STEP 5 | 配置常规设置。

1. 在 Web 浏览器中使用安全连接 (HTTPS)，通过您分配给管理接口的 IP 地址和密码登录 Panorama Web 界面 (https://<IP address>)。

© 2019 Palo Alto Networks, Inc.

2. 选择 **Panorama** > **Setup** > **Management**（Panorama > 设置 > 管理），然后编辑“General Settings（常规设置）”。
3. 输入服务器的 **Hostname**（主机名），然后输入网络 **Domain**（域）名。域名只是一个标签；Panorama 不会使用它来加入域。
4. 对准 Panorama 与受管防火墙上的时钟，以使用相同的 **Time Zone**（时区），例如 GMT 或 UTC。如果您打算使用 Cortex 数据湖，则必须配置 NTP 以使 Panorama 可以与 Cortex 数据湖保持同步。

   当 Panorama 接收日志和受管防火墙生成日志时，时间戳将被加以记录。对准 Panorama 与防火墙上的时区可确保时间戳同步，且 Panorama 上查询日志和生成报告的流程相互协调。
5. 输入 **Latitude**（纬度）和 **Longitude**（经度），以实现在时间地图上精确地定位 Panorama 管理服务器。
6. 输入您在订单执行电子邮件中收到的 **Serial Number**（序列号）。
7. 单击 **OK**（确定）保存更改。

STEP 6 | （可选）修改管理接口的设置。

1. 选择 **Panorama** > **Setup**（设置）> **Interfaces**（接口），然后单击 **Management**（管理）。
2. 如果防火墙使用已转换为专用 IP 地址 (NAT) 的公共 IP 地址连接到 Panorama 管理服务器，则在 **Public IP Address**（公共 **IP** 地址）字段内输入公共 IP， 在 **IP Address**（**IP** 地址）字段内输入专用 IP，以便将这两个地址推送到您的防火墙。
3. 选择要在接口上允许的网络连接服务（例如 **SSH** 访问）。

   请不要选择 *Telnet* 或 *HTTP*。这些服务采用明文，因此不如其他服务安全。
4. 单击 **OK**（确定）保存对接口所作的更改。

STEP 7 | Commit（提交）配置更改。

选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

STEP 8 | 后续步骤...

1. 如有需要，扩展 Panorama 虚拟设备上的日志存储容量。
2. （最佳做法）替换默认证书（Panorama 用于加密经由管理 (MGT) 接口的 HTTPS 通信的证书）。
3. 激活 Panorama 支持许可证。
4. 在 Panorama 虚拟设备连接到互联网时激活/检索防火墙管理许可证。
5. 安装 Panorama 的内容和软件更新。
6. 设置 Panorama 的管理访问权限

设置 Panorama 虚拟设备为日志收集器

如果需要日志收集用的专用虚拟设备，请在日志收集器模式下在 ESXi、AWS、AWS GovCloud、Azure、Google Cloud Platform、KVM 或 Hyper-V 上配置 Panorama 虚拟设备。为此，您先要对 Panorama 模式下的虚拟设备执行初始配置，包括许可、安装软件和内容更新及配置管理 (MGT) 接口。然后，将 Panorama 虚拟设备切换到日志收集器模式，完成日志收集器配置。此外，如果您想使用专用 M 系列设备接口（推荐），而不是 MGT 接口用于日志收集和收集器组通信，您必须先为 Panorama 管理服务器配置接口，然后为日志收集器配置这些接口，提交收集器组后再执行 Panorama 提交。

执行以下步骤将新的虚拟设备设置为日志收集器，或者转换之前用作 Panorama 管理服务器的现有虚拟设备。

将 虚拟设备从 *Panorama* 模式切换到日志收集器模式将重新启动设备，删除本地日志收集器，删除任何现有的日志数据，并删除除管理访问权限设置之外的所有配置。切换模式不会删除许可证、软件更新或内容更新。

© 2019 Palo Alto Networks, Inc.

STEP 1 | 设置将管理日志收集器的 Panorama 虚拟设备管理服务器（如果尚未设置）。

然后执行以下任务之一：

- 设置 Panorama 虚拟设备
- 设置 M 系列设备

STEP 2 | 记录 Panorama 管理服务器的管理 IP 地址。

如果在高可用性 (HA) 配置中部署 Panorama，您需要在每个高可用性对端设备的 IP 地址。

1. 登录 Panorama 管理服务器的 Web 界面。
2. 选择 **Panorama** > **Setup**（设置）> **Management**（管理），查看 Management Interface Settings（管理接口设置），记录单独（非高可用性）或主动（高可用性）Panorama 的 **IP Address**（**IP** 地址）。
3. 对于高可用性部署，选择 **Panorama** > **High Availability**（高可用性），查看 Setup（设置）部分，记录被动 Panorama 的 **Peer HA IP Address**（对端设备高可用性 **IP** 地址）。

STEP 3 | 设置将要用作专用日志收集器的 Panorama 虚拟设备。

如果您之前将此设备部署为 Panorama 管理服务器，您可以跳过此步骤，因为 MGT 接口已配置，许可证和更新已安装。

日志收集器模式下的 Panorama 虚拟设备没有用于配置任务的 Web 界面，只有 CLI。因此，在更改 Panorama 虚拟设备的模式之前，使用 Panorama 模式下的 Web 界面：

1. 在以下其中一个支持管理程序中设置 Panorama 虚拟设备：
   - 在 ESXi 服务器上安装 Panorama
   - 在 AWS 上安装 Panorama。
   - 在 AWS GovCloud 上安装 Panorama
   - 在 Azure 上安装 Panorama。
   - 在 Google Cloud Platform 上安装 Panorama。
   - 在 Hyper-V 上安装 Panorama
2. 执行 Panorama 虚拟设备的初始配置。
3. 注册 Panorama 和安装许可证。
4. 安装 Panorama 的内容和软件更新。

STEP 4 | （仅限 Azure 上的 Panorama）修改管理员密码。

专用日志收集器仅支持管理员用户（管理），以便更改为日志收集器模式。修改管理员密码，允许您以管理员用户（管理）身份登录。

1. 登录到 Panorama Web 界面。
2. 选择 **Panorama** > **Administrators**（管理员），然后选择**admin**（管理）。
3. 输入 **Password**（密码），**Confirm Password**（确认密码），并单击**OK**（确认）。
4. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

STEP 5 | （仅限 AWS 和 Azure 上的 Panorama）删除管理员用户之外的所有用户。

1. 以管理员身份登录到 Panorama Web 界面。
2. 选择 **Panorama** > **Administrators**（管理员）。
3. 选择管理之外的现有管理员，并 **Delete**（删除）。
4. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

STEP 6 | 登录到 Panorama 命令行界面。

STEP 7 | 从 Panorama 模式切换到日志收集器模式。

1. 要切换到日志收集器模式，请输入以下命令：

© 2019 Palo Alto Networks, Inc.

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

2. 输入 **Y** 确认模式更改。重启虚拟设备。如果重新启动进程终止了终端模拟软件会话，重新连接虚拟设备以查看 Panorama 登录提示。

   如果您看到 ***CMS Login***（*CMS* 登录）提示，这意味着日志收集器没有完成重新启动。看到提示时按 *Enter* 键，而不输入用户名或密码。

3. 重新登录至此 CLI。
4. 验证切换到日志收集器模式是否成功：

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

如果模式更改成功，输出显示：

```
system-mode: logger
```

STEP 8 | 启用日志收集器和 Panorama 管理服务器之间的连接。

在日志收集器 CLI 中输入以下命令，*<IPaddress1>* 是单独（非高可用性）或主动（高可用性）Panorama 的 MGT 接口，*<IPaddress2>* 是被动（高可用性）Panorama 的 MGT 接口（如适用）。

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

STEP 9 | 记录日志收集器的序列号。

您需要此序列号在 Panorama 管理服务器上，将日志收集器添加为受管收集器。

1. 在日志收集器命令行界面中，输入以下命令以显示它的序列号。

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

2. 记录序列号。

STEP 10 | 将日志收集器添加为 Panorama 管理服务器的受管收集器。

1. 选择 **Panorama** > **Managed Collectors**（Panorama > 受管收集器），**Add**（添加）受管收集器。
2. 在 **General**（常规）设置中，输入为日志收集器记录的序列号（**Collector S/N**（收集器序列号））。
3. 在 **Panorama Server IP**（**Panorama** 服务器 **IP**）字段中，输入单独（非高可用性）或主动（高可用性）Panorama 的 IP 地址或 FQDN。对于高可用性部署，在 **Panorama Server IP 2**（**Panorama** 服务器 **IP 2**）字段中输入被动 Panorama 对端设备的 IP 地址或 FQDN。

   这些 IP 地址必须指定启用 **Device Management and Device Log Collection**（设备管理和设备日志收集）服务的 Panorama 接口。默认情况下，仅在 MGT 接口上启用这些服务。但是，您可能会在设置 M 系列设备作为 Panorama 管理服务器时在其他接口上启用这些服务。
4. 选择 **Interfaces**（接口），单击 **Management**（管理），然后输入专用日志收集器的**Public IP Address**（公共 **IP** 地址）。
5. 单击 **OK**（确定）两次保存对日志收集器所作的更改。
6. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并将更改 **Commit**（提交）到 Panorama 配置。

© 2019 Palo Alto Networks, Inc.

7. 核实 **Panorama** > **Managed Collectors**（受管收集器）是否列出您已添加的日志收集器。Connected（已连接）列显示表明日志收集器已连接到 Panorama 的复选标记。您可能需要等待几分钟，等页面显示更新后的连接状态。

   此时，*Configuration Status*（配置状态）列显示 *Out of Sync*（不同步），*Run Time Status*（运行时间状态）列应显示 *disconnected*（已断开连接）。在配置收集器组后，状态将更改为同步中和已连接。

STEP 11 | 启用日志记录硬盘。

1. 选择 **Panorama** > **Managed Collectors**（Panorama > 受管收集器），然后编辑日志收集器。
2. 选择 **Disks**（磁盘），然后**Add**（添加）每个磁盘。
3. 单击 **OK**（确定）保存更改。
4. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并将更改 **Commit**（提交）到 Panorama 配置。

STEP 12 | （推荐）如果 Panorama 管理服务器和日志收集器使用 **Ethernet1**、**Ethernet2**、**Ethernet3**、**Ethernet4** 和 **Ethernet5** 接口进行 **Device Log Collection**（设备日志收集）（从防火墙接收日志）和 **Collector Group Communication**（收集器组通信），请配置这些接口。

如果您以前将日志收集器部署为 Panorama 管理服务器并配置这些接口，则必须重新配置它们，因为切换到日志收集器模式将删除除管理访问设置以外的所有配置。

1. 如果您尚未完成以下操作，请配置 Panorama 管理服务器上的每个接口（MGT 接口除外）：
   1. 选择 **Panorama** > **Setup**（设置）> **Interfaces**（接口），然后单击接口名称。
   2. 选择 *<interface-name>* 以启用接口。
   3. 根据您网络的 IP 协议，填写以下一个或两个字段集：
      - 对于 ESXi
        - IPv4—**Public IP Address**（公共 **IP** 地址），**IP Address**（**IP** 地址），**Netmask**（子网掩码）和 **Default Gateway**（默认网关）

          IPv6 — **IPv6 Address/Prefix Length**（**IPv6** 地址/前缀长度）和 **Default IPv6 Gateway**（默认 **IPv6** 网关）
      - 对于 AWS、Azure 和 Google™ Cloud Platform
        - 公共 **IP** 地址
   4. 选择接口支持的设备管理服务：

      Device Management and Device Log Collection（设备管理和设备日志收集）— 您可以分配一个或多个接口。

      Collector Group Communication（收集器组通信）— 您只能分配一个接口。

      Device Deployment（设备部署）（软件和内容更新）— 您只能分配一个接口。
   5. 单击 **OK**（确定）保存更改。
2. 配置日志收集器上的每个接口（MGT 接口除外）：
   1. 选择 **Panorama** > **Managed Collectors**（Panorama > 受管收集器），然后编辑日志收集器。
   2. 选择 **Interfaces**（接口），并单击接口名称。
   3. 选择 *<interface-name>* 以启用接口。
   4. 根据您网络的 IP 协议，填写以下一个或两个字段集：
      - 对于 ESXi
        - IPv4—**Public IP Address**（公共 **IP** 地址），**IP Address**（**IP** 地址），**Netmask**（子网掩码）和 **Default Gateway**（默认网关）

© 2019 Palo Alto Networks, Inc.

IPv6 — **IPv6 Address/Prefix Length**（**IPv6** 地址/前缀长度）和 **Default IPv6 Gateway**（默认 **IPv6** 网关）

- 对于 AWS 和 Azure
  - 公共 **IP** 地址

5. 选择接口支持的设备管理服务：

   Device Log Collection（设备日志收集）— 您可以分配一个或多个接口。

   Collector Group Communication（收集器组通信）— 您只能分配一个接口。

6. 单击 **OK**（确定）保存对接口所作的更改。

3. 单击 **OK**（确定）保存对日志收集器所作的更改。
4. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并将更改 **Commit**（提交）到 Panorama 配置。

STEP 13 | （可选）如果您的部署使用自定义证书在 Panorama 和受管设备之间进行身份验证，请部署自定义客户端设备证书。有关更多信息，请参阅使用自定义证书设置身份验证。

1. 选择 **Panorama** > **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件），然后从下拉列表中选择证书配置文件或单击 **New Certificate Profile**（新建证书配置文件）以创建证书配置文件。
2. 选择日志收集器的 **Panorama** > **Managed Collectors**（受管收集器）> **Add**（添加）> **Communication**（通信）。
3. 选中 **Secure Client Communication**（安全客户端通信）复选框。
4. 选择 Type（类型）下拉列表中的设备证书类型。
   - 如果您使用本地设备证书，请从各自下拉列表中选择 **Certificate**（证书）和 **Certificate Profile**（证书配置文件）。
   - 如果您使用 SCEP 作为设备证书，请从各自下拉列表中选择 **SCEP Profile**（**SCEP** 配置文件）和 **Certificate Profile**（证书配置文件）。
5. 单击 **OK**（确定）。

STEP 14 | （可选）在日志收集器上配置安全服务器通信。有关更多信息，请参阅使用自定义证书设置身份验证。

1. 选择 **Panorama** > **Managed Collectors**（受管收集器）> > **Communication**（通信）。
2. 验证 **Custom Certificate Only**（仅允许自定义证书）复选框未选中。这允许您在迁移到自定义证书的同时继续管理所有设备。

   如果选中 *Custom Certificate Only*（仅允许自定义证书）复选框，则日志收集器不会进行身份验证，并且无法使用预定义证书从设备接收日志。

3. 从 **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）下拉列表中选择 SSL/TLS 服务配置文件。此 SSL/TLS 服务配置文件适用于日志收集器和发送日志的设备之间的所有 SSL 连接。
4. 从 **Certificate Profile**（证书配置文件）下拉列表中选择证书配置文件。
5. 选择 **Authorize Client Based on Serial Number**（根据序列号对客户端进行身份验证）让服务器根据受管设备的序列号检查客户端。客户端证书必须将特殊关键字 $UDID 设置为要根据序列号进行授权的 CN。
6. 在 **Disconnect Wait Time (min)**（断开连接等待时间（分钟））中，输入 Panorama 在与其受管设备断开并重新建立连接之前所需的分钟数。该字段默认为空，范围为 0 至 44,640 分钟。

   在您提交新配置之前，断开连接等待时间不会开始倒计时。

7. （可选）配置授权列表。

   1. 单击 Authorization List（授权列表）下的 **Add**（添加）。

© 2019 Palo Alto Networks, Inc.

2. 选择 **Subject**（主题）或 **Subject Alt Name**（主题备用名称）作为标识符类型。
3. 输入所选类型的标识符。
4. 单击 **OK**（确定）。
5. 选择 **Check Authorization List**（检查授权列表）以执行授权列表。

8. 单击 **OK**（确定）。
9. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**）。

STEP 15 | 将日志收集器分配到一个收集器组。

1. 配置收集器组。您必须执行 Panorama 提交，然后收集器组提交与 Panorama 同步日志收集器配置，在日志收集器上将 Eth1、Eth2、Eth3、Eth4 和 Eth5 接口（如果配置）置于运行状态。

   在任何单个收集器组中，所有日志收集器均必须在相同的 *Panorama* 型号上运行：均为 *M-600* 设备、均为 *M-500* 设备、均为 *M-200* 设备或均为 *Panorama* 虚拟设备。

   作为最佳做法，如果将多个日志收集器添加到单个收集器组，请 *Enable log redundancy across collectors*（启用跨收集器记录冗余）。此选项要求每个日志收集器具有相同数量的日志记录磁盘。

2. 选择 **Panorama** > **Managed Collectors**（Panorama > 受管收集器），核实日志收集器配置是否已与 Panorama 同步。

   Configuration Status（配置状态）列应显示 In Sync（同步），Run Time Status（运行时间状态）列应显示 connected（已连接）。

3. 访问日志收集器命令行界面，输入以下命令核实它的接口是否正在运行：

   ```
   > show interface all
   ```

   在输出结果中，每个正在运行的接口的 `state` 显示为 `up`。

4. 如果收集器组有多个日志收集器，排除网络资源连接问题 为日志收集器使用的每个接口运行 Ping 连接测试，核实这些收集器是否能彼此通信。对于 `source` IP 地址，指定一个日志收集器的接口。对于 `host` IP 地址，指定同一收集器组中另一个日志收集器的匹配接口。

STEP 16 | 后续步骤...

使日志收集器能够接收防火墙日志：

1. 配置 Panorama 的日志转发。
2. 验证 Panorama 日志转发。

使用本地日志收集器设置 Panorama 虚拟设备

从 Panorama 8.0 或更早版本升级到 Panorama 8.1 或更高版本后，如果 Panorama 虚拟设备处于传统模式，则切换到 Panorama 模式以创建本地日志收集器、添加多个日志记录磁盘（无现有日志丢失）、增加日志存储容量至 24TB、并启用快速报告生成。

一旦从传统模式更改为 *Panorama* 模式，传统模式将不再可用。

升级到 Panorama 8.1 后，第一步是将虚拟设备上的系统资源增加到 Panorama 模式所需的最低限度。增加资源时 Panorama 会重新启动，因此在维护窗口中执行此过程。您必须安装更大的系统磁盘 (81GB)，并根据日志存储容量增加 CPU 和内存，以及添加虚拟日志记录盘。新的日志记录磁盘至少必须具有设备当前在传统模式下使用的容量，并且不能小于 2TB。添加虚拟磁盘可让您将现有日志迁移到日志收集器，并使日志收集器存储新日志。

© 2019 Palo Alto Networks, Inc.

如果将 Panorama 部署在高可用性配置中，请首先在辅助对端设备上执行以下步骤，然后在主要对端设备上执行以下步骤。

STEP 1 | 确定虚拟设备在 Panorama 模式下运行之前需要增加的系统资源。

即使您确定 *Panorama* 已经具有足够的资源，还必须运行此步骤中指定的命令。

1. 访问 Panorama CLI：
   1. 使用终端模拟软件（如 PuTTY），打开您为 Panorama MGT 接口指定的 IP 地址的 SSH 会话。
   2. 看到提示时登录到 CLI。
2. 通过运行以下命令检查必须增加的资源：

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

当提示继续时输入 **y**。输出指定您必须增加的资源。例如：

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

STEP 2 | 增加 CPU 和内存，并使用较大的磁盘替换系统磁盘。

1. 访问 VMware ESXi vSphere Client，选择 **Virtual Machines**（虚拟机），右击 Panorama 虚拟机，然后选择 **Power**（电源）> **Power Off**（关闭电源）。
2. 右击 Panorama 虚拟设备，然后选择 **Edit Settings**（编辑设置）。
3. 选择 **Memory**（内存）并输入新的 **Memory Size**（内存大小）。
4. 选择 **CPU**，并指定 CPU 数量（**Number of virtual sockets**（虚拟插槽数量）乘以 **Number of cores per socket**（每个插槽的内核数量））。
5. 添加虚拟磁盘。

   您将使用此磁盘替换现有的系统磁盘。

   1. 在 **Hardware**（硬件）设置中，**Add**（添加）磁盘，选择 **Hard Disk**（硬盘）作为硬件类型，然后单击 **Next**（下一步）。
   2. **Create a new virtual disk**（创建新虚拟磁盘），单击 **Next**（下一步）。
   3. 将 **Disk Size**（磁盘大小）设置为刚好 81GB，然后选择 **Thick Provision Lazy Zeroed**（密集配置延迟置零）磁盘格式。
   4. 选择 **Specify a datastore or datastore structure**（指定数据存储或数据存储结构）作为地点，**Browse**（浏览）到至少 81GB 的数据存储，单击 **OK**（确定），然后单击 **Next**（下一步）。
   5. 选择 SCSI **Virtual Device Node**（虚拟设备节点）（您可使用默认选择），单击 **Next**（下一步）。

      如果选择 *SCSI* 以外的格式，*Panorama* 将无法启动。

   6. 验证设置是否正确，然后单击 **Finish**（完成）和 **OK**（确定）。
6. 右击 Panorama 虚拟设备，然后选择 **Power**（电源）> **Power On**（打开电源）。等待 Panorama 重新启动后再继续。
7. 返回到 Panorama CLI 并将数据从原始系统磁盘复制到新系统磁盘：

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


© 2019 Palo Alto Networks, Inc.

当提示继续时输入 **y**。

复制过程大约需要 20 到 25 分钟，Panorama 会在此期间重新启动。当该过程完成后，输出会提示您关闭 Panorama。

8. 返回到 vSphere Client 控制台，右击 Panorama 虚拟设备，然后选择 **Power**（电源）> **Power Off**（关闭电源）。
9. 右击 Panorama 虚拟设备，然后选择 **Edit Settings**（编辑设置）。
10. 选择原始系统磁盘，单击 **Remove**（删除），选择 **Remove from virtual machine**（从虚拟机中删除），然后单击 **OK**（确定）。
11. 右击 Panorama 虚拟设备，然后选择 **Edit Settings**（编辑设置）。
12. 选择新系统盘，将 **Virtual Device Node**（虚拟设备节点）设置为 **SCSI (0:0)**，然后单击 **OK**（确定）。
13. 右击 Panorama 虚拟设备，然后选择 **Power**（电源）> **Power On**（打开电源）。继续之前，请等待 Panorama 在新系统磁盘上重新启动（大约 15 分钟）。

STEP 3 | 添加虚拟日志记录磁盘。

这是您将迁移现有日志的磁盘。

1. 在 VMware ESXi vSphere Client 中，右击 Panorama 虚拟设备，然后选择 **Power**（电源）> **Power Off**（关闭电源）。
2. 右击 Panorama 虚拟设备，然后选择 **Edit Settings**（编辑设置）。
3. 重复步骤以添加虚拟磁盘。根据需要的日志存储量将 **Disk Size**（磁盘大小）设置为 2TB 的倍数。容量至少必须与 Panorama 当前用于日志的现有虚拟磁盘或 NFS 存储一样大。磁盘容量必须是 2TB 的倍数，最高可达 24TB。例如，如果现有磁盘具有 5TB 的日志存储，则至少必须添加 6TB 的新磁盘。

   切换到 Panorama 模式后，Panorama 会自动将新磁盘分割成 2TB 分区，每个分区将作为单独的虚拟磁盘运行。
4. 右击 Panorama 虚拟设备，然后选择 **Power**（电源）> **Power On**（打开电源）。等待 Panorama 重新启动后再继续。

STEP 4 | 从传统模式切换到 Panorama 模式。

切换模式后，设备再次重新引导，然后自动创建本地日志收集器和收集器组。现有日志将不能用于查询或报告，直到您稍后在此过程中将其迁移。

1. 返回到 Panorama CLI 并运行以下命令。

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

   当提示继续时输入 **y**。重新启动后，Panorama 会自动创建本地日志收集器（名为 Panorama）并创建收集器组（名为 default）以包含它。Panorama 还会配置您添加的虚拟日志记录磁盘，并将其分成单独的 2TB 磁盘。等待该过程完成且 Panorama 重新启动（大约五分钟），然后继续。
2. 登录到 Panorama Web 界面。
3. 在 **Dashboard**（仪表盘）的 **General Information**（一般信息）设置中，验证 **Mode**（模式）现在为 **panorama**。

   在高可用性部署中，辅助对端设备此时处于暂挂状态，因为其模式 (Panorama) 与主要对端设备（传统）模式不匹配。稍后在此过程中将主要对端设备切换为 Panorama 模式后，您将取消暂挂辅助对端设备。
4. 选择 **Panorama** > **Collector Groups**（收集器组）以验证 **default**（默认）收集器组是否已创建，本地日志收集器是否已成为默认收集器组的一部分。
5. 将配置推送到受管设备。
   - 如果没有暂挂更改：
     1. 选择 **Commit**（提交）> **Push to Devices**（推送到设备）和 **Edit Selections**（编辑选择）。

© 2019 Palo Alto Networks, Inc.

2. 选择 **Collector Group**（收集器组），确保已选中 **default**（默认）收集器组。
3. 单击 **OK**（确定）和 **Push**（推送）。

- 如果有暂挂更改：

1. 选择 **Commit**（提交）> **Commit and Push**（提交并推送），然后 **Edit Selections**（编辑选择）。
2. 验证是否已包含您的 **Device Group**（设备组）设备和 **Templates**（模板）。
3. 选择 **Collector Group**（收集器组），确保已选中 **default**（默认）收集器组。
4. 单击 **OK**（确定）和 **Commit and Push**（提交并推送）。

6. 选择 **Panorama** > **Managed Collectors**（受管收集器），并验证列是否显示本地日志收集器的以下信息：

- 收集器名称 — 默认为 Panorama 主机名。它应该在 **default**（默认）收集器组下列出。
- 已连接 — 选中标记
- 配置状态 — 同步中
- 运行时间状态 — 已连接

STEP 5 | （仅限高可用性）将主要 Panorama 从传统模式切换到 Panorama 模式。



此步骤会触发故障转移。

1. 在主要 Panorama 上重复步骤 1 至步骤 4。

   等待主要 Panorama 重新启动并返回到主要 HA 状态。如果未启用抢先，则必须手动执行故障恢复：选择 **Panorama** > **High Availability**（高可用性），然后在操作命令部分中 **Make local Panorama functional**（运行本地 **Panorama**）。
2. 在主要 Panorama 上选择 **Dashboard**（仪表盘），并在 High Availability（高可用性）部分中选择 **Sync to peer**（同步到对端设备），单击 **Yes**（是），然后等待 **Running Config**（运行配置）显示 **Synchronized**（已同步）状态。
3. 在辅助 Panorama 上选择 **Panorama** > **High Availability**（高可用性），然后在 Operational Commands（操作命令）部分中选择 **Make local Panorama functional**（运行本地 **Panorama**）。

   此步骤对于将辅助 Panorama 从其暂挂的高可用性状态移出是必需执行的。

STEP 6 | 将现有日志迁移到新的虚拟日志记录磁盘。

如果您在高可用性配置中部署 Panorama，请仅在主要对端设备上执行此操作。

1. 返回到 Panorama CLI。
2. 开始日志迁移：

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

进程持续时间因您正在迁移的日志数据量而异。要检查迁移的状态，请运行以下命令：

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

迁移完成后，输出显示：`migration has been done`。

3. 验证现有日志是否可用。
   1. 登录到 Panorama Web 界面。
   2. 选择 **Panorama** > **Monitor**（监控），选择您知道与某些现有日志匹配的日志类型（例如，**Panorama** > **Monitor**（监控）> **System**（系统）），然后验证日志是否显示。

© 2019 Palo Alto Networks, Inc.

STEP 7 | 后续步骤...

配置 Panorama 的日志转发以便日志收集器从防火墙接收新日志。

在 Panorama 模式下设置 Panorama 虚拟设备

在 Panorama 模式下，Panorama™ 虚拟设备可以充当带本地日志收集功能的 Panorama 管理服务器。默认情况下，当至少有一个虚拟日志记录磁盘附加到初始部署上 Amazon Web Services (AWS)、 AWS GovCloud Azure、Google Cloud Platform、 KVM、 Hyper-V、 ESXi 或 vCloud Air 中的 Panorama 虚拟设备时，可在 Panorama 模式下部署 Panorama 虚拟设备。



虽然仍受支持，但不建议在生产环境中从具有 *50GB* 日志记录磁盘的传统模式切换到 *Panorama* 模式。如果您切换到具有 *50GB* 日志记录磁盘的 *Panorama* 模式，您将无法添加额外日志记录磁盘。

STEP 1 | 登录到 Panorama 命令行界面。

STEP 2 | 切换到 Panorama 模式。

1. 更改为 Panorama 模式：

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

2. 输入 **y** 确认模式更改。重启 Panorama 虚拟设备。如果重新启动进程终止了终端模拟软件会话，重新连接 Panorama 虚拟设备以查看 Panorama 登录提示。

   如果您看到 `CMS Login`（`CMS` 登录）提示，这意味着 Panorama 虚拟设备没有完成重新启动。看到提示时按 Enter 键，而不输入用户名或密码。

STEP 3 | 验证切换到 Panorama 模式是否成功。

1. 重新登录至此 CLI。
2. 验证切换到 Panorama 模式是否成功：

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

如果模式更改成功，输出显示：

```
> system mode:panorama
```

在仅管理模式下设置 Panorama 虚拟设备

在仅管理模式下，Panorama 虚拟设备可以严格地充当不带本地日志收集功能的 Panorama 管理服务器运行。默认情况下，Panorama 模式下的 Panorama 虚拟设备专用于初始部署。因为更改为仅管理模式不允许将日志转发给 Panorama 管理服务器（因为仅管理模式下的 Panorama 虚拟设备不支持日志收集），因此建议在初始部署后将 Panorama 虚拟设备立即更改为仅管理模式。更改为仅管理模式后，Panorama 虚拟设备上存储的任何现有日志数据均将无法访问，且 ACC 和报告功能无法查询 Panorama 虚拟设备上存储的日志。

STEP 1 | 登录到 Panorama 命令行界面。

STEP 2 | 切换到仅管理模式。

1. 更改为仅管理模式：

© 2019 Palo Alto Networks, Inc.

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

2. 输入 **y** 确认模式更改。重启 Panorama 虚拟设备。如果重新启动进程终止了终端模拟软件会话，重新连接 Panorama 虚拟设备以查看 Panorama 登录提示。

   如果您看到 `CMS Login`（`CMS` 登录）提示，这意味着 Panorama 虚拟设备没有完成重新启动。看到提示时按 Enter 键，而不输入用户名或密码。

STEP 3 | 验证切换到仅管理模式是否成功。

1. 重新登录至此 CLI。
2. 验证切换到仅管理模式是否成功：

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

如果模式更改成功，输出显示：

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

扩展 Panorama 虚拟设备上的日志存储容量

执行 Panorama 虚拟设备的初始配置后，可用的日志存储容量和扩展选项取决于虚拟平台（VMware ESXi、vCloud Air、 AWS、 AWS GovCloud、Azure、 Google Cloud Platform、KVM 或 Hyper-V）和模式（传统、Panorama 或日志收集器模式）：有关详细信息，请参阅 Panorama 型号。

如要在 Panorama 虚拟设备上扩展日志存储容量，您必须添加额外日志记录磁盘。不支持扩展现有日志记录磁盘的日志存储容量，并且 Panorama 不识别额外存储容量。例如，如果您添加了一个 2TB 日志记录磁盘，然后将现有日志记录磁盘扩展到 4TB，Panorama 会继续认为日志记录磁盘的存储容量为 2TB，而忽略额外的 2TB 存储容量。



如需额外日志存储，您也可以将防火墙日志转发到专用日志收集器（请参阅配置受管收集器）或配置从 Panorama 到外部目标的日志转发。

在 Panorama 增加日志存储容量前，确定 Panorama 日志存储要求。

- 当在传统模式下在 Panorama 虚拟设备上添加存储时保留现有日志
- 向 ESXi 服务器上的 Panorama 添加虚拟磁盘
- 向 vCloud Air 中的 Panorama 添加虚拟磁盘
- 向 AWS 中的 Panorama 添加虚拟磁盘
- 向 Azure 中的 Panorama 添加虚拟磁盘
- 向 Google Cloud Platform 中的 Panorama 添加虚拟磁盘
- 向 KVM 中的 Panorama 添加虚拟磁盘
- 向 Hyper-V 中的 Panorama 添加虚拟磁盘
- 将 Panorama ESXi 服务器安装到 NFS 数据存储

当在传统模式下在 *Panorama* 虚拟设备上添加存储时保留现有日志

传统模式下的 Panorama 虚拟设备只能将一个虚拟磁盘用于日志记录。因此，如果您添加一个专用于日志记录的虚拟磁盘，则 Panorama 在系统磁盘上停止使用默认 11GB 日志存储，自动将任何现有日志复制到新日志记录磁盘上。（Panorama 继续使用系统磁盘存储数据，而不是日志。）

如果您将存储容量最高 2TB 的现有专用日志记录磁盘替换为最高 8TB 的磁盘，您会丢失现有磁盘上的日志。要保留日志，您的选择有：

© 2019 Palo Alto Networks, Inc.

- 配置到外部目标的日志转发后再替换虚拟磁盘。

- 为新 8TB 磁盘设置新的 Panorama 虚拟设备，能够访问包含有您需要日志的旧磁盘的 Panorama。要将防火墙日志转发到新 Panorama 虚拟设备，一个选择是重新配置防火墙以连接新 IP 地址（选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后编辑 Panorama Settings（Panorama 设置）），在新 Panorama 上添加防火墙作为受管设备，并 配置 Panorama 的日志转发。要在新 Panorama 上重新使用旧 Panorama IP 地址，另一个选择是在旧 Panorama 上导出配置，然后在新 Panorama 导入并加载配置。

- 将日志从旧磁盘复制到新磁盘。复制可能需要几个小时，这取决于磁盘当前存储了多少日志，Panorama 在复制过程中不能收集日志。有关说明，请联系 Palo Alto Networks 客户支持部门。

向 *ESXi* 服务器上的 *Panorama* 添加虚拟磁盘

要在 Panorama 虚拟设备上扩展日志存储容量，可以添加虚拟日志记录磁盘。如果设备处于 Panorama 模式，可以添加 1 至 12 个 2TB 虚拟日志记录磁盘或 1 个 24TB 日志记录磁盘，最大不超过 24TB。如果设备处于传统模式，则可以在 ESXi 5.5 及更高版本上添加最多 8TB 的虚拟日志记录磁盘，或在早期版本的 ESXi 上添加最多 2TB 的磁盘。此外，建议添加相同磁盘配置格式的日志记录磁盘，以避免多个不同配置格式的磁盘可能造成的性能异常情况。

发生故障时，如果 *Panorama* 失去与新虚拟磁盘的连接，*Panorama* 可能会丢失日志。

为了实现冗余，请使用 *RAID* 配置中的虚拟磁盘。*RAID10* 为具有大量日志记录特性的设备提供了最佳写入性能。

如果有必要，您可以替换 ESXi 服务器上的虚拟磁盘。

STEP 1 | 将额外磁盘添加到 Panorama

在所有模式下，*Panorama VM* 上的第一个日志记录磁盘至少必须为 *2TB* 才能添加额外磁盘。如果第一个日志记录磁盘小于 *2TB*，则将无法添加额外磁盘空间。

1. 访问 VMware vSphere Client，然后选择 **Virtual Machines**（虚拟机）。
2. 右击 Panorama 虚拟设备，然后选择 **Power**（电源）> **Power Off**（关闭电源）。
3. 右击 Panorama 虚拟设备，然后选择 **Edit Settings**（编辑设置）。
4. 在 **Hardware**（硬件）选项卡中，单击 **Add**（添加）以启动 Add Hardware（添加硬件）向导。
5. 选择 **Hard Disk**（硬盘）作为硬件类型，然后单击 **Next**（下一步）。
6. **Create a new virtual disk**（创建新虚拟磁盘），单击 **Next**（下一步）。
7. 设置 **Disk Size**（磁盘大小）。如果 Panorama 虚拟设备处于 Panorama 模式，请将大小设置为至少 2TB。如果设备处于传统模式，则可以将大小设置为 8TB。

   在 *Panorama* 模式下，您可以添加大于 *2TB* 的磁盘大小，*Panorama* 将自动创建尽可能多的 *2TB* 分区。例如，如果磁盘 *sdc* 是 *24Tb*，它将创建 *12* 个 *2TB* 分区。这些磁盘将被命名为 *sdc1-12*。
8. 选择 **Disk Provisioning**（磁盘配置）格式，然后点击 **Next**（下一步）。
9. **Specify a datastore or datastore structure**（指定数据存储或数据存储结构），**Browse**（浏览）到具有足够空间用于指定 **Disk Size**（磁盘大小）的数据存储，单击 **OK**（确定），然后单击 **Next**（下一步）。
10. 选择 SCSI **Virtual Device Node**（虚拟设备节点）（您可使用默认选择），单击 **Next**（下一步）。

© 2019 Palo Alto Networks, Inc.

选择的节点必须为 *SCSI* 格式；如果您选择其他格式，*Panorama* 无法重新启动。

11. 验证设置是否正确，然后单击 **Finish**（完成）和 **OK**（确定）。

    新磁盘随后将显示在虚拟设备的设备列表中。
12. 如果有必要，重复步骤 4 至步骤 11 以将额外磁盘添加到 Panorama 虚拟设备。
13. 右击 Panorama 虚拟设备，然后选择 **Power**（电源）> **Power On**（打开电源）。首次使用时虚拟磁盘会进行初始化。新磁盘的大小决定了初始化需要花费多长时间。

STEP 2 | 配置每个磁盘。

以下示例使用 sdc 虚拟磁盘。

1. 登录到 Panorama 命令行界面。
2. 输入以下命令以查看 Panorama 虚拟设备上的磁盘：

   `show system disk details`

   用户将看到以下响应：

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

3. 输入以下命令并在提示输入所有磁盘时确认请求 `Reason：Admindisabled` 响应：

   `request system disk add sdc`

   `requestsystem disk add` 命令在“仅管理”模式下的 *Panorama* 管理服务器上不可用，因为此模式不支持日志记录。如果没有看到该命令，则在 Panorama 模式下设置 Panorama 虚拟设备以启用日志记录磁盘。一旦进入 *Panorama* 模式，请登录到 Panorama 命令行界面，并继续步骤 4 以验证磁盘添加状态。
4. 输入 **`show system disk details`** 命令以验证磁盘添加状态。继续执行步骤 3（当所有新添加的磁盘响应显示 `Reason：Adminenabled`。

STEP 3 | 让磁盘可用于日志记录。

1. 登录到 Panorama Web 界面。
2. 选择 **Panorama** > **Managed Collectors**（Panorama > 受管收集器），然后编辑日志收集器。
3. 选择 **Disks**（磁盘），并添加每个新添加的磁盘。
4. 单击 **OK**（确定）。
5. 选择 **Commit**（提交）> **Commit and Push**（提交并推送），并 **Commit and Push**（提交并推送）更改。

STEP 4 | 配置 Panorama 以接收日志。

此步骤适用于 Panorama 模式下的新 Panorama 部署。如果正在将日志记录磁盘添加到现有的 Panorama 虚拟设备，请继续步骤 5。

1. 配置受管收集器。

© 2019 Palo Alto Networks, Inc.

2. 配置收集器组。
3. 配置 Panorama 的日志转发。

STEP 5 | 验证 Panorama 日志存储容量是否已增加。

1. 登录到 Panorama Web 界面。
2. 选择 **Panorama** > **Collector Groups**（收集器组），然后选择 Panorama 虚拟设备所属的收集器组。
3. 验证 **Log Storage**（日志存储）容量是否准确显示磁盘容量。

向 *vCloud Air* 中的 *Panorama* 添加虚拟磁盘

您可以添加虚拟日志记录磁盘以扩展 Panorama™ 虚拟设备上的日志存储容量。如果设备处于 Panorama 模式，可以添加 1 至 12 个 2TB 虚拟日志记录磁盘或 1 个 24TB 日志记录磁盘，最大不超过 24TB。如果设备处于传统模式，则可以添加一个高达 8TB 的虚拟日志记录磁盘。

发生故障时，如果 *Panorama* 失去与新虚拟磁盘的连接，*Panorama* 可能会丢失日志。

如果有必要，您可以替换 vCloud Air 上的虚拟磁盘。

STEP 1 | 将额外磁盘添加到 Panorama。

在所有模式下，*Panorama VM* 上的第一个日志记录磁盘至少必须为 *2TB* 才能添加额外磁盘。如果第一个日志记录磁盘小于 *2TB*，则将无法添加额外磁盘空间。

1. 访问 vCloud Air Web 控制台，然后选择您的 **Virtual Private Cloud On Demand**（按需虚拟私有云）区域。
2. 在 **Virtual Machines**（虚拟机）选项卡中选择 Panorama 虚拟设备。
3. **Add another disk**（添加其他磁盘）（**Actions**（操作）> **Edit Resources**（编辑资源））。
4. 设置 **Storage**（存储）大小。如果 Panorama 虚拟设备处于 Panorama 模式，请将大小设置为至少 2TB。如果设备处于传统模式，则可以将大小设置为 8TB。

   在 *Panorama* 模式下，您可以添加大于 *2TB* 的磁盘大小，*Panorama* 将自动创建尽可能多的 *2TB* 分区。例如，如果磁盘 *sdc* 是 *24TB*，*Panorama* 将创建 *12* 个 *2TB* 分区。这些磁盘将被命名为 *sdc1 - sdc12*。
5. 将存储层设置为 **Standard**（标准）或 **SSD-Accelerated**（SSD-加速）。
6. 如果有必要，重复前面的步骤以将额外磁盘添加到 Panorama 虚拟设备。
7. **Save**（保持）更改。

STEP 2 | 配置每个磁盘。

以下示例使用 sdc 虚拟磁盘。

1. 登录到 Panorama 命令行界面。
2. 输入以下命令以查看 Panorama 虚拟设备上的磁盘：

   `show system disk details`

   用户将看到以下响应：

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


© 2019 Palo Alto Networks, Inc.

```
Size : 2048 MB
Status : Available
Reason : Admin disabled
```

3. 输入以下命令并在提示输入所有磁盘时确认请求 `Reason：Admindisabled` 响应：

   `request system disk add sdc`

   `request system disk add` 命令在“仅管理”模式下的 *Panorama* 管理服务器上不可用，因为此模式不支持日志记录。如果没有看到该命令，则在 Panorama 模式下设置 Panorama 虚拟设备以启用日志记录磁盘。一旦进入 *Panorama* 模式，请登录到 Panorama 命令行界面，并继续步骤 4 以验证磁盘添加状态。

4. 输入 **`show system disk details`** 命令以验证磁盘添加状态。当所有新添加的磁盘响应显示 `Reason：Adminenabled`。

STEP 3 | 让磁盘可用于日志记录。

1. 登录到 Panorama Web 界面。
2. 选择 **Panorama** > **Managed Collectors**（Panorama > 受管收集器），然后编辑日志收集器。
3. 选择 **Disks**（磁盘），**Add**（添加）每个新磁盘。
4. 单击 **OK**（确定）。
5. 选择 **Commit**（提交）> **Commit and Push**（提交并推送），并 **Commit and Push**（提交并推送）更改。

STEP 4 | 配置 Panorama 以接收日志。

此步骤适用于 Panorama 模式下的新 Panorama 部署。如果要将日志记录磁盘添加到现有的 Panorama 虚拟设备，请继续下一步。

1. 配置受管收集器。
2. 配置收集器组。
3. 配置 Panorama 的日志转发。

STEP 5 | 验证 Panorama 日志存储容量是否已增加。

1. 登录到 Panorama Web 界面。
2. 选择 **Panorama** > **Collector Groups**（收集器组），然后选择 Panorama 虚拟设备所属的收集器组。
3. 验证 **Log Storage**（日志存储）容量是否准确显示您的新磁盘容量。

向 *AWS* 中的 *Panorama* 添加虚拟磁盘

在 AWS 上安装 Panorama 或在 AWS GovCloud 上安装 Panorama后，添加虚拟日志记录磁盘到 Panorama™ 虚拟设备实例，以便为受管防火墙生成的日志提供存储空间。您可以将虚拟磁盘添加到 Panorama 模式下的 Panorama 虚拟设备的本地日志收集器中，也可以添加到专用日志收集器中。要添加虚拟磁盘，必须有权访问 Amazon Web Service 控制台、Panorama 命令行界面 (CLI) 以及 Panorama Web 界面。

AWS 上的 Panorama 虚拟设备仅支持 2TB 日志记录磁盘，最多支持共计 24TB 的日志存储。因为 Panorama 虚拟设备已将日志记录磁盘分成多个 2TB 分区，因此，您不能添加小于 2TB 的日志记录磁盘，也不能添加不能被 2TB 整除的日志记录磁盘。例如，如果想添加 4TB 的日志记录磁盘，Panorama 将创建 2 个 2TB 分区。但是，您不能添加 5TB 的日志记录磁盘，因为剩余的 1TB 无法作为一个分区。

STEP 1 | 登录到 AWS Web Service 控制台，然后选择 EC2 仪表盘。

- Amazon Web Service 控制台
- AWS GovCloud Web Service 控制台

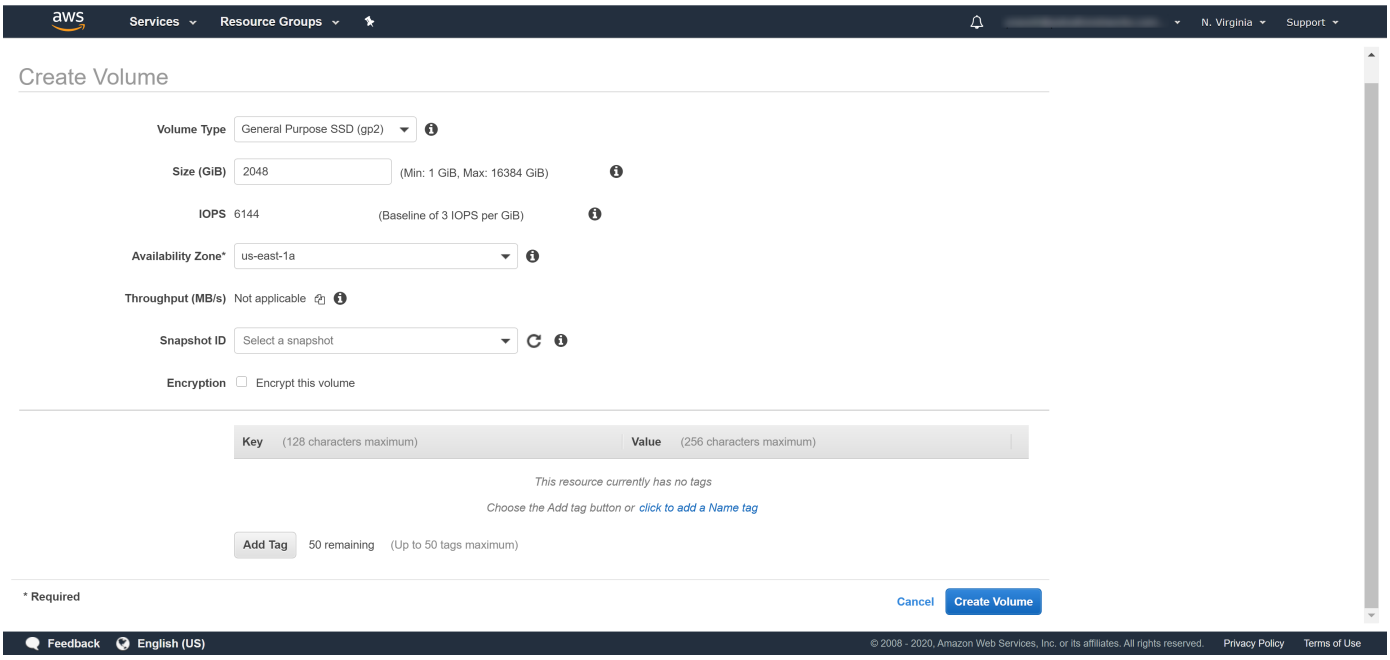
STEP 2 | 向 Panorama 添加虚拟日志记录磁盘。

1. 在 EC2 仪表盘上，选择 **Volumes**（卷）和 **Create Volume**（创建卷）：

© 2019 Palo Alto Networks, Inc.

- 选择您喜欢的卷类型。对于一般用途，请选择 **General Purpose SSD (GP2)**（通用 **SSD(GP2)**）。
- 将卷的 **Size**（大小）配置为 2048 GiB。
- 选择存放您的 Panorama 虚拟设备实例位置的相同可用性区域。
- （可选）解密卷。
- （可选）向卷添加标记。

2. 单击 **Create Volume**（创建卷）。



3. 在“卷”页面，选择您的卷，然后选择 **Actions**（操作）> **Attach Volume**（附加卷）。
4. 附加 Panorama 虚拟设备实例。

STEP 3 | 配置每个磁盘。

以下示例使用 sdc 虚拟磁盘。

1. 登录到 Panorama 命令行界面。
2. 输入以下命令以查看 Panorama 虚拟设备上的磁盘：

   `show system disk details`

   用户将看到以下响应：

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

3. 输入以下命令并在提示输入所有磁盘时确认请求 `Reason：Admindisabled` 响应：

   `request system disk add sdc`

© 2019 Palo Alto Networks, Inc.



requestsystem disk add 命令在“仅管理”模式下的 *Panorama* 管理服务器上不可用，因为此模式不支持日志记录。如果没有看到该命令，则在 Panorama 模式下设置 Panorama 虚拟设备以启用日志记录磁盘。一旦进入 *Panorama* 模式，请登录到 Panorama 命令行界面，并继续步骤 4 以验证磁盘添加状态。

4. 输入 **show system disk details** 命令以验证磁盘添加状态。当所有新添加的磁盘响应显示 `Reason：Adminenabled`。

STEP 4 | 让磁盘可用于日志记录。

1. 登录到 Panorama Web 界面。
2. 编辑日志收集器（**Panorama** > **Managed Collectors**（受管收集器））。
3. 选择 **Disks**（磁盘），并 **Add**（添加）每个新添加的磁盘。
4. 单击 **OK**（确定）。
5. 选择 **Commit**（提交）> **Commit and Push**（提交并推送），并 **Commit and Push**（提交并推送）更改。

STEP 5 | （仅限 Panorama 模式下的 Panorama 部署）配置 Panorama 以接收日志。

如果正在将日志记录磁盘添加到现有的 Panorama 虚拟设备，请跳至步骤 6。

1. 配置收集器组。
2. 配置 Panorama 的日志转发。

STEP 6 | 验证 Panorama 日志存储容量是否已增加。

1. 登录到 Panorama Web 界面。
2. 选择 Panorama 虚拟设备所属的收集器组（**Panorama** > **Collector Groups**（收集器组））。
3. 验证 **Log Storage**（日志存储）容量是否准确显示磁盘容量。

向 *Azure* 中的 *Panorama* 添加虚拟磁盘

在 Azure 上安装 Panorama 后，添加虚拟日志记录磁盘到 Panorama™ 虚拟设备实例，以便为受管防火墙生成的日志提供存储空间。您可以将虚拟磁盘添加到 Panorama 模式下的 Panorama 虚拟设备的本地日志收集器中，也可以添加到专用日志收集器中。要添加虚拟磁盘，必须有权访问 Microsoft Azure 门户、Panorama 命令行界面 (CLI) 以及 Panorama Web 界面。

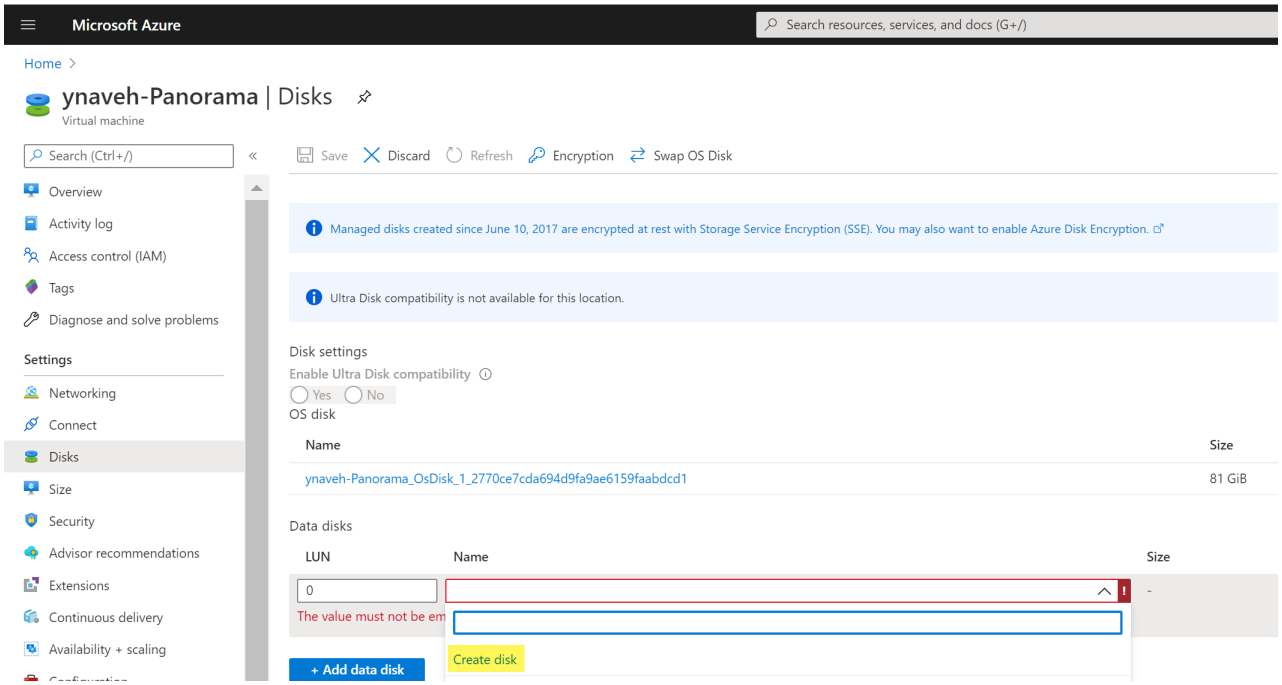
Azure 上的 Panorama 虚拟设备仅支持 2TB 日志记录磁盘，最多支持共计 24TB 的日志存储。因为 Panorama 虚拟设备已将日志记录磁盘分成多个 2TB 分区，因此，您不能添加小于 2TB 的日志记录磁盘，也不能添加不能被 2TB 整除的日志记录磁盘。例如，如果想添加 4TB 的日志记录磁盘，Panorama 将创建 2 个 2TB 分区。但是，您不能添加 5TB 的日志记录磁盘，因为剩余的 1TB 无法作为一个分区。

STEP 1 | 登录到Microsoft Azure 门户。

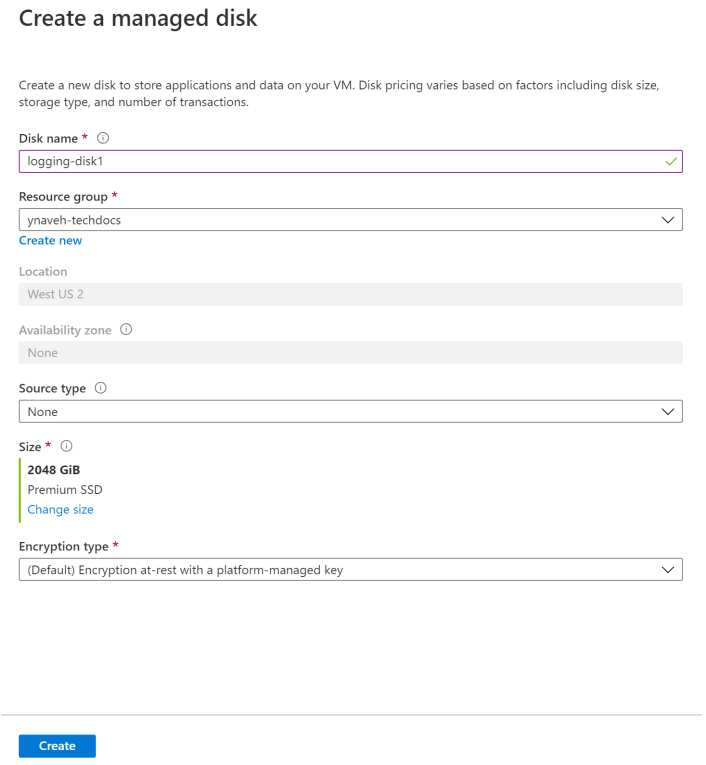
STEP 2 | 向 Panorama 添加虚拟日志记录磁盘。

1. 在 Azure 仪表盘上，选择想要添加日志记录磁盘的 Panorama **Virtual Machines**（虚拟机）。
2. 选择 **Disks**（磁盘）。
3. **+Add data disk**（+添加数据磁盘）。
4. 在新磁盘的下拉列表中**Create disk**（创建磁盘）。

© 2019 Palo Alto Networks, Inc.

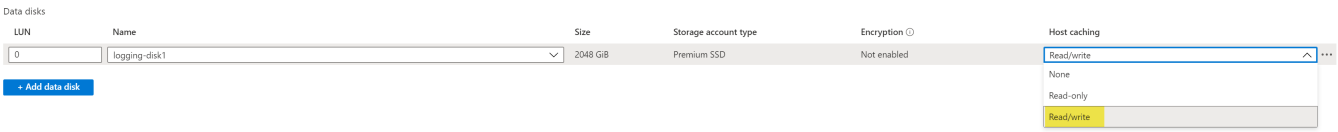


5. 配置日志记录磁盘。
    1. 输入磁盘 **Name**（名称）。
    2. 选择资源组。如果 **Create new**（创建新）资源组，请输入组名称。
    3. 验证 **Account type**（账户类型）（此字段自动填充）。
    4. 在 **Source type**（源类型）下拉列表中，选择 **None**（无）。
    5. 选择 **Change Size**（更改大小），然后选择 2048 GiB 日志记录磁盘。
    6. **Create**（创建）新日志记录磁盘。



© 2019 Palo Alto Networks, Inc.

7. 对于 **Host caching**（主机缓存），选择 **Read/write**（读取/写入）。



STEP 3 | 启用每个磁盘。

以下示例使用 sdc 虚拟磁盘。

1. 登录到 Panorama 命令行界面。
2. 输入以下命令以查看 Panorama 虚拟设备上的磁盘：

   `show system disk details`

   用户将看到以下响应：

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

3. 输入以下命令并在提示输入所有磁盘时确认请求 `Reason：Admindisabled` 响应：

   `request system disk add sdc`

   `requestsystem disk add` 命令在“仅管理”模式下的 *Panorama* 管理服务器上不可用，因为此模式不支持日志记录。如果没有看到该命令，则在 Panorama 模式下设置 Panorama 虚拟设备以启用日志记录磁盘。一旦进入 *Panorama* 模式，请登录到 Panorama 命令行界面，并继续步骤 4 以验证磁盘添加状态。

4. 输入 **`show system disk details`** 命令以验证磁盘添加状态。当所有新添加的磁盘响应显示 `Reason：Adminenabled`。

STEP 4 | 让磁盘可用于日志记录。

1. 登录到 Panorama Web 界面。
2. 编辑日志收集器（**Panorama** > **Managed Collectors**（受管收集器））。
3. 选择 **Disks**（磁盘），并 **Add**（添加）每个新添加的磁盘。
4. 单击 **OK**（确定）。
5. 选择 **Commit**（提交）> **Commit and Push**（提交并推送），并 **Commit and Push**（提交并推送）更改。

STEP 5 | （仅限 Panorama 模式下的 Panorama 部署）配置 Panorama 以接收日志。

如果正在将日志记录磁盘添加到现有的 Panorama 虚拟设备，请跳至步骤 6。

1. 配置收集器组。
2. 配置 Panorama 的日志转发。

STEP 6 | 验证 Panorama 日志存储容量是否已增加。

1. 登录到 Panorama Web 界面。

© 2019 Palo Alto Networks, Inc.

2. 选择 Panorama 虚拟设备所属的收集器组（**Panorama** > **Collector Groups**（收集器组））。
3. 验证 **Log Storage**（日志存储）容量是否准确显示磁盘容量。

向 *Google Cloud Platform* 中的 *Panorama* 添加虚拟磁盘

在 Google Cloud Platform 上安装 Panorama 后，添加虚拟日志记录磁盘到 Panorama™ 虚拟设备实例，以便为受管防火墙生成的日志提供存储空间。您可以将虚拟磁盘添加到 Panorama 模式下的 Panorama 虚拟设备的本地日志收集器中，也可以添加到专用日志收集器中。Google Cloud Platform 上的 Panorama 虚拟设备仅支持 2TB 日志记录磁盘，最多支持共计 24TB 的日志存储。因为 Panorama 虚拟设备已将日志记录磁盘分成多个 2TB 分区，因此，您不能添加小于 2TB 的日志记录磁盘，也不能添加不能被 2TB 整除的日志记录磁盘。例如，如果想添加 4TB 的日志记录磁盘，Panorama 将创建 2 个 2TB 分区。但是，您不能添加 5TB 的日志记录磁盘，因为剩余的 1TB 无法作为一个分区。

STEP 1 | 登录到 Google Cloud 控制台。

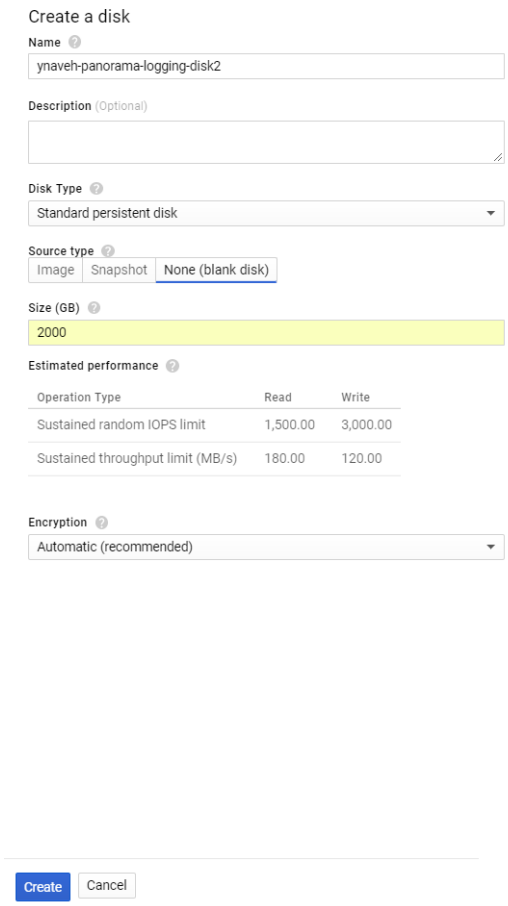
STEP 2 | 添加虚拟日志记录磁盘。

1. 在产品服务菜单中，选择并 **Edit**（编辑）Panorama 虚拟设备实例（**Compute Engine** > **VM Instances**（**VM** 实例））。
2. 在额外磁盘部分， **Add Item**（添加项目）。
3. **Create disk**（创建磁盘）（**Name**（名称）下拉列表）。

STEP 3 | 配置虚拟日志记录磁盘。

1. 输入**Name**（名称）。
2. 展开 **Disk Type**（磁盘类型）下拉菜单，然后选择所需类别。
3. 对于**Source type**（源类型），选择**None (empty disk)**（无（空磁盘））。
4. 设置虚拟日志记录磁盘的 **Size (GB)**（大小**(GB)**）。
5. 单击 **Create**（创建）。

© 2019 Palo Alto Networks, Inc.



6. **Save**（保存）更改以更新 Panorama 虚拟设备实例。

STEP 4 | 配置每个磁盘。

以下示例使用 sdc 虚拟磁盘。

1. 登录到 Panorama 命令行界面。
2. 输入以下命令以查看 Panorama 虚拟设备上的磁盘：

   `show system disk details`

   用户将看到以下响应：

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

3. 输入以下命令并在提示输入所有磁盘时确认请求 `Reason：Admin disabled` 响应：

   `request system disk add sdc`

© 2019 Palo Alto Networks, Inc.

request system disk add 命令在仅管理模式下的 *Panorama* 管理服务器上不可用，因为此模式不支持日志记录。如果没有看到该命令，则在 Panorama 模式下设置 Panorama 虚拟设备以启用日志记录磁盘。一旦进入 *Panorama* 模式，请登录到 Panorama 命令行界面，并继续步骤 4 以验证磁盘添加状态。

4. 输入 **show system disk details** 命令以验证磁盘添加状态。当所有新添加的磁盘响应显示 `Reason：Admin enabled` 时继续下一步。

STEP 5 | 让磁盘可用于日志记录。

1. 登录到 Panorama Web 界面。
2. 编辑日志收集器（**Panorama** > **Managed Collectors**（受管收集器））。
3. 选择 **Disks**（磁盘），并 **Add**（添加）每个新添加的磁盘。
4. 单击 **OK**（确定）。
5. 选择 **Commit**（提交）> **Commit and Push**（提交并推送），并 **Commit and Push**（提交并推送）更改。

STEP 6 | （仅限 Panorama 模式下的 Panorama 部署）配置 Panorama 以接收日志。

如果正在将日志记录磁盘添加到现有的 Panorama 虚拟设备，请跳至步骤 7。

1. 配置收集器组。
2. 配置 Panorama 的日志转发。

STEP 7 | 验证 Panorama 日志存储容量是否已增加。

1. 登录到 Panorama Web 界面。
2. 选择 Panorama 虚拟设备所属的收集器组（**Panorama** > **Collector Groups**（收集器组））。
3. 验证 **Log Storage**（日志存储）容量是否准确显示磁盘容量。

向 *KVM* 中的 *Panorama* 添加虚拟磁盘

在 KVM 上安装 Panorama 后，添加虚拟日志记录磁盘到 Panorama™ 虚拟设备实例，以便为受管防火墙生成的日志提供存储空间。您可以将虚拟磁盘添加到 Panorama 模式下的 Panorama 虚拟设备的本地日志收集器中，也可以添加到专用日志收集器中。KVM 上的 Panorama 虚拟设备仅支持 2TB 日志记录磁盘，最多支持共计 24TB 的日志存储。因为 Panorama 虚拟设备已将日志记录磁盘分成多个 2TB 分区，因此，您不能添加小于 2TB 的日志记录磁盘，也不能添加不能被 2TB 整除的日志记录磁盘。例如，如果想添加 4TB 的日志记录磁盘，Panorama 将创建 2 个 2TB 分区。但是，您不能添加 5TB 的日志记录磁盘，因为剩余的 1TB 无法作为一个分区。

STEP 1 | **Shutdown**（关闭）虚拟机管理器上 Panorama 虚拟设备实例。

STEP 2 | 双击虚拟机管理器上 Panorama 虚拟设备实例，并**Show virtual hardware details**（显示虚拟硬件详细信息）。

STEP 3 | 添加虚拟日志记录磁盘。根据需要多次重复此步骤。

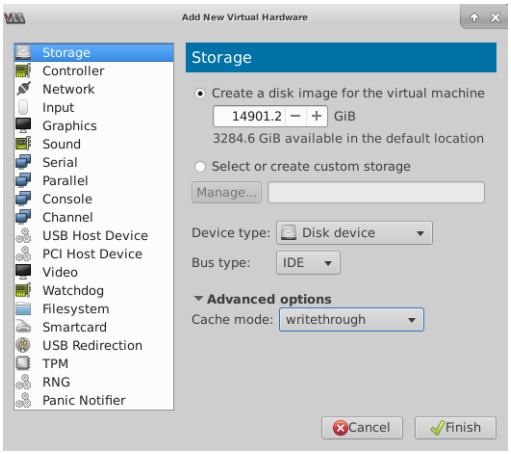
1. **Create a disk image for a virtual image**（为虚拟映像创建磁盘映像）（**Add Hardware**（添加硬件）> **Storage**（存储）），根据您的虚拟机管理器将虚拟磁盘存储容量配置为适当的 2TB 值：2000GB 或 14901.2GiB。

   某些虚拟机管理器使用 *GiB (gibibyte)* 来分配内存，这视版本而言。必须正确转换所需存储容量，避免配置虚拟日志记录磁盘，并发送 *Panorama* 虚拟设备至维护模式。

2. 在 **Device type**（设备类型）下拉列表中，选择 **Disk device**（磁盘设备）。
3. **Bus type**（总线类型）下拉列表中，根据您的配置选择 **VirtIO** 或 **IDE**。

© 2019 Palo Alto Networks, Inc.

4. 展开 **Advanced options**（高级选项），并在 **Cache mode**（缓存模式）下拉列表中选择 **writethrough**。
5. 单击 **Finish**（完成）。



STEP 4 | **Power on**（开启）Panorama 虚拟设备实例。

STEP 5 | 配置每个磁盘。

以下示例使用 sdc 虚拟磁盘。

1. 登录到 Panorama 命令行界面。
2. 输入以下命令以查看 Panorama 虚拟设备上的磁盘：

   `show system disk details`

   用户将看到以下响应：

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

3. 输入以下命令并在提示输入所有磁盘时确认请求 `Reason：Admin disabled` 响应：

   `request system disk add sdc`

   `request system disk add` 命令在仅管理模式下的 *Panorama* 管理服务器上不可用，因为此模式不支持日志记录。如果没有看到该命令，则在 Panorama 模式下设置 Panorama 虚拟设备以启用日志记录磁盘。一旦进入 *Panorama* 模式，请登录到 Panorama 命令行界面，并继续步骤 4 以验证磁盘添加状态。

4. 输入 **`show system disk details`** 命令以验证磁盘添加状态。当所有新添加的磁盘响应显示 `Reason：Admin enabled` 时继续下一步。

STEP 6 | 让磁盘可用于日志记录。

1. 登录到 Panorama Web 界面。
2. 编辑日志收集器（**Panorama** > **Managed Collectors**（受管收集器））。

© 2019 Palo Alto Networks, Inc.

3. 选择 **Disks**（磁盘），并 **Add**（添加）每个新添加的磁盘。
4. 单击 **OK**（确定）。
5. 选择 **Commit**（提交）> **Commit and Push**（提交并推送），并 **Commit and Push**（提交并推送）更改。

STEP 7 | （仅限 Panorama 模式下的 Panorama 部署）配置 Panorama 以接收日志。

如果正在将日志记录磁盘添加到现有的 Panorama 虚拟设备，请跳至步骤 8。

1. 配置收集器组。
2. 配置 Panorama 的日志转发。

STEP 8 | 验证 Panorama 日志存储容量是否已增加。

1. 登录到 Panorama Web 界面。
2. 选择 Panorama 虚拟设备所属的收集器组（**Panorama** > **Collector Groups**（收集器组））。
3. 验证 **Log Storage**（日志存储）容量是否准确显示磁盘容量。

向 *Hyper-V* 中的 *Panorama* 添加虚拟磁盘

在在 Hyper-V 上安装 Panorama后，添加虚拟日志记录磁盘到 Panorama™ 虚拟设备实例，以便为受管防火墙生成的日志提供存储空间。您可以将虚拟磁盘添加到 Panorama 模式下的 Panorama 虚拟设备的本地日志收集器中，也可以添加到专用日志收集器中。Hyper-V 上的 Panorama 虚拟设备仅支持 2TB 日志记录磁盘，最多支持共计 24TB 的日志存储。因为 Panorama 虚拟设备已将日志记录磁盘分成多个 2TB 分区，因此，您不能添加小于 2TB 的日志记录磁盘，也不能添加不能被 2TB 整除的日志记录磁盘。例如，如果想添加 4TB 的日志记录磁盘，Panorama 将创建 2 个 2TB 分区。但是，您不能添加 5TB 的日志记录磁盘，因为剩余的 1TB 无法作为一个分区。

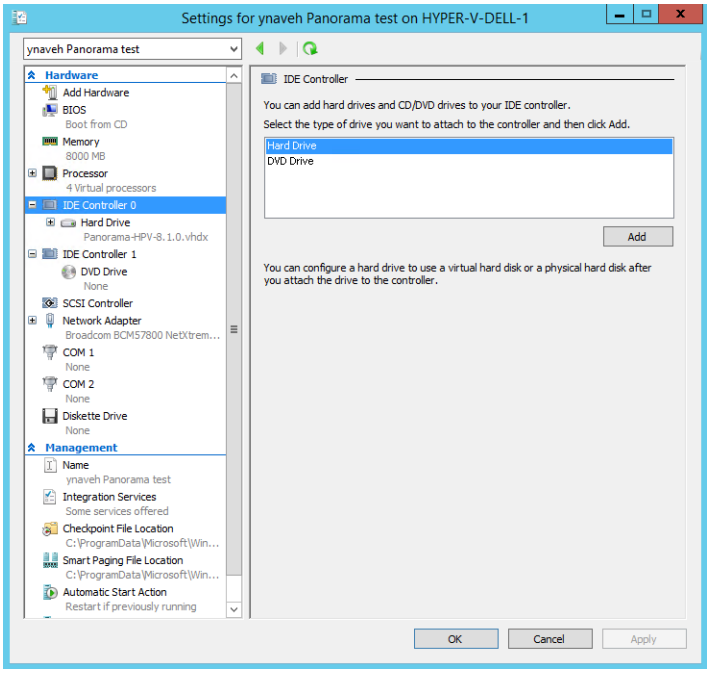
STEP 1 | 关闭 Panorama 虚拟设备。

1. 在 Hyper-V 管理器上，从 **Virtual Machines(虚拟机)**列表中选择 Panorama 虚拟设备实例。
2. 选择 **Action**（操作）> **Turn Off**（关闭）以关闭 Panorama 虚拟设备。

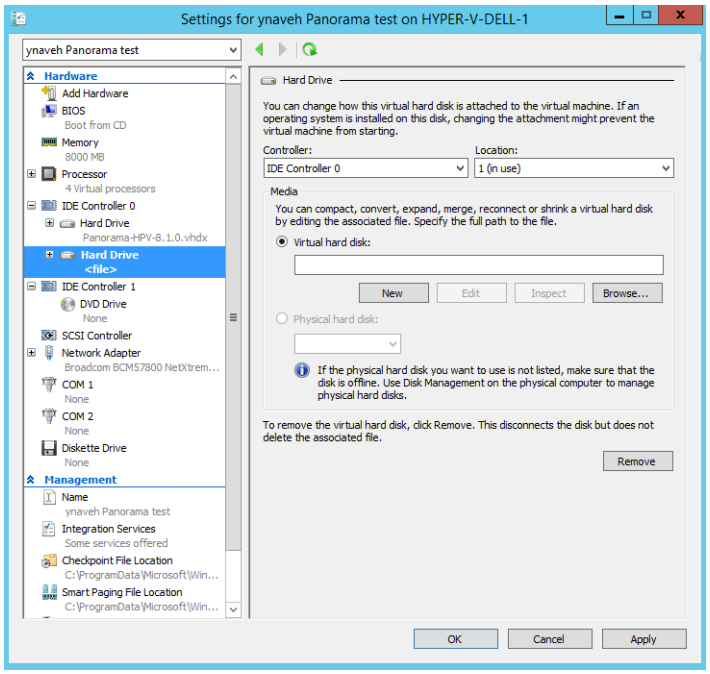
STEP 2 | 添加虚拟日志记录磁盘。根据需要多次重复此步骤。

1. 从 **Virtual Machines**（虚拟机）列表选择 Panorama 虚拟设备，然后选择 **Action**（操作）> **Settings**（设置）。
2. 在 **Hardware**（硬件）列表中选择 **IDE Controller 0**（**IDE** 控制器 **0**）。
3. 从 **IDE Controller**（**IDE** 控制器）驱动器列表中选择 **Hard Drive**（硬盘驱动器），然后 **Add**（添加）新的虚拟日志记录磁盘。

© 2019 Palo Alto Networks, Inc.



4. 选择在 **IDE Controller 0**（**IDE** 控制器 **0**）中创建的新 **Hard Drive**（硬盘驱动器）。
5. 在 **Media**（媒体）中添加 **New**（新）硬盘。

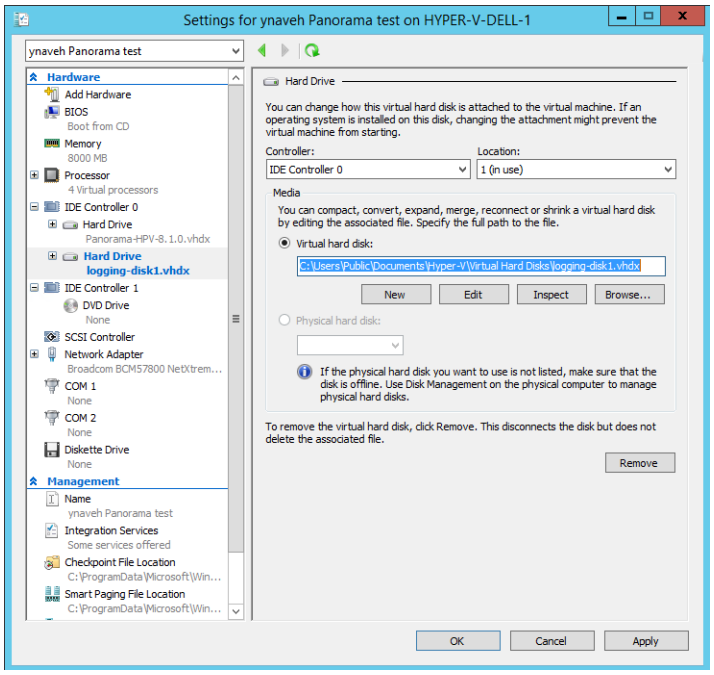


STEP 3 | 配置新的虚拟日志记录磁盘。

1. 如果看到“开始之前”提示，则单击 **Next**（下一步）以开始添加虚拟日志记录磁盘。
2. 对于磁盘格式，请选择 **VHDX**。单击 **Next**（下一步）以继续
3. 对于磁盘类型，根据需要选择 **Fixed Size**（固定大小）或 **Dynamically Expanding**（动态扩展）。单击 **Next**（下一步）以继续。
4. 指定虚拟日志记录磁盘文件的 **Name**（名称）和 **Location**（位置）。单击 **Next**（下一步）以继续。
5. 要配置磁盘，请选择 **Create a new virtual hard disk**（创建新虚拟硬盘），然后输入磁盘大小。单击 **Next**（下一步）以继续。

© 2019 Palo Alto Networks, Inc.

6. 查看摘要，**Finish**（完成）添加虚拟硬盘日志记录。
7. **Apply**（应用）新硬盘添加。



STEP 4 | 开启 Panorama 虚拟设备。

1. 从 **Virtual Machines(虚拟机)**列表中选择 Panorama 虚拟设备实例。
2. 选择 **Action**（操作）> **Start**（开始）以启动 Panorama 虚拟设备。

STEP 5 | 配置每个磁盘。

以下示例使用 sdc 虚拟磁盘。

1. 登录到 Panorama 命令行界面。
2. 输入以下命令以查看 Panorama 虚拟设备上的磁盘：

   `show system disk details`

   用户将看到以下响应：

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

3. 输入以下命令并在提示输入所有磁盘时确认请求 `Reason：Admin disabled` 响应：

   `request system disk add sdc`

   `request system disk add` 命令在仅管理模式下的 *Panorama* 管理服务器上不可用，因为此模式不支持日志记录。如果没有看到该命令，则在 Panorama 模式下设

© 2019 Palo Alto Networks, Inc.

置 Panorama 虚拟设备以启用日志记录磁盘。一旦进入 *Panorama* 模式，请登录到 Panorama 命令行界面，并继续步骤 4 以验证磁盘添加状态。

4. 输入 **`show system disk details`** 命令以验证磁盘添加状态。当所有新添加的磁盘响应显示 `Reason：Admin enabled` 时继续下一步。

STEP 6 | 让磁盘可用于日志记录。

1. 登录到 Panorama Web 界面。
2. 编辑日志收集器（**Panorama** > **Managed Collectors**（受管收集器））。
3. 选择 **Disks**（磁盘），并 **Add**（添加）每个新添加的磁盘。
4. 单击 **OK**（确定）。
5. 选择 **Commit**（提交）> **Commit and Push**（提交并推送），并 **Commit and Push**（提交并推送）更改。

STEP 7 | （仅限 Panorama 模式下的 Panorama 部署）配置 Panorama 以接收日志。

如果正在将日志记录磁盘添加到现有的 Panorama 虚拟设备，请跳至步骤 8。

1. 配置收集器组。
2. 配置 Panorama 的日志转发。

STEP 8 | 验证 Panorama 日志存储容量是否已增加。

1. 登录到 Panorama Web 界面。
2. 选择 Panorama 虚拟设备所属的收集器组（**Panorama** > **Collector Groups**（收集器组））。
3. 验证 **Log Storage**（日志存储）容量是否准确显示磁盘容量。

将 *Panorama ESXi* 服务器安装到 *NFS* 数据存储

当传统模式下的 Panorama 虚拟设备在 ESXi 服务器上运行时，将它安装到网络文件系统 (NFS) 数据存储既可提供将日志写入集中位置的功能，又可扩大超出虚拟磁盘支持的日志存储容量。（ESXi 5.5 及更高版本可支持容量达 8TB 的虚拟磁盘。更低版本的 ESXi 可支持容量达 2TB 的虚拟磁盘。）在 Panorama 高可用性 (HA) 配置中设置 NFS 数据存储之前，请参阅Panorama 高可用性的日志记录注意事项。

Panorama 模式下的 *Panorama* 虚拟设备不支持 *NFS*。

STEP 1 | 选择 **Panorama** > **Setup** > **Operations**（Panorama > 设置 > 操作），然后在“Miscellaneous（其他）”部分中单击 **Storage Partition Setup**（存储分区设置）。

STEP 2 | 将 **Storage Partition**（存储分区）类型设置为 **NFS V3**。

STEP 3 | 输入 NFS **Server**（服务器）的 IP 地址。

STEP 4 | 输入用于存储日志文件的 **Log Directory**（日志目录）路径。例如 export/panorama。

STEP 5 | 对于 **Protocol**（协议），选择 **TCP** 或 **UDP**，然后输入用于访问 NFS 服务器的 **Port**（端口）。

要通过 *TCP* 使用 *NFS*，则 *NFS* 服务器必须支持 *TCP*。常见的 *NFS* 端口为 *UDP/TCP 111*（对于 *RPC*）和 *UDP/TCP 2049*（对于 *NFS*）。

STEP 6 | 对于 NFS 的最佳性能，在 **Read Size**（读取大小）和 **Write Size**（写入大小）字段中，指定客户端和服务器之间来回传递的数据块的最大大小。定义读取/写入大小，优化在 Panorama 和 NFS 数据存储之间传输数据的数据量和速度。

© 2019 Palo Alto Networks, Inc.

STEP 7 | （可选）选择 **Copy On Setup**（设置时复制）以将存储在 Panorama 上的现有日志复制到 NFS 卷。如果 Panorama 拥有许多日志，则此选项可能会启动对大量数据的转移。

STEP 8 | 单击 **Test Logging Partition**（测试日志记录分区）以验证 Panorama 可以访问 NFS **Server**（服务器）和 **Log Directory**（日志目录）。

STEP 9 | 单击 **OK**（确定）保存更改。

STEP 10 | 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。在您重新启动之前，Panorama 虚拟设备会一直将日志写入本地存储磁盘。

STEP 11 | 选择 **Panorama** > **Setup** > **Operations**（Panorama > 设置 > 操作），然后在“Device Operations（设备操作）”部分中选择 **Reboot Panorama**（重新启动 Panorama）。重新启动之后，Panorama 将开始向 NFS 数据存储写入日志。

增加 Panorama 虚拟设备上的 CPU 和内存

当您执行 Panorama 虚拟设备的初始配置时，可以根据设备处于 Panorama 模式还是仅管理模式并根据日志存储容量或受管防火墙数量来指定内存和 CPU 数量。如果稍后添加存储容量或受管防火墙，则还必须增加内存和 CPU。日志收集器模式下的 Panorama 虚拟设备必须满足系统要求，不需要将 CPU 和内存增加到超过最低要求。查看设置 Panorama 虚拟设备的前提条件了解每个 Panorama 模式的 CPU 和内存要求。

- 增加 ESXi 服务器上的 Panorama 的 CPU 和内存
- 增加 vCloud Air 上的 Panorama 的 CPU 和内存
- 增加 AWS 上的 Panorama 的 CPU 和内存
- 增加 Azure 上的 Panorama 的 CPU 和内存
- 增加 Google Cloud Platform 上的 Panorama 的 CPU 和内存
- 增加 KVM 上的 Panorama 的 CPU 和内存
- 增加 Hyper-V 上的 Panorama 的 CPU 和内存

增加 *ESXi* 服务器上的 *Panorama* 的 *CPU* 和内存

有关 Panorama 要求的最低 CPU 和内存，请参阅增加 Panorama 虚拟设备上的 CPU 和内存。

STEP 1 | 访问 VMware vSphere Client，然后选择 **Virtual Machines**（虚拟机）。

STEP 2 | 右击 Panorama 虚拟设备，然后选择 **Power**（电源）> **Power Off**（关闭电源）。

STEP 3 | 右击 Panorama 虚拟设备，然后选择 **Edit Settings**（编辑设置）。

STEP 4 | 选择 **Memory**（内存）并输入新的 **Memory Size**（内存大小）。

STEP 5 | 选择 **CPU**，并指定 CPU 数量（**Number of virtual sockets**（虚拟插槽数量）乘以 **Number of cores per socket**（每个插槽的内核数量））。

STEP 6 | 单击 **OK**（确定）保存更改。

STEP 7 | 右击 Panorama 虚拟设备，然后选择 **Power**（电源）> **Power On**（打开电源）。

增加 *vCloud Air* 上的 *Panorama* 的 *CPU* 和内存

有关 Panorama 要求的最低 CPU 和内存，请参阅增加 Panorama 虚拟设备上的 CPU 和内存。

© 2019 Palo Alto Networks, Inc.

STEP 1 | 访问 vCloud Air Web 控制台，然后选择您的 **Virtual Private Cloud OnDemand**（按需虚拟私有云）区域。

STEP 2 | 在 **Virtual Machines**（虚拟机）选项卡中，选择 Panorama 虚拟机和 **Power Off**（关闭电源）。

STEP 3 | 选择 **Actions** > **Edit Resources**（操作 > 编辑资源）。

STEP 4 | 设置 **CPU** 和 **Memory**（内存）。

STEP 5 | **Save**（保持）更改。

STEP 6 | 选择 Panorama 虚拟机，然后选择 **Power On**（打开电源）。

增加 *AWS* 上的 *Panorama* 的 *CPU* 和内存

对于 Panorama™ 要求的最小 CPU 和内存，请参阅增加 Panorama 虚拟设备上的 CPU 和内存。

如果在部署虚拟机后调整其大小，则日志收集器模式下的 *Panorama* 虚拟设备可能不会保留在日志收集器模式下，从而导致日志数据丢失。

STEP 1 | 登录到 AWS Web Service 控制台，然后选择 EC2 仪表盘。

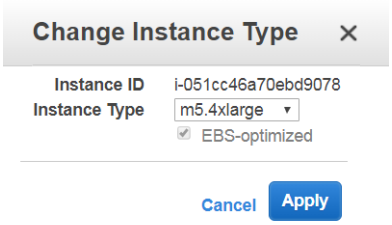
- Amazon Web Service 控制台
- AWS GovCloud Web Service 控制台

STEP 2 | 在 EC2 仪表盘上，选择 **Instances**（实例），然后选择 Panorama 虚拟设备实例。

STEP 3 | 选择 **Actions**（操作）> **Instance State**（实例状态）> **Stop**（停止）以关闭 Panorama 虚拟设备实例。

STEP 4 | 选择 **Actions**（操作）> **Instance Settings**（实例设置）> **Change Instance Type**（更改实例类型）以更改 Panorama 虚拟设备实例类型。

STEP 5 | 选择您想升级的 **Instance Type**（实例类型），然后 **Apply**（应用）。



STEP 6 | 选择 **Actions**（操作）> **Instance State**（实例状态）> **Start**（开始）以打开 Panorama 虚拟设备实例。

增加 *Azure* 上的 *Panorama* 的 *CPU* 和内存

对于 Panorama™ 要求的最小 CPU 和内存，请参阅增加 Panorama 虚拟设备上的 CPU 和内存。

如果在部署虚拟机后调整其大小，则日志收集器模式下的 *Panorama* 虚拟设备可能不会保留在日志收集器模式下，从而导致日志数据丢失。

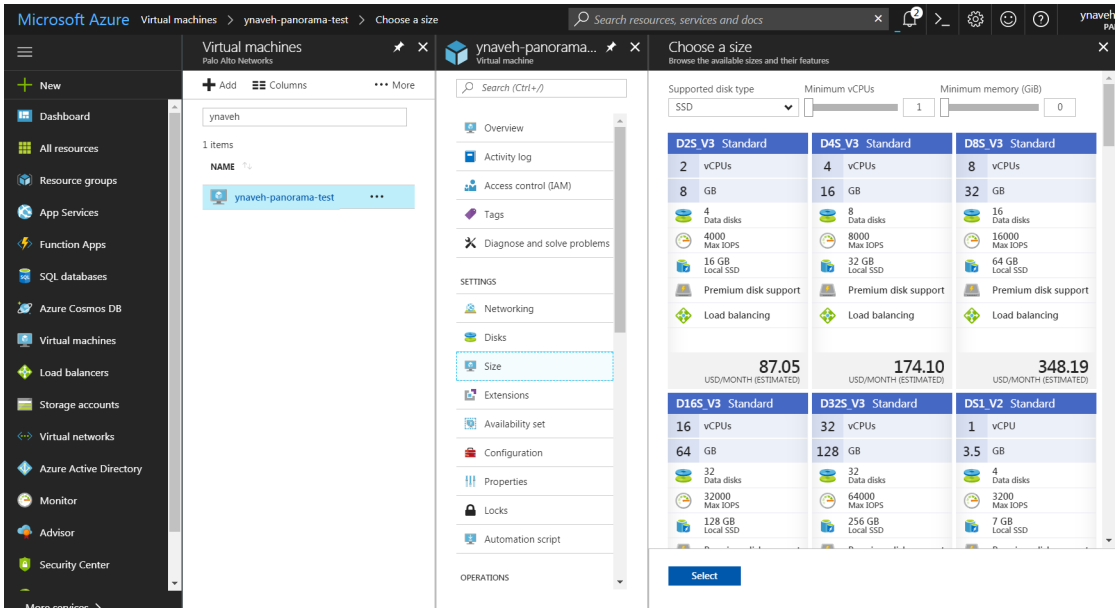
STEP 1 | 登录到Microsoft Azure 门户。

© 2019 Palo Alto Networks, Inc.

STEP 2 | 在 Azure 仪表盘上，从 **Virtual machines**（虚拟机）部分选择 Panorama 虚拟设备。

STEP 3 | 选择 **Overview**（概述），然后 **Stop**（停止）Panorama 虚拟设备。

STEP 4 | 选择新虚拟机的 **Size**（大小），然后 **Select**（选择）。



STEP 5 | 选择 **Overview**（概述），然后 **Start**（开始）Panorama 虚拟设备。

增加 *Google Cloud Platform* 上的 *Panorama* 的 *CPU* 和内存

对于 Panorama™ 要求的最小 CPU 和内存，请参阅增加 Panorama 虚拟设备上的 CPU 和内存。

如果在部署虚拟机后调整其大小，则日志收集器模式下的 *Panorama* 虚拟设备可能不会保留在日志收集器模式下，从而导致日志数据丢失。

STEP 1 | 登录到 Google Cloud 控制台。

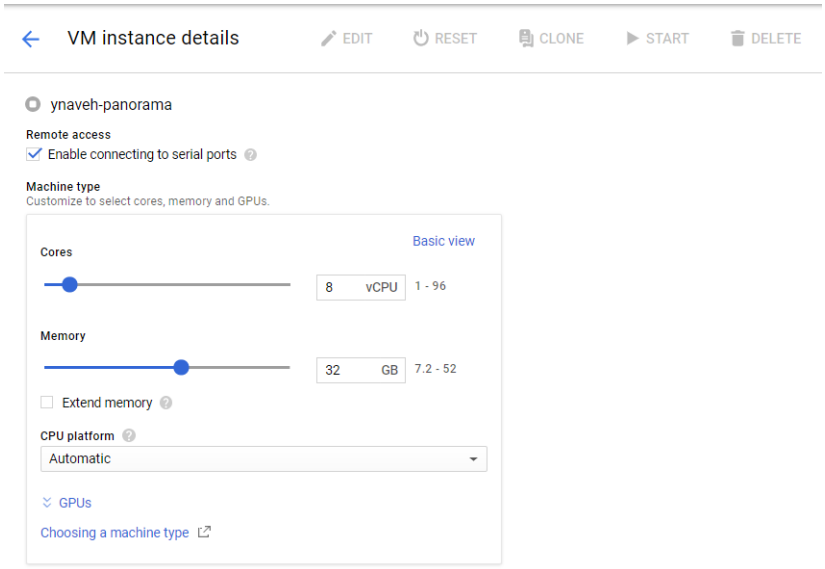
STEP 2 | 停止 Panorama 虚拟设备实例。

1. 在产品服务菜单选择 Panorama 虚拟设备实例（**Compute Engine** > **VM Instances**（**VM** 实例））。
2. **Stop**（停止）Panorama 虚拟设备实例。可能需要 2-3 分钟的时间来完全关闭 Panorama 虚拟设备。

STEP 3 | 重新配置 Panorama 虚拟设备实例。

1. **Edit**（编辑）Panorama 虚拟设备实例详细信息。
2. 在机器类型下，**Customize**（自定义）Panorama 虚拟设备的 CPU 内核和内存。

© 2019 Palo Alto Networks, Inc.



STEP 4 | **Save**（保存）更改以更新 Panorama 虚拟设备实例。

STEP 5 | **Start**（启动） Panorama 虚拟设备。

增加 *KVM* 上的 *Panorama* 的 *CPU* 和内存

对于 Panorama™ 要求的最小 CPU 和内存，请参阅增加 Panorama 虚拟设备上的 CPU 和内存。

如果在部署虚拟机后调整其大小，则日志收集器模式下的 *Panorama* 虚拟设备可能不会保留在日志收集器模式下，从而导致日志数据丢失。

STEP 1 | **Shutdown**（关闭） 虚拟机管理器上 Panorama 虚拟设备实例。

STEP 2 | 双击虚拟机管理器上 Panorama 虚拟设备实例，并**Show virtual hardware details**（显示虚拟硬件详细信息）。

STEP 3 | 编辑已分配的 Panorama 虚拟设备 CPU 内核。

1. 编辑当前已分配的 **CPU**。
2. **Apply**（应用） 重新配置的 CPU 内核分配。

STEP 4 | 编辑已分配的 Panorama 虚拟设备内存。

1. 编辑当前已分配的 **Memory**（内存）。
2. **Apply**（应用） 重新配置的内存分配。

STEP 5 | **Power on**（开启） Panorama 虚拟设备实例。

增加 *Hyper-V* 上的 *Panorama* 的 *CPU* 和内存

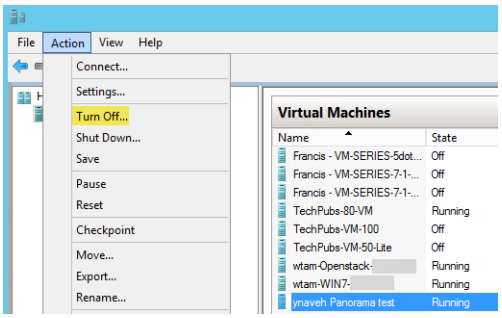
对于 Panorama™ 要求的最小 CPU 和内存，请参阅增加 Panorama 虚拟设备上的 CPU 和内存。

如果在部署虚拟机后调整其大小，则日志收集器模式下的 *Panorama* 虚拟设备可能不会保留在日志收集器模式下，从而导致日志数据丢失。

STEP 1 | 关闭 Panorama 虚拟设备。

© 2019 Palo Alto Networks, Inc.

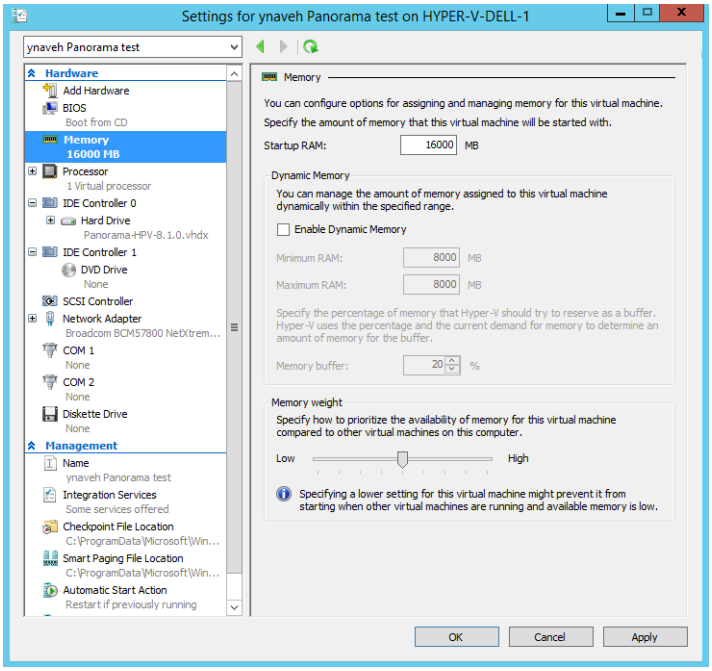
1. 在 Hyper-V 管理器上，从 **Virtual Machines(虚拟机)**列表中选择 Panorama 虚拟设备实例。
2. 选择 **Action**（操作）> **Turn Off**（关闭）以关闭 Panorama 虚拟设备。



STEP 2 | 在Hyper-V 管理器上，从 **Virtual Machines**（虚拟机）列表中选择 Panorama 虚拟设备实例，然后选择 **Action**（操作）> **Settings**（设置）以编辑 Panorama 虚拟设备资源。

STEP 3 | 编辑已分配的 Panorama 虚拟设备内存。

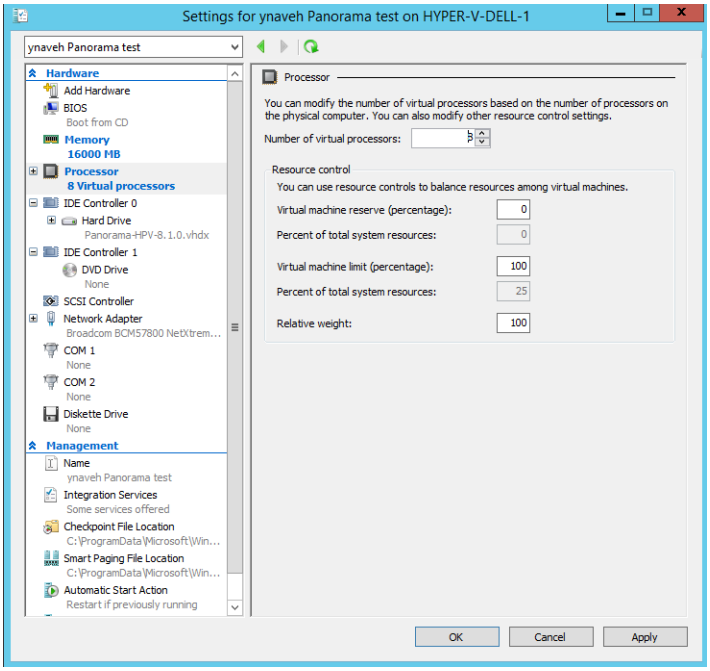
1. 在 **Hardware**（硬件）列表中，选择 **Memory**（内存）。
2. 编辑当前已分配的 **Startup RAM**（启动 **RAM**）。



STEP 4 | 编辑已分配的 Panorama 虚拟设备 CPU 内核。

1. 在 **Hardware**（硬件）列表中，选择 **Processor**（处理器）。
2. 编辑当前已分配的 **Number of virtual processors**（虚拟处理器数量）。

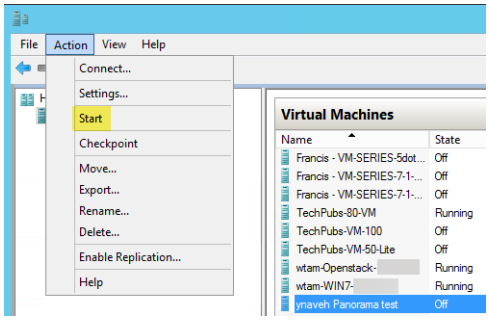
© 2019 Palo Alto Networks, Inc.



STEP 5 | **Apply**（应用）重新分配的内存和 CPU 内核。

STEP 6 | 开启 Panorama 虚拟设备。

1. 从 **Virtual Machines(虚拟机)**列表中选择 Panorama 虚拟设备实例。
2. 选择 **Action**（操作）> **Start**（开始）以启动 Panorama 虚拟设备。



增加 Panorama 虚拟设备上的系统磁盘

当您管理大规模防火墙部署时，将 Panorama 虚拟设备的系统磁盘容量扩展到 224GB 以支持大型数据集，从而为动态更新等活动提供充足磁盘空间。此外，如果您打算在 Panorama 模式下使用 Panorama 虚拟设备来管理 SD-WAN 部署，则 224GB 系统磁盘可扩展存储空间来监控和报告受管防火墙运行状况数据

- 增加 ESXi 服务器上 Panorama 的系统磁盘
- 增加 Google 云平台上 Panorama 的系统磁盘

增加 *ESXi* 服务器上 *Panorama* 的系统磁盘

添加 224GB 系统磁盘以替换默认的 81GB 系统磁盘。对于 Panorama 虚拟设备的最低资源要求，请参阅设置 Panorama 虚拟设备的前提条件。

不支持将 *Panorama* 虚拟设备系统磁盘减少至 *81GB*。

© 2019 Palo Alto Networks, Inc.

STEP 1 | （最佳实践）保存并导出 Panorama 和防火墙配置。

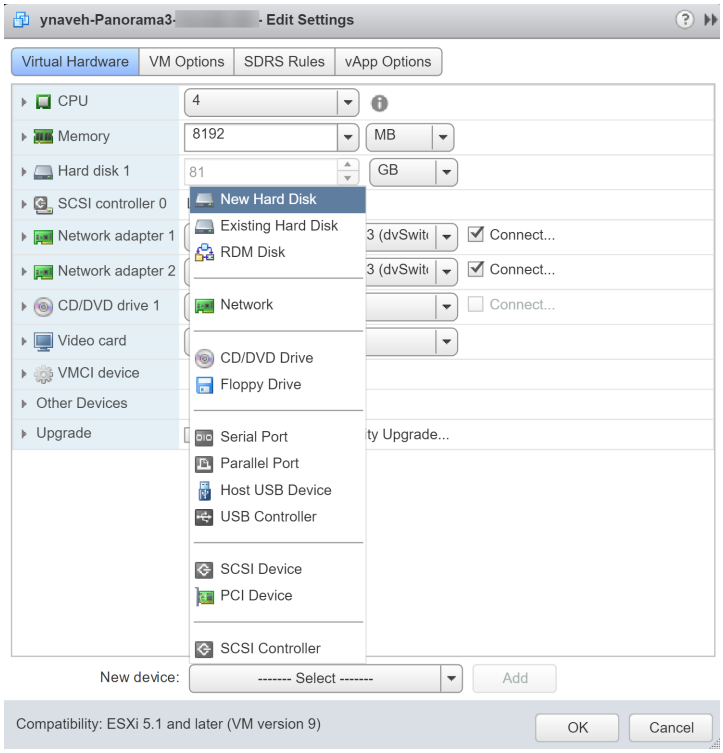
保存并导出您的 Panorama 和防火墙配置，以确保在出现任何问题时可以恢复 Panorama。

STEP 2 | 访问 VMware vSphere Client 并导航至您的 Panorama 虚拟设备。

STEP 3 | 右击 Panorama 虚拟设备，然后选择 **Power**（电源）> **Power Off**（关闭电源）。

STEP 4 | 添加新的 224GB 系统磁盘。

1. 右击 Panorama 虚拟设备，然后选择 **Edit Settings**（编辑设置）。
2. 选择 **New Hard Disk**（新硬盘）作为 **New Device**（新设备），并 **Add**（添加）该新设备。
3. 配置 224GB 新硬盘并单击 **OK**（确定）。



STEP 5 | 右击 Panorama 虚拟设备，然后选择 **Power**（电源）> **Power On**（打开电源）。

Panorama 可能需要 *30* 分钟来初始化新系统磁盘。在此期间，*Panorama Web* 界面和 *CLI* 不可用。

STEP 6 | 将磁盘数据从旧系统磁盘迁移到新系统磁盘。

在本示例中，我们要迁移到新添加的标记为 sdb 的系统磁盘。

1. 登录到 Panorama 命令行界面。
2. 输入以下命令以查看可用于迁移的系统磁盘：

```
admin> request system clone-system-disk target ?
```

3. 使用以下命令将磁盘数据迁移到新系统磁盘：

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


© 2019 Palo Alto Networks, Inc.

当提示开始磁盘迁移时，输入 **y**。

如要开始迁移，*Panorama* 将重启，至少需要 *20* 分钟才能完成磁盘迁移。在此期间，*Panorama Web* 界面和 *CLI* 不可用。

4. 通过 Web 控制台监控磁盘迁移。Panorama 显示以下消息，表明磁盘迁移已完成，然后才能继续下一步。

```
==================================
Disk Cloning Utility (Version 1.0)
==================================
SOURCE - Disk sda (82944 MB)
TARGET - Disk sdb (229376 MB)

Gathering disks info
Finished gathering disks info

Preparing disks
Finished preparing disks

Copying data
Finished copying data

Making disk bootable
Finished making disk bootable

Disk cloning procedure completed. Please shutdown the sytem and switch disks..._
```

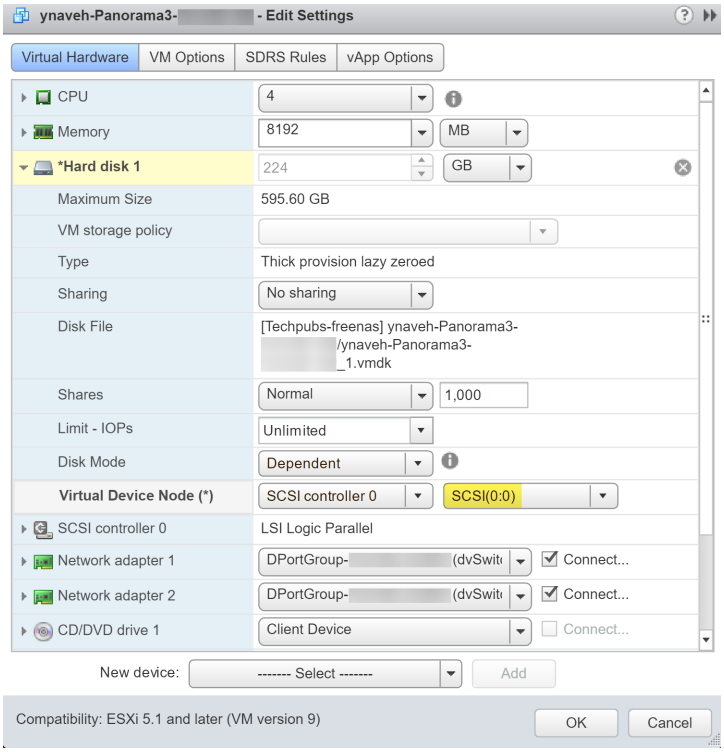
STEP 7 | 删除旧系统磁盘。

1. 访问 VMware vSphere Client 并导航至您的 Panorama 虚拟设备。
2. 右击 Panorama 虚拟设备，然后选择 **Power**（电源）> **Power Off**（关闭电源）。
3. 右击 Panorama 虚拟设备，然后选择 **Edit Settings**（编辑设置）。
4. 删除旧的 81GB 系统磁盘并单击 **OK**（确定）。

STEP 8 | 修改新系统磁盘的虚拟设备节点。

1. 展开新系统磁盘的设置选项。
2. 选择 **SCSI(0:0)** 作为 **Virtual Device Node**（虚拟设备节点）。
3. 单击 **OK**（确定）保存您的配置更改。

© 2019 Palo Alto Networks, Inc.



STEP 9 | 右击 Panorama 虚拟设备，然后选择 **Power**（电源）> **Power On**（打开电源）。

STEP 10 | 验证您是否成功迁移至新系统磁盘。

1. 登录到 Panorama 命令行界面。
2. 输入以下命令以查看系统磁盘分区。

   您必须添加 `/dev/root`、`/dev/sda5`、`/dev/sda6` 和 `/dev/sda8` 分区以确认磁盘大小已增加。

```
admin> show system disk-space
```

```
admin@Panorama-Ynaveh> show system disk-space

Filesystem      Size  Used Avail Use% Mounted on
/dev/root        16G  3.4G   12G  23% /
none            4.0G   60K  4.0G   1% /dev
/dev/sda5        76G  1.8G   71G   3% /opt/pancfg
/dev/sda6        23G  5.0G   17G  24% /opt/panrepo
tmpfs           4.0G  110M  3.8G   3% /dev/shm
cgroup_root     4.0G     0  4.0G   0% /cgroup
/dev/sda8        92G   52G   35G  60% /opt/panlogs
/dev/loop0       50G  7.4G   40G  16% /opt/mongobuffer
tmpfs            12M     0   12M   0% /opt/pancfg/mgmt/ssl/private
```

增加 *Google* 云平台上 *Panorama* 的系统磁盘

添加 224GB 系统磁盘以替换默认的 81GB 系统磁盘。对于 Panorama 虚拟设备的最低资源要求，请参阅设置 Panorama 虚拟设备的前提条件。

STEP 1 | （最佳实践）保存并导出 Panorama 和防火墙配置。

保存并导出您的 Panorama 和防火墙配置，以确保在出现任何问题时可以恢复 Panorama。

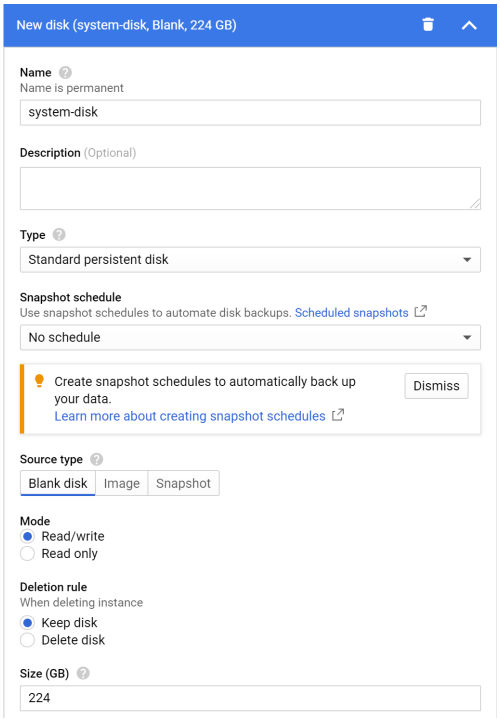
STEP 2 | 登录到 Google Cloud 控制台。

© 2019 Palo Alto Networks, Inc.

STEP 3 | 在 **VM Instances**（**VM** 实例）中，**Stop**（停止）Panorama VM 实例。

STEP 4 | 添加新的 224GB 系统磁盘。

1. 选择 Panorama VM 实例，然后选择 **Edit**（编辑）。
2. 在 **Additional disks**（额外磁盘）部分，**Add new disk**（添加新磁盘）。
3. 配置 224GB 新磁盘并单击 **OK**（确定）。



STEP 5 | 在 **VM Instances**（**VM** 实例）中，**Start**（开始）Panorama VM 实例。

STEP 6 | 将磁盘数据从旧系统磁盘迁移到新系统磁盘。

在本示例中，我们要迁移到新添加的标记为 sdb 的系统磁盘。

1. 登录到 Panorama 命令行界面。
2. 输入以下命令以查看可用于迁移的系统磁盘：

```
admin> request system clone-system-disk target ?
```

3. 使用以下命令将磁盘数据迁移到新系统磁盘：

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

当提示开始磁盘迁移时，输入 **Y**。

如要开始迁移，*Panorama* 将重启，至少需要 *20* 分钟才能完成磁盘迁移。在此期间，*Panorama Web* 界面和 *CLI* 不可用。

4. 通过尝试登录到 Panorama CLI 来监控磁盘迁移。在系统磁盘完成迁移后，Panorama 管理服务器处于维护模式，在维护模式下可以登录到 Panorama CLI。

STEP 7 | 附加新的 224GB 系统磁盘。

1. 在 **VM Instances**（**VM** 实例）中，**Stop**（停止）Panorama VM 实例。

© 2019 Palo Alto Networks, Inc.

2. 选择 Panorama VM 实例，然后选择 **Edit**（编辑）。
3. 在 **Additional disks**（额外磁盘）部分，分离新的 224GB 系统磁盘。
4. 在 **Boot Disk**（启动盘）部分，分离旧的 81GB 系统磁盘。
5. 在 **Boot Disk**（启动盘）部分，**Add item**（添加项）并选择新的 224GB 系统磁盘。
6. **Save**（保存）您的配置更改。

STEP 8 | 在 **VM Instances**（**VM** 实例）中，**Start**（开始）Panorama VM 实例。

STEP 9 | 验证您是否成功迁移至新系统磁盘。

1. 登录到 Panorama 命令行界面。
2. 输入以下命令以查看系统磁盘分区。

   您必须添加 `/dev/root`、`/dev/sda5`、`/dev/sda6` 和 `/dev/sda8` 分区以确认磁盘大小已增加。

```
admin> show system disk-space
```

```
admin@Panorama-Ynaveh> show system disk-space

Filesystem      Size  Used Avail Use% Mounted on
/dev/root        16G  3.4G   12G  23% /
none            4.0G   60K  4.0G   1% /dev
/dev/sda5        76G  1.8G   71G   3% /opt/pancfg
/dev/sda6        23G  5.0G   17G  24% /opt/panrepo
tmpfs           4.0G  110M  3.8G   3% /dev/shm
cgroup_root     4.0G     0  4.0G   0% /cgroup
/dev/sda8        92G   52G   35G  60% /opt/panlogs
/dev/loop0       50G  7.4G   40G  16% /opt/mongobuffer
tmpfs            12M     0   12M   0% /opt/pancfg/mgmt/ssl/private
```

完成 Panorama 虚拟设备设置

在执行 Panorama 虚拟设备的初始配置后，继续执行以下任务以进行其他配置：

- 激活 Panorama 支持许可证
- 在 Panorama 虚拟设备连接到互联网时激活/检索防火墙管理许可证
- 安装 Panorama 的内容和软件更新
- 访问和导航 Panorama 管理界面
- 设置 Panorama 的管理访问权限
- 管理防火墙

© 2019 Palo Alto Networks, Inc.

设置 M 系列设备

M-600、M-500 和 M-200 设备是您可以在仅管理模式（可作为不带本地日志收集功能的 Panorama 管理服务器）、Panorama 模式（可作为带本地日志收集功能的 Panorama 管理服务器）或日志收集器模式（可作为专用日志收集器）下部署的高性能硬件设备。这些设备提供可分配给各种 Panorama 服务的多个接口，如防火墙管理和日志收集。在设置设备前，请考虑如何配置接口以优化安全性，启用网络分段（大规模部署中），并负载平衡 Panorama 服务的流量。

- M 系列设备接口
- 执行 M 系列设备的初始配置
- M 系列设置概述
- 将 M 系列设备设为日志收集器
- 增加 M 系列设备上的存储容量
- 配置 Panorama 以使用多个接口

M 系列设备接口

Panorama M-600、M-500、M-200 和 M-100 设备具有多个接口，用于与其他系统（如受管防火墙和 Panorama 管理员的客户端系统）进行通信。Panorama 与这些系统进行通信以执行各种服务，包括管理设备（防火墙、日志收集器、WildFire 设备和设备群集）、收集日志、与收集器组进行通信、将软件和内容更新部署到设备以及提供对 Panorama 的管理访问权限。默认情况下，Panorama 使用其管理 (MGT) 接口执行所有这些服务。但是，您可以通过预留 MGT 接口进行管理访问并为其他服务分配不同的接口来提高安全性。在具有多个子网络和大量日志流量的大规模网络中，使用多个接口进行设备管理和日志收集也可实现网络分段和负载均衡（请参阅配置 Panorama 以使用多个接口）。

将 Panorama 服务分配给不同接口时，请记住只有 MGT 接口才允许对 Panorama 的管理访问权限以执行配置和监控任务。当您执行 M 系列设备的初始配置时，您可以将任何接口分配给其他服务。《M 系列设备硬件参考指南》说明了接口可将电缆连接至何处。M-100 设备在其所有接口上均支持 1Gbps 吞吐量：MGT、Eth1、Eth2 和 Eth3。除了这些接口外，M-500 设备在其 Eth4 和 Eth5 接口上支持 10Gbps 吞吐量。

M 系列设备不支持使用链接聚合控制协议 *(LACP)* 来聚合接口。

支持的接口

接口可用于设备管理、日志收集、收集器组通信、许可和软件更新。有关网络分段的更多信息，请参阅配置 Panorama 以使用多个接口。

接口	最高速度	M-600 设备	M-500 设备	M-200 设备
管理 (MGT)	1Gbps	✓	✓	✓
Ethernet 1 (Eth1)	1Gbps	✓	✓	✓
Ethernet 2 (Eth2)	1Gbps	✓	✓	✓
Ethernet 3 (Eth3)	1Gbps	✓	✓	✓
Ethernet 4 (Eth4)	10Gbps	✓	✓	—

© 2019 Palo Alto Networks, Inc.

接口	最高速度	M-600 设备	M-500 设备	M-200 设备
Ethernet 5 (Eth5)	10Gbps	✓	✓	—

日志记录速率

查看所有 M 系列设备型号的日志记录速率。如要实现下列日志记录速率，M 系列设备必须是收集器组中的单个日志收集器，并且您必须安装您的 M 系列型号的所有日志记录磁盘。例如，如要 M-500 设备实现 30,000 条日志/秒，则 12 个 1TB 或 2TB 日志记录磁盘都必须安装。

型号功能和特点	M-600 设备	M-500 设备	M-200 设备
Panorama 在“仅管理”模式下的最大日志记录速率	不支持本地日志存储		
Panorama 在 Panorama 模式下的最大日志记录速率	25,000 条日志/秒	20,000 条日志/秒	10,000 条日志/秒
Panorama 在“日志收集器”模式下的最大日志记录速率	50,000 条日志/秒	30,000 条日志/秒	28,000 条日志/秒
设备的最大日志存储容量	48TB（12 个 8TB RAID 磁盘）	• 24TB（24 个 2TB RAID 磁盘） • 12TB（24 个 1TB RAID 磁盘）	16TB（4 个 8TB RAID 磁盘）
设备的默认日志存储容量	16TB（4 个 8TB RAID 磁盘）	4TB（4 个 2TB RAID 磁盘）	16TB（4 个 8TB RAID 磁盘）
设备的 SSD 存储容量（用于存储 M 系列设备生成的日志）	240GB	240GB	240GB
NFS 附加日志存储	不可用		

执行 M 系列设备的初始配置

默认情况下，Panorama 的 IP 地址为 192.168.1.1，用户名/密码为 admin/admin。为了安全起见，在继续执行其他配置任务之前，必须更改这些设置。您必须从管理 (MGT) 接口或者通过与 M-600、M-500 或 M-200 设备上控制台端口的直接串行端口连接执行以下初始配置任务。



如果您在日志收集器模式下使用 *10GB* 接口配置 *M-Series* 设备，则必须完成整个配置过程才能使 *10GB* 接口显示为 *Up*（启用）。

STEP 1 | 从网络管理员收集所需的接口和服务器信息。

- 收集您计划配置的每个接口（MGT、Eth1、Eth2、Eth3、Eth4、Eth5）的 IP 地址、子网掩码（对于 IPv4）或前缀长度（对于 IPv6）和默认网关。只有 MGT 接口为必需接口。

© 2019 Palo Alto Networks, Inc.

Palo Alto Networks 建议您为 *MGT* 接口指定所有这些设置。如果忽略其中某些设置（如默认网关）的值，则以后更改配置时只能通过控制台端口访问 *Panorama*。如果没有指定所有这些设置，则不能提交其他接口的配置。

如果您计划将设备用作 Panorama 管理服务器，则 Palo Alto Networks 建议仅将 MGT 接口用于管理 Panorama，并使用其他接口管理设备、收集日志、与收集器组通信以及将更新部署到设备（请参阅 M 系列设备接口）。

- 收集 DNS 服务器的 IP 地址。

STEP 2 | 从您的计算机访问 M 系列设备。

1. 按以下方式之一连接到 M 系列设备：
   - 使用串行电缆将计算机与 M 系列设备上的控制台端口相连，并使用终端模拟软件 (9600-8-N-1) 进行连接。
   - 使用 RJ-45 以太网电缆将计算机与 M 系列设备上的 MGT 端口相连。从浏览器中访问 https://192.168.1.1。访问此 URL 可能需要将计算机的 IP 地址更改为 192.168.1.0 网络中的地址（如 192.168.1.2）。
2. 收到提示时，使用默认用户名和密码 (admin/admin) 登录到设备。设备开始初始化。

STEP 3 | 更改默认的管理密码。

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

请务必使用密码强度最佳实践来确保密码强度，并查看密码复杂性设置。

1. 单击 Web 界面左下部分的 **admin**（管理员）链接。
2. 输入 **Old Password**（旧密码）、**New Password**（新密码）和 **Confirm New Password**（确认新密码），然后单击 **OK**（确定）。将新密码保存在安全位置。

要确保 *MGT* 接口保持安全，请配置 *Minimum Password Complexity settings*（最小密码复杂性）（选择 *Panorama* > *Setup*（设置）> *Management*（管理）），指定管理员必须更改其密码的间隔时间。

STEP 4 | 配置将用于管理 Panorama、管理设备、收集日志、与收集器组通信并将更新部署到设备的每个接口的网络访问设置。

1. 选择 **Panorama** > **Setup**（设置）> **Interfaces**（接口），然后单击接口名称。
2. （仅限非 MGT 接口）**Enable**（启用）接口。
3. 编辑 Panorama 将使用的每个接口的网络访问设置。只有 MGT 接口为必填项。Eth1、Eth2、Eth3、Eth4 和 Eth5 接口是可选项，只在您计划使用 M 系列设备作为 Panorama 管理服务器时适用。
   1. 根据您网络的 IP 协议，填写以下一个或两个字段集：

      IPv4—**Public IP Address**（公共 **IP** 地址），**IP Address**（**IP** 地址），**Netmask**（子网掩码）和 **Default Gateway**（默认网关）

      如果防火墙使用已转换为专用 *IP* 地址 *(NAT)* 的公共 *IP* 地址连接到 *Panorama* 管理服务器，则在 *Public IP Address*（公共 *IP* 地址）字段内输入公共 *IP*，在 *IP Address*（*IP* 地址）字段内输入专用 *IP*，以便将这两个地址推送到您的防火墙。

      IPv6 — **IPv6 Address/Prefix Length**（**IPv6** 地址/前缀长度）和 **Default IPv6 Gateway**（默认 **IPv6** 网关）

© 2019 Palo Alto Networks, Inc.

2. 选择接口支持的设备管理服务：

   Device Management and Device Log Collection（设备管理和设备日志收集）— 您可以分配一个或多个接口。

   Collector Group Communication（收集器组通信）— 您只能分配一个接口。

   Device Deployment（设备部署）（软件和内容更新）— 您只能分配一个接口。
3. （可选）选择接口支持的 Network Connectivity Services（网络连接服务）。

   （仅限 *MGT* 接口）禁用 *Telnet* 和 *HTTP*；这些服务使用明文，因此比其他服务安全性更低。
4. 单击 **OK**（确定）保存更改。

STEP 5 | 配置主机名和常规设置。

1. 选择 **Panorama** > **Setup** > **Management**（Panorama > 设置 > 管理），然后编辑“General Settings（常规设置）”。
2. 对准 Panorama 与受管防火墙上的时钟，以使用相同的 **Time Zone**（时区），例如 GMT 或 UTC。如果您打算使用 Cortex 数据湖，则必须配置 NTP 以使 Panorama 可以与 Cortex 数据湖保持同步。

   防火墙会记录自己生成日志的时间戳，Panorama 会记录接收日志的时间戳。调整时区可确保同步时间戳，且在 Panorama 上查询日志和生成报告的过程相互协调。
3. 输入服务器的 **Hostname**（主机名）。Panorama 将此名称用作设备的显示名称/标签。例如，此名称是显示在命令行界面提示符中的名称。如果您在 **Panorama** > **Managed Collectors**（Panorama > 受管收集器）页面上将设备添加为受管收集器，则此名称也会显示在“Collector Name（收集器名称）”字段中。
4. （可选）输入 **Latitude**（纬度）和 **Longitude**（经度）以便在世界地图上准确定位 M 系列设备。**App Scope** > **Traffic Maps**（App Scope > 流量映射）和 **App Scope** > **Threat Maps**（App Scope > 威胁映射）使用这些值。
5. 单击**OK**（确定）保存您的输入。

STEP 6 | 配置 DNS 服务器和 Palo Alto Networks 更新服务器。

1. 选择 **Panorama** > **Setup** > **Services**（Panorama > 设置 > 服务），并编辑设置。
2. 输入 **Primary DNS Server**（主 **DNS** 服务器）和 **Secondary DNS Server**（辅助 **DNS** 服务器）（可选）的 IP 地址。
3. 输入 **Update Server**（更新服务器）的 URL 或静态地址（默认为 updates.paloaltonetworks.com）。

   如果想要 *Panorama* 验证从中下载软件或内容包的更新服务器是否拥有信任的证书签发机构签发的 *SSL* 证书，则应选中 *Verify Update Server Identity*（验证更新服务器身份）。此选项可为 *Panorama* 管理服务器和更新服务器之间的通信添加额外的安全级别。
4. 单击**OK**（确定）保存您的输入。

STEP 7 | Commit（提交）配置更改。

选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

如果您计划使用 *M* 系列设备作为 *Panorama* 管理服务器，且已配置 *MGT* 接口以外的接口，则在配置受管收集器时必须将这些接口分配用于 *Device Log Collection*（设备日志收集）和 *Collector Group Communication*（收集器组通信）。为了这些接口能够工作，您必须为受管收集器配置收集器组，执行收集器组提交。

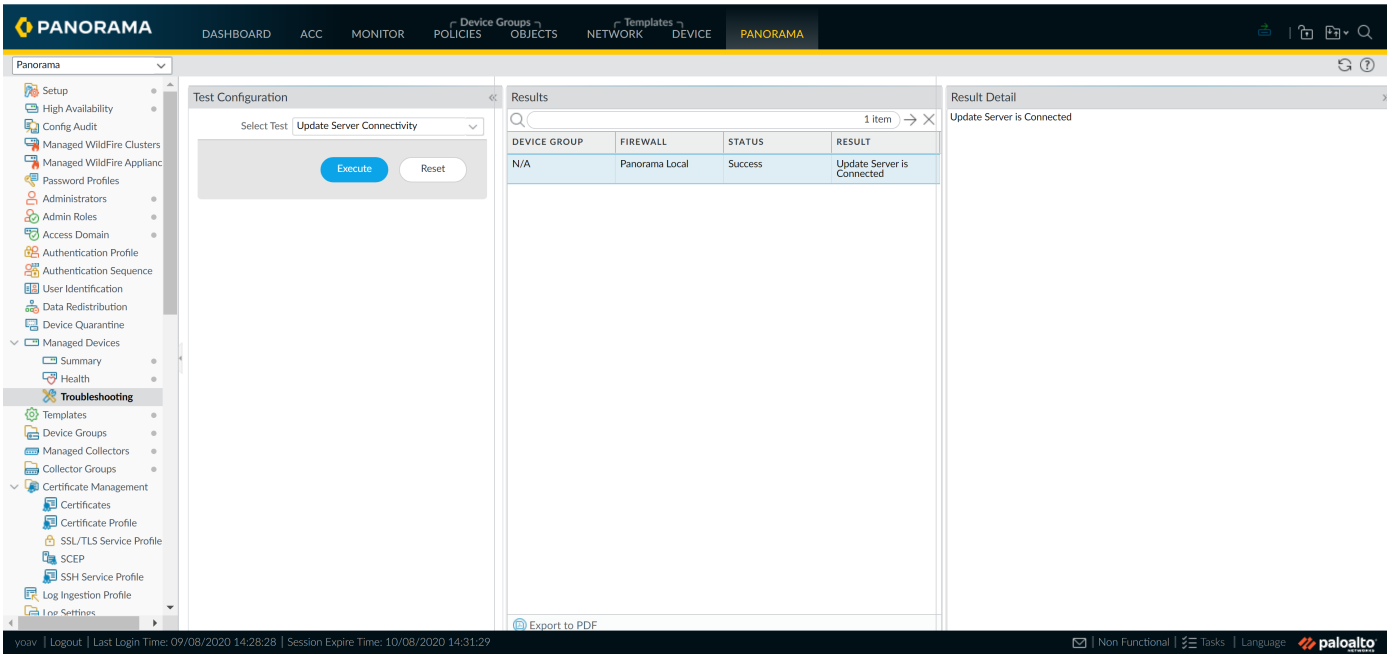
STEP 8 | 验证 Panorama 管理所需外部服务（例如 Palo Alto Networks 更新服务器）的网络访问权限。

1. 按以下方式之一连接到 M 系列设备：

© 2019 Palo Alto Networks, Inc.

- 使用串行电缆将计算机与 M 系列设备上的控制台端口相连。然后，使用终端模拟软件 (9600-8-N-1) 进行连接。
- 使用终端模拟软件（如 PuTTY），打开您在初始配置中为 M 系列设备的 MGT 接口指定的 IP 地址的 SSH 会话。

2. 看到提示时登录到 CLI。使用初始配置过程中指定的默认 admin 帐户和密码。
3. 使用“更新服务器连接”测试验证是否能联网到 Palo Alto Networks 更新服务器，如下例所示。
   1. 选择 **Panorama** > **Managed Devices**（受管设备）> **Troubleshooting**（故障排除），并从 Select Test（选择测试）下拉列表中选择 **Updates Server Connectivity**（更新服务器连接）。
   2. **Execute**（执行）更新服务器连接测试。



4. 使用以下 CLI 命令从更新服务器检索关于 Panorama 支持授权的信息：

```
admin> request support check
```

如果网络畅通，更新服务器回应 Panorama 的支持状态。因为 Panorama 没有注册，所以更新服务器返回以下消息：

```
Contact Us
https://www.paloaltonetworks.com/company/contact-us.html
Support Home
https://www.paloaltonetworks.com/support/tabs/overview.html
Device not found on this update server
```

STEP 9 | 后续步骤...

1. 注册 Panorama 和安装许可证。
2. 安装 Panorama 的内容和软件更新。

作为最佳做法，替换默认证书（*Panorama* 用于加密经由 *MGT* 接口的 *HTTPS* 通信的证书）。

© 2019 Palo Alto Networks, Inc.

M 系列设置概述

使用以下过程设置 M 系列设备：

- 在仅管理模式下设置 M 系列设备
- 在 Panorama 模式下设置 M 系列设备
- 在日志收集器模式下设置 M 系列设备

在仅管理模式下设置 *M* 系列设备

STEP 1 | 将 M 系列设备安装到机架上。有关说明，请参阅《M 系列设备硬件参考指南》。

STEP 2 | 执行 M 系列设备的初始配置

STEP 3 | 注册 Panorama 和安装许可证

STEP 4 | 安装 Panorama 的内容和软件更新

STEP 5 | 更改为仅管理模式。

1. 登录到 Panorama 命令行界面。
2. 从 Panorama 模式切换到仅管理模式：

   request system system-mode management-only
3. 输入 **y** 确认模式更改。重新启动 Panorama 管理服务器。如果重新启动进程终止了终端模拟软件会话，重新连接 Panorama 管理服务器以查看 Panorama 登录提示。

   如果您看到 `CMS Login` 提示，这意味着 Panorama 管理服务器没有完成重新启动。看到提示时按 Enter 键，而不输入用户名或密码。
4. 重新登录至此 CLI。
5. 验证切换到仅管理模式是否成功：

   show system info | match system-mode

   如果模式更改成功，输出显示：

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

STEP 6 | 设置 Panorama 的管理访问权限

STEP 7 | 管理防火墙

STEP 8 | 管理日志收集

在 *Panorama* 模式下设置 *M* 系列设备

STEP 1 | 将 M 系列设备安装到机架上。有关说明，请参阅《M 系列设备硬件参考指南》。

STEP 2 | 执行 M 系列设备的初始配置。

STEP 3 | 注册 Panorama 和安装许可证。

STEP 4 | 安装 Panorama 的内容和软件更新。

STEP 5 | 配置每个阵列。需要执行此任务使 RAID 磁盘可用于日志记录。或者，您可以添加磁盘来增加 M 系列设备上的存储容量。

© 2019 Palo Alto Networks, Inc.

STEP 6 | 设置 Panorama 的管理访问权限。

STEP 7 | 管理防火墙。

STEP 8 | 管理日志收集。

在日志收集器模式下设置 *M* 系列设备

STEP 1 | 将 M 系列设备安装到机架上。有关说明，请参阅《M 系列设备硬件参考指南》。

STEP 2 | 执行 M 系列设备的初始配置

STEP 3 | 注册 Panorama 和安装许可证

STEP 4 | 安装 Panorama 的内容和软件更新

STEP 5 | 请参阅步骤 配置每个阵列。需要执行此任务使 RAID 磁盘可用于日志记录。或者，您可以添加磁盘来增加 M 系列设备上的存储容量。

STEP 6 | 将 M 系列设备设为日志收集器

STEP 7 | 管理日志收集

将 M 系列设备设为日志收集器

如果您需要专用设备进行日志收集，则在日志收集器模式下配置 M-200、M-500 或 M-600 设备。为此，您先要对 Panorama 模式下的设备执行初始配置，包括许可、安装软件和内容更新及配置管理 (MGT) 接口。然后，将 M 系列设备切换到日志收集器模式，完成日志收集器配置。此外，如果您想使用专用 M 系列设备接口（推荐），而不是 MGT 接口用于日志收集和收集器组通信，您必须先为 Panorama 管理服务器配置接口，然后为日志收集器配置这些接口，提交收集器组后再执行 Panorama 提交。

执行以下步骤将新的 M 系列设备设置为日志收集器，或者转换之前用作 Panorama 管理服务器的现有 M 系列设备。

如果您在日志收集器模式下使用 *10GB* 接口配置 *M-Series* 设备，则必须完成整个配置过程才能使 *10GB* 接口显示为 `Up`（启用）。

将 *M* 系列设备从 *Panorama* 模式切换到日志收集器模式将重新启动设备，删除本地日志收集器，删除任何现有的日志数据，并删除除管理访问权限设置之外的所有配置。切换模式不会删除许可证、软件更新或内容更新。

STEP 1 | 设置将管理日志收集器的 Panorama 管理服务器（如果尚未设置）。

然后执行以下任务之一：

- 设置 Panorama 虚拟设备
- 设置 M 系列设备

STEP 2 | 记录 Panorama 管理服务器的管理 IP 地址。

如果在高可用性 (HA) 配置中部署 Panorama，您需要在每个高可用性对端设备的 IP 地址。

1. 登录 Panorama 管理服务器的 Web 界面。
2. 选择 **Panorama** > **Setup**（设置）> **Management**（管理），查看 Management Interface Settings（管理接口设置），记录单独（非高可用性）或主动（高可用性）Panorama 的 **IP Address**（**IP** 地址）。

© 2019 Palo Alto Networks, Inc.

3. 对于高可用性部署，选择 **Panorama** > **High Availability**（高可用性），查看 Setup（设置）部分，记录被动 Panorama 的 **Peer HA IP Address**（对端设备高可用性 **IP** 地址）。

STEP 3 | 设置将要用作专用日志收集器的 M 系列设备。

如果您之前将此设备部署为 Panorama 管理服务器，您可以跳过此步骤，因为 MGT 接口已配置，许可证和更新已安装。

日志收集器模式下的 M 系列设备没有用于配置任务的 Web 界面，只有 CLI。因此，在更改 M 系列设备的模式之前，使用 Panorama 模式下的 Web 界面：

1. 执行 M 系列设备的初始配置。
2. 注册 Panorama 和安装许可证。
3. 安装 Panorama 的内容和软件更新。

STEP 4 | 访问 M 系列设备的 CLI。

1. 按以下方式之一连接到 M 系列设备：
   - 使用串行电缆将计算机与 M 系列设备上的控制台端口相连。然后，使用终端模拟软件 (9600-8-N-1) 进行连接。
   - 使用终端模拟软件（如 PuTTY），打开您在初始配置中为 M 系列设备的 MGT 接口指定的 IP 地址的 SSH 会话。
2. 看到提示时登录到 CLI。使用初始配置过程中指定的默认 admin 帐户和密码。

STEP 5 | 从 Panorama 模式切换到日志收集器模式。

1. 要切换到日志收集器模式，请输入以下命令：

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

2. 输入 **Y** 确认模式更改。M 系列设备重新启动。如果重新启动进程终止了终端模拟软件会话，重新连接 M 系列设备以查看 Panorama 登录提示。

   如果您看到 ***CMS Login***（*CMS* 登录）提示，这意味着日志收集器没有完成重新启动。看到提示时按 *Enter* 键，而不输入用户名或密码。

3. 重新登录至此 CLI。
4. 验证切换到日志收集器模式是否成功：

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

如果模式更改成功，输出显示：

```
system-mode: logger
```

STEP 6 | 将日志记录磁盘配置为 RAID1 对。

如果您之前将此设备部署为 Panorama 管理服务器，您可以跳过此步骤，因为磁盘对已配置且可用。

配置驱动器所需的时间从几分钟到几个小时不等，具体时间取决于驱动器上的数据量。

1. 确定 M 系列设备上存在的哪些磁盘对配置为 RAID 对：

```
> show system raid detail
```


© 2019 Palo Alto Networks, Inc.

执行剩余步骤配置 present 磁盘的每个磁盘对。本示例使用磁盘对 A1/A2。

2. 要在此对中添加第一个磁盘，输入以下命令并在收到提示时输入 **y** 确认请求：

```
> request system raid add A1
```

等待此过程完成后再在此对中添加另一个磁盘。要监视 RAID 配置的流程，请重新输入：

```
> show system raid detail
```

第一个磁盘的此过程完成后，输出显示磁盘对状态为 Available，但是 degraded。

3. 在此对中添加第二个磁盘：

```
> request system raid add A2
```

4. 验证磁盘状态是否完成：

```
> show system raid detail
```

第二个磁盘的此过程完成后，输出显示磁盘对状态为 Available，但是 clean：

```
Disk Pair A      Available
Status        clean
```

STEP 7 | 启用日志收集器和 Panorama 管理服务器之间的连接。

在日志收集器 CLI 中输入以下命令，*<IPaddress1>* 是单独（非高可用性）或主动（高可用性）Panorama 的 MGT 接口，*<IPaddress2>* 是被动（高可用性）Panorama 的 MGT 接口（如适用）。

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

STEP 8 | 记录日志收集器的序列号。

您需要此序列号在 Panorama 管理服务器上，将日志收集器添加为受管收集器。

1. 在日志收集器命令行界面中，输入以下命令以显示它的序列号。

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

2. 记录序列号。

STEP 9 | 将日志收集器添加为 Panorama 管理服务器的受管收集器。

1. 选择 **Panorama** > **Managed Collectors**（Panorama > 受管收集器），**Add**（添加）受管收集器。
2. 在 **General**（常规）设置中，输入为日志收集器记录的序列号（**Collector S/N**（收集器序列号））。
3. 在 **Panorama Server IP**（**Panorama** 服务器 **IP**）字段中，输入单独（非高可用性）或主动（高可用性）Panorama 的 IP 地址或 FQDN。对于高可用性部署，在 **Panorama Server IP 2**（**Panorama** 服务器 **IP 2**）字段中输入被动 Panorama 对端设备的 IP 地址或 FQDN。

© 2019 Palo Alto Networks, Inc.

这些 IP 地址必须指定启用 **Device Management and Device Log Collection**（设备管理和设备日志收集）服务的 Panorama 接口。默认情况下，仅在 MGT 接口上启用这些服务。但是，您可能会在设置 M 系列设备作为 Panorama 管理服务器时在其他接口上启用这些服务。

4. 选择 **Interfaces**（接口），单击 **Management**（管理），根据网络的 IP 协议为 MGT 接口配置以下一个或两个字段集。
   - IPv4 — **IP Address**（**IP** 地址）、**Netmask**（子网掩码）和 **Default Gateway**（默认网关）
   - IPv6 — **IPv6 Address/Prefix Length**（**IPv6** 地址/前缀长度）和 **Default IPv6 Gateway**（默认 **IPv6** 网关）
5. 单击 **OK**（确定）两次保存对日志收集器所作的更改。
6. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并将更改 **Commit**（提交）到 Panorama 配置。

   必须执行此步骤才能启用日志记录磁盘。
7. 核实 **Panorama** > **Managed Collectors**（受管收集器）是否列出您已添加的日志收集器。Connected（已连接）列显示表明日志收集器已连接到 Panorama 的复选标记。您可能需要等待几分钟，等页面显示更新后的连接状态。

   此时，*Configuration Status*（配置状态）列显示 *Out of Sync*（不同步），*Run Time Status*（运行时间状态）列应显示 *disconnected*（已断开连接）。在配置收集器组后，状态将更改为 *In Sync*（同步中）和 *connected*（已连接）（步骤将日志收集器分配到一个收集器组。）。

STEP 10 | 启用日志记录硬盘。

1. 选择 **Panorama** > **Managed Collectors**（Panorama > 受管收集器），然后编辑日志收集器。
2. 选择 **Disks**（磁盘），**Add**（添加）每个 RAID 磁盘对。
3. 单击 **OK**（确定）保存更改。
4. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并将更改 **Commit**（提交）到 Panorama 配置。

STEP 11 | （推荐）如果 Panorama 管理服务器和日志收集器使用 **Ethernet1**、**Ethernet2**、**Ethernet3**、**Ethernet4** 和 **Ethernet5** 接口进行 **Device Log Collection**（设备日志收集）（从防火墙接收日志）和 **Collector Group Communication**（收集器组通信），请配置这些接口。

如果您以前将日志收集器部署为 Panorama 管理服务器并配置这些接口，则必须重新配置它们，因为切换到日志收集器模式（从 Panorama 模式切换到日志收集器模式。）将删除除管理访问设置以外的所有配置。

1. 如果您尚未完成以下操作，请配置 Panorama 管理服务器上的每个接口（MGT 接口除外）：
   1. 选择 **Panorama** > **Setup**（设置）> **Interfaces**（接口），然后单击接口名称。
   2. 选择 *<interface-name>* 以启用接口。
   3. 根据您网络的 IP 协议，填写以下一个或两个字段集：

      IPv4 — **IP Address**（**IP** 地址）、**Netmask**（子网掩码）和 **Default Gateway**（默认网关）

      IPv6 — **IPv6 Address/Prefix Length**（**IPv6** 地址/前缀长度）和 **Default IPv6 Gateway**（默认 **IPv6** 网关）
   4. 选择接口支持的设备管理服务：

      Device Management and Device Log Collection（设备管理和设备日志收集）— 您可以分配一个或多个接口。

      Collector Group Communication（收集器组通信）— 您只能分配一个接口。

      Device Deployment（设备部署）（软件和内容更新）— 您只能分配一个接口。

© 2019 Palo Alto Networks, Inc.

5. 单击 **OK**（确定）保存更改。

2. 配置日志收集器上的每个接口（MGT 接口除外）：
   1. 选择 **Panorama** > **Managed Collectors**（Panorama > 受管收集器），然后编辑日志收集器。
   2. 选择 **Interfaces**（接口），并单击接口名称。
   3. 选择 *<interface-name>* 以启用接口。
   4. 根据您网络的 IP 协议，填写以下一个或两个字段集：

      IPv4 — **IP Address**（IP 地址）、**Netmask**（子网掩码）和 **Default Gateway**（默认网关）

      IPv6 — **IPv6 Address/Prefix Length**（IPv6 地址/前缀长度）和 **Default IPv6 Gateway**（默认 IPv6 网关）
   5. 选择接口支持的设备管理服务：

      Device Log Collection（设备日志收集）— 您可以分配一个或多个接口。

      Collector Group Communication（收集器组通信）— 您只能分配一个接口。
   6. 单击 **OK**（确定）保存对接口所作的更改。
3. 单击 **OK**（确定）保存对日志收集器所作的更改。
4. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并将更改 **Commit**（提交）到 Panorama 配置。

STEP 12 | （可选）如果您的部署使用自定义证书在 Panorama 和受管设备之间进行身份验证，请部署自定义客户端设备证书。有关更多信息，请参阅使用自定义证书设置身份验证。

1. 选择 **Panorama** > **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件），然后从下拉列表中选择证书配置文件或单击 **New Certificate Profile**（新建证书配置文件）以创建证书配置文件。
2. 选择日志收集器的 **Panorama** > **Managed Collectors**（受管收集器）> **Add**（添加）> **Communication**（通信）。
3. 选中 **Secure Client Communication**（安全客户端通信）复选框。
4. 选择 Type（类型）下拉列表中的设备证书类型。
   - 如果您使用本地设备证书，请从各自下拉列表中选择 **Certificate**（证书）和 **Certificate Profile**（证书配置文件）。
   - 如果您使用 SCEP 作为设备证书，请从各自下拉列表中选择 **SCEP Profile**（SCEP 配置文件）和 **Certificate Profile**（证书配置文件）。
5. 单击 **OK**（确定）。

STEP 13 | （可选）在日志收集器上配置 Secure Server Communication（安全服务器通信）。有关更多信息，请参阅使用自定义证书设置身份验证。

1. 选择 **Panorama** > **Managed Collectors**（受管收集器）> > **Communication**（通信）。
2. 验证 **Custom Certificate Only**（仅允许自定义证书）复选框未选中。这允许您在迁移到自定义证书的同时继续管理所有设备。

   如果选中 *Custom Certificate Only*（仅允许自定义证书）复选框，则日志收集器不会进行身份验证，并且无法使用预定义证书从设备接收日志。
3. 从 **SSL/TLS Service Profile**（SSL/TLS 服务配置文件）下拉列表中选择 SSL/TLS 服务配置文件。此 SSL/TLS 服务配置文件适用于日志收集器和发送日志的设备之间的所有 SSL 连接。
4. 从 **Certificate Profile**（证书配置文件）下拉列表中选择证书配置文件。
5. 选择 **Authorize Client Based on Serial Number**（根据序列号对客户端进行身份验证）让服务器根据受管设备的序列号检查客户端。客户端证书必须将特殊关键字 $UDID 设置为要根据序列号进行授权的 CN。
6. 在 **Disconnect Wait Time (min)**（断开连接等待时间（分钟））中，输入 Panorama 在与其受管设备断开并重新建立连接之前所需的分钟数。该字段默认为空，范围为 0 至 44,640 分钟。

© 2019 Palo Alto Networks, Inc.

在您提交新配置之前，断开连接等待时间不会开始倒计时。

7. （可选）配置授权列表。
   1. 单击 Authorization List（授权列表）下的 **Add**（添加）。
   2. 选择 **Subject**（主题）或 **Subject Alt Name**（主题备用名称）作为标识符类型。
   3. 输入所选类型的标识符。
   4. 单击 **OK**（确定）。
   5. 选择 **Check Authorization List**（检查授权列表）以执行授权列表。
8. 单击 **OK**（确定）。
9. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**）。

STEP 14 | 将日志收集器分配到一个收集器组。

1. 配置收集器组。您必须执行 Panorama 提交，然后收集器组提交与 Panorama 同步日志收集器配置，在日志收集器上将 Eth1、Eth2、Eth3、Eth4 和 Eth5 接口（如果配置）置于运行状态。

   在任何单个收集器组中，所有日志收集器均必须在相同的 *Panorama* 型号上运行：均为 *M-600* 设备、均为 *M-500* 设备、均为 *M-200* 设备或均为 *Panorama* 虚拟设备。

   作为最佳做法，如果将多个日志收集器添加到单个收集器组，请 *Enable log redundancy across collectors*（启用跨收集器记录冗余）。此选项要求每个日志收集器具有相同数量的日志记录磁盘。
2. 选择 **Panorama** > **Managed Collectors**（Panorama > 受管收集器），核实日志收集器配置是否已与 Panorama 同步。

   Configuration Status（配置状态）列应显示 In Sync（同步），Run Time Status（运行时间状态）列应显示 connected（已连接）。
3. 访问日志收集器命令行界面，输入以下命令核实它的接口是否正在运行：

   ```
   > show interface all
   ```

   在输出结果中，每个正在运行的接口的 `state` 显示为 `up`。
4. 如果收集器组有多个日志收集器，排除网络资源连接问题 为日志收集器使用的每个接口运行 Ping 连接测试，核实这些收集器是否能彼此通信。对于 `source` IP 地址，指定一个日志收集器的接口。对于 `host` IP 地址，指定同一收集器组中另一个日志收集器的匹配接口。

STEP 15 | 后续步骤...

使日志收集器能够接收防火墙日志：

1. 配置 Panorama 的日志转发。
2. 验证 Panorama 日志转发。

增加 M 系列设备上的存储容量

在您执行 M 系列设备的初始配置后，可以通过将现有驱动器对升级到更大容量的驱动器或在空驱动器插槽中安装其他驱动器对来增加设备的日志存储容量。例如，您可以在 M-500 设备上选择将现有 1TB 驱动器升级到 2TB 驱动器，或者可在空驱动器插槽（B1 到 D2）中添加 2TB 驱动器。

M 系列设备在磁盘发生故障时利用 *RAID 1* 实现数据冗余。因此，*RAID 1* 阵列中的驱动器对必须相同。但是，您可以自由混合不同 *RAID 1* 阵列的驱动器容量。例如，*A1/A2 RAID 1* 阵列中的驱动器可以是 *1TB* 驱动器，*B1/B2 RAID 1* 阵列中的驱动器可以是 *2TB* 驱动器。

© 2019 Palo Alto Networks, Inc.

下表列出了 M 系列设备支持的最大驱动器插槽数量和可用驱动器容量。

由于每个驱动器对（例如 *A1/A2*）都位于 *RAID 1* 阵列中，因此总存储容量为安装的总驱动器数量的一半。例如，如果 *M-500* 设备已在驱动器插槽 *A1/A2* 和 *B1/B2* 中安装 *2TB* 驱动器，则 *A1/A2* 阵列提供 *2TB* 的总存储空间，*B1/B2* 阵列提供总共 *4TB* 的另外 *2TB*。

设备	支持的驱动器插槽数量	支持的驱动器容量
M-200 设备	4	8TB
M-500 设备	24	1TB 或 2TB
M-600 设备	12	8TB

增加日志存储容量前，确定 Panorama 日志存储要求。如果您需要的日志存储容量大于单个 M 系列设备所支持的容量，您可以添加专用日志收集器（请参阅配置受管收集器）或者可以配置从 Panorama 到外部目标的日志转发。

将驱动器添加到已经部署的 *M* 系列设备时，不需要为扩展存储容量而将 *M* 系列设备下线。当额外的驱动器变得可配置可用时，*M* 系列设备将会在所有可用驱动器之间重新分发日志。此日志重新分发过程在后台执行，不会影响正常运行时间或 *M* 系列设备的可用性。但是，此过程确实会降低最大日志记录速率。*Redistribution State*（重新分发状态）列（*Panorama* > *Collector Groups*（*Panorama* > 收集器组））将以百分比表示进程的完成状态。

- 向 M 系列设备添加磁盘
- 在运行 Panorama 7.0.8 或更新版本的 M 系列设备上升级驱动器
- 在运行 Panorama 7.0.7 或以前版本的 M 系列设备上升级驱动器

向 *M* 系列设备添加磁盘

STEP 1 | 在合适的驱动器托架中安装新驱动器。

确保在下一个打开的驱动器托架中按顺序添加驱动器。例如，在将驱动器添加到 C1 和 C2 之前将驱动器添加到 B1 和 B2。

STEP 2 | 访问 M 系列设备上的命令行界面 (CLI)。

按以下两种方式之一连接到 M 系列设备：

- 使用串行电缆将计算机与控制台端口相连，并使用终端模拟软件 (9600-8-N-1) 连接上 M 系列设备。
- 使用终端模拟软件（如 PuTTY）打开与 M 系列设备 IP 地址的安全外壳 (SSH) 会话。

STEP 3 | 收到提示时，登录到设备。

使用默认的管理员帐户和分配的密码。

STEP 4 | 配置每个阵列。

在驱动器上执行数据镜像所需的时间从几分钟到几个小时不等，具体时间取决于驱动器上的数据量。

以下示例使用托架 B1 和 B2 中的驱动器。

1. 输入以下命令并在收到提示时确认请求：

© 2019 Palo Alto Networks, Inc.

```
> request system raid add B1
> request system raid add B2
```

2. 要监视 RAID 配置的流程，请输入以下命令：

```
> show system raid detail
```

当 RAID 设置完成时，会显示以下响应：

```
Disk Pair A       Available
   Status         clean
   Disk id A1     Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : active sync
   Disk id A2     Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : active sync
Disk Pair B        Available
   Status          clean
   Disk id B1      Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : active sync
   Disk id B2     Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : active sync
```

STEP 5 | 让阵列可用于日志记录。

要启用阵列进行日志记录，您必须先将设备添加为 Panorama 上的受管收集器。如果尚未添加，则请参阅配置受管收集器。

1. 登录到管理此日志收集器的 Panorama 管理服务器的 Web 界面。
2. 选择 **Panorama** > **Managed Collectors**（Panorama > 受管收集器），然后编辑日志收集器。
3. 选择 **Disks**（磁盘），并 **Add**（添加）每个阵列。
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。
6. 选择 **Commit**（提交）> **Push to Devices**（推送到设备），选择收集器组，然后 **Push**（推送）您的更改。

在运行 *Panorama 7.0.8* 或更新版本的 *M* 系列设备上升级驱动器

STEP 1 | 访问 M 系列设备上的命令行界面 (CLI)。

按以下两种方式之一连接到 M 系列设备：

- 使用串行电缆将计算机与控制台端口相连，并使用终端模拟软件 (9600-8-N-1) 连接上 M 系列设备。
- 使用终端模拟软件（如 PuTTY）打开与 M 系列设备 IP 地址的安全外壳 (SSH) 会话。

STEP 2 | 收到提示时，登录到设备。

使用默认的管理员帐户和分配的密码。

© 2019 Palo Alto Networks, Inc.

STEP 3 | 验证已安装驱动器的 RAID 1 状态是否显示至少有两个正在工作的 RAID 1 阵列。升级期间，您一次升级一个 RAID 1 阵列，所以此设备必须至少有一个其他可用的 RAID 1 阵列。如果您尝试从配置中移除唯一正在工作的阵列，此设备会显示中止错误。

输入以下命令以查看 RAID 状态：

```
> show system raid detail
```

例如，以下显示了有两个可用阵列（磁盘对 A 和磁盘对 B）的 M-500 设备的输出。如果只有一个可用阵列，在升级驱动器之前，您必须添加再添加一个阵列，如向 M 系列设备添加额外磁盘所示。

```
Disk Pair A                              Available
   Status                                    clean
   Disk id A1                              Present
       model          : ST91000640NS
       size           : 953869 MB
       status         : active sync
   Disk id A2                              Present
       model          : ST91000640NS
       size           : 953869 MB
       status         : active sync
Disk Pair B                              Available
   Status                                    clean
   Disk id B1                              Present
       model          : ST91000640NS
       size           : 953869 MB
       status         : active sync
   Disk id B2                              Present
       model          : ST91000640NS
       size           : 953869 MB
       status         : active sync
```

STEP 4 | 移除第一个 1TB 驱动器，将它更换为 2TB 驱动器。

1. 要从 RAID 1 阵列配置中移除第一个驱动器（在此例中为 A1），输入以下命令并在收到提示时输入 **y** 确认请求：

   ```
   > request system raid remove A1
   ```

2. 从驱动器插槽实际取出第一个驱动器。按驱动器插槽 A1 中驱动器托架上的弹出按钮以释放驱动器托架杆。然后将托架杆朝您的方向拉出，使驱动器从此设备中滑出。
3. 去掉 2TB 驱动器的包装，将驱动器放在您刚取出的驱动器旁边的格架上。注意此驱动器如何安装在托架中的，因为您会将 2TB 驱动器安装在同一托架中。
4. 拆下将 1TB 驱动器固定在托架上的四颗螺丝，然后从托架取出驱动器。
5. 使用取出 1TB 驱动器时拆下的四颗螺丝，将 2TB 驱动器安装到托架中，然后将托架连同 2TB 驱动器插入驱动器插槽 A1 中。
6. 输入以下命令确认已识别 2TB 驱动器：

   ```
   show system raid detail
   ```

   验证 A1 磁盘显示正确的型号和大小（大约 2TB）。如果型号和尺寸不正确，请再次运行上述命令，直到显示正确的型号和尺寸。

   如果始终显示错误的型号和尺寸，请输入以下命令：

© 2019 Palo Alto Networks, Inc.

```
request system raid remove A1
```

运行上述命令后等待 30 秒，然后取出磁盘并重新插入磁盘并重复运行 **show system raid detail** 命令验证大小和型号。

STEP 5 | 将 RAID 1 阵列中安装的另一个 1TB 驱动器的数据复制到此阵列中新安装的 2TB 驱动器。



复制此数据所需的时间从几分钟到几个小时不等，具体时间取决于驱动器上的数据量。

1. 要将驱动器插槽 A2 中的 1TB 驱动器的数据复制到驱动器插槽 A1 中新安装的 2TB 驱动器，输入以下命令并在看到提示时输入 **y**。

```
> request system raid copy from A2 to A1
```

2. 要查看复制过程的状态，请运行以下命令：

```
> show system raid detail
```

继续运行此命令，查看 RAID 详细信息输出，直到您看到此阵列（在此例中为 A1/A2）显示 `Available`。



此时，驱动器 *A2* 将显示 *`not in use`*，因为驱动器尺寸不匹配。

STEP 6 | 将 RAID 1 阵列中第二个驱动器升级为 2TB 驱动器。

1. 取出 RAID 1 阵列配置的第二个 1TB 驱动器（在当前示例中，从驱动器插槽 A2）：

```
> request system raid remove A2
```

2. 将新安装好 2TB 驱动器的托架插入驱动器插槽 A2，将它添加到 RAID 1 阵列配置：

```
> request system raid add A2
```

此系统将数据从 A2 复制到 A1，制作驱动器镜像。

3. 要查看复制过程的状态，请运行以下命令：

```
> show system raid detail
```

继续查看 RAID 详细信息输出，直到您看到此阵列（在此例中为 A1/A2）显示 `Available`，并且两个磁盘均显示 `active sync`。

```
Disk Pair A        Available
   Status          clean
   Disk id A1      Present
       model         : ST2000NX0253
       size          : 1907138 MB
       status        : active sync
Disk id A2      Present
       model         : ST2000NX0253
       size          : 1907138 MB
```


© 2019 Palo Alto Networks, Inc.

```
        status       : active sync
```

STEP 7 | 根据需要为其他 RAID 1 阵列升级驱动器。

要将其他 RAID 1 阵列升级到 2TB 驱动器，重复此程序更换驱动器指示符（如适用）。例如，将 A1 改为 B1，将 A2 改为 B2 来升级 B1/B2 RAID 1 阵列中的驱动器。

在运行 *Panorama 7.0.7* 或以前版本的 *M* 系列设备上升级驱动器

在运行 *Panorama 7.0.7* 或以前版本的 *M* 系列设备上升级驱动器后，*1TB* 驱动器上的日志才变得可用。即使这可以接受，但我们仍然建议您在维护窗口期间执行此升级。

如果保留日志很重要，您必须升级到 *Panorama 7.0.8* 或最新版本，然后使用在运行 Panorama 7.0.8 或更新版本的 M 系列设备上升级驱动器过程。

STEP 1 | 访问 M 系列设备上的命令行界面 (CLI)。

按以下两种方式之一连接到 M 系列设备：

- 使用串行电缆将计算机与控制台端口相连，并使用终端模拟软件 (9600-8-N-1) 连接上 M 系列设备。
- 使用终端模拟软件（如 PuTTY）打开与 M 系列设备 IP 地址的安全外壳 (SSH) 会话。

STEP 2 | 收到提示时，登录到设备。

使用默认的管理员帐户和分配的密码。

STEP 3 | 验证已安装驱动器的 RAID 1 状态是否显示至少有两个正在工作的 RAID 1 阵列。升级期间，您一次升级一个 RAID 1 阵列，所以此设备必须至少有一个其他可用的 RAID 1 阵列。如果您尝试从配置中移除唯一正在工作的阵列，此设备会显示中止错误。

输入以下命令以查看 RAID 状态：

```
> show system raid detail
```

例如，以下显示了有两个可用阵列（磁盘对 A 和磁盘对 B）的 M-500 设备的输出。如果只有一个可用阵列，在升级驱动器之前，您必须添加再添加一个阵列，如向 M 系列设备添加磁盘所示。

```
Disk Pair A                              Available
   Status                                    clean
   Disk id A1                              Present
       model          : ST91000640NS
       size           : 953869 MB
       status         : active sync
   Disk id A2                              Present
       model          : ST91000640NS
       size           : 953869 MB
       status         : active sync
Disk Pair B                              Available
   Status                                    clean
   Disk id B1                              Present
       model          : ST91000640NS
       size           : 953869 MB
       status         : active sync
   Disk id B2                              Present
       model          : ST91000640NS
       size           : 953869 MB
       status         : active sync
```


© 2019 Palo Alto Networks, Inc.

STEP 4 | 从第一个 RAID 1 阵列配置中移除前两个 1TB 驱动器，然后实际取出这两个驱动器。

1. 要从 RAID 1 阵列配置中移除这些驱动器（在此例中为 A1 和 A2），输入以下命令并在收到提示时输入 **y** 确认每个请求：

```
> request system raid remove A1
> request system raid remove A2
```

2. 从驱动器插槽实际取出这些驱动器。按各个驱动器托架上的弹出按钮以释放驱动器托架杆。然后将托架杆朝您的方向拉出，使驱动器从此设备中滑出。
3. 去掉两个 2TB 驱动器的包装，将它们放在您刚取出的驱动器旁边的格架上。注意这些驱动器如何安装在托架中的，因为您会将 2TB 驱动器安装在这些同样的托架中。
4. 拆下将各个驱动器固定在托架上的四颗螺丝，然后从托架取出驱动器。
5. 使用取出驱动器时拆下的四颗螺丝，将 2TB 驱动器安装到托架中，然后将托架连同新安装的 2TB 驱动器插入驱动器插槽中（在此例中为 A1 和 A2）。

STEP 5 | 为新安装的 2TB 驱动器创建一个新的 RAID 1 阵列，确保这两个驱动器都在新阵列中。

1. 要创建包含驱动器插槽 A1 中的驱动器的新阵列，输入以下命令：

```
> request system raid add A1
```

2. 要查看并确认新 RAID 1 阵列配置的状态，请输入以下命令：

```
> show system raid detail
```

以下输出显示 `Disk Pair A` 阵列为 `Available`。



此时，驱动器 *A2* 将显示 *`not in use`*（未使用）。

```
Disk Pair A        Available
   Status          clean, degraded
   Disk id A1      Present
       model         : ST91000640NS
       size          : 953869 MB
       status        : active sync
   Disk id A2        Present
       model         : ST91000640NS
       size          : 953869 MB
       status        : not in use
```

3. 在新阵列中添加第二个磁盘。在本例中，添加 A2：

```
> request system raid add A2
```

4. 继续运行 **`show system raid detail`** 命令查看 RAID 输出，直到此磁盘对的状态显示 `clean`（干净），两个磁盘都显示 `active sync`（主动同步）。

STEP 6 | 根据需要为其他 RAID 1 阵列升级驱动器。

要将其他 RAID 1 阵列升级到 2TB 驱动器，重复此程序更换驱动器指示符（如适用）。例如，将 A1 改为 B1，将 A2 改为 B2 来升级 B1/B2 RAID 1 阵列中的驱动器。

© 2019 Palo Alto Networks, Inc.

配置 Panorama 以使用多个接口

在大型网络中，您可以通过实施网络分段来提高安全性并减少拥塞，其中包括根据资源使用情况，用户角色和安全要求对子网进行分段。Panorama 通过让您使用多个M 系列设备接口 管理设备（防火墙、日志收集器、WildFire 设备和设备群集）和收集日志来支持网络分段；您可以将不同的接口分配给不同子网中的设备。

使用多个接口收集日志还可提供负载平衡的好处，这对于防火墙以很高的速率将日志转发给日志收集器的环境特别有用。如果您在收集器组 log forwarding preference list（日志转发偏好列表）中启用 **forward to all Log Collectors**（转发到所有日志收集器）设置，日志会在所有已配置接口发送。否则，日志将在单个接口上转发，如果该接口禁用，则继续在下一个已配置接口上进行日志转发。例如，您配置 Eth1/1、Eth1/2 和 Eth1/3 用于日志转发。如果 Eth1/1 接口禁用，则会继续通过 Eth1/2 进行日志转发。

由于管理员通过 MGT 接口访问和管理 Panorama，因此保护该接口尤为重要。提高 MGT 接口安全性的一种方法是将 Panorama 服务卸载到其他接口。除了设备管理和日志收集外，您还可以将收集器组通信以及软件和内容更新的部署卸载到防火墙、日志收集器、WildFire 设备和设备群集。通过卸载这些服务，您可以预留用于管理通信的 MGT 接口，并将其分配给与防火墙、日志收集器、WildFire 设备和设备群集所在的子网分段的安全子网。

- 用于网络分段示例的多个接口
- 配置 Panorama 进行网络分段

用于网络分段示例的多个接口

图 10: 多个 Panorama 接口 说明在 Panorama 模式和日志收集器模式下使用 M-500 设备上的多个界面的部署。在本示例中，接口支持网络分段，如下所述：

- **Panorama** 管理网络 — 为了保护 Panorama Web 界面、CLI 和 XML API 免遭未经授权的访问，Panorama 上的 MGT 接口连接到只有管理员才能访问的子网。
- 互联网 — Panorama 使用 MGT 接口与 Palo Alto Networks 更新服务器等外部服务进行通信。
- **Perimeter Gateway**和数据中心 — Panorama 使用一对独立的接口来管理这些子网的每个子网中的防火墙和日志收集器。与查询日志收集器获取报告信息相比，管理防火墙通常会产生更少的流量。因此，Panorama 使用 1Gbps 接口（Eth1 和 Eth2）管理防火墙，并使用 10Gbps 接口（Eth4 和 Eth5）查询和管理日志收集器。每个日志收集器都使用其 MGT 接口对查询作出响应，但使用其 Eth4 和 Eth5 接口处理与收集来自防火墙的日志相关联的更多流量。
- 软件和内容更新 — 两个子网中的防火墙和日志收集器都通过 Panorama 上的 Eth3 接口检索软件和内容更新。

© 2019 Palo Alto Networks, Inc.

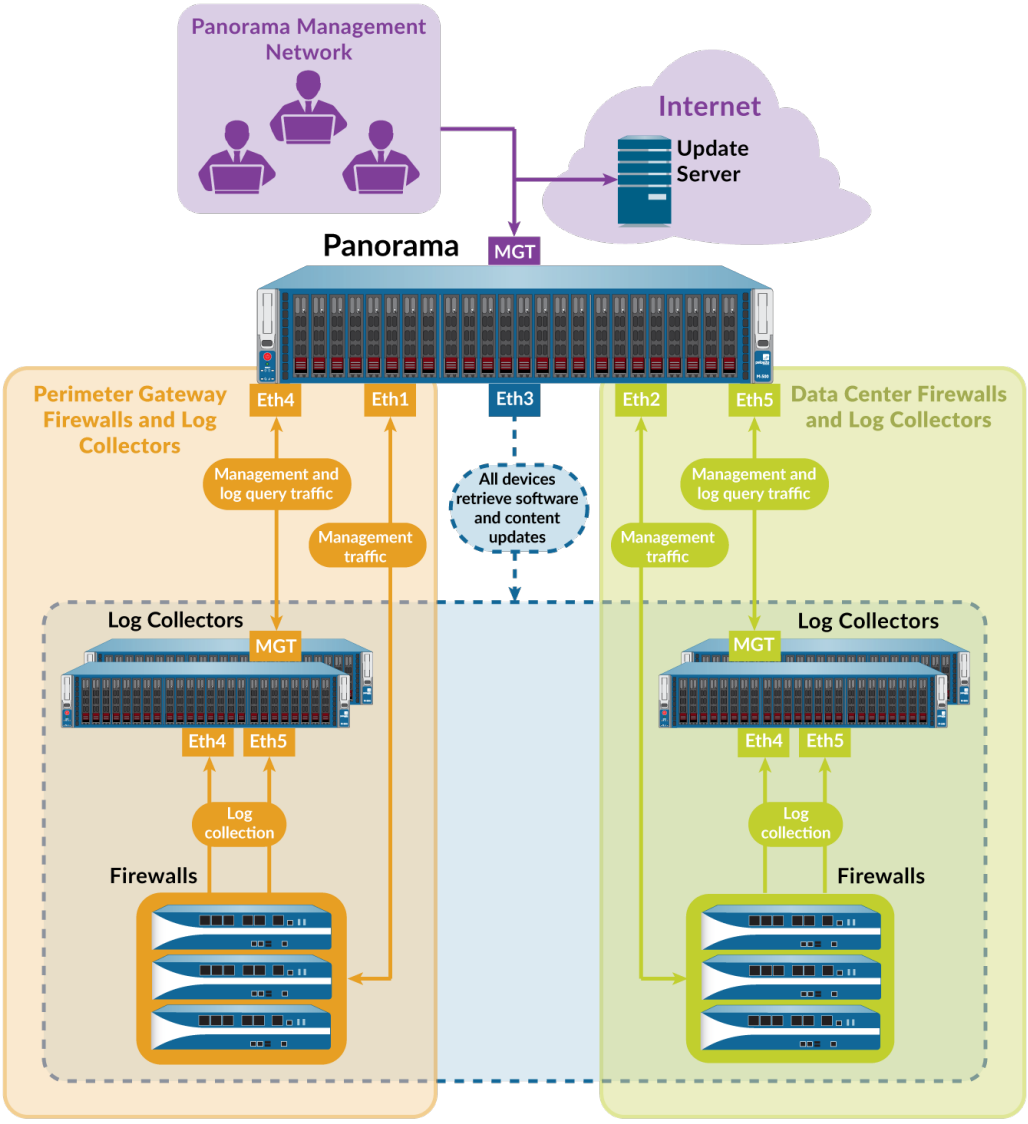


图 10: 多个 **Panorama** 接口

配置 *Panorama* 进行网络分段

要将 Panorama 服务从 MGT 接口卸载到其他接口，请先配置 Panorama 管理服务器上的接口。如果您的网络存在大量日志流量，请记住 M-500 和 M-600 设备上的 Eth4 和 Eth5 接口支持比其他接口 (1Gbps) 更高的吞吐量 (10Gbps)。然后，将每个子网中的日志收集器配置为与 Panorama 上的特定接口连接。对于每个日志收集器，还可以选择用于收集器组通信的接口以及用于从防火墙收集日志的一个或多个接口。最后，将每个子网中的防火墙配置为与 Panorama 上的接口连接。

如果您在日志收集器模式下使用 *10GB* 接口配置 *M-Series* 设备，则必须完成整个配置过程才能使 *10GB* 接口显示为 *Up*（启用）。

Palo Alto Networks 建议您指定 *MGT* 接口的 *IP* 地址、网络掩码（对于 *IPv4*）或前缀长度（对于 *IPv6*）和默认网关。如果省略其中一个设置（如默认网关），则只能通过控制台端口访问 *M* 系列设备以便将来更改配置。

执行以下步骤将 Panorama 和专用日志收集器配置为使用多个接口：

© 2019 Palo Alto Networks, Inc.

STEP 1 | 确认 Panorama 设备和防火墙支持多个接口，并具有必备软件版本和配置。

- M 系列设备必须运行 Panorama 8.0 或更高版本才能使用单独的接口部署更新并使用多个接口进行设备管理和日志收集。M-200 和 M-600 设备必须运行 Panorama 8.1 或更高版本。部署在 ESXi、vCloud、Air、Hyper-V 和 KVM 上的 Panorama 必须运行 Panorama 8.1 或更高版本。
- 如果您将 Panorama 或日志收集器部署为虚拟设备，请验证 Panorama 虚拟设备支持的接口。
- M 系列设备必须运行 Panorama 6.1 或更高版本才能使用单独的接口进行日志收集或收集器组通信。
- 每个 Panorama 管理服务器的初始配置已完成。这包括 MGT 接口的配置。
- 日志收集器和收集器组已配置。这包括日志收集器上的 MGT 接口的配置。
- 防火墙的初始配置已完成，并且您已将防火墙添加到 Panorama 作为受管设备，以及将每个子网中的防火墙分配给单独的模板。
- WildFire 设备的初始配置已完成，并且您已将 WildFire 设备添加到 Panorama 作为受管设备。

STEP 2 | 在单独（非 HA）或主动 (HA) Panorama 管理服务器上配置接口。



由于 *MGT* 接口已在初始 *Panorama* 配置期间配置，因此您无需再次配置。

为每个接口执行这些步骤：

1. 登录到 Panorama Web 界面在单独（非 HA）或主动 (HA) Panorama 管理服务器上。
2. 选择 **Panorama** > **Setup**（设置）> **Interfaces**（接口）。
3. 单击 Interface Name（接口名称）以编辑该接口。
4. 选择 <*interface-name*> 以启用接口。
5. 根据网络的 IP 协议，配置以下一个或两个字段集：
   - IPv4 — **IP Address**（**IP** 地址）、**Netmask**（子网掩码）和 **Default Gateway**（默认网关）
   - IPv6 — **IPv6 Address/Prefix Length**（**IPv6** 地址/前缀长度）和 **Default IPv6 Gateway**（默认 **IPv6** 网关）
6. 选择接口支持的服务。
   - **Device Management and Device Log Collection**（设备管理和设备日志收集）— 管理防火墙，日志收集器和 WildFire 设备和设备群集，收集日志收集器生成的日志，并查询日志收集器以获取报告信息。要支持分段网络，您可以在多个接口上启用这些服务。
   - **Collector Group Communication**（收集器组通信）— 与 Panorama 在所有子网中管理的收集器组通信。
   - **Device Deployment**（设备部署）— 将软件和内容更新部署到所有子网中的受管防火墙，日志收集器以及 WildFire 设备和设备群集。
7. 单击 **OK**（确定）保存对接口所作的更改。
8. 单击 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。
9. 单击 **Commit**（提交）> **Push to Devices**（推送到设备），并推送更改到包含您修改过的日志收集器的收集器组。

STEP 3 | （仅 HA）配置被动 Panorama 管理服务器的接口。

1. 登录到 Panorama Web 界面主动 Panorama 管理服务器。
2. 选择 **Panorama** > **Managed Collectors**（受管收集器），然后选择被动 HA 对端设备。
3. 选择 **Interfaces**（接口），然后单击接口进行编辑。
4. 选中 **Enable Interface**（启用接口）复选框以启用此接口。
5. 根据网络的 IP 协议，配置以下一个或两个字段集：
   - IPv4 — **IP Address**（**IP** 地址）、**Netmask**（子网掩码）和 **Default Gateway**（默认网关）
   - IPv6 — **IPv6 Address/Prefix Length**（**IPv6** 地址/前缀长度）和 **Default IPv6 Gateway**（默认 **IPv6** 网关）

© 2019 Palo Alto Networks, Inc.

6. 选择接口支持的服务。
   - **Device Management and Device Log Collection**（设备管理和设备日志收集）— 管理防火墙，日志收集器和 WildFire 设备和设备群集，收集日志收集器生成的日志，并查询日志收集器以获取报告信息。要支持分段网络，您可以在多个接口上启用这些服务。
   - **Collector Group Communication**（收集器组通信）— 与 Panorama 在所有子网中管理的收集器组通信。
   - **Device Deployment**（设备部署）— 将软件和内容更新部署到所有子网中的受管防火墙，日志收集器以及 WildFire 设备和设备群集。
7. 单击 **OK**（确定）保存对接口所作的更改。
8. 选择 **Commit**（提交）> **Commit and Push**（提交并推送）以将更改提交到 Panorama 并将更改推送到包含修改的被动 HA 对端设备的收集器组。

STEP 4 | 将每个日志收集器配置为与 Panorama 接口连接。

要支持分段网络，您可以将每个子网中的日志收集器连接至单独的 Panorama 接口。接口必须启用 **Device Management and Device Log Collection**（设备管理和设备日志收集），如上一步所述。

1. 登录到 Panorama Web 界面在单独（非 HA）或主动 (HA) Panorama 管理服务器上。
2. 选择 **Panorama** > **Managed Collectors**（Panorama > 受管收集器），然后编辑日志收集器。
3. 在 **Panorama Server IP**（**Panorama** 服务器 **IP**）字段中，输入单独（非 HA）或主动 (HA) Panorama 上的接口的 IP 地址。
4. （仅限 HA）在 **Panorama Server IP 2**（**Panorama** 服务器 **IP 2**）字段中，输入将支持 **Device Management and Device Log Collection**（设备管理和设备日志收集）的被动 Panorama 上的接口的 IP 地址（如果在主动 Panorama 上发生故障转移）。
5. 单击 **OK**（确定）保存更改。
6. 选择 **Commit**（提交）> **Commit and Push**（提交并推送）以将更改提交到 Panorama 并将更改推送到包含修改的日志收集器的收集器组。
7. 在每个专用日志收集器上完成以下步骤：
   1. 使用模拟软件（例如 PuTTY）访问日志收集器 CLI，以使用其 MGT 接口 IP 地址打开与日志收集器的 SSH 会话。系统提示时，使用 Panorama 管理员凭据登录。
   2. 运行以下命令，其中 *<IPaddress1>* 适用于单独（非 HA）或主动 (HA) Panorama，*<IPaddress2>* 适用于被动 Panorama（如果适用）。

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

STEP 5 | （仅限 HA）配置被动 Panorama 管理服务器上的接口以便在主动 Panorama 发生故障转移时部署更新。

1. 登录到 Panorama Web 界面被动 Panorama 管理服务器。
2. 选择 **Panorama** > **Setup**（设置）> **Interfaces**（接口）。
3. 单击 Interface Name（接口名称）以编辑该接口。
4. 选择 *<interface-name>* 以启用接口。
5. 根据网络的 IP 协议，配置以下一个或两个字段集：
   - IPv4 — **IP Address**（**IP** 地址）、**Netmask**（子网掩码）和 **Default Gateway**（默认网关）
   - IPv6 — **IPv6 Address/Prefix Length**（**IPv6** 地址/前缀长度）和 **Default IPv6 Gateway**（默认 **IPv6** 网关）
6. 选择 **Device Deployment**（设备部署）。
7. 单击 **OK**（确定）保存更改。

© 2019 Palo Alto Networks, Inc.

8. 单击 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

STEP 6 | 配置日志收集器将用于从防火墙收集日志并与其他日志收集器通信的接口。



由于 *MGT* 接口已在日志收集器的初始配置期间配置，因此您无需再次配置。

1. 登录到 Panorama Web 界面在单独（非 HA）或主动 (HA) Panorama 管理服务器上。
2. 选择 **Panorama** > **Managed Collectors**（Panorama > 受管收集器），然后编辑日志收集器。
3. 选择 **Interfaces**（接口）并为每个接口执行以下步骤：
   1. 单击接口名称以编辑该接口。
   2. 选择 *<interface-name>* 以启用接口。
   3. 根据您网络的 IP 协议，配置以下一个或两个字段集。

      IPv4 — **IP Address**（**IP** 地址）、**Netmask**（子网掩码）和 **Default Gateway**（默认网关）

      IPv6 — **IPv6 Address/Prefix Length**（**IPv6** 地址/前缀长度）和 **Default IPv6 Gateway**（默认 **IPv6** 网关）
   4. 选择接口支持的功能：

      Device Log Collection（设备日志收集）— 从防火墙收集日志。您可以通过启用多个接口执行此功能来平衡日志记录流量。

      Collector Group Communication（收集器组通信）— 与收集器组中的其他日志收集器通信。
   5. 单击 **OK**（确定）保存对接口所作的更改。
4. 单击 **OK**（确定）保存对日志收集器所作的更改。
5. 选择 **Commit**（提交）> **Commit and Push**（提交并推送）以将更改提交到 Panorama 并将更改推送到包含修改的日志收集器的收集器组。
6. 选择 **Panorama** > **Managed Collectors**（受管收集器）以核实日志收集器是否已与 Panorama 同步且连接。

   配置状态列应显示 `InSync`，运行时间状态列应显示 `connected`。

STEP 7 | 将防火墙配置为与 Panorama 接口连接。

要支持分段网络，您可以将每个子网中的防火墙连接至单独的 Panorama 接口。接口必须启用 **Device Management and Device Log Collection**（设备管理和设备日志收集）。此步骤假定您使用单独的模板配置不同子网中的防火墙。



在此示例部署中，*Panorama* 使用这些接口来管理防火墙，但不收集防火墙日志。您可以指定在配置收集器组时将收集防火墙日志的专用日志收集器。

1. 登录到 Panorama Web 界面在单独（非 HA）或主动 (HA) Panorama 管理服务器上。
2. 在 Panorama 上，选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），选择 **Template**（模板），然后编辑 Panorama 设置。
3. 在第一个 **Panorama Servers**（**Panorama** 服务器）字段中，输入单独（非 HA）或主动 (HA) Panorama 上的接口的 IP 地址。
4. （仅限 HA）在第二个 **Panorama Servers**（**Panorama** 服务器）字段中，输入将支持设备管理的被动 Panorama 上的接口的 IP 地址（如果发生故障转移）。
5. 单击 **OK**（确定）保存更改。
6. 选择 **Commit**（提交）> **Commit and Push**（提交并推送）以将更改提交到 Panorama 并将模板更改推送到防火墙。
7. 选择 **Panorama** > **Managed Devices**（受管设备）以核实防火墙是否已与 Panorama 同步且连接。

   Device State（设备状态）列应显示 `Connected`。共享策略和模板列应显示 `InSync`。

© 2019 Palo Alto Networks, Inc.

注册 Panorama 和安装许可证

在可以开始使用 Panorama 进行集中管理、日志记录和报告之前，您必须注册、激活和检索 Panorama 设备管理和支持许可证。Panorama 的每个实例均需要能让您管理防火墙和获得支持的有效许可证。防火墙设备管理许可证强制规定了 Panorama 可以管理的最大防火墙数量。该许可证基于防火墙序列号，而非基于各防火墙上虚拟设备的数量。支持的许可证能启用 Panorama 软件更新和动态内容更新（例如，对于最新应用程序和威胁签名）。此外，AWS 和 Azure 上的 Panorama 虚拟设备必须从 Palo Alto Network 购买，不能在 AWS 或 Azure 市场购买。

Panorama 虚拟设备升级到 PAN-OS 8.1 后，如果容量许可证未安装成功，或 Panorama 管理的防火墙总数超出设备管理许可证，则系统会提示您。如果未安装许可证，则必须在自升级之日起 180 天内安装有效的设备。如果受管防火墙数量超出设备管理许可证，则必须在 180 天内删除防火墙，以符合设备管理许可证要求，或是升级您的设备管理许可证。自升级之日 180 天内，如果未能安装有效的设备管理许可证，或是不满足现有设备管理许可证的限值，所有提交均失败。如需购买设备管理许可证，请联系 Palo Alto Networks 销售代表或授权分销商。

如果您要使用基于云的 Cortex 数据湖，除了防火墙管理许可证和高级支持许可证外，还需要 Cortex 数据湖许可证。要购买许可证，请联系 Palo Alto Networks 系统工程师或分销商。



如果您在 *Panorama* 虚拟设备上运行防火墙管理的模拟许可证，且希望应用所购买的 *Panorama* 许可证，可以执行任务注册 Panorama 和在 Panorama 虚拟设备连接到互联网时激活/检索防火墙管理许可证。

- 注册 Panorama
- 激活 Panorama 支持许可证
- 在 Panorama 虚拟设备连接到互联网时激活/检索防火墙管理许可证
- 在 Panorama 虚拟设备未连接到互联网时激活/检索防火墙管理许可证
- 在 M 系列设备上激活/检索防火墙管理许可证

注册 Panorama

STEP 1 | 记录下 Panorama 序列号或身份验证代码，并记录下您的销售订单号或客户 ID。

关于身份验证代码、销售订单号或客户 ID，请参阅 Palo Alto Networks 客户服务在您下达 Panorama 订单时发送给您的订单执行电子邮件。

对于序列号，位置取决于型号：

- M 系列设备 — 登录到 Panorama Web 界面，记录下 General Information（一般信息）部分的 **Dashboard**（仪表盘）选项卡中的 **Serial #**（序列号）值。
- Panorama 虚拟设备 — 请参阅订单执行电子邮件。

STEP 2 | 注册 Panorama。步骤取决于您是否已拥有支持站点的登录信息。

- 如果这是您首次注册 Palo Alto Networks 设备，并且您尚未登录：
  1. 转到 Palo Alto Networks 客户支持站点。
  2. 单击页面底部的 **Register**（注册）（**Overview**（概述）> **Get Help**（获取帮助）> **Register**（注册）），输入您的 **Email Address**（电子邮件地址），并输入页面上显示的代码，然后单击 **Submit**（提交）。
  3. 填写 **Create Contact Details**（创建联系人详细信息）部分中的字段。
  4. 输入 **Display Name**（显示名称）、**Confirm Email Address**（确认电子邮件地址）和 **Password/Confirm Password**（密码/确认密码）。
  5. 输入 Panorama **Device Serial Number**（设备序列号）或 **Auth Code**（身份验证代码）。

© 2019 Palo Alto Networks, Inc.

6. 输入您的 **Sales Order Number**（销售订单号）或 **Customer ID**（客户 ID）。
7. 单击 **Submit**（提交）。

- 如果您已经拥有支持帐户：

1. 登录到 Palo Alto Networks 客户支持站点。
2. 单击 **Assets**（资产）> **Devices**（设备）> **Register New Device**（注册新设备）。
3. 选择 **Register device using Serial Number or Authorization Code**（使用序列号或授权代码注册设备），并单击 **Submit**（提交）。
4. 如果 Panorama 管理服务器未与互联网连接，则单击 **Device will be used offline**（设备将离线使用），并选择 **OS Release**（OS 发行）版本。
5. 输入 Panorama **Serial Number**（序列号）。
6. 如果已购买 4 小时的 RMA，则输入所需的位置信息（如星号所示）。
7. **Agree and Submit**（同意并提交）EULA。

   看到注册完成信息后，关闭 Device Registration（设备注册）对话框。

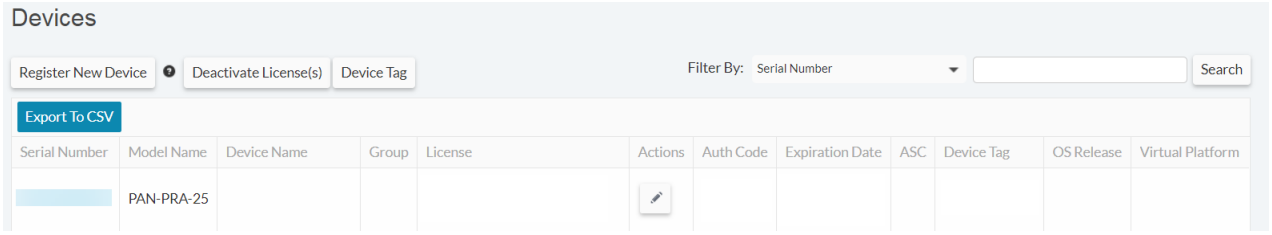
激活 Panorama 支持许可证

在 Panorama M 系列设备或 Panorama 虚拟设备上激活 Panorama 支持许可证之前，您必须注册 Panorama。

如果支持许可证已经过期，*Panorama* 仍可以管理防火墙并收集日志，但软件更新和内容更新将不可用。*Panorama* 上的软件和内容版本必须与受管防火墙上的软件和内容版本相同，或者高于后者，否则会出现错误。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 1 | 登录到 Palo Alto Networks 客户支持门户激活授权代码。

1. 选择 **Assets**（资产）> **Devices**（设备），然后输入您的 Panorama 序列号以按 **Serial Number**（序列号）进行筛选。.



2. 选择 Action（操作）列中的铅笔图标，选择 **Activate Auth-Code**（激活授权代码）并输入您的支持许可证 **Authorization Code**（授权代码），然后单击 **Agree and Submit**（同意并提交）。

STEP 2 | 登录到 Panorama Web 界面，然后选择 **Panorama** > **Support**（支持）> **Activate feature using authorization code**（使用授权代码激活功能）。

STEP 3 | 输入 **Authorization Code**（授权代码），并单击 **OK**（确定）。

STEP 4 | 验证是否已激活订阅。查看页面 Support（支持）部分中的详细信息（例如，**Expiry Date**（到期日期）、支持 **Level**（级别）和 **Description**（说明））。

© 2019 Palo Alto Networks, Inc.

在 Panorama 虚拟设备连接到互联网时激活/检索防火墙管理许可证

为了在 Panorama 上管理设备，您需要激活 PAN-OS 生成的防火墙管理许可证。您激活的设备管理许可证将决定 Panorama 可以管理的设备数量。日志收集器和 WildFire 设备不被视为受管设备，并且不会计入设备管理许可证分配的设备数量。

在 Panorama 虚拟设备上激活和检索防火墙管理许可证之前，您必须注册 Panorama。如果您正在运行评估许可证且希望应用所购买的许可证，则您还必须注册且激活/检索购买的许可证。此外，您必须随后将 Panorama 序列号从评估序列号更改为产品序列号。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 选择 **Panorama** > **Setup** > **Management**（Panorama > 设置 > 管理），然后编辑“General Settings（常规设置）”。

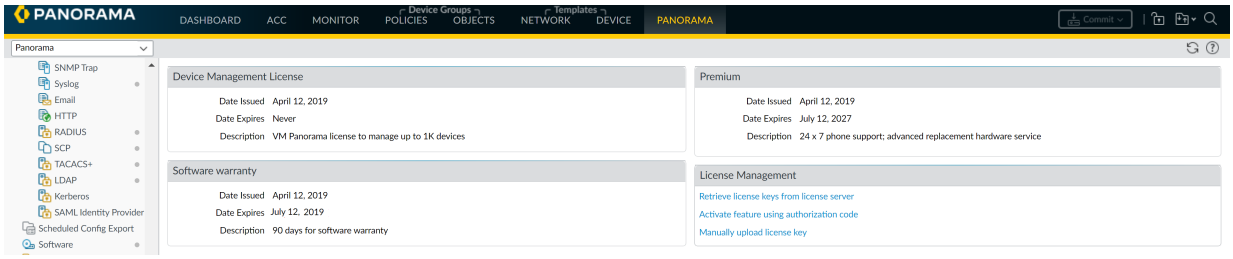
STEP 3 | 输入 Panorama **Serial Number**（序列号）（订单执行电子邮件包含），然后单击 **OK**（确定）。

STEP 4 | 选择 **Panorama** > **Licenses**（许可证）以激活或检索防火墙管理许可证：

- **Retrieve license keys from license server**（从许可证服务器检索许可证密钥）— Panorama 从 Panorama 更新服务器自动检索并激活防火墙管理许可证。
- **Activate feature using authorization code**（使用授权码激活功能）— 输入防火墙管理许可证授权码，然后单击 **OK**（确定）以激活许可证。授权码可从订单履行电子邮件获取，也可通过查找 Panorama 管理服务器登录到 Palo Alto Networks 客户支持网站 来获取。
- **Manually upload license key**（手动上传许可证密钥）— 登录到 Palo Alto Networks 客户支持网站，找到 Panorama 管理服务器，然后下载防火墙管理许可证密钥到您的本地设备。下载许可证密钥后，单击 **Choose File**（选择文件）以选择许可证密钥，然后单击 **OK**（确定）。

STEP 5 | 确认防火墙管理许可证已激活。

此时会出现“设备管理许可证”部分，其中显示内容包括许可证发放日期、许可证到期日期、以及对防火墙管理许可证的描述。



在 Panorama 虚拟设备未连接到互联网时激活/检索防火墙管理许可证

在 Panorama 虚拟设备上激活和检索防火墙管理许可证之前，您必须注册 Panorama。为了在 Panorama 上管理设备，您需要激活设备管理许可证。此设备管理许可证将决定 Panorama 可以管理的设备数量。日志收集器和 WildFire 设备不被视为受管设备，并且不会计入设备管理许可证分配的设备数量。如果您正在运行评估许可证且希望应用所购买的许可证，则您还必须注册且激活/检索购买的许可证。

升级到 PAN-OS 8.1 后，在 Panorama 完成重启后首次登录 Panorama Web 界面时，系统将提示您检索有效的 Panorama 管理许可证。要在 Panorama 虚拟设备离线或无法访问 Palo Alto Networks 更新服务器时激活或检索有效的管理许可证，您必须获取 Panorama 虚拟设备相关的设备信息，并将其上传到客户支持网站。

© 2019 Palo Alto Networks, Inc.

STEP 1 | 登录到 Panorama Web 界面。

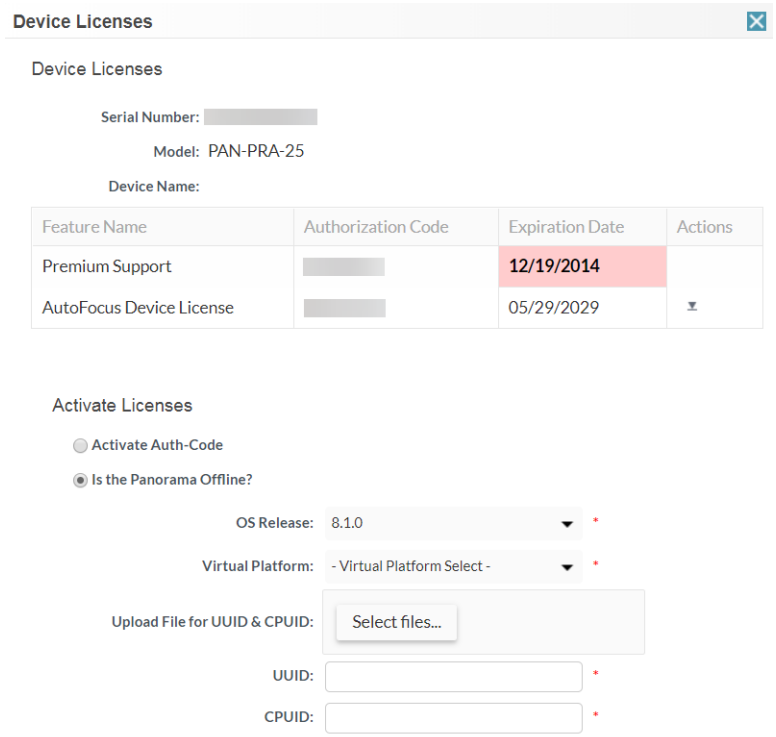
STEP 2 | （仅限初始部署）输入 Panorama **Serial Number**（序列号）。

1. 选择 **Panorama** > **Setup** > **Management**（Panorama > 设置 > 管理），然后编辑“General Settings（常规设置）”。
2. 输入 Panorama **Serial Number**（序列号）（订单执行电子邮件包含），然后单击 **OK**（确定）。
3. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

STEP 3 | 上传 Panorama 虚拟设备信息到客户支持网站。

1. 在“检索管理许可证”对话框中，单击 **here**（此处）链接以收集 UUID、CPUID、Panorama 版本和虚拟平台等信息。单击 **Download Link**（下载链接）下载所需 Panorama 信息的 XML 文件，可上传至客户支持门户。

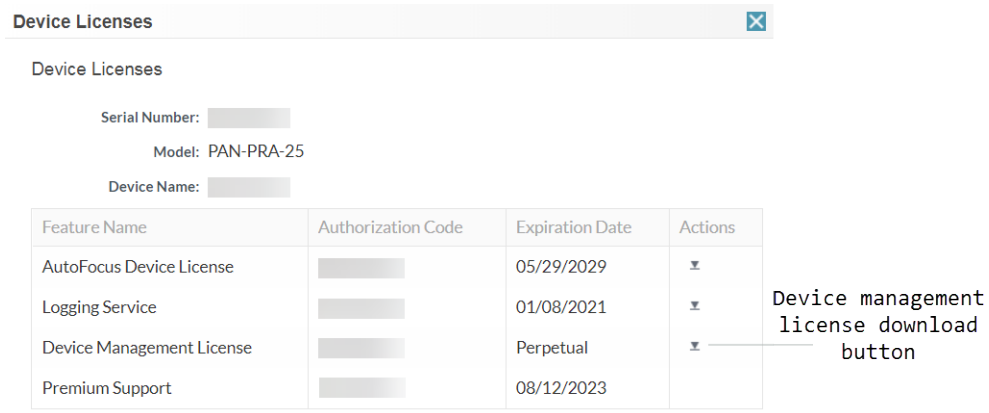
   初始部署时，可能需要注销，并返回到 Web 界面以查看对话框。
2. 登录到 Palo Alto Networks 客户支持站点。
3. 单击右上角的 **Get Support**（获取支持）。
4. 选择 **Assets**（资产）> **Devices**（设备），找到 Panorama 虚拟设备，然后单击操作列中的编辑图标 ()。
5. 选择 **Is the Panorama Offline?**（**Panorama** 是否脱机？），然后输入在步骤 2 中收集的 Panorama 信息，或是单击 **Select files...**（选择文件...）上传所下载的 XML 文件。
6. **Agree and Submit**（同意并提交）EULA。



STEP 4 | 安装设备管理许可证。

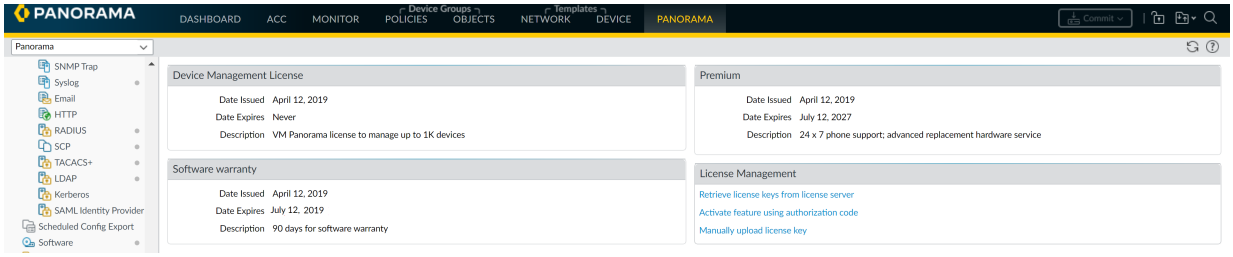
1. 在“操作”列中，下载设备管理许可证。

© 2019 Palo Alto Networks, Inc.



2. 在 Panorama Web 界面中，单击 **Panorama** > **Licenses**（许可证）和 **Manually upload license key**（手动上传许可密钥）。
3. 单击 **Choose file**（选择文件），找到已下载的设备管理许可证密钥，然后单击 **OK**（确定）。

STEP 5 | 通过验证设备管理许可证是否显示许可证信息来确认该设备管理许可证是否已成功上传。



在 M 系列设备上激活/检索防火墙管理许可证

为了在 Panorama 上管理设备，您需要激活容量许可证。此容量许可证将决定 Panorama 可以管理的设备数量。日志收集器和 WildFire 设备不被视为受管设备，且不会计入容量许可证分配的设备数量。

在 M 系列设备上激活和检索 Panorama 防火墙管理许可证之前：

- 注册 Panorama。
- 找到您所购产品/订阅的对应身份验证代码。当您下达订单后，Palo Alto Networks 客户服务会通过电子邮件向您发送与所购买设备相关联的身份验证代码。如果找不到此电子邮件，请联系 Palo Alto Networks 客户支持部门以获取您的授权代码，然后再继续操作。

在激活和检索许可证后，**Panorama** > **Licenses**（Panorama > 许可证）页面会显示相关的发行日期、到期日期和许可证可让 Panorama 管理的防火墙数量。

要激活和检索许可证，可以选择：

- 使用 Web 界面激活和检索许可证。

  如果 Panorama 准备好连接到 Palo Alto Networks 更新服务器（已完成任务执行 M 系列设备的初始配置），但您尚未在 Palo Alto Networks 客户支持网站上激活许可证，可以选择此选项。

  1. 选择 **Panorama** > **Licenses**（Panorama > 许可证），并单击 **Activate feature using authorization code**（使用身份验证代码激活功能）。
  2. 输入 **Authorization Code**（授权代码），并单击 **OK**（确定）。Panorama 检索和激活许可证。

- 从许可证服务器检索许可证密钥。

© 2019 Palo Alto Networks, Inc.

如果 Panorama 没有准备好连接到更新服务器（如尚未完成初始设置 M 系列设备），则可以在 Panorama 准备好连接时在支持网站上激活许可证，然后可以使用 Web 界面检索已激活的许可证。检索已激活的许可证的过程比同时检索和激活的过程更快。

1. 在 Palo Alto Networks 客户支持站点上激活许可证。
    1. 在能够访问互联网的主机上，使用 Web 浏览器访问 Palo Alto Networks 客户支持网站并登录。
    2. 选择 **Assets**（资产）> **Devices**（设备），找到 M 系列设备，然后单击 操作列中的编辑图标 ()。
    3. 选择 **Activate Auth-Code**（激活授权代码），输入 **Authorization Code**（授权代码），然后单击 **Agree and Submit**（同意并提交）以激活许可证。
2. 配置 Panorama 连接到更新服务器：请参阅执行 M 系列设备的初始配置。
3. 选择 **Panorama** > **Licenses**（Panorama > 许可证），并单击 **Retrieve license keys from the license server**（从许可证服务器检索许可证密钥）。Panorama 检索已激活的许可证。

- 手动将许可证从主机上传到 Panorama。Panorama 必须能够访问该主机。

如果已设置 Panorama（已完成任务执行 M 系列设备的初始配置），但没有连接到更新服务器、在支持网站上激活许可证、将许可证下载到已连接到更新服务器的主机，则可以将许可证上传到 Panorama。

1. 从 Palo Alto Networks 客户支持网站激活和下载许可证。
    1. 在能够访问互联网的主机上，使用 Web 浏览器访问 Palo Alto Networks 客户支持网站并登录。
    2. 选择 **Assets**（资产）> **Devices**（设备），找到 M 系列设备，然后单击 操作列中的编辑图标 ()。
    3. 选择 **Activate Auth-Code**（激活授权代码），输入 **Authorization Code**（授权代码），然后单击 **Agree and Submit**（同意并提交）以激活许可证。
    4. 在 Action（操作）列中，单击下载图标并将许可证密钥文件保存到主机。
2. 在 Panorama Web 界面中，选择 **Panorama** > **Licenses**（许可证），单击 **Manually upload license key**（手动上传许可密钥），然后单击 **Browse**（浏览）。
3. 选择要下载到主机的密钥文件，并单击 **Open**（打开）。
4. 单击 **OK**（确定）上传激活的许可证密钥。

© 2019 Palo Alto Networks, Inc.

安装 Panorama 设备证书

在 PAN-OS 9.1.3 和更高版本中，您必须在 Panorama™ 管理服务器上安装设备证书以成功通过 Palo Alto Networks 客户支持门户 (CSP) 对 Panorama 进行身份验证，如此才能利用零接触配置 (ZTP)、设备遥测、IoT 和企业数据丢失防护 (DLP) 等云服务。Panorama 必须能够访问互联网才能成功安装设备证书。

如果您正在使用云服务插件，则必须安装云服务插件 1.5 或更高版本才能成功安装 *Panorama* 设备证书。

STEP 1 | 注册 Panorama通过 Palo Alto Networks 客户支持门户 (CSP)。

STEP 2 | 配置网络时间协议 (NTP) 服务器。

需要 NTP 服务器来验证设备证书到期日期，确保设备证书不会提前过期或失效。

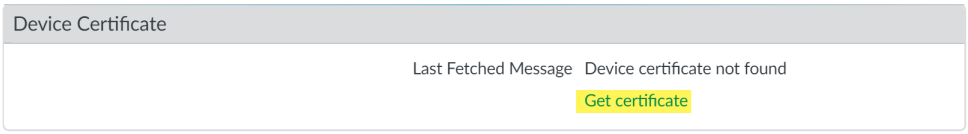
1. 登录到 Panorama Web 界面。
2. 选择 **Panorama** > **Setup**（设置）> **Services**（服务）。
3. 选择 **NTP**，然后输入主机名 `pool.ntp.org` 作为 **Primary NTP Server**（主 **NTP** 服务器）或输入主 NTP 服务器的 IP 地址。
4. （可选）输入 **Secondary NTP Server**（辅助 **NTP** 服务器）地址。
5. （可选）要对 NTP 服务器中的时间更新进行身份验证，对于 **Authentication Type**（身份验证类型），请为每个服务器选择以下其中一个选项。
   - **None**（无）（默认）— 禁用 NTP 身份验证。
   - **Symmetric Key**（对称式密钥）— 防火墙使用对称式密钥交换（共享密钥）对时间更新进行身份验证。
     - **Key ID**（密钥 **ID**）— 输入密钥 ID (1-65534)
     - **Algorithm**（算法）— 选择要用于 NTP 身份验证的算法（**MDS** 或 **SHA1**）
6. 单击 **OK**（确定）保存您的配置更改。
7. 选择 **Commit**（提交）和 **Commit to Panorama**（提交到 **Panorama**）。

STEP 3 | 生成一次性密码 (OTP)。

1. 登录到客户支持门户。
2. 选择 **Assets**（资产）> **Device Certificates**（设备证书）和 **Generate OTP**（生成 **OTP**）。
3. 对于 **Device Type**（设备类型），选择 **Generate OTP for Panorama**（为 **Panorama** 生成 **OTP**）和 **Generate OTP**（生成 **OTP**）。
4. 选择 **Panorama Device**（**Panorama** 设备）序列号。
5. **Generate OTP**（生成 **OTP**）并复制该 OTP。

STEP 4 | 登录到 Panorama Web 界面 作为管理员用户。

STEP 5 | 选择 **Panorama** > **Setup**（设置）> **Management**（管理）> **Device Certificate Settings**（设备证书设置），并 **Get certificate**（获取证书）。



STEP 6 | 输入您之前生成的 **One-time Password**（一次性密码），然后单击 **OK**（确定）。

STEP 7 | Panorama 成功检索和安装证书。

© 2019 Palo Alto Networks, Inc.

Device Certificate	
Current Device Certificate Status	Valid
Not Valid Before	2020/04/01 21:52:28 PDT
Not Valid After	2020/06/30 21:52:28 PDT
Last Fetched Message	Successfully fetched device certificate
Last Fetched Status	success
Last Fetched Timestamp	2020/04/01 22:02:28 PDT

© 2019 Palo Alto Networks, Inc.

安装 Panorama 的内容和软件更新

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。

- Panorama、日志收集器、防火墙和 WildFire 的版本兼容性
- 在高可用性配置中安装 Panorama 更新
- 使用互联网连接安装 Panorama 更新
- 不使用互联网连接安装 Panorama 更新
- 不使用互联网连接自动安装 Panorama 更新
- 将 Panorama 日志迁移到新日志格式

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。将防火墙升级至 PAN-OS 10.0 之前，首先必须将 Panorama 升级至 10.0。

  Panorama 6.1 及更高版本无法将配置推送到运行 *PAN-OS 6.0.0* 至 *PAN-OS 6.0.3* 版本的防火墙。
- 运行 PAN-OS 10.0 的 Panorama 可以管理运行相同或更早 PAN-OS 10.0 版本的 WildFire® 设备和 WildFire 设备群集。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）。

  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。

在高可用性配置中安装 Panorama 更新

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）。

在更新 Panorama 前，请参阅发行说明以了解 PAN-OS 10.0 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：

- 使用互联网连接安装 Panorama 更新
- 未连接互联网时安装 Panorama 更新

© 2019 Palo Alto Networks, Inc.

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 | 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）），单击 **Suspend local Panorama**（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 3 | 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：

- 使用互联网连接安装 Panorama 更新
- 未连接互联网时安装 Panorama 更新

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 4 | 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 5 | （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

使用互联网连接安装 Panorama 更新

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 以高可用性 (HA) 配置运行，请升级每个对端设备上的 Panorama 软件（请参阅为具有高可用性配置的 Panorama 安装更新）。

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，需要您执行使用本地日志收集器设置 Panorama 虚拟设备时所述的其他设置。

PAN-OS® 9.0 已引入了用于本地和专用日志收集器的新日志数据格式。在向 PAN-OS 10.0 升级路径中，现有日志数据会在升级到 PAN-OS 10.0 时自动迁移到新格式。在重新格式化期间，**ACC** 或 **Monitor**（监控）选项卡中不会显示日志数据。此外，在重新格式化未完成之前，新的日志数据不会转发到日志收集器。重新格式化时，会将新日志写入到防火墙系统磁盘，且在此程序成功完成后，新日志会转发到相应的日志收集器。

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 10.0 所需的最低内容发行版本。

对于 Azure 上的 Panorama，您必须先执行其他步骤，然后才能成功升级软件版本。要进行升级，必须导出 Panorama 配置，升级内容和软件版本，并在成功升级后将配置导入到 Panorama 管理服务器。

© 2019 Palo Alto Networks, Inc.

STEP 1 | 验证您计划安装的更新适用于您的 Panorama 部署。

- 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 | 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. **Save named Panorama configuration snapshot**（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）。
2. **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 3 | （根据需要）安装内容更新。



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 9）。

1. **Check Now**（立即检查）（**Panorama** > **Dynamic Updates**（动态更新））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. （根据需要）在更新 Panorama 的内容发布版本前，请确保 升级受管防火墙，然后将日志收集器（请参阅当 Panorama 连接上互联网时升级日志收集器）升级到相同（或更高版本）的内容发布版本。

   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 4 | 确定到 PAN-OS 10.0 的升级路径。

在从当前运行的 PAN-OS 版本升级到 PAN-OS 10.0 的路径中，您无法跳过任何功能发行版本的安装。查看发行说明中的已知问题和对默认行为的更改，以及新功能指南中的升级/降级考虑因素，了解通过其作为升级路径的一部分的每个版本。

（从 7.1 或更早版本升级时需要）PAN-OS 8.0 引入了新的日志存储格式。升级到 PAN-OS 8.0 后，在继续升级之前，必须将 Panorama 日志迁移到新日志格式。日志迁移是一次性任务；如果您已迁移日志收集器上的日志以升级到 PAN-OS 8.0，则无需再次迁移它们。

© 2019 Palo Alto Networks, Inc.



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 5 | 安装 Panorama 10.0。

1. **Check Now**（立即检查）（**Panorama** > **Software**（软件））最新更新。如果有软件版本可用，“操作”列会显示 **Download**（下载）。
2. 找到并 **Download**（下载）您正在升级的发行版本的型号特定文件。例如，要将 M-Series 设备升级到 Panorama 10.0.0，请下载 `Panorama_m-10.0.0` 映像；要将 Panorama 虚拟设备升级到 Panorama 10.0.0，请下载 `Panorama_pc-10.0.0` 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. （在从当前运行的 PAN-OS 版本升级到 PAN-OS 10.0.0 的路径中，您无法跳过任何功能发行版本的安装。）安装下载的映像，然后重启。
   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））。
4. （仅在升级到 PAN-OS 9.1.1 或更高版本时需要）对 PAN-OS 10.0 基本映像完成上述步骤后，请重复步骤 1 至 3 以升级到目标维护版本。

STEP 6 | 成功升级到 PAN-OS 10.0 后，请检查日志格式迁移状态。

1. 登录到 Panorama 命令行界面日志收集器。
2. 运行以下命令以检查日志格式迁移的状态：

```
admin> debug logdb show-es-upgrade-time
```

示例 — 日志格式迁移仍在运行时的响应：

```
Response
from logger 23456212: 50.98% of indices upgraded complete. Approximately
less than a minute remaining until migration is complete. Once the
log migration is complete, please run the 'show log-collector-es-cluster
health' command to check the ElasticSearch cluster status to verify
logging and reporting functionality is restored.
```

日志格式迁移完成后的响应：

```
Response
from logger 23456212: 100% of indices complete. Please run the 'show
log-collector-es-cluster health' command to check the ElasticSearch
cluster status to verify logging and reporting functionality is
restored.
```

3. 日志格式迁移结束后继续进行下一步之前，运行以下命令以检查 ElasticSearch 群集的状态：

```
admin> show log-collector-es-cluster health
```


© 2019 Palo Alto Networks, Inc.

当 ElasticSearch 群集的健康 `status` 显示为 `green`时，可继续进行下一步：

```
admin@Panorama(primary-active)> show log-collector-es-cluster health

{
  "cluster_name" : "__pan_cluster__",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 2,
  "number_of_data_nodes" : 2,
  "active_primary_shards" : 21,
  "active_shards" : 26,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0,
  "task_max_waiting_in_queue_millis" : 0,
  "active_shards_percent_as_number" : 100.0
}
```

STEP 7 | （仅限 Azure 上的 Panorama）从步骤 2 加载导出的 Panorama 配置。

1. **Import named Panorama configuration snapshot**（导入已命名 **Panorama** 配置快照）（**Panorama** > **Setup**（设置）> **Operations**（操作）），**Browse**（浏览）并选择 Panorama 配置文件，然后单击 **OK**（确定）。
2. 单击 **Load named Panorama configuration snapshot**（加载已命名的 **Panorama** 配置快照），选择刚才导入的配置的 **Name**（名称），然后在必要时输入 **Decryption Key**（解密密钥），并单击 **OK**（确定）。
3. 登录到 Panorama 命令行界面。
4. 通过输入以下命令提交 Panorama 配置：

```
admin> configure
```

```
admin> commit force
```

STEP 8 | （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 9 | （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。

© 2019 Palo Alto Networks, Inc.

未连接互联网时安装 Panorama 更新

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 以高可用性 (HA) 配置部署，必须升级每个对端设备（请参阅为具有高可用性配置的 Panorama 安装更新）。

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，需要您执行使用本地日志收集器设置 Panorama 虚拟设备时所述的其他设置。

PAN-OS® 9.0 引入了用于本地和专用日志收集器的新日志数据格式。在向 PAN-OS 10.0 升级路径中，现有日志数据会在升级到 PAN-OS 10.0 时自动迁移到新格式。在重新格式化期间，**ACC** 或 **Monitor**（监控）选项卡中不会显示日志数据。此外，在重新格式化未完成之前，新的日志数据不会转发到日志收集器。重新格式化时，会将新日志写入到防火墙系统磁盘，且在此程序成功完成后，新日志会转发到相应的日志收集器。

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® 10.0 所需的最低内容发行版本。

对于 Azure 上的 Panorama，您必须先执行其他步骤，然后才能成功升级软件版本。要进行升级，必须导出 Panorama 配置，升级内容和软件版本，并在成功升级后将配置导入到 Panorama 管理服务器。

STEP 1 | 验证您计划安装的更新适用于您的 Panorama 部署。

- 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 | 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. **Save named Panorama configuration snapshot**（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）。
2. **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 3 | 确定您需要安装的内容更新。



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。

1. 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。

2. （根据需要）在更新 Panorama 的内容发布版本前，请确保 升级受管防火墙，然后将日志收集器（请参阅当 Panorama 连接上互联网时升级日志收集器）升级到相同（或更高版本）的内容发布版本。

STEP 4 | 确定到 PAN-OS 10.0 的升级路径。

© 2019 Palo Alto Networks, Inc.

在从当前运行的 PAN-OS 版本升级到 PAN-OS 10.0 的路径中，您无法跳过任何功能发行版本的安装。查看发行说明中的已知问题和对默认行为的更改，以及新功能指南中的升级/降级考虑因素，了解通过其作为升级路径的一部分的每个版本。

（从 7.1 或更早版本升级时需要）PAN-OS 8.0 引入了新的日志存储格式。升级到 PAN-OS 8.0 后，在继续升级之前，必须将 Panorama 日志迁移到新日志格式。日志迁移是一次性任务；如果您已迁移日志收集器上的日志以升级到 PAN-OS 8.0，则无需再次迁移它们。



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 5 | （根据需要）将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 | 根据需要安装内容更新。



在安装软件更新之前，必须安装内容更新。 首先，您必须升级防火墙；然后在将其安装到 *Panorama* 管理服务器之前升级日志收集器。

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。

在 Panorama 中（**Panorama** > **Dynamic Updates**（动态更新）），请为每种内容类型执行以下步骤：

1. 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）。
2. 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 7 | 将软件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。

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. 对于升级路径中的第一个（或下一个）Panorama 版本，请确定型号特定文件。例如，要将 M-Series 设备升级到 Panorama 10.0.0，请下载 `Panorama_m-10.0.0` 映像；要将 Panorama 虚拟设备升级到 Panorama 10.0.0，请下载 `Panorama_pc-10.0.0` 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）（*M* 系列设备）或 *Panorama Updates*（*Panorama* 更新）（虚拟设备）快速找到 *Panorama* 映像。
    3. 单击文件名并将文件保存到主机。
    4. 重复上述子步骤 2 以了解升级路径中的任何其他发行版本，如步骤 4 中所述。

© 2019 Palo Alto Networks, Inc.

STEP 8 | 安装 Panorama 10.0。

对于升级路径中的每个版本（从最早版本开始），请执行以下步骤：

1. 单击 Upload（上传）（**Panorama** > **Software**（软件））。
2. **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）。
3. 安装软件映像并重新启动。

   对于高可用性配置，为具有高可用性配置的 Panorama 安装更新；否则：

   1. 安装下载的映像。
   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））。
4. 对路径中的每个版本，请根据需要重复上述步骤 1 至3。

STEP 9 | 成功升级到 PAN-OS 10.0 后，请检查日志格式迁移状态。

1. 登录到 Panorama 命令行界面日志收集器。
2. 运行以下命令以检查日志格式迁移的状态：

```
admin> debug logdb show-es-upgrade-time
```

示例 — 日志格式迁移仍在运行时的响应：

```
Response from logger 23456212: 50.98% of indices upgraded complete.
 Approximately less than a minute remaining until migration is complete.
 Once the log migration is complete, please run the 'show log-collector-
es-cluster health' command to check the ElasticSearch cluster status to
 verify logging and reporting functionality is restored.
```

日志格式迁移完成后的响应：

```
Response from logger 23456212: 100% of indices complete. Please
 run the 'show log-collector-es-cluster health' command to check
 the ElasticSearch cluster status to verify logging and reporting
 functionality is restored.
```

3. 日志格式迁移结束后，在继续下一步之前，运行以下命令以检查 ElasticSearch 群集的状态：

```
admin> show log-collector-es-cluster health
```

当 ElasticSearch 群集的健康 `status` 显示为 `green`时，可继续进行下一步：

© 2019 Palo Alto Networks, Inc.

```
admin@Panorama(primary-active)> show log-collector-es-cluster health

{
  "cluster_name" : "__pan_cluster__",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 2,
  "number_of_data_nodes" : 2,
  "active_primary_shards" : 21,
  "active_shards" : 26,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0,
  "task_max_waiting_in_queue_millis" : 0,
  "active_shards_percent_as_number" : 100.0
}
```

STEP 10 | （仅限 Azure 上的 Panorama）从步骤 2 加载导出的 Panorama 配置。

1. **Import named Panorama configuration snapshot**（导入已命名 **Panorama** 配置快照）（**Panorama** > **Setup**（设置）> **Operations**（操作）），**Browse**（浏览）并选择 Panorama 配置文件，然后单击 **OK**（确定）。
2. 单击 **Load named Panorama configuration snapshot**（加载已命名的 **Panorama** 配置快照），选择刚才导入的配置的 **Name**（名称），然后在必要时输入 **Decryption Key**（解密密钥），并单击 **OK**（确定）。
3. 登录到 Panorama 命令行界面。
4. 通过输入以下命令提交 Panorama 配置：

```
admin> configure
```

```
admin> commit force
```

STEP 11 | （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

不使用互联网连接自动安装 Panorama 更新

自动下载动态更新到物理隔离网络中的防火墙、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，将已连接互联网的 Panorama 配置为自动下载动态更新到 SCP 服务器。将物理隔离 Panorama 配置为根据动态更新计划从 SCP 服务器自动下载并安装动态更新。当可访问互联网的 Panorama 下载动态更新到 SCP 服务器或当物理隔离 Panorama 从 SCP 服务器下载并安装动态更新时，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 的以下动态更新计划：

在将动态更新文件成功下载到 *SCP* 服务器后，不要操作或更改其名称。*Panorama* 不能下载和安装具有已修改文件名称的动态更新。此外，为使自动动态更新成功，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* 均已开启且不在重新启动中。

本示例显示如何为应用程序和威胁动态更新配置自动内容更新。

STEP 1 | 部署一个 SCP 服务器。

© 2019 Palo Alto Networks, Inc.

从已连接互联网的 Panorama 下载受管防火墙、日志收集器和 WildFire 设备的动态更新。物理隔离 Panorama 从 SCP 服务器下载动态更新，然后将更新安装在受管防火墙、WildFire 设备和日志收集器上。



创建用于动态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* 服务器删除的动态更新的可能性。

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，并将动态更新下载到 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。

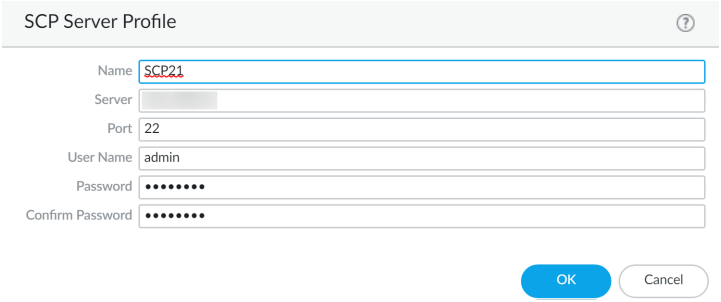
此 Panorama 与 SCP 服务器进行通信，以在受管防火墙、日志收集器和 WildFire 设备上下载并安装动态更新。

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 | 配置已连接互联网的 Panorama 以下载动态更新到 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。

© 2019 Palo Alto Networks, Inc.



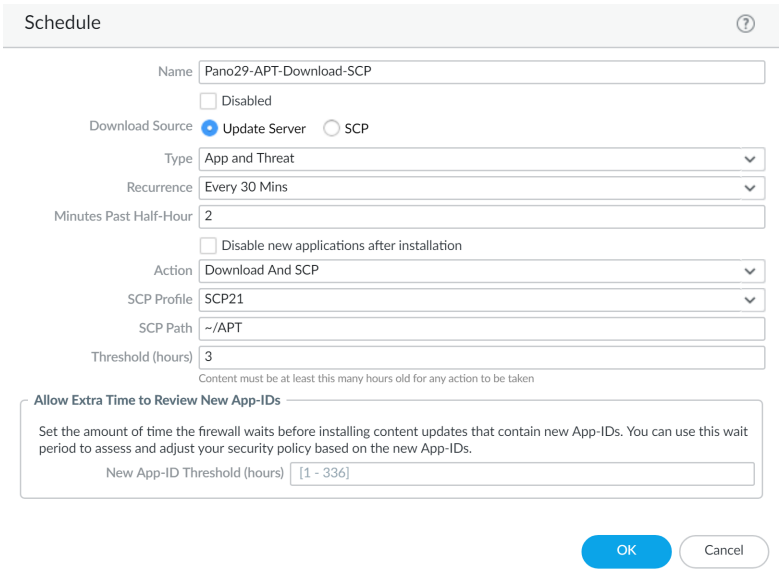
3. 创建动态更新计划，以定期将动态更新下载到 SCP 服务器。

   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 设备上的每种类型动态更新创建计划。

   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）动态更新计划。
   2. 为动态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. 选择动态更新 **Type**（类型）。
   5. 选择 **Recurrence**（重复）以设置 Panorama 检查 Palo Alto Networks 更新服务器查看新动态更新的间隔。

      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动态更新，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. 输入动态更新类型的 **SCP Path**（**SCP** 路径）。
   9. （可选）输入动态更新的 **Threshold**（阈值）（以小时为单位）。Panorama 仅下载达到此存在小时数（或更久）的动态更新
   10. 单击 **OK**（确定）保存更改。

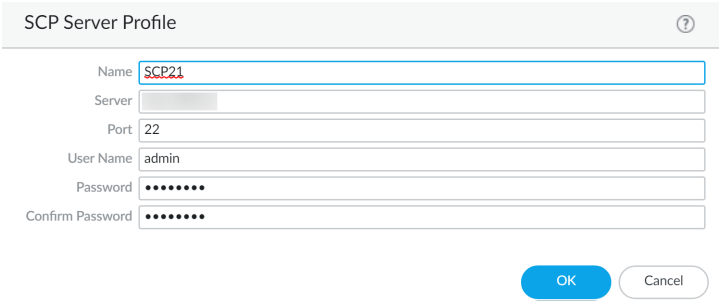


4. **Commit**（提交）更改。

© 2019 Palo Alto Networks, Inc.

STEP 5 | 配置物理隔离 Panorama 以从 SCP 服务器下载动态更新，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. 创建动态更新计划，以定期从 SCP 服务器下载并安装动态更新。

   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 设备上的每种类型动态更新创建计划。

   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）动态更新计划。
   2. 为动态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. 输入动态更新类型的 **SCP Path**（SCP 路径）。
   6. 选择动态更新 **Type**（类型）。
   7. 选择 **Recurrence**（重复）以设置 Panorama 检查 Palo Alto Networks 更新服务器查看新动态更新的间隔。

      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动态更新，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），您必须手动将动态更新安装在受管防火墙上。
   9. 选择要安装动态更新的 **Devices**（设备）。
   10. （可选）输入动态更新的 **Threshold**（阈值）（以小时为单位）。Panorama 仅下载达到此存在小时数（或更久）的动态更新
   11. 单击 **OK**（确定）保存更改。

© 2019 Palo Alto Networks, Inc.



4. **Commit**（提交）更改。

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
```


© 2019 Palo Alto Networks, Inc.

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> 开始
```

- 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> 状态 Slot:
 all
Migration State: In Progress
Percent Complete: 0.04
Estimated Time Remaining: 451 hour(s) 47 min(s)
```

- 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> 停止
```


© 2019 Palo Alto Networks, Inc.

过渡到另一 Panorama 型号

当您的网络要求发生变化时（例如，日志记录速率提高），您可以将 Panorama 管理服务器和专用日志收集器迁移到能够更好地满足这些要求的 Panorama 型号。

- 从 Panorama 虚拟设备迁移到 M 系列设备
- 从 Panorama 虚拟设备迁移到不同的管理程序
- 从 M 系列设备迁移到 Panorama 虚拟设备
- 从 M-100 设备迁移到 M-500 设备

从 Panorama 虚拟设备迁移到 M 系列设备

您可以将 Panorama 配置从 Panorama 虚拟设备迁移到处于 Panorama 模式下的 M 系列设备。但是，您无法迁移日志，因为 Panorama 虚拟设备上的日志格式与 M 系列设备上的日志格式不兼容。因此，如果想要保持对 Panorama 虚拟设备上所存储的旧日志的访问，您必须在迁移完成之后继续运行 Panorama 虚拟设备。M 系列设备将收集防火墙在迁移完成之后所推送的新日志。在迁移前日志过期之后或因为时间推移而失去相关性之后，您可以关闭 Panorama 虚拟设备。

PAN-OS 8.1 或更高版本不再支持传统模式。如果旧 Panorama 虚拟设备处于传统模式，则必须在迁移到新管理程序前将 Panorama 更改为 Panorama 模式，以保留日志设置和日志收集器转发配置。将传统模式下的旧 Panorama 配置导入到 Panorama 模式下的新 Panorama 后，可能会导致所有日志和日志转发设置被删除。

您无法在管理程序之间迁移日志。因此，如果想要保持对旧 Panorama 虚拟设备上所存储的旧日志的访问，您必须在迁移完成之后继续运行旧 Panorama 虚拟设备，并将其添加为新 Panorama 虚拟设备上的受管日志收集器。这样，新 Panorama 虚拟设备可收集防火墙在迁移后转发的新日志，同时保留对旧日志数据的访问。在迁移前日志过期之后或因为时间推移而失去相关性之后，您可以关闭 Panorama 虚拟设备。



如果在专用日志收集器（日志收集器模式下的 *M* 系列设备）上存储防火墙，而不是 *Panorama* 虚拟设备，您可以通过迁移专用日志收集器到 *Panorama* 模式下的 *M* 系列设备来保持日志访问。

STEP 1 | 计划迁移。

- ❑ 如果 M 系列设备要求使用当前软件的更高版本（M-500 设备要求 Panorama 7.0 或更高版本），则在执行迁移之前，应在 Panorama 虚拟设备上升级软件。M-600 和 M-200 设备要求使用 Panorama 8.1 或更高版本）。有关软件版本的重要详细信息，请参阅 Panorama、日志收集器、防火墙和 WildFire 的版本兼容性。
- ❑ 为迁移安排维护时间窗口。虽然防火墙可以在 Panorama 虚拟设备离线后缓冲日志，并在 M 系列设备上线后转发日志，但在维护时间窗口期间完成迁移能够最大限度地降低日志将超过缓冲容量并在 Panoramacom 型号间过渡期间丢失的风险。
- ❑ 考虑在完成对访问现有日志的迁移后是否保留对 Panorama 虚拟设备的访问权限。最有效的方法是，向 Panorama 虚拟设备分配一个新的 IP 地址，并对 M 系列设备重新使用其旧 IP 地址。这样可确保 Panorama 虚拟设备仍然处于可访问状态，且无需您在每一个防火墙上重新配置 Panorama IP 地址，防火墙即可指向 M 系列设备。

STEP 2 | 购买新的 M 系列设备，并将您的订阅迁移到新型号。

1. 购买新的 M 系列设备。
2. 购买新支持许可证和迁移许可证。
3. 在购买新的 M 系列设备时，请先向您的销售代表提供要淘汰的 Panorama 虚拟设备的序列号和设备管理授权码，以及您选择的许可证迁移日期。收到 M 系列设备后，请注册设备，并使用 Palo Alto Networks 提供的迁移和支持授权码激活设备管理和支持许可证。在迁移当日，Panorama 虚拟设备上的设备管理许可证将停用，您无法再使用 Panorama 虚拟设备管理设备或收集日志。但是，支持许

© 2019 Palo Alto Networks, Inc.

可证会被保留，且仍支持 Panorama 设备。您可以在生效日期后完成迁移，但是不能在现已停用的 Panorama 虚拟设备上提交任何配置更改。

STEP 3 | （仅限传统模式）在旧 Panorama 虚拟设备上更改到 Panorama 模式。

要执行此步骤，需要保留 *Panorama* 虚拟设备的日志数据、设置和日志转发配置。如果在传统模式下导出 *Panorama* 配置，这些设置将会丢失。如果未在继续下一步前将 *Panorama* 更改到 *Panorama* 模式，则必须完成步骤9。

如果 *Panorama* 虚拟设备已处于 *Panorama* 或“仅管理”模式，请继续执行下一步。

1. 在 Panorama 模式下设置 Panorama 虚拟设备。
2. 将 Panorama 日志迁移到新日志格式如果想保留旧 Panorama 虚拟设备上现有日志数据。

STEP 4 | 从 Panorama 虚拟设备导出 Panorama 配置。

1. 登录到 Panorama 虚拟设备，然后选择 **Panorama** > **Setup** > **Operations**（Panorama > 设置 > 操作）。
2. 单击 **Save named Panorama configuration snapshot**（保存已命名的 **Panorama** 配置快照），输入 **Name**（名称）以标识该配置，然后单击 **OK**（确定）。
3. 单击 **Export named Panorama configuration snapshot**（导出已命名的 **Panorama** 配置快照），选择您刚才所保存配置的 **Name**（名称），然后单击 **OK**（确定）。Panorama 会向您的客户端系统将配置导出为 XML 文件。

STEP 5 | 如果您不需要在迁移完成之后访问 Panorama 虚拟设备，则关闭其电源，或者如果您需要访问它，则向其管理 (MGT) 接口分配一个新 IP 地址。

若要关闭 Panorama 虚拟设备的电源，请参阅 VMware 产品的文档。

若要在 Panorama 虚拟设备上更改 IP 地址：

1. 选择 **Panorama** > **Setup** > **Management**（Panorama > 设置 > 管理），然后编辑“Management Interface Settings（管理界面设置）”。
2. 输入新 **IP Address**（**IP** 地址），然后单击 **OK**（确定）。
3. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

STEP 6 | 对 M 系列设备执行初始设置。

1. 将 M 系列设备安装到机架上。有关说明，请参阅《M 系列设备硬件参考指南》。
2. 执行 M 系列设备的初始配置以定义激活许可证和安全更新时所需的网络连接。
3. 注册 Panorama。
4. 激活 Panorama 支持许可证。
5. 在 M 系列设备上激活/检索防火墙管理许可证。使用与迁移许可证相关联的身份验证代码。
6. 安装 Panorama 的内容和软件更新。安装与 Panorama 虚拟设备上运行版本相同的版本。

STEP 7 | 加载您从 Panorama 虚拟设备导出到 M 系列设备的 Panorama 配置快照。

1. 在 M 系列设备上，选择 **Panorama** > **Setup**（设置）> **Operations**（操作）。
2. 单击 **Import named Panorama configuration snapshot**（导入已命名 **Panorama** 配置快照），**Browse**（浏览）到您从 Panorama 虚拟设备导出的 Panorama 配置文件，然后单击 **OK**（确定）。
3. 单击 **Load named Panorama configuration snapshot**（加载已命名的 **Panorama** 配置快照），选择刚才导入的配置的 **Name**（名称），选择 **Decryption Key**（解密密钥）（Panorama 的主秘钥），然后单击 **OK**（确定）。Panorama 将使用加载的配置覆盖其当前待选配置。在加载配置文件时，Panorama 会显示任何出现的错误。
4. 如果出现错误，请将错误保存到本地文件中。解决每一个错误，以确保迁移的配置有效。

© 2019 Palo Alto Networks, Inc.

STEP 8 | 在 M 系列设备上修改配置。

如果 M 系列设备将使用不同于 Panorama 虚拟设备的值，则必须执行此项操作。如果您将保持对 Panorama 虚拟设备的访问权限以访问其日志，则应对 M 系列设备使用一个不同的主机名和 IP 地址。

1. 选择 **Panorama** > **Setup**（设置）> **Management**（管理）。
2. 编辑 General Settings（常规设置），修改 **Hostname**（主机名），然后单击 **OK**（确定）。
3. 编辑 Management Interface Settings（管理接口设置），按需要修改值，然后单击 **OK**（确定）。

STEP 9 | 将默认受管收集器和收集器组添加回 M 系列设备。

从 Panorama 虚拟设备加载配置后（步骤 7），会删除每个 M 系列设备上预定义的默认受管收集器和收集器组。

1. 配置受管收集器（该收集器位于 M 系列设备本地）。
2. 为默认受管收集器配置收集器组。
3. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并将更改 **Commit**（提交）到 Panorama 配置。

STEP 10 | 使 M 系列设备与防火墙同步，以继续执行防火墙管理。

在维护窗口时间内完成此步骤，以最大限度地减少网络中断。

1. 在 M 系列设备上，选择 **Panorama** > **Managed Devices**（受管设备），然后验证 Device State（设备状态）列对防火墙显示 **Connected**（已连接）。

   此时，Shared Policy（共享策略）（设备组）和 Template（模板）列对防火墙均显示 **Out of sync**（不同步）。
2. 将更改推送到设备组和模板：
   1. 选择 **Commit**（提交）> **Push to Devices**（推送到设备）和 **Edit Selections**（编辑选择）。
   2. 选择 **Device Groups**（设备组），选择每个设备组，并选择 **Include Device and Network Templates**（包含设备和网络模板），然后单击 **OK**（确定）。
   3. **Push**（推送）您的更改。
3. 在 **Panorama** > **Managed Devices**（受管设备）页面中，验证 Shared Policy（共享策略）和 Template（模板）列均对防火墙显示 **In sync**（同步中）。

从 Panorama 虚拟设备迁移到不同的管理程序

在仅管理模式或 Panorama 模式下，将 Panorama 虚拟设备的 Panorama 配置从一个受支持的管理程序迁移到另一个受支持的管理程序。迁移 Panorama 虚拟设备到新管理程序之前，请查看Panorama 型号，以确保支持您迁移到的新管理程序。此外，如果 Panorama 配置有多个接口（设备管理配置包括用于设备管理、日志收集、收集器组通信、许可和软件更新的多个接口），则查看设置 Panorama 虚拟设备的前提条件，以确认正在迁移到的目标程序文件支持多个接口。

PAN-OS 8.1 或更高版本不再支持传统模式。如果旧 Panorama 虚拟设备处于传统模式，则必须在迁移到新管理程序前将 Panorama 更改为 Panorama 模式，以保留日志设置和日志收集器转发配置。将传统模式下的旧 Panorama 配置导入到 Panorama 模式下的新 Panorama 后，可能会导致所有日志和日志转发设置被删除。

您不能从 Panorama 虚拟设备迁移日志。因此，如果想要保持对旧 Panorama 虚拟设备上所存储日志的访问，您必须在迁移完成之后继续以日志收集器模式运行旧 Panorama 虚拟设备，并将其添加为新 Panorama 虚拟设备上的受管日志收集器。这样，新 Panorama 虚拟设备可收集防火墙在迁移后转发的新日志，同时保留对旧日志数据的访问。在迁移前日志过期之后或因为时间推移而失去相关性之后，您可以关闭 Panorama 虚拟设备。

© 2019 Palo Alto Networks, Inc.

如果在专用日志收集器（日志收集器模式下的 *Panorama* 虚拟设备）上存储防火墙，而不是 *Panorama* 虚拟设备，您可以通过迁移专用日志收集器到 *Panorama* 模式下的 *Panorama* 虚拟设备来保持对日志的访问。

STEP 1 | 计划迁移。

- 如果新的 Panorama 虚拟设备需要使用当前软件的更高版本，迁移前先在 Panorama 虚拟设备上升级软件。WS 和 Microsoft Azure 上的 Panorama 需要 8.1 或更高版本；Google Cloud Platform (GCP) 需要 8.1.1 或更高版本；KVM 和 AWS GovCloud 需要 8.1.2 或更高版本；Hyper-V 需要 8.1.3 或更高版本。有关软件版本的重要详情，请参阅Panorama、日志收集器、防火墙和 WildFire 的版本兼容性。
- 为迁移安排维护时间窗口。虽然防火墙可以在 Panorama 虚拟设备离线后缓冲日志，并在新的 Panorama 虚拟设备上线后转发日志，但在维护时间窗口期间完成迁移能够最大限度地降低日志超过缓冲容量和在管理程序间过渡时丢失的风险。
- 考虑在完成对访问现有日志的迁移后是否保留对旧的 Panorama 虚拟设备的访问权限。最有效的方法是，向旧的 Panorama 虚拟设备分配一个新的 IP 地址，并对 Panorama 虚拟设备重新使用其旧 IP 地址。这样可确保旧的 Panorama 虚拟设备仍然处于可访问状态，且无需您在每一个防火墙上重新配置 Panorama IP 地址，防火墙即可指向新的 Panorama 虚拟设备。

STEP 2 | 购买新的 Panorama 虚拟设备，并将您的订阅迁移到虚拟设备。

1. 购买新的 Panorama 虚拟设备许可证。
2. 购买新支持许可证和迁移许可证。
3. 在购买新的 Panorama 虚拟设备许可证时，请先向您的销售代表提供要淘汰的 Panorama 虚拟设备的序列号和设备管理授权码，以及您选择的许可证迁移日期。新的 Panorama 虚拟设备部署完成后，请注册设备，并使用 Palo Alto Networks 提供的迁移和支持授权码激活设备管理和支持许可证。在迁移当日，旧 Panorama 虚拟设备上的设备管理许可证将停用，您无法再使用旧 Panorama 虚拟设备管理设备或收集日志。但是，支持许可证会被保留，且仍支持 Panorama 设备。您可以在生效日期后完成迁移，但是不能在现已停用的 Panorama 虚拟设备上提交任何配置更改。

STEP 3 | （仅限传统模式）在旧 Panorama 虚拟设备上更改到 Panorama 模式。

要执行此步骤，需要保留 *Panorama* 虚拟设备的日志数据、设置和日志转发配置。如果在传统模式下导出 *Panorama* 配置，这些设置将会丢失。如果未在继续下一步前将 *Panorama* 更改到 *Panorama* 模式，则必须完成步骤 10。

如果 *Panorama* 虚拟设备已处于 *Panorama* 或“仅管理”模式，请继续执行下一步。

1. 在 Panorama 模式下设置 Panorama 虚拟设备。
2. 将 Panorama 日志迁移到新日志格式如果想保留旧 Panorama 虚拟设备上现有日志数据。

STEP 4 | 从旧 Panorama 虚拟设备导出 Panorama 配置。

1. 登录到 Panorama Web 界面。
2. 选择 **Panorama** > **Setup** > **Operations**（Panorama > 设置 > 操作）。
3. 单击 **Save named Panorama configuration snapshot**（保存已命名的 **Panorama** 配置快照），输入 **Name**（名称）以标识该配置，然后单击 **OK**（确定）。
4. 单击 **Export named Panorama configuration snapshot**（导出已命名的 **Panorama** 配置快照），选择您刚才所保存配置的 **Name**（名称），然后单击 **OK**（确定）。Panorama 会向您的客户端系统将配置导出为 XML 文件。

STEP 5 | 如果您不需要在迁移完成之后访问旧 Panorama 虚拟设备，则关闭其电源，或者如果您需要访问它，则向其管理 (MGT) 接口分配一个新 IP 地址。

要关闭 Panorama 虚拟设备电源，请参阅已部署旧 Panorama 虚拟设备的管理程序的受支持文档。

若要在 Panorama 虚拟设备上更改 IP 地址：

© 2019 Palo Alto Networks, Inc.

1. 在旧 Panorama 虚拟设备的 Web 界面，选择**Panorama** > **Setup**（设置） > **Management**（管理），并“编辑管理界面设置”。
2. 输入新 **IP Address**（IP 地址），然后单击 **OK**（确定）。
3. 选择 **Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

STEP 6 | 执行新 Panorama 虚拟设备的初始设置。

1. 设置 Panorama 虚拟设备。
2. 执行 Panorama 虚拟设备的初始配置以定义激活许可证和安装更新所需的网络连接。
3. 注册 Panorama。
4. 激活 Panorama 支持许可证。
5. 在 Panorama 虚拟设备连接到互联网时激活/检索防火墙管理许可证。使用与迁移许可证相关联的身份验证代码。
6. 安装 Panorama 的内容和软件更新。安装与旧 Panorama 虚拟设备上运行版本相同的版本。

STEP 7 | 加载您从旧 Panorama 虚拟设备导出到新 Panorama 虚拟设备的 Panorama 配置快照。

1. 新的 Panorama 虚拟设备的登录到 Panorama Web 界面。
2. 选择 **Panorama** > **Setup** > **Operations**（Panorama > 设置 > 操作）。
3. 单击 **Import named Panorama configuration snapshot**（导入已命名 **Panorama** 配置快照），**Browse**（浏览）到您从 Panorama 虚拟设备导出的 Panorama 配置文件，然后单击 **OK**（确定）。
4. 单击 **Load named Panorama configuration snapshot**（加载已命名的 **Panorama** 配置快照），选择刚才导入的配置的 **Name**（名称），将 **Decryption Key**（解密密钥）留作空白，并单击 **OK**（确定）。Panorama 将使用加载的配置覆盖其当前待选配置。在加载配置文件时，Panorama 会显示任何出现的错误。
5. 如果出现错误，请将错误保存到本地文件中。解决每一个错误，以确保迁移的配置有效。

STEP 8 | 在新 Panorama 虚拟设备上修改配置。

如果新 Panorama 虚拟设备将使用不同于旧 Panorama 虚拟设备的值，则必须执行此项操作。如果您将保持对旧 Panorama 虚拟设备的访问权限以访问其日志，则应对新 Panorama 虚拟设备使用一个不同的主机名和 IP 地址。

部署在 *AWS*、*AWS GovCloud*、*Microsoft Azure* 和 *GCP* 上的 *Panorama* 不支持多接口配置。如果迁移到其中一个管理程序，则必须重新配置设备管理、日志收集、收集器组通信、许可和软件更新，以便在 *MGT* 接口上运行。

1. 选择 **Panorama** > **Setup**（设置） > **Management**（管理）。
2. 编辑 General Settings（常规设置），修改 **Hostname**（主机名），然后单击 **OK**（确定）。
3. 编辑 Management Interface Settings（管理接口设置），按需要修改值，然后单击 **OK**（确定）。

STEP 9 | 将默认受管收集器和收集器组添加到新的 Panorama 虚拟设备。

从旧 Panorama 虚拟设备加载配置后（步骤 7），会在 Panorama 模式下删除每个 Panorama 虚拟设备上预定义的默认受管收集器和收集器组。

1. 配置受管收集器（该收集器位于 Panorama 虚拟设备本地）。
2. 为默认受管收集器配置收集器组。
3. 选择 **Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**），并将更改 **Commit**（提交）到 Panorama 配置。

STEP 10 | （仅限传统模式）如果在传统模式下从 Panorama 虚拟设备导出 Panorama 配置，则配置 Panorama 的日志转发。

© 2019 Palo Alto Networks, Inc.

STEP 11 | 使新 Panorama 虚拟设备与防火墙同步，以继续执行防火墙管理。

在维护窗口时间内完成此步骤，以最大限度地减少网络中断。

1. 在新 Panorama 虚拟设备上，选择 **Panorama** > **Managed Devices**（受管设备），然后确认“设备状态”列对显示防火墙 **Connected**（已连接）。

   此时，Shared Policy（共享策略）（设备组）和 Template（模板）列对防火墙均显示 **Out of sync**（不同步）。
2. 将更改推送到设备组和模板：
   1. 选择 **Commit**（提交）> **Push to Devices**（推送到设备）和 **Edit Selections**（编辑选择）。
   2. 选择 **Device Groups**（设备组），选择每个设备组，并选择 **Include Device and Network Templates**（包含设备和网络模板），然后单击 **OK**（确定）。
   3. **Push**（推送）您的更改。
3. 在 **Panorama** > **Managed Devices**（受管设备）页面中，验证 Shared Policy（共享策略）和 Template（模板）列均对防火墙显示 **In sync**（同步中）。

从 M 系列设备迁移到 Panorama 虚拟设备

您可以将 Panorama 配置从 M-100、 M-200、M-500、 M-600 设备迁移到 Panorama 模式下的 Panorama 虚拟设备。但是，您无法迁移日志，因为 M 系列设备上的日志格式与 Panorama 虚拟设备上的日志格式不兼容。因此，如果要保留对 M 系列设备上存储的旧日志的访问权限，则必须在迁移后继续将 M 系列设备作为专用日志收集器运行，并将其作为 Panorama 虚拟设备添加到受管收集器。

如果 Panorama 管理服务器是高可用性配置的一部分，则必须部署相同管理程序或云环境的第二个 Panorama 虚拟设备，并购买必要的设备管理和支持许可证。有关 HA 要求的完整列表，请参阅 Panorama 高可用性前提条件。

STEP 1 | 计划迁移。

- 在迁移到 Panorama 虚拟设备之前，将 M-Series 设备升级到 PAN-OS 10.0 或更高版本。要升级 Panorama，请参阅安装 Panorama 的内容和软件更新。有关软件版本的重要详细信息，请参阅 Panorama、日志收集器、防火墙和 WildFire 的版本兼容性。
- 为迁移安排维护时间窗口。虽然防火墙可以在 M 系列设备离线后缓冲日志，并在 Panorama 虚拟设备上线后转发日志，但在维护时间窗口期间完成迁移能够最大限度地降低日志在过渡到不同的 Panorama 型号间超过缓冲容量的风险。

STEP 2 | 购买新的 Panorama 虚拟设备的管理和支持许可证。

1. 要购买新的设备管理和支持许可证，请联系您的销售代表。
2. 向您的销售代表提供计划淘汰的 M 系列设备的序列号、您在购买新的 Panorama 虚拟设备时收到的序列号和支持身份验证代码以及您希望完成从旧设备到新虚拟设备迁移的日期。在该迁移日期之前，请在新的虚拟设备上注册序列号并激活支持身份验证代码，这样您才可以开始迁移。旧 M 系列设备上的容量身份验证代码会在您提供的预期迁移完成日期被自动删除。

STEP 3 | 执行 Panorama 虚拟设备的初始设置。

1. 设置 Panorama 虚拟设备。
2. 执行 Panorama 虚拟设备的初始配置以定义激活许可证和安全更新时所需的网络连接。
3. 注册 Panorama。
4. 激活 Panorama 支持许可证。
5. 在 Panorama 虚拟设备连接到互联网时激活/检索防火墙管理许可证
6. 安装 Panorama 的内容和软件更新。安装与 M 系列设备上运行版本相同的版本。

© 2019 Palo Alto Networks, Inc.

STEP 4 | 编辑 M 系列设备 Panorama 接口配置，以仅使用管理界面。

Panorama 虚拟设备仅支持用于设备管理和日志收集的管理界面。

1. 为 M 系列设备登录到 Panorama Web 界面。
2. 选择 **Panorama** > **Setup**（设置）> **Management**（管理）。
3. 编辑 General Settings（常规设置），修改 **Hostname**（主机名），然后单击 **OK**（确定）。
4. 选择 **Interfaces**（接口），然后编辑 **Management**（管理）界面以启用所需服务。
5. 禁用剩余界面的服务。
6. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**）。

STEP 5 | 添加新 Panorama 虚拟设备的 IP 地址。

在 M 系列设备上，添加 Panorama 虚拟设备的公共 IP 地址作为第二个 Panorama 服务器，以管理来自新 Panorama 管理服务器的设备。如果在 AWS、Azure 或 Google™ Cloud Platform 上部署 Panorama 虚拟设备，请使用公共 IP 地址。

1. 选择 **Device**（设备）> **Setup**（设置）。
2. 从模板下拉列表选择包含 Panorama 服务器配置的模板或模板堆栈。
3. 编辑 Panorama 设置。
4. 输入 Panorama 虚拟设备公共 IP 地址，并单击 **OK**（确定）。
5. 选择 **Commit**（提交）> **Commit and Push**（提交并推送）。

STEP 6 | 从 M 系列设备导出配置。

1. 选择 **Panorama** > **Setup** > **Operations**（Panorama > 设置 > 操作）。
2. 单击 **Save named Panorama configuration snapshot**（保存已命名的 **Panorama** 配置快照），输入 **Name**（名称）以标识该配置，然后单击 **OK**（确定）。
3. 单击 **Export named Panorama configuration snapshot**（导出已命名的 **Panorama** 配置快照），选择您刚才所保存配置的 **Name**（名称），然后单击 **OK**（确定）。Panorama 会向您的客户端系统将配置导出为 XML 文件。将配置保存到 Panorama 设备外部的位置。

STEP 7 | 关闭 M 系列设备的电源，或将新的 IP 地址分配给管理(MGT)接口。



如果 *M* 系列设备处于 *Panorama* 模式，且日志存储在需要访问新的 *Panorama* 虚拟设备的本地日志收集器上，则必须更改 *M* 系列设备的 *IP* 地址，以将其作为受管日志收集器添加到 *Panorama* 虚拟设备。

- 关闭 **M** 系列设备：

1. 登录到 Panorama Web 界面。
2. 选择 **Panorama** > **Setup**（设置）> **Operations**（操作），以及单击设备操作下的 **Shutdown Panorama**（关闭 **Panorama**）。单击 **Yes**（是）以确认关闭。

- 在 **M** 系列设备上更改 **IP** 地址：

1. 登录到 Panorama Web 界面。
2. 选择 **Panorama** > **Setup** > **Management**（Panorama > 设置 > 管理），然后编辑“Management Interface Settings（管理界面设置）”。
3. 输入新 **IP Address**（**IP** 地址），然后单击 **OK**（确定）。
4. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

STEP 8 | 加载您从 M 系列设备导出到 Panorama 虚拟设备的 Panorama 配置快照。

1. 登录到 Panorama 虚拟设备的 Panorama Web 界面，然后选择 **Panorama** > **Setup**（设置）> **Operations**（操作）。

© 2019 Palo Alto Networks, Inc.

2. 单击 **Import named Panorama configuration snapshot**（导入已命名 **Panorama** 配置快照），**Browse**（浏览）到您从 M 系列设备导出的 Panorama 配置文件，然后单击 **OK**（确定）。
3. 单击 **Load named Panorama configuration snapshot**（加载已命名的 **Panorama** 配置快照），选择刚才导入的配置的 **Name**（名称），选择 **Decryption Key**（解密密钥）（Panorama 的主秘钥），然后单击 **OK**（确定）。Panorama 将使用加载的配置覆盖其当前待选配置。在加载配置文件时，Panorama 会显示任何出现的错误。

如果出现错误，请将错误保存到本地文件中。解决每一个错误，以确保迁移的配置有效。一旦提交成功，配置就被加载。

STEP 9 | 将 M 系列设备更改为日志收集器模式，以保留现有日志数据。

如果在日志记录磁盘仍插入 *M* 系列设备时更改为日志收集器模式，日志记录数据将被删除。更改模式之前，必须删除日志记录磁盘，以避免日志数据丢失。

生成每个磁盘对的元数据后，需重新构建索引。因此，根据数据大小，此过程需要较长时间才能完成。若要加快这一过程，您可以启动多个 *CLI* 会话并在每一个会话中运行元数据再生命令，为每一个磁盘对同时完成此过程。有关详细信息，请参阅重新生成 M 系列设备 RAID 对的元数据。

1. 从旧 M 系列设备中移除 RAID 磁盘。
   1. 按下电源按钮以关闭 M 系列设备，直到系统关闭。
   2. 移除磁盘对。有关详细信息，请参阅《M 系列设备硬件参考指南》中的磁盘更换程序。
2. 按下电源按钮以打开 M 系列设备。
3. 配置 `admin`（管理员）超级用户管理员帐户。

   如果 `admin`（管理员）管理员帐户已创建，那么继续下一步。

   必须在切换到“日志收集器”模式之前创建具有超级用户权限的 *admin*（管理员）帐户，否则在切换模式之后您将失去对 *M* 系列设备的访问权限。
4. 为旧的 M 系列设备登录到 Panorama CLI。
5. 从 Panorama 模式切换到日志收集器模式。
   - 要切换到日志收集器模式，请输入以下命令：

     ```
     > request system system-mode logger
     ```
   - 输入 **Y** 确认模式更改。M 系列设备重新启动。如果重新启动进程终止了终端模拟软件会话，重新连接 M 系列设备以查看 Panorama 登录提示。

     如果您看到 ***CMS Login***（*CMS* 登录）提示，这意味着日志收集器没有完成重新启动。看到提示时按 *Enter* 键，而不输入用户名或密码。
   - 重新登录至此 CLI。
   - 验证切换到日志收集器模式是否成功：

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

     如果模式更改成功，输出显示：

     ```
     > system-mode: logger
     ```
6. 将磁盘插入到旧的 M 系列设备。有关详细信息，请参阅《M 系列设备硬件参考指南》中的磁盘更换程序。

© 2019 Palo Alto Networks, Inc.

您必须维持磁盘对的关联。尽管您可以把磁盘对从 A1/A2 插槽置入到 B1/B2 插槽，但您必须保持磁盘对处于同一插槽中；否则，Panorama 可能无法成功地恢复数据。

7. 为每个磁盘对运行以下 CLI 命令即可启用磁盘对：

```
> request system raid add <slot> force no-format
```

例如：

```
> request system raid add A1 force no-format
> request system raid add A2 force no-format
```

Force 和 **no-format** 是必需的命令参数。**Force** 参数使磁盘对与新设备相关联。**No-format** 参数则防止驱动器的重新格式化，并保留存储在磁盘上的日志。

8. 生成每个磁盘对的元数据。

```
> request metadata-regenerate slot <slot_number>
```

例如：

```
> request metadata-regenerate slot 1
```

9. 启用日志收集器和 Panorama 管理服务器之间的连接。

在日志收集器 CLI 中输入以下命令，*<IPaddress1>* 是单独（非高可用性）或主动（高可用性）Panorama 的 MGT 接口，*<IPaddress2>* 是被动（高可用性）Panorama 的 MGT 接口（如适用）。

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

STEP 10 | 使 Panorama 虚拟设备与防火墙同步，以继续执行防火墙管理。

在维护窗口时间内完成此步骤，以最大限度地减少网络中断。

1. 在 Panorama 虚拟设备上，选择 **Panorama** > **Managed Devices**（受管设备），然后验证设备状态列对防火墙显示 **Connected**（已连接）。

此时，Shared Policy（共享策略）（设备组）和 Template（模板）列对防火墙均显示 **Out of sync**（不同步）。

2. 将更改推送到设备组和模板：
   1. 选择 **Commit**（提交）> **Push to Devices**（推送到设备）和 **Edit Selections**（编辑选择）。
   2. 选择 **Device Groups**（设备组），选择每个设备组，并选择 **Include Device and Network Templates**（包含设备和网络模板）。
   3. 选择 **Collector Groups**（收集器组），选择每个收集器组，然后单击 **OK**（确定）。
   4. **Push**（推送）您的更改。
3. 在 **Panorama** > **Managed Devices**（受管设备）页面中，验证 Shared Policy（共享策略）和 Template（模板）列均对防火墙显示 **In sync**（同步中）。

© 2019 Palo Alto Networks, Inc.

STEP 11 | （仅限 HA）设置 Panorama HA 对端设备。

如果 Panorama 管理服务器处于高可用性配置，请执行 HA 对端设备上的步骤。

1. 执行 Panorama 虚拟设备的初始设置。
2. 编辑 M 系列设备 Panorama 接口配置，以仅使用管理界面。
3. 添加新 Panorama 虚拟设备的 IP 地址。
4. 关闭 M 系列设备的电源，或将新的 IP 地址分配给管理(MGT)接口。
5. 将 M 系列设备更改为日志收集器模式，以保留现有日志数据。

STEP 12 | （仅限 HA）修改 Panorama 虚拟设备 HA 对端设备配置。

1. 在 HA 对端设备上， 登录到 Panorama Web 界面，选择 **Panorama** > **High Availability**（高可用性），然后编辑 **Setup**（设置）。
2. 在 **Peer HA IP Address**（对端设备高可用性 **IP** 地址）字段中，输入对端设备的新 IP 地址，然后单击 **OK**（确定）。
3. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改
4. 在高可用性对端设备的其他对端设备上重复这些步骤 。

STEP 13 | （仅限 HA）同步 Panorama 对端设备。

1. 访问其中一个高可用性对端设备上的 **Dashboard**（仪表盘），然后选择 **Widgets**（小部件）> **System**（系统）> **High Availability**（高可用性）以显示高可用性小部件。
2. **Sync to peer**（同步到对端设备），单击 **Yes**（是），然后等待 **Running Config**（运行配置）显示 **Synchronized**（已同步）。
3. 访问剩余高可用性对端设备上的 **Dashboard**（仪表盘），然后选择 **Widgets**（小部件）> **System**（系统）> **High Availability**（高可用性）以显示高可用性小部件。
4. 确认 **Running Config**（运行配置）显示 **Synchronized**（已同步）。

从 M-100 设备迁移到 M-500 设备

您可以将 Panorama 配置和防火墙日志从 M-100 设备迁移到 Panorama 模式下的 M-500 设备（Panorama 管理服务器）。您也可以将防火墙日志从 M-100 设备迁移到日志收集器模式下的 M-500 设备（专用日志收集器）。因为同一个收集器组中的所有日志收集器必须为相同 Panorama 型号，所以您必须迁移任何收集器组中的所有 M-100 系列设备，或者不迁移其中任何一个设备。

在以下程序中，Panorama 管理服务器部署在主动/被动高可用性 (HA) 配置中，您将迁移配置以及日志，而 M-500 设备将重新使用来自 M-100 设备的 IP 地址。



此程序将假定您不再使用 *M-100* 执行设备管理或日志收集。如果您计划将已停用的 *M-100* 设备用作专用日志收集器，则 *M-100* 需要提供设备管理许可证。如果没有设备管理许可证，您将无法将 *M-100* 用作专用日志收集器。

如果您不打算将 *M-100* 设备用作专用日志收集器，但 *M-100* 设备中包含您在以后必须访问的日志数据，则可以使用现有日志数据进行查询，并生成报告。*Palo Alto Networks* 推荐在停用 *M-100* 设备前查阅日志保留策略。



如果您将仅迁移日志而不是 *Panorama* 配置，则执行将日志迁移到日志收集器模式下的新 M 系列设备或将日志迁移到 Panorama 模式下的新 M 系列设备下的任务。

如果要迁移到未在高可用性配置中部署，且新的 *Panorama* 必须访问现有专用日志收集器上的日志的新 *Panorama* 管理服务器，执行任务非高可用性 Panorama 发生故障/RMA 时迁移日志收集器。

STEP 1 | 计划迁移。

© 2019 Palo Alto Networks, Inc.

- 如果 M-100 设备的当前版本早于 7.0，则在该设备上升级软件；M-500 设备要求使用 Panorama 7.0 或更高版本。有关软件版本的重要详细信息，请参阅 Panorama、日志收集器、防火墙和 WildFire 的版本兼容性。
- 如果您希望保留 Panorama 和日志收集器在迁移之前向外部目标生成的系统和配置日志，则转发系统和配置日志。Panorama 模式下的 M 系列设备将这些类型的日志存储在其 SSD 上，而您无法在型号之间移动其 SSD。您只能移动 RAID 驱动器，后者将存储防火墙日志。
- 为迁移安排维护时间窗口。虽然防火墙可以在 M-100 设备离线后缓冲日志，并在 M-500 设备上线后转发日志，但在维护时间窗口期间完成迁移能够最大限度地降低日志将超过缓冲容量并在 Panoramacom 型号间过渡期间丢失的风险。

STEP 2 | 购买新的 M-500 设备，并将您的订阅迁移到新型号。

1. 购买新的 M-500 设备。
2. 购买新支持许可证和迁移许可证。
3. 在购买新的 M-500 设备时，请先向您的销售代表提供要淘汰的 1-100 设备的序列号和设备管理授权码，以及您选择的许可证迁移日期。收到 M-500 设备后，请注册设备，并使用 Palo Alto Networks 提供的迁移和支持授权码激活设备管理和支持许可证。在迁移当日，M-100 设备上的设备管理许可证将停用，您无法再使用 M-100 设备管理设备或收集日志。但是，支持许可证会被保留，且仍支持 Panorama 设备。您可以在生效日期后完成迁移，但不能在现已停用的 M-100 设备上提交任何配置更改。

STEP 3 | 从 Panorama 模式下的每一个 M-100 设备导出 Panorama 配置。

在每一个 M-100 设备高性能对端设备上执行此任务：

1. 登录到 M-100 设备，然后选择 **Panorama** > **Setup**（设置）> **Operations**（操作）。
2. 单击 **Save named Panorama configuration snapshot**（保存已命名的 **Panorama** 配置快照），输入 **Name**（名称）以标识该配置，然后单击 **OK**（确定）。
3. 单击 **Export named Panorama configuration snapshot**（导出已命名的 **Panorama** 配置快照），选择您刚才所保存配置的 **Name**（名称），然后单击 **OK**（确定）。Panorama 会向您的客户端系统将配置导出为 XML 文件。

STEP 4 | 关闭每一个 Panorama 模式下的 M-100 设备的电源。

1. 登录到您将要关闭电源的 M-100 设备高可用性对端设备。
2. 选择 **Panorama** > **Setup** > **Operations**（Panorama > 设置 > 操作），然后单击 **Shutdown Panorama**（关闭 Panorama）。

STEP 5 | 对每个 M-500 设备执行初始设置。

1. 将 M-500 设备安装到机架上。有关说明，请参阅《M-500 设备硬件参考指南》。
2. 执行 M 系列设备的初始配置以定义激活许可证和安全更新时所需的网络连接。
3. 注册 Panorama。
4. 激活 Panorama 支持许可证。
5. 激活防火墙管理许可证。使用与迁移许可证相关联的身份验证代码。
6. 安装 Panorama 的内容和软件更新。安装与 M-100 设备上运行版本相同的版本。
7. （仅限专用日志收集器）将 M 系列设备设为日志收集器。

STEP 6 | 将您从 M-100 设备导出的 Panorama 配置快照加载到 Panorama 模式下的每一个 M-500 设备（两个高可用性对端设备）。

在每一个 M-500 设备高性能对端设备上执行此任务：

1. 登录到 M-500 设备，然后选择 **Panorama** > **Setup**（设置）> **Operations**（操作）。

© 2019 Palo Alto Networks, Inc.

2. 单击 **Import named Panorama configuration snapshot**（导入已命名的 **Panorama** 配置快照），**Browse**（浏览）到您从与 M-500 设备具有相同高可用性优先级（主要或辅助）的 M-100 设备导出的配置文件，然后单击 **OK**（确定）。
3. 单击 **Load named Panorama configuration snapshot**（加载已命名的 **Panorama** 配置快照），选择刚才导入的配置的 **Name**（名称），选择 **Decryption Key**（解密密钥）（Panorama 的主秘钥），然后单击 **OK**（确定）。Panorama 将使用加载的配置覆盖其当前待选配置。在加载配置文件时，Panorama 会显示任何出现的错误。如果出现错误，请将错误保存到本地文件中。解决每一个错误，以确保迁移的配置有效。
4. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），然后选择 **Validate Commit**（验证提交）。在继续操作之前，解决任何错误。
5. 将更改 **Commit**（提交）到 Panorama 配置。

STEP 7 | 在 Panorama 模式下的 M-500 设备高可用性对端设备之间同步配置。

1. 在主动 M-500 设备上，选择 **Dashboard**（仪表盘）选项卡，然后在 High Availability（高可用性）小部件中，单击 **Sync to peer**（同步到对端设备）。
2. 在 High Availability（高可用性）小部件中，验证 **Local**（本地）（主要 M-500 设备）处于 **active**（主动）状态，**Peer**（对端设备）处于被动状态，**Running Config**（运行配置）处于 **synchronized**（已同步）状态。

STEP 8 | 将 RAID 驱动器从各 M-100 设备移动到其替用的 M-500 设备，以迁移从防火墙收集的日志。

在以下任务中，跳过任何您已经在 M-500 设备上完成的步骤。

- 将日志迁移到 Panorama 模式下的新 M 系列设备。从 M-100 设备迁移日志，但只限于在 M-100 设备将默认受管收集器用于日志收集时。
- 将日志迁移到日志收集器模式下的新 M 系列设备。

STEP 9 | 使 Panorama 模式下的 M-500 设备与防火墙同步，以继续执行防火墙管理。

在维护窗口时间内完成此步骤，以最大限度地减少网络中断。

1. 在主动 M-500 设备中，选择 **Panorama** > **Managed Devices**（受管设备），然后验证 Device State（设备状态）列对防火墙显示 **Connected**（已连接）。

   此时，Shared Policy（共享策略）（设备组）和 Template（模板）列对防火墙均显示 **Out of sync**（不同步）。
2. 将更改推送到设备组和模板：
   1. 选择 **Commit**（提交）> **Push to Devices**（推送到设备）和 **Edit Selections**（编辑选择）。
   2. 选择 **Device Groups**（设备组），选择每个设备组，并选择 **Include Device and Network Templates**（包含设备和网络模板），然后单击 **OK**（确定）。
   3. **Push**（推送）您的更改。
3. 在 **Panorama** > **Managed Devices**（受管设备）页面中，验证 Shared Policy（共享策略）和 Template（模板）列均对防火墙显示 **In sync**（同步中）。

© 2019 Palo Alto Networks, Inc.

访问和导航 Panorama 管理界面

Panorama 提供了三个管理界面：

- **Web** 界面 — Panorama Web 界面的外观与防火墙 Web 界面类似。如果您已经非常熟悉防火墙，则能够轻松导航和完成管理任务，以及从 Panorama Web 界面生成报告。此图形界面使您能够使用 HTTPS 访问 Panorama，并且这是执行管理任务的最佳方式。请参阅登录到 Panorama Web 界面和导航 Panorama Web 界面。如果需要启用 HTTP 访问 Panorama，可以编辑 **Panorama** > **Setup** > **Management**（Panorama > 设置 > 管理）选项卡上的“Management Interface Settings（管理界面设置）”。
- 命令行界面 **(CLI)** — CLI 是一个简约的界面，允许您快速输入命令，以完成一系列任务。CLI 支持两种命令模式 — 操作和配置，同时每个均有其自己的命令和状态层级。熟悉命令的嵌套结构和语法后，CLI 允许快速响应，提供高效的管理。请参阅登录到 Panorama 命令行界面。
- **XML API** — 基于 XML 的 API 作为一种使用 HTTP/HTTPS 请求和响应而执行的 Web 服务提供。它使您能够简化操作并与现有内部开发的应用程序和存储库进行整合。了解有关使用 Panorama API 的详细信息，请参阅《PAN-OS 和 Panorama XML API 使用指南》。

登录到 Panorama Web 界面

STEP 1 | 启动互联网浏览器，使用安全连接 (https://<IP address>) 输入 Panorama IP 地址。

STEP 2 | 根据帐户使用的身份验证类型登录 Panorama。如果首次登录 Panorama，请使用默认值 **admin** 作为用户名和密码。

- **SAML** — 单击 **Use Single Sign-On**（使用单点登录）(SSO)。如果 Panorama 为管理员执行授权（角色分配），请输入您的 **Username**（用户名）并 **Continue**（继续）。如果 SAML 标识提供商 (IdP) 执行授权，直接 **Continue**（继续），无需输入 **Username**（用户名）。在这两种情况下，Panorama 都将重定向到 IdP，提示您输入用户名和密码。对 IdP 进行身份验证后，将显示Panorama Web 界面。
- 任何其他类型的身份验证 — 输入您的用户 **Name**（名称）和 **Password**（密码）。如果登录页面有横幅和复选框，请阅读登录横幅并选择 **I Accept and Acknowledge the Statement Below**（我接受并确认以下陈述）。然后单击 **Login**（登录）。

STEP 3 | 阅读并 **Close**（关闭）当日任何消息。

导航 Panorama Web 界面

使用 Panorama Web 界面配置 Panorama，管理和监视防火墙、日志收集器、WildFire 设备和设备群集，并通过 **Context**（上下文）下拉菜单访问每个防火墙的 Web 界面。有关每个 Web 界面选项卡中选项和字段的详细信息，请参阅 Panorama 的在线帮助。以下是对选项卡的概述：

选项卡	说明
仪表盘	查看有关 Panorama 型号和网络访问设置的一般信息。该选项卡包含显示有关应用程序、日志、系统资源和系统设置的信息的小部件。
ACC	根据 Panorama 从受管防火墙收集的信息，查看网络的整体风险和威胁级别。
监视	查看和管理日志和报告。

© 2019 Palo Alto Networks, Inc.

选项卡	说明
Device Groups（设备组）> **Policies**（策略）	创建集中策略规则，将它们应用到多个防火墙/设备组。 您必须为要显示的此选项卡 添加设备组。
Device Groups（设备组）> **Objects**（对象）	定义策略规则可以引用的以及受管防火墙/设备组可以共享的策略对象。 您必须为要显示的此选项卡 添加设备组。
Templates（模板）> **Network**（网络）	配置可应用于多个防火墙的网络设置（如网络配置文件）。 您必须为要显示的此选项卡 添加模板。
Templates（模板）> **Device**（设备）	配置可应用于多个防火墙的设备设置（如服务器配置文件和管理角色）。 您必须为要显示的此选项卡 添加模板。
Panorama	配置 Panorama，管理许可证，设置高可用性，访问软件更新和安全警告，管理管理性访问权限，以及管理已部署的防火墙、日志收集器、WildFire 设备和设备群集。

登录到 Panorama 命令行界面

您可以使用串行端口连接登录到 Panorama 命令行界面，或使用安全外壳 (SSH) 客户端远程访问它。

- 使用 SSH 登录 Panorama CLI。

  相同的说明适用于日志收集器模式下的 M 系列设备。

  （可选）您可以针对命令行界面为管理员配置基于 SSH 密钥的身份验证。

  1. 请确保符合以下前提条件：
     - 您有可访问 Panorama 网络的计算机。
     - 您知道 Panorama IP 地址。
     - 管理接口支持 SSH，这是默认设置。如果管理员已禁用 SSH 且您要重新启用它：选择 **Panorama** > **Setup**（设置）> **Interfaces**（接口），单击 **Management**（管理），选择 **SSH**，单击 **OK**（确定），选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），然后将更改 **Commit**（提交）到 Panorama 配置。
  2. 要使用 SSH 访问 CLI：
     1. 在 SSH 客户端中输入 Panorama IP 地址并使用端口 22。
     2. 在出现提示时，输入您的管理访问凭据。登录后，会显示当日消息，之后是处于操作模式的 CLI 提示符。例如：

        ```
        admin@ABC_Sydney>
        ```

- 使用串行端口连接登录 Panorama CLI。
  1. 确保具备下列条件：
     - 通过 DB-9 串行端口将 Panorama 连接到计算机的非调制解调器串行电缆
     - 在计算机上运行的终端模拟程序

© 2019 Palo Alto Networks, Inc.

2. 在终端模拟软件中使用以下设置进行连接：9600 波特、8 个数据位、1 个停止位、无奇偶校验、无硬件流控制。
3. 在出现提示时，输入您的管理访问凭据。登录后，会显示 message of the day（当日消息），之后是处于操作模式的 CLI 提示符。

- **转换到配置配置模式。**

  若要切换到配置模式，请在收到提示时输入以下命令：

```
admin@ABC_Sydney> configure
```

  提示更改为 `admin@ABC_Sydney#`。

© 2019 Palo Alto Networks, Inc.

设置 Panorama 的管理访问权限

Panorama 实施基于角色的访问控制 (RBAC)，使您能够指定管理员的权限和责任。以下主题介绍了如何创建管理员角色、访问域和帐户来访问 Panorama Web 界面和命令行界面 (CLI)：

- 配置管理角色配置文件
- 配置访问域
- 配置管理帐户和身份验证

配置管理角色配置文件

管理角色配置文件为自定义 管理角色，它们可让您定义细化的管理访问特权，从而确保对敏感公司信息和最终用户隐私的保护。最佳的做法是，创建仅允许管理员访问执行其工作时所需管理界面的区域的管理角色配置文件。

STEP 1 | 配置防火墙管理员角色配置文件。

您必须在防火墙上创建管理员角色配置文件，并将其分配到 Panorama 管理服务器管理员角色配置文件，以允许管理员在 Panorama 和受管防火墙 Web 界面之间进行上下文切换。

STEP 2 | 选择 **Panorama** > **Admin Roles**（Panorama > 管理角色），然后单击 **Add**（添加）。

STEP 3 | 输入配置文件的 **Name**（名称），然后选择 **Role**（角色）类型：**Panorama** 或设备组和模板。

STEP 4 | 通过切换图标至所需的设置，配置对 Panorama（**Web UI**（**Web** 用户界面））和防火墙（**Context Switch UI**（上下文切换用户界面））的各个功能区域的访问权限。“启用（读写）”、“只读”或“禁用”。



如果具有自定义角色将向受管防火墙提交设备组或模板更改，则您必须给予这些角色对 *Panorama* > *Device Groups*（*Panorama* > 设备组）和 *Panorama* > *Templates*（*Panorama* > 模板）的读写访问权限。如果您从较早的 *Panorama* 版本进行升级，则升级过程会提供对这些节点的只读访问权限。

您无法通过 Panorama 角色下的上下文切换特权来管理对防火墙 CLI 或 XML API 的访问权限。

STEP 5 | 如果 **Role**（角色）类型为 **Panorama**，则通过切换每一个功能区域的“已启用/已禁用”图标，配置对 **XML API** 的访问权限。

STEP 6 | 如果 **Role**（角色）类型为 **Panorama**，则为 **Command Line**（命令行）界面选择访问级别：**None**（无）（默认）、**superuser**（超级用户）、**superreader**（超级读者）或 **panorama-admin**（**Panorama** 管理员）。

STEP 7 | 要启用上下文切换，请选择您在步骤 1 中创建的 **Device Admin Role**（设备管理员角色）。

STEP 8 | 单击 **OK**（确定）保存配置文件。

配置访问域

使用访问域以定义设备组和模板管理员对特定设备组和模板的访问权限，并控制这些管理员切换上下文至受管防火墙 Web 界面的能力。Panorama 最多支持 4,000 个访问域。

STEP 1 | 选择 **Panorama** > **Access Domain**（Panorama > 访问域），然后单击 **Add**（添加）。

© 2019 Palo Alto Networks, Inc.

STEP 2 | 输入 **Name**（名称）以标识访问域。

STEP 3 | 为 **Shared Objects**（共享对象）选择访问权限：

- **write**（写入）— 管理员可以在共享对象上执行所有操作。这是默认值。
- **Read**（读取）— 管理员可以在共享对象上执行显示和克隆操作，但无法执行其他操作。当添加非共享对象或克隆共享对象时，目标必须为访问域内而非共享位置内的设备组。
- **shared-only**（仅共享）— 管理员只能将对象添加至共享位置。管理员可以显示、编辑和删除共享对象，但无法移动或克隆它们。

选择此选项的后果是，管理员无法对非共享对象执行除显示以外的任何操作。您可能会选择此选项的典型原因之一是，组织要求所有对象都处于一个单独的全局性存储库中。

STEP 4 | 切换 **Device Groups**（设备组）选项卡中的图标，以启用对访问域中设备组的读写访问权限或只读访问权限。

如果您将对 *Shared Objects*（共享对象）的访问权限设置为 *shared-only*（仅共享），则 *Panorama* 会将只读访问权限应用于您为其指定了读写访问权限的任何设备组中的对象。

STEP 5 | 选择 **Templates**（模板）选项卡，然后 **Add**（添加）您想要分配到访问域中的每一个模板。

STEP 6 | 选择 **Device Context**（设备上下文）选项卡，选择将份额分配到访问域中的防火墙，然后单击 **OK**（确定）。管理员可以通过在 Panorama 中使用 **Context**（上下文）下拉列表来访问这些防火墙的 Web 界面。

配置管理帐户和身份验证

如果您已经配置身份验证配置文件或不需要身份验证配置文件对管理员进行身份验证，则可以准备配置 Panorama 管理员帐户。或者，您可以执行以下列出的其中一项其他流程，配置管理账户已进行特定类型的身份验证。

- 配置 Panorama 管理员帐户
- 为 Panorama 管理员配置本地或外部身份验证
- 针对 Web 界面为 Panorama 管理员配置基于证书的身份验证
- 针对命令行界面为管理员配置基于 SSH 密钥的身份验证
- 为 Panorama 管理员配置 RADIUS 身份验证
- 为 Panorama 管理员配置 TACACS+ 身份验证
- 为 Panorama 管理员配置 SAML 身份验证

配置 *Panorama* 管理员帐户

管理帐户指定 Panorama 管理员的管理角色和身份验证。用于分配角色和执行身份验证的服务决定是否在 Panorama、外部服务器或两者上添加帐户（请参阅管理身份验证）。对于外部身份验证服务，您必须在添加管理帐户之前配置身份验证配置文件（请参阅配置管理帐户和身份验证）。如果您已经配置身份验证配置文件或将使用 Panorama 的本地身份验证机制，请执行以下步骤在 Panorama 上添加管理帐户。

您无法将管理员帐户添加到专用日志收集器（日志收集器模式下的 *M* 系列设备）。只有具备默认用户名 *(admin)* 的预定义管理员帐户可以在专用日志收集器上使用。

STEP 1 | 选择 **Panorama** > **Administrators**（管理员），并 **Add**（添加）帐户。

STEP 2 | 输入管理员的用户 **Name**（名称）。

STEP 3 | 如果为管理员配置其中之一，请选择 **Authentication Profile**（身份验证配置文件）或序列。

© 2019 Palo Alto Networks, Inc.

如果 Panorama 将使用 Kerberos SSO 或外部服务来执行身份验证，则需要身份验证配置文件。

如果 Panorama 将使用本地认证，则将 **Authentication Profile**（身份验证配置文件）设置为 **None**（无），输入 **Password**（密码），然后 **Confirm Password**（确认密码）。

STEP 4 | 选择 **Administrator Type**（管理员类型）：

- **Dynamic**（动态）— 选择预定义管理员角色。
- **Custom Panorama Admin**（自定义 **Panorama** 管理员）— 选择您为该管理员创建的管理角色 **Profile**（配置文件）（请参阅配置管理角色配置文件）。
- **Device Group and Template Admin**（设备组和模板管理员）— 按照下一步所述将访问域映射到管理角色。

STEP 5 | （仅限设备组和模板管理员）在 Access Domain to Administrator Role（将访问域映射到管理员角色）部分中，单击 **Add**（添加），从下拉列表中选择访问域（请参阅配置访问域），单击相邻的管理员角色单元格，然后选择管理员角色配置文件。

STEP 6 | 单击 **OK**（确定）保存更改。

STEP 7 | 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

为 *Panorama* 管理员配置本地或外部身份验证

您可以使用外部身份验证服务或本地 Panorama 服务对访问 Panorama 的管理员进行身份验证。这些身份验证方法提示管理员响应一个或多个身份验证质询，例如输入用户名和密码的登录页面。



如果您使用外部服务来管理身份验证和授权（角色和访问域分配），请参阅：

- 为 Panorama 管理员配置 RADIUS 身份验证
- 为 Panorama 管理员配置 TACACS+ 身份验证
- 为 Panorama 管理员配置 SAML 身份验证

要在没有质询-响应机制的情况下对管理员进行身份验证，您可以针对 Web 界面为 Panorama 管理员配置基于证书的身份验证和针对命令行界面为管理员配置基于 SSH 密钥的身份验证。

STEP 1 | （仅限外部身份验证）将 Panorama 与外部服务器相连接，以对管理员身份进行验证。

1. 选择 **Panorama** > **Server Profiles**（服务器配置文件），选择服务类型（**RADIUS**、**TACACS+**、**SAML**、**LDAP** 或 **Kerberos**），然后配置服务器配置文件：
   - 为 Panorama 管理员配置 RADIUS 身份验证。

     您可以使用 *RADIUS* 服务器来支持 *RADIUS* 身份验证服务或多重因素身份验证 (MFA) 服务。

   - 为 Panorama 管理员配置 TACACS+ 身份验证。
   - 添加 SAML IdP 服务器配置文件。您不能将 Kerberos 单点登录 (SSO) 与 SAML SSO 组合；您只能使用一种类型的 SSO 服务。
   - 添加 Kerberos 服务器配置文件。
   - 添加 LDAP 服务器配置文件。

STEP 2 | （可选）如果 Panorama 使用本地身份验证，则定义密码复杂性和到期设置。

这些设置增加了攻击者得到密码的难度，从而有助于防止 Panorama 的未授权访问。

© 2019 Palo Alto Networks, Inc.

1. （确定所有本地管理员帐户的全局密码复杂性和过期设置。

    1. 选择 **Panorama** > **Setup**（设置）> **Management**（管理），然后编辑最低密码复杂性设置。
    2. 选择 **Enabled**（启用）。
    3. 定义密码设置并单击 **OK**（确定）。
2. 定义密码配置文件。

    将配置文件分配给要覆盖全局密码到期设置的管理员帐户。

    1. 选择 **Panorama** > **Password Profiles**（密码配置文件），**Add**（添加）配置文件。
    2. 输入 **Name**（名称）以标识配置文件。
    3. 定义密码过期设置并单击 **OK**（确定）。

STEP 3 | （仅限 Kerberos SSO）创建 Kerberos 密钥表。

密钥表是包含 Panorama 的 Kerberos 帐户信息的文件。要支持 Kerberos SSO，您的网络必须具有 Kerberos 基础架构。

STEP 4 | 配置身份验证配置文件。



如果您的管理帐户存储在多种类型的服务器上，您可以为每种类型的服务器创建一个身份验证配置文件，并将所有配置文件添加到身份验证序列。

在身份验证配置文件中，指定身份验证服务的 **Type**（类型）和相关设置：

- 外部服务 — 选择外部服务器 **Type**（类型），然后选择您为其创建的 **Server Profile**（服务器配置文件）。
- 本地身份验证 — 将 **Type**（类型）设置为 **None**（无）。
- **Kerberos SSO** — 指定 **Kerberos Realm**（**Kerberos** 域）并 **Import**（导入）创建的 **Kerberos Keytab**（**Kerberos** 密钥表）。

STEP 5 | （仅限设备组和模板管理员）配置访问域。

配置一个或多个访问域。

STEP 6 | （仅限自定义角色）配置管理角色配置文件。

配置一个或多个管理角色配置文件。

对于自定义 Panorama 管理员，配置文件定义帐户的访问权限。对于设备组和模板管理员，配置文件为与帐户相关联的一个或多个访问域定义访问权限。

STEP 7 | 配置管理员。

1. 配置 Panorama 管理员帐户。

    - 分配您配置的 **Authentication Profile**（身份验证配置文件）或序列。
    - （仅限设备组和模板管理员）将访问域映射到管理角色配置文件。
    - （仅限本地身份验证）如果您已配置身份验证配置文件，请选择 **Password Profile**（密码配置文件）。
2. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。
3. （可选）测试身份验证服务器连接，验证 Panorama 是否可以使用身份验证配置文件来对管理员进行身份验证。

© 2019 Palo Alto Networks, Inc.

针对 *Web* 界面为 *Panorama* 管理员配置基于证书的身份验证

作为一种比基于密码的面向 Panorama Web 界面的身份验证更加安全的替代性方案，您可以为处于 Panorama 本地的管理员帐户配置基于认证的身份验证。基于证书的身份验证执行数字签名（而非密码）的交换和验证。

对任何管理员配置基于证书的身份验证将禁用所有管理员在 *Panorama* 上的用户名/密码登录，因此所有管理员随后必须使用证书才能登录。

STEP 1 | 在 Panorama 上生成证书签发结构 (CA) 证书。

您将使用该 CA 证书对每个管理员的客户端证书进行签名。

创建自签名根 CA 证书。

或者，您也可以从您的企业 *CA* 导入证书。

STEP 2 | 配置确保对 Web 界面进行安全访问所用的证书配置文件。

1. 选择 **Panorama** > **Certificate Management** > **Certificate Profile**（Panorama > 证书管理 > 证书配置文件），然后单击 **Add**（添加）。
2. 输入证书配置文件的 **Name**（名称），然后将 **Username Field**（用户名字段）设置为 **Subject**（主题）。
3. 在 CA Certificates（CA 证书）部分中选择 **Add**（添加），然后选择您刚才创建的 **CA Certificate**（**CA** 证书）。
4. 单击 **OK**（确定）保存配置文件。

STEP 3 | 将 Panorama 配置为使用证书配置文件来验证管理员的身份。

1. 选择 **Panorama** > **Setup** > **Management**（Panorama > 设置 > 管理），然后编辑“Authentication Settings（身份验证设置）”。
2. 选择您刚才创建的 **Certificate Profile**（证书配置文件），然后单击 **OK**（确定）。

STEP 4 | 配置管理员帐户使用客户端证书身份验证。

配置 Panorama 管理员帐户为每一个将访问 Panorama Web 界面的管理员。勾选 **Use only client certificate authentication (Web)**（仅使用客户端证书身份验证 **(Web)**）复选框。

如果您已经部署企业 CA 生成的客户端证书，请跳转至步骤 8。否则，继续执行步骤 5。

STEP 5 | 为每个管理员生成客户端证书。

在 Panorama 上生成证书。在 **Signed By**（签名者）下拉列表中，选择您创建的 CA 证书。

STEP 6 | 导出客户端证书。

1. 导出证书。
2. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

   Panorama 将重新启动，然后终止您的登录会话。此后，管理员只能从使用您生成的客户端证书的客户端系统对 Web 界面进行访问。

STEP 7 | 将客户端证书导入到要访问 Web 界面的每个管理员的客户端系统。

根据需要参阅您的 Web 浏览器文档以完成此步骤。

STEP 8 | 验证管理员是否可以对 Web 界面进行访问。

© 2019 Palo Alto Networks, Inc.

1. 在具有客户端证书的计算机上的浏览器中，打开 Panorama IP 地址。
2. 收到提示时，选择您导入的证书，然后单击 **OK**（确定）。浏览器随即显示证书警告。
3. 将该证书添加到浏览器异常列表。
4. 单击 **Login**（登录）。会显示 Web 界面，不提示您输入用户名或密码。

针对命令行界面为管理员配置基于 *SSH* 密钥的身份验证

对使用安全外壳 (SSH) 来访问 Panorama CLI 的管理员而言，SSH 密钥提供了一种比密码更安全的身份认证方法。SSH 密钥几乎消除了暴力攻击风险，提供了双重身份验证选项（私钥和口令），不用通过网络发送密码。SSH 密钥还会启用自动化脚本对 CLI 进行访问。

STEP 1 | 使用 SSH 密钥生成工具，在管理员的客户端系统上创建非对称密钥对。

支持的密钥格式为 IETF SECSH 和开放式 SSH。支持的算法为 DSA（1024 位）和 RSA（768-4096 位）。

有关生成密钥对的命令，请参阅您的 SSH 客户端文档。

公钥和私钥是两个分开的文件。将两者保存到 Panorama 可以访问的位置。为了增强安全性，请输入加密私钥的口令。Panorama 会在管理员登录时提示其输入此密码。

STEP 2 | 配置管理员帐户使用公钥身份验证。

1. 配置 Panorama 管理员帐户。
   - 配置两种身份验证方法之一，以将其用作 SSH 密钥身份验证失败时的应急方案：

     外部身份验证服务 — 选择 **Authentication Profile**（身份验证配置文件）。

     本地身份验证 — 将 **Authentication Profile**（身份验证配置文件）设置为 **None**（无），输入 **Password**（密码），然后 **Confirm Password**（确认密码）。
   - 勾选 **Use Public Key Authentication (SSH)**（使用公钥身份验证 **(SSH)**）复选框，单击 **Import Key**（导入密钥），**Browse**（浏览）到您刚才生成的公钥，然后单击 **OK**（确定）。
2. 单击 **OK**（确定）保存管理帐户。
3. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

STEP 3 | 配置 SSH 客户端以使用私钥向 Panorama 进行身份验证。

在管理员的客户端系统上执行这项任务。根据需要参阅您的 SSH 客户端文档以完成此步骤。

STEP 4 | 验证该管理员可以使用 SSH 密钥身份验证访问 Panorama CLI。

1. 使用管理员客户端系统上的浏览器，转到 Panorama IP 地址。
2. 以管理员的身份登录到 Panorama CLI。输入用户名后，您会看到以下输出内容（以密钥值为例）：

   ```
   Authenticating with public key “dsa-key-20130415”
   ```
3. 如果收到提示，请输入您在创建密钥时定义的密码。

为 *Panorama* 管理员配置 *RADIUS* 身份验证

您可以使用 RADIUS 服务器来验证 Panorama Web 界面的管理访问权限。您也可以在 RADIUS 服务器上定义供应商特定属性 (VSA) 来管理管理员授权。使用 SAML 使您能够通过目录服务来快速更改管理员的角色、访问域和用户组，这通常比在 Panorama 上重新配置设置更为容易。



您可以使用 RADIUS 服务器来验证 *Panorama Web* 界面的管理访问权限。您也可以在 *RADIUS* 服务器上定义供应商特定属性 (VSA) 来管理管理员授权。使用 *SAML* 使您能够通过目录服务来快速更改管理员的角色、访问域和用户组，这通常比在 *Panorama* 上重新配置设置更为容易。

© 2019 Palo Alto Networks, Inc.

您可以将 Palo Alto Networks RADIUS 词典导入到 *RADIUS* 服务器，以定义实现 *Panorama* 和 *RADIUS* 服务器之间通信的身份验证属性。

您还可以使用 *RADIUS* 为管理员实施多重因素身份验证 (MFA)。

STEP 1 | 添加 RADIUS 服务器配置文件。

配置文件定义 Panorama 如何连接到 RADIUS 服务器。

1. 选择 **Panorama** > **Server Profiles**（服务器配置文件）> **RADIUS**，并 **Add**（添加）配置文件。
2. 输入 **Profile Name**（配置文件名称）以标识服务器配置文件。
3. 输入身份验证请求超时后以秒为单位的 **Timeout**（超时）（默认为 3；范围为 1-20）。



如果您使用服务器配置文件将 *Panorama* 与 *MFA* 服务进行集成，请输入能够让管理员拥有足够的时间对身份验证质询做出响应的时间间隔。例如，如果 *MFA* 服务提示输入一次性密码 *(OTP)*，则管理员需要时间查看其端点设备上的 *OTP*，然后在 *MFA* 登录页面输入 *OTP*。

4. 选择 Panorama 用来对 RADIUS 服务器进行身份验证的 **Authentication Protocol**（身份验证协议）（默认为 **CHAP**）。



如果 *RADIUS* 服务器支持该协议，请选择 *CHAP*；该协议比 *PAP* 更安全。

5. **Add**（添加）每个 RADIUS 服务器，并输入以下内容：
   - 输入标识服务器的 **Name**（名称）
   - **RADIUS Server**（**RADIUS** 服务器）IP 地址或 FQDN。
   - **Secret**（密钥）/**Confirm Secret**（确认密钥）（加密用户名和密码的密钥）
   - 用于身份验证请求的服务器 **Port**（端口）（默认为 1812）
6. 单击 **OK**（确定）保存服务器配置文件。

STEP 2 | 将 RADIUS 服务器配置文件分配到身份验证配置文件。

身份验证配置文件定义了一组管理员通用的身份验证设置。

1. 选择 **Panorama** > **Authentication Profile**（身份验证配置文件），并 **Add**（添加）配置文件。
2. 输入 **Name**（名称）以标识身份验证配置文件。
3. 将 **Type**（类型）设置为 **RADIUS**。
4. 选择您配置的 **Server Profile**（服务器配置文件）。
5. 选择 **Retrieve user group from RADIUS**（从 **RADIUS** 中检索用户组），以从 RADIUS 服务器上定义的 VSA 收集用户组信息。

   Panorama 与您在身份验证配置文件允许列表中指定的组在组信息方面进行匹配。
6. 选择 **Advanced**（高级），并在允许列表中 **Add**（添加）允许使用此身份验证配置文件进行身份验证的管理员。
7. 单击 **OK**（确定）保存身份验证配置文件。

STEP 3 | 配置 Panorama 以便为所有管理员使用身份验证配置文件。

1. 选择 **Panorama** > **Setup**（设置）> **Management**（管理），然后编辑身份验证设置。
2. 选择您配置的 **Authentication Profile**（身份验证配置文件），然后单击 **OK**（确定）。

STEP 4 | 配置为管理员定义授权设置的角色和访问域。

1. 如果管理员使用自定义角色而不是预先定义（动态）角色，请配置管理员角色配置文件。
2. 如果管理员使用设备组和模板角色，则配置访问域。

STEP 5 | 提交更改。

© 2019 Palo Alto Networks, Inc.

选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

STEP 6 | 配置 RADIUS 服务器。

有关执行以下步骤的具体说明，请参阅 RADIUS 服务器文档：

1. 添加作为 RADIUS 客户端的 Panorama IP 地址或主机名。
2. 添加管理员帐户。

   如果 *RADIUS* 服务器配置文件将 *CHAP* 指定为 *Authentication Protocol*（身份验证协议），则必须使用可逆加密密码定义帐户。否则，*CHAP* 身份验证将失败。
3. 定义 Panorama 的供应商代码 (25461)，并为每个管理员的角色、访问域和用户组定义 RADIUS VSA。

   预定义用户的动态管理员角色时，使用小写字母指定角色（例如，输入 **`superuser`**，而不是 **`SuperUser`**）。

STEP 7 | 验证 RADIUS 服务器是否为管理员执行身份验证和授权。

1. 使用您添加到 RADIUS 服务器的管理员帐户登录 Panorama Web 界面。
2. 验证您是否只能访问与管理员关联的角色允许的 Web 界面页面。
3. 在 **Monitor**（监控）、**Policies**（策略）和 **Objects**（对象）选项卡中，验证您是否只能访问与管理员关联的访问域允许的设备组。

为 *Panorama* 管理员配置 *TACACS+* 身份验证

您可以使用 TACACS+ 服务器来验证 Panorama Web 界面的管理访问权限。您也可以在 TACACS+ 服务器上定义供应商特定属性 (VSA) 来管理管理员授权。使用 SAML 使您能够通过目录服务来快速更改管理员的角色、访问域和用户组，这通常比在 Panorama 上重新配置设置更为容易。

STEP 1 | 添加 TACACS+ 服务器配置文件。

配置文件定义 Panorama 如何连接到 TACACS+ 服务器。

1. 选择 **Panorama** > **Server Profiles**（服务器配置文件）> **TACACS+**，并 **Add**（添加）配置文件。
2. 输入 **Profile Name**（配置文件名称）以标识服务器配置文件。
3. 输入身份验证请求超时后以秒为单位的 **Timeout**（超时）（默认为 3；范围为 1-20）。
4. 选择 Panorama 用来对 TACACS+ 服务器进行身份验证的 **Authentication Protocol**（身份验证协议）（默认为 **CHAP**）。

   如果 *TACACS+* 服务器支持该协议，请选择 *CHAP*；该协议比 *PAP* 更安全。
5. **Add**（添加）每个 TACACS+ 服务器，并输入以下内容：
   - 输入标识服务器的 **Name**（名称）
   - **TACACS+ Server**（**TACACS+** 服务器）IP 地址或 FQDN
   - **Secret**（密钥）/**Confirm Secret**（确认密钥）（加密用户名和密码的密钥）
   - 用于身份验证请求的服务器 **Port**（端口）（默认为 49）
6. 单击 **OK**（确定）保存服务器配置文件。

STEP 2 | 将 TACACS+ 服务器配置文件分配到身份验证配置文件。

身份验证配置文件定义了一组管理员通用的身份验证设置。

1. 选择 **Panorama** > **Authentication Profile**（身份验证配置文件），并 **Add**（添加）配置文件。
2. 输入 **Name**（名称）以标识配置文件。
3. 将 **Type**（类型）设置为 **TACACS+**。

© 2019 Palo Alto Networks, Inc.

4. 选择您配置的 **Server Profile**（服务器配置文件）。
5. 选择 **Retrieve user group from TACACS+**（从 **TACACS+** 中检索用户组），以从 TACACS+ 服务器上定义的 VSA 收集用户组信息。

   Panorama 与您在身份验证配置文件允许列表中指定的组在组信息方面进行匹配。
6. 选择 **Advanced**（高级），并在允许列表中 **Add**（添加）允许使用此身份验证配置文件进行身份验证的管理员。
7. 单击 **OK**（确定）保存身份验证配置文件。

STEP 3 | 配置 Panorama 以便为所有管理员使用身份验证配置文件。

1. 选择 **Panorama** > **Setup**（设置）> **Management**（管理），然后编辑身份验证设置。
2. 选择您配置的 **Authentication Profile**（身份验证配置文件），然后单击 **OK**（确定）。

STEP 4 | 配置为管理员定义授权设置的角色和访问域。

1. 如果管理员将使用自定义角色而不是预先定义（动态）角色，请配置管理角色配置文件。
2. 如果管理员使用设备组和模板角色，则配置访问域。

STEP 5 | 提交更改。

选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

STEP 6 | 配置 TACACS+ 服务器对管理员进行身份验证和授权。

有关执行以下步骤的具体说明，请参阅 TACACS+ 服务器文档：

1. 添加作为 TACACS+ 客户端的 Panorama IP 地址或主机名。
2. 添加管理员帐户。

   如果您选择将 *CHAP* 指定为 *Authentication Protocol*（身份验证协议），则必须使用可逆加密密码定义帐户。否则，*CHAP* 身份验证将失败。
3. 为每个管理员的角色、访问域和用户组定义 TACACS+ VSA。

   预定义用户的动态管理员角色时，使用小写字母指定角色（例如，输入 ***superuser***，而不是 ***SuperUser***）。

STEP 7 | 验证 TACACS+ 服务器是否为管理员执行身份验证和授权。

1. 使用您添加到 TACACS+ 服务器的管理员帐户登录 Panorama Web 界面。
2. 验证您是否只能访问与管理员关联的角色允许的 Web 界面页面。
3. 在 **Monitor**（监控）、**Policies**（策略）和 **Objects**（对象）选项卡中，验证您是否只能访问与管理员关联的访问域允许的虚拟系统。

为 *Panorama* 管理员配置 *SAML* 身份验证

您可以使用 安全声明标记语言 (SAML) 2.0 来验证 Panorama Web 界面（但不是 CLI）的管理访问权限。您还可以使用 SAML 属性来管理管理员授权。SAML 属性使您能够通过目录服务（而不是重新配置 Panorama 上的设置）来快速更改管理员的角色、访问域和用户组。

要配置 SAML 单点登录 (SSO) 和单点退出 (SLO)，必须注册 Panorama 和标识提供商 (IdP)，以实现相互之间的通信。如果 IdP 提供包含注册信息的元数据文件，可将其导入 Panorama 以注册 IdP 并创建 IdP 服务器配置文件。服务器配置文件定义如何连接到 IdP，并指定 IdP 用于签署 SAML 消息的证书。您还可以为 Panorama 使用证书来签署 SAML 消息。可以使用证书，也可以不使用证书，但建议确保 Panorama 和 IdP 之间的通信安全。

STEP 1 | （推荐）获取 IdP 和 Panorama 将用于签署 SAML 消息的证书。

© 2019 Palo Alto Networks, Inc.

如果证书没有指定密钥使用属性，默认情况下允许所有用法，包括签名消息。在这种情况下，可以通过任何方法获取证书。

如果证书明确指定密钥使用属性，则其中一个属性必须为数字签名，该属性在 Panorama 上生成的证书不可用。在这种情况下，必须导入证书：

- **Panorama** 用于签署 **SAML** 消息的证书 — 从企业证书颁发机构 (CA) 或第三方 CA 导入证书。
- **IdP** 用于签署 **SAML** 消息的证书 — 从 IdP 导入包含证书的元数据文件（请参阅下一步）。IdP 证书仅限于以下算法：
  - 公钥算法 — RSA（1,024 位或更大）和 ECDSA（所有大小）。
  - 签名算法 — SHA1、SHA256、SHA384 和 SHA512。

STEP 2 | 添加 SAML IdP 服务器配置文件。

服务器配置文件将 IdP 注册到 Panorama，并定义连接方式。

在此示例中，从 IdP 导入 SAML 元数据文件，以便 Panorama 能够自动创建服务器配置文件并填充连接、注册和 IdP 证书信息。



如果 *IdP* 不提供元数据文件，请选择 *Panorama* > *Server Profiles*（服务器配置文件）> *SAML Identity Provider*（*SAML* 标识提供商），*Add*（添加）服务器配置文件，并手动输入信息（请咨询您的 *IdP* 管理员了解有关值的信息）。

1. 将 SAML 元数据文件从 IdP 导出到 Panorama 可以访问的客户端系统。

   文件中指定的证书必须符合上述步骤中列出的要求。有关导出文件的说明，请参阅您的 IdP 文档。
2. 选择 **Panorama** > **Server Profiles**（服务器配置文件）> **SAML Identity Provider**（**SAML** 标识提供商），并将元数据文件 **Import**（导入）到 Panorama 中。
3. 输入 **Profile Name**（配置文件名称）以标识服务器配置文件。
4. **Browse**（浏览）到 **Identity Provider Metadata**（标识提供商元数据）文件。
5. （推荐）选择 **Validate Identity Provider Certificate**（验证标识提供商证书）（默认），让 Panorama 验证 **Identity Provider Certificate**（标识提供商证书）。

   只有在将服务器配置文件分配给身份验证配置文件并 **Commit**（提交）后，才会进行验证。Panorama 使用身份验证配置文件中的 **Certificate Profile**（证书配置文件）来验证证书。

   验证证书是提高安全性的最佳实践。
6. 输入 **Maximum Clock Skew**（最大时钟偏差），这是 Panorama 验证 IdP 消息时，IdP 与 Panorama 的系统时间之间允许的差异（以秒为单位）（默认为 60；范围为 1 到 900）。如果差异超过该值，则身份验证失败。
7. 单击 **OK**（确定）保存服务器配置文件。
8. 单击服务器配置文件名称以显示配置文件设置。验证导入的信息是否正确，并在必要时进行编辑。

STEP 3 | 配置身份验证配置文件。

身份验证配置文件指定 SAML IdP 服务器配置文件并定义身份验证过程的选项，例如 SLO。

1. 选择 **Panorama** > **Authentication Profile**（身份验证配置文件），并 **Add**（添加）配置文件。
2. 输入 **Name**（名称）以标识配置文件。
3. 将 **Type**（类型）设置为 **SAML**。
4. 选择您配置的 **IdP Server Profile**（**IdP** 服务器配置文件）。
5. 选择 **Certificate for Signing Requests**（签名请求证书）。

   Panorama 使用此证书对发送给 IdP 的消息进行签名。
6. （可选）**Enable Single Logout**（启用单点退出）（默认情况下禁用）。

© 2019 Palo Alto Networks, Inc.

7. 选择 Panorama 将用于验证 **Identity Provider Certificate**（标识提供商证书）的 **Certificate Profile**（证书配置文件）。
8. 输入 IdP 消息用于标识用户的 **Username Attribute**（用户名属性）（默认为 **username**（用户名））。

   预定义用户的动态管理员角色时，使用小写字母指定角色（例如，输入 ***superuser***，而不是 ***SuperUser***）。如果您通过 *IdP* 标识存储管理管理员授权，还请指定 *Admin Role Attribute*（管理员角色属性）和 *Access Domain Attribute*（访问域属性）。
9. 选择 **Advanced**（高级），并 **Add**（添加）允许使用此身份验证配置文件进行身份验证的管理员。
10. 单击 **OK**（确定）保存身份验证配置文件。

STEP 4 | 配置 Panorama 以便为所有管理员使用身份验证配置文件。

1. 选择 **Panorama** > **Setup**（设置）> **Management**（管理），编辑身份验证设置，然后选择配置的 **Authentication Profile**（身份验证配置文件）。
2. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**）以激活对 Panorama 所作的更改，并验证分配给 SAML IdP 服务器配置文件的 **Identity Provider Certificate**（标识提供商证书）。

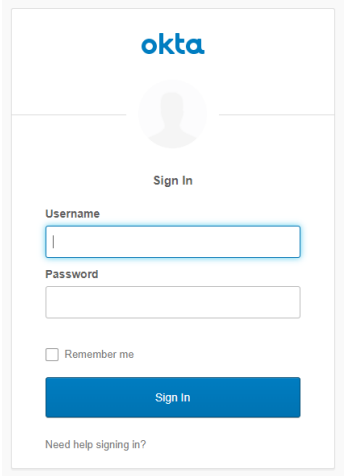
STEP 5 | 创建一个 SAML 元数据文件以便在 IdP 上注册 Panorama。

1. 选择 **Panorama** > **Authentication Profile**（身份验证配置文件），并在配置的身份验证配置文件的身份验证列中单击 **Metadata**（元数据）。
2. 将 **Management Choice**（管理选择）设置为 **Interface**（接口）（默认选择），并选择管理 (MGT) 接口。
3. 单击 **OK**（确定），并将元数据文件保存到客户端系统。
4. 将元数据文件导入 IdP 服务器以注册 Panorama。如需了解相关说明，请参阅 IdP 文档。

STEP 6 | 验证管理员是否可以使用 SAML SSO 进行身份验证。

1. 前往 Panorama Web 界面的 URL。
2. 单击 **Use Single Sign-On**（使用单点登录）。
3. 单击 **Continue**（继续）。

   Panorama 将重定向，以便对显示登录页面的 IdP 进行身份验证。例如：



4. 使用您的 SSO 用户名和密码登录。

   在 IdP 上成功进行身份验证后，将重定向到显示 Web 界面的 Panorama。
5. 使用您的 Panorama 管理员帐户请求访问另一个 SSO 应用程序。

   成功访问表示 SAML SSO 身份验证成功。

© 2019 Palo Alto Networks, Inc.

使用自定义证书设置身份验证

默认情况下，Palo Alto Networks 服务使用预定义证书进行相互身份验证，以建立用于管理访问和设备间通信的 SSL 连接。但是，您可以使用自定义证书配置身份验证。此外，您可以使用自定义证书保护 Panorama HA 对端设备之间的高可用性 (HA) 连接。自定义证书允许您建立唯一的信任链，以确保 Panorama 与受管防火墙和日志收集器之间的相互身份验证。请参阅证书管理以获取有关证书以及如何在 Panorama、日志收集器和防火墙上部署的详细信息。

以下主题介绍如何使用 Panorama 配置和管理自定义证书。

- SSL/TLS 连接如何进行相互身份验证？
- 在 Panorama 上使用自定义证书配置身份验证
- 在受管设备上使用自定义证书配置身份验证
- 添加新客户端设备
- 更改证书

SSL/TLS 连接如何进行相互身份验证？

在常规 SSL 连接中，只有服务器需要通过提供其证书来向客户端标识自己。但是，在相互 SSL 身份验证中，客户端也会将其证书提供给服务器。Panorama、主要 Panorama HA 对端设备、日志收集器、WildFire 设备、以及 PAN-DB 设备均可充当服务器。防火墙、日志收集器、WildFire 设备和辅助 Panorama HA 对端设备可以充当客户端。设备充当的角色取决于部署。例如，在下图中，Panorama 管理许多防火墙和收集器组，并充当防火墙和日志收集器的服务器。日志收集器充当向其发送日志的防火墙的服务器。

要在部署中部署用于相互身份验证的自定义证书，您需要：

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

  另外，可使用证书配置文件定义 证书撤销状态 (OCSP/CRL)，并根据撤销状态采取操作。
- 客户端证书和配置文件 — 每个受管设备都需要客户端证书和证书配置文件。客户端设备使用其证书向服务器设备标识自己。您可以使用简单证书注册协议 (SCEP)，从受信任的第三方 CA 购买证书或在本地生成自签名证书，从企业 PKI 部署证书。

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

  您可以在每个客户端设备上配置客户端证书和证书配置文件，或者将配置从 Panorama 推送到每个设备作为模板的一部分。

© 2019 Palo Alto Networks, Inc.

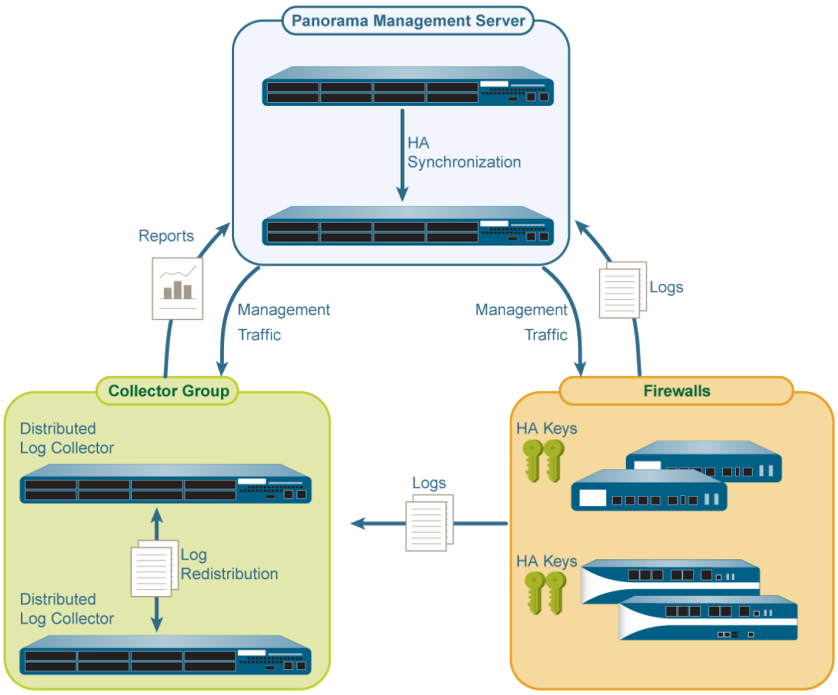


图 **11: SSL/TLS** 身份验证

在 Panorama 上使用自定义证书配置身份验证

完成以下过程可将服务器端 (Panorama) 配置为使用自定义证书而不是预定义证书与部署中的受管设备进行相互身份验证。请参阅在 HA 对端设备之间使用自定义证书设置身份验证在 Panorama HA 对中配置自定义证书。

STEP 1 | 部署服务器证书。

通过在 Panorama 上生成自签名证书或从企业证书颁发机构 (CA) 或受信任的第三方 CA 获取证书，您可以在 Panorama 或服务器日志收集器上部署证书。

STEP 2 | 在 Panorama 上，配置证书配置文件。此证书配置文件定义要使用的证书以及要在其中查找 IP 地址或 FQDN 的证书字段。

1. 选择 **Panorama** > **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件）。
2. 配置证书配置文件。

如果将中间 *CA* 配置为证书配置文件的一部分，则还必须包含根 *CA*。

STEP 3 | 配置 SSL/TLS 服务配置文件。

1. 选择 **Panorama** > **Certificate Management**（证书管理）> **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）。
2. 配置 SSL/TLS 配置文件定义 Panorama 及其受管设备用于 SSL/TLS 服务的证书和协议。

STEP 4 | 在 Panorama 或日志收集器上以服务器角色配置安全服务器通信。

1. 选择以下导航路径之一：
   - 对于 Panorama：**Panorama** > **Setup**（设置）> **Management**（管理），然后 **Edit**（编辑）安全通信设置

© 2019 Palo Alto Networks, Inc.

- 对于日志收集器：**Panorama** > **Managed Collectors**（受管收集器）> > **Communication**（通信）

2. 选择 **Customize Secure Server Communication**（自定义安全服务器通信）选项。
3. 验证 **Allow Custom Certificate Only**（仅允许自定义证书）复选框未选中。这允许您在迁移到自定义证书的同时继续管理所有设备。



如果选中 *Custom Certificate Only*（仅允许自定义证书）复选框，则 *Panorama* 不会进行身份验证，并且无法使用预定义证书管理设备。

4. 选择 **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）。此 SSL/TLS 服务配置文件适用于 Panorama、防火墙、日志收集器和 Panorama HA 对端设备之间的所有 SSL 连接。
5. 选择 **Certificate Profile**（证书配置文件）标识用于建立与客户端（如防火墙）的安全通信的证书。
6. （可选）配置授权列表。授权列表增加证书身份验证之外的额外安全层。授权列表检查客户证书主题或主题备用名称。如果与客户端证书一起提供的主题或主题备用名称与授权列表上的标识符不匹配，则身份验证被拒绝。

   您也可以根据其序列号对客户端设备进行身份验证。

   1. **Add**（添加）授权列表。
   2. 选择在证书配置文件中配置的 **Subject**（主题）或 **Subject Alt Name**（主题备用名称）作为标识符类型。
   3. 如果标识符为 Subject（主题），则输入通用名，如果标识符为 Subject Alt Name（主题备用名称），则输入 IP 地址、主机名或电子邮件。
   4. 单击 **OK**（确定）。
   5. 选择 **Check Authorization List**（检查授权列表）以执行授权列表。
7. 选择 **Authorize Client Based on Serial Number**（根据序列号对客户端进行授权）让服务器根据受管设备的序列号对客户端进行身份验证。客户端证书中的 CN 或主题必须具有特殊关键字 $UDID 才能启用此类型的身份验证。
8. 在 **Customize Communication**（自定义通信）部分中选择 **Data Redistribution**（数据重新分发）选项，以使用自定义证书来保护与数据重新分发客户端进行的传出通信。
9. 在 **Disconnect Wait Time (min)**（断开连接等待时间（分钟））中，指定 Panorama 在与其受管设备断开当前会话并重新建立连接之前应等待多长时间。该字段默认为空，范围为 0 至 44,640 分钟。将此字段保留为空与将其设置为 0 相同。



在您提交新配置之前，断开连接等待时间不会开始倒计时。

10. 单击 **OK**（确定）。
11. **Commit**（提交）更改。

在受管设备上使用自定义证书配置身份验证

完成以下过程可将客户端（防火墙或日志收集器）配置为使用自定义证书而不是预定义证书与部署中的受管设备进行相互身份验证。

STEP 1 | 升级每个受管防火墙或日志收集器。所有受管设备必须运行 PAN-OS 8.0 版或更高版本才能执行自定义证书身份验证。

升级防火墙。升级后，每个防火墙都使用默认的预定义证书连接到 Panorama。

STEP 2 | 获取或生成设备证书。

通过在 Panorama 上生成自签名证书或从企业证书颁发机构 (CA) 或受信任的第三方 CA 获取证书，您可以在 Panorama 或服务器日志收集器上部署证书。

如果根据序列号对客户端设备进行授权，请将通用名设置为 $UDID 或符号 CN=$UDID（在 SCEP 配置文件中）。

© 2019 Palo Alto Networks, Inc.

- 您可以在 Panorama 上生成自签名证书或从企业 CA 或受信任的第三方 CA 获取证书。
- 如果您使用 SCEP 作为设备证书，请配置 SCEP 配置文件。SCEP 允许您自动将证书部署到受管设备。当具有 SCEP 配置文件的新客户端设备尝试使用 Panorama 进行身份验证时，证书由 SCEP 服务器发送到设备。

STEP 3 | 配置客户端设备的证书配置文件。

您可以单独在每个客户端设备上配置此配置，或者您可以将此配置推送到受管设备作为模板的一部分。

1. 选择以下导航路径之一：
   - 对于防火墙 — 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件）。
   - 对于日志收集器 — 选择 **Panorama** > **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件）。
2. 配置证书配置文件。

STEP 4 | 在每个防火墙或日志收集器上部署自定义证书。

1. 选择以下导航路径之一：
   - 对于防火墙：选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后 **Edit**（编辑）Panorama 设置。
   - 对于日志收集器：选择 **Panorama** > **Managed Collectors**（受管收集器），并 **Add**（添加）新的日志收集器或选择现有的日志收集器。选择 **Communication**（通信）。
2. 选中 **Secure Client Communication**（安全客户端通信）复选框（仅限防火墙）。
3. 选择 **Certificate Type**（证书类型）。
   - 如果您使用本地设备证书，请选择 **Certificate**（证书）和 **Certificate Profile**（证书配置文件）。
   - 如果您使用 SCEP 部署设备证书，请选择 **SCEP Profile**（**SCEP** 配置文件）和 **Certificate Profile**（证书配置文件）。
   - 如果您正在使用默认 Panorama 证书，请选择 **Predefined**（预定义）。
4. （可选）启用 **Check Server Identity**（检查服务器标识）。防火墙或日志收集器根据 Panorama 的 IP 地址或 FQDN 检查服务器证书中的 CN 以验证其身份。
5. 单击 **OK**（确定）。
6. **Commit**（提交）更改。

   提交更改后，受管设备不会终止其与 Panorama 的当前会话，直到断开等待时间完成。

STEP 5 | 选择您想要为其使用自定义证书的传入通信类型：

- **HA** 通信
- **WildFire** 通信
- 数据重新分发

STEP 6 | 在所有受管设备上部署自定义证书后，使用自定义证书执行身份验证。

WildFire 设备目前不支持自定义证书。如果您的 *Panorama* 正在管理 *WildFire* 设备，请勿选择 *Allow Custom Certificates Only*（仅允许自定义证书）。

1. 选择 **Panorama** > **Setup**（设置）> **Management**（管理），然后 **Edit**（编辑）Panorama 设置。
2. 选择 **Allow Custom Certificate Only**（仅允许自定义证书）。
3. 单击 **OK**（确定）。
4. **Commit**（提交）更改。

   提交此更改后，Panorama 管理的所有设备都必须使用自定义证书。否则，Panorama 和设备之间的身份验证将失败。

© 2019 Palo Alto Networks, Inc.

添加新客户端设备

将新防火墙或日志收集器添加到 Panorama 时，工作流程取决于这些设备是否配置为仅将自定义证书用于相互进行身份验证。

- 如果未在 Panorama 上选择仅自定义证书，则可以将设备添加到 Panorama，然后按照步骤在受管设备上使用自定义证书配置身份验证中的过程开始部署自定义证书。
- 如果在 Panorama 上选择仅自定义证书，则必须在将自定义证书添加到 Panorama 之前将其部署到防火墙。否则，受管设备将无法使用 Panorama 进行身份验证。这可以通过防火墙 Web 界面手动完成，也可以通过引导作为 bootstrap.xml 文件的一部分来完成。

更改证书

如果部署中的自定义证书已过期或已被撤销并需要替换，则可以完成下列任务之一。

- 更改服务器证书
- 更改客户端证书
- 更改根或中间 CA 证书

更改服务器证书

完成以下任务以替换服务器证书。

STEP 1 | 部署新的服务器证书。

您可以通过在 Panorama 上生成自签名证书或从企业 CA 或受信任的第三方 CA 获取证书，在 Panorama 或服务器日志收集器上部署证书。

STEP 2 | 更改 SSL/TLS 服务配置文件中的证书。

1. 选择 **Panorama** > **Certificate Management**（证书管理）> **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件），然后选择 SSL/TLS 服务配置文件。
2. 选择 **Certificate**（证书）。
3. 单击 **OK**（确定）。

STEP 3 | 重新建立服务器（Panorama 或日志收集器）和客户端设备之间的连接。

1. 选择 **Panorama** > **Setup**（设置）> **Management**（管理）并 **Edit**（编辑）Panorama 的 Panorama Settings（Panorama 设置），或者选择日志收集器的 **Panorama** > **Managed Collectors**（受管收集器）> **Add**（添加）> **Communication**（通信）。
2. 设置 **Disconnect Wait Time**（断开等待时间）。
3. 单击 **OK**（确定）。
4. **Commit**（提交）更改。

更改客户端证书

完成以下任务以替换客户端证书。

STEP 1 | 获取或生成设备证书。

您可以通过在 Panorama 上生成自签名证书或从企业 CA 或受信任的第三方 CA 获取证书，在 Panorama 或服务器日志收集器上部署证书。

如果根据序列号对客户端设备进行授权，请将通用名设置为 $UDID 或符号 CN=$UDID（在 SCEP 配置文件中）。

- 您可以在 Panorama 上生成自签名证书或从企业 CA 或受信任的第三方 CA 获取证书。

© 2019 Palo Alto Networks, Inc.

- 如果您使用 SCEP 作为设备证书，请配置 SCEP 配置文件。SCEP 允许您自动将证书部署到受管设备。当具有 SCEP 配置文件的新客户端设备尝试使用 Panorama 进行身份验证时，证书由 SCEP 服务器发送到设备。

STEP 2 | 更改证书配置文件中的证书。

1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件），然后选择证书配置文件。
2. 在 CA 证书下，**Add**（添加）要分配给证书配置文件的新证书。
3. 单击 **OK**（确定）。
4. **Commit**（提交）更改。

更改根或中间 *CA* 证书

完成以下任务以替换根或中间 CA 证书。

STEP 1 | 配置服务器以接受来自客户端的预定义证书。

1. 选择 **Panorama** > **Setup**（设置）> **Management**（管理），然后 **Edit**（编辑）Panorama 设置。
2. 取消选择 **Custom Certificate Only**（仅允许自定义证书）。
3. 选择 **None**（无）从证书配置文件下拉菜单中选择。
4. 单击 **OK**（确定）。
5. **Commit**（提交）更改。

STEP 2 | 部署新的根或中间 CA 证书。

您可以通过在 Panorama 上生成自签名证书或从企业 CA 或受信任的第三方 CA 获取证书，在 Panorama 或服务器日志收集器上部署证书。

STEP 3 | 更新服务器证书配置文件中的 CA 证书。

1. 选择 **Panorama** > **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件），然后选择要更新的证书配置文件。
2. **Delete**（删除）旧的 CA 证书。
3. **Add**（添加）新的 CA 证书。
4. 单击 **OK**（确定）。

STEP 4 | 生成或导入新的客户端证书。

1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）。
2. 创建自签名根 CA 证书或从企业 CA 导入证书。

STEP 5 | 更新客户端证书配置文件中的 CA 证书。

1. 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后单击防火墙的 Panorama Settings（Panorama 设置）中的 **Edit**（编辑）图标，或者选择日志收集器的 **Panorama** > **Managed Collectors**（受管收集器）> **Add**（添加）> **Communication**（通信），然后选择要更新的证书配置文件。
2. **Delete**（删除）旧的 CA 证书。
3. **Add**（添加）新的 CA 证书。
4. 单击 **OK**（确定）。

STEP 6 | 在所有受管设备上更新 CA 证书后，执行自定义证书身份验证。

1. 选择 **Panorama** > **Setup**（设置）> **Management**（管理），然后 **Edit**（编辑）Panorama 设置。
2. 选择 **Custom Certificate Only**（仅允许自定义证书）。
3. 单击 **OK**（确定）。

© 2019 Palo Alto Networks, Inc.

4. **Commit**（提交）更改。

   提交此更改后，Panorama 管理的所有设备都必须使用自定义证书。否则，Panorama 和设备之间的身份验证将失败。

© 2019 Palo Alto Networks, Inc.

管理防火墙

要使用 Panorama™ 管理服务器管理 Palo Alto Networks 防火墙，您必须添加防火墙作为受管设备，然后将其分配到设备组和模板或模板堆栈。以下任务最适合于第一次防火墙部署。在继续之前，请参阅计划您的 Panorama 部署了解部署选项。

- 添加防火墙作为受管设备
- 为受管防火墙安装设备证书
- 设置零接触配置
- 管理设备组
- 管理模板和模板堆栈
- 从 Panorama 管理主密钥
- 重新分发数据到受管防火墙
- 设置企业数据丢失防护 (DLP)
- 从防火墙过渡到 Panorama Management
- 在 Panorama 上监控设备
- 用例 ：使用 Panorama 配置防火墙

要查看 Panorama Web 界面上的 **Objects**（对象）和 **Policies**（策略）选项卡，您必须首先创建至少一个设备组。要查看 **Network**（网络）和 **Device**（设备）选项卡，您必须创建至少一个模板。这些选项卡包含了您在网络上配置和管理防火墙时所用的选项。

添加防火墙作为受管设备

要使用 Panorama 管理防火墙，您将需要启用防火墙和 Panorama 之间的连接。此连接要求您输入将要管理的每个防火墙上的 Panorama IP 地址，并在 Panorama 上输入每个防火墙的序列号。添加防火墙作为受管设备时，可以在初始部署时将新防火墙关联到设备组、模板堆栈、收集器组、和日志收集器。此外，您还可以在防火墙首次连接到 Panorama 时自动将配置推送到新添加的防火墙，从而确保防火墙能够立即进行配置并随时开始保护您的网络。



您只能批量导入单个 *vsys* 防火墙，由 *Panorama* 进行管理。

防火墙使用 Panorama 服务器 IP 地址设置 SSL 连接以注册 Panorama。使用 2,048 位证书使 Panorama 和防火墙进行相互验证身份，并使用 AES-256 加密 SSL 连接进行配置管理和日志收集。准备 Panorama，并且每个防火墙如下所示：

STEP 1 | 配置防火墙以便与 Panorama 进行通信。

为 Panorama 将管理的每个防火墙重复此步骤。

1. 在防火墙上执行初始配置，使其可以访问且能够在网络上与 Panorama 进行通行。
2. 配置计划要在防火墙上使用的每个数据接口并将其连接到安全区域，以便从 Pnorama 推送配置和策略。
3. 将 Panorama IP 地址添加到防火墙。
    1. 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后 Edit（编辑）Panorama 设置。
    2. 在第一个字段中输入 Panorama IP 地址。

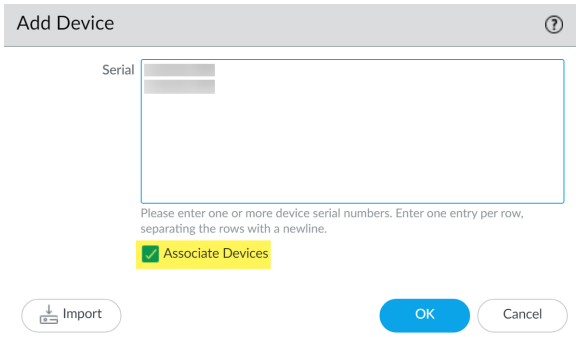
        

        Panorama 发布用于设备管理、日志收集、报告、和动态更新的单个 *IP* 地址。输入互联网绑定的外部 *IP* 地址，确保 *Panorama* 可以成功访问现有和新的受管设备和日志收集器。如果已配置 *Panorama* 内部 *IP* 地址，则您可能无法管理某些设备。例如，如果您 在 AWS 上安装 Panorama，并输入内部 *IP* 地址，则 *Panorama* 无法管理 *AWS* 安全组之外的受管设备或日志收集器。
    3. （可选）如果您已在 Panorama 中设置高可用性对，请在第二个字段中输入辅助 Panorama IP 地址。
    4. 单击 **OK**（确定）。
    5. 选择 **Commit**（提交）并 **Commit**（提交）更改。

STEP 2 | 将一个或多个防火墙添加到 Panorama。

- 添加一个或多个防火墙
    1. 添加新的受管设备（**Panorama** > **Managed Devices**（受管设备）> **Summary**（摘要））。
    2. 输入防火墙 **Serial**（序列）号。如果添加多个防火墙，则在单独一行中输入每个序列号。如果想在初始部署时将新防火墙关联到设备组、模板堆栈、收集器组或日志收集器，请继续下一步。要手动分配每个防火墙，请单击 **OK**（确定），并继续步骤 3。
    3. 选择 **Associate Devices**（关联设备）复选框，并单击 **OK**（确定）。

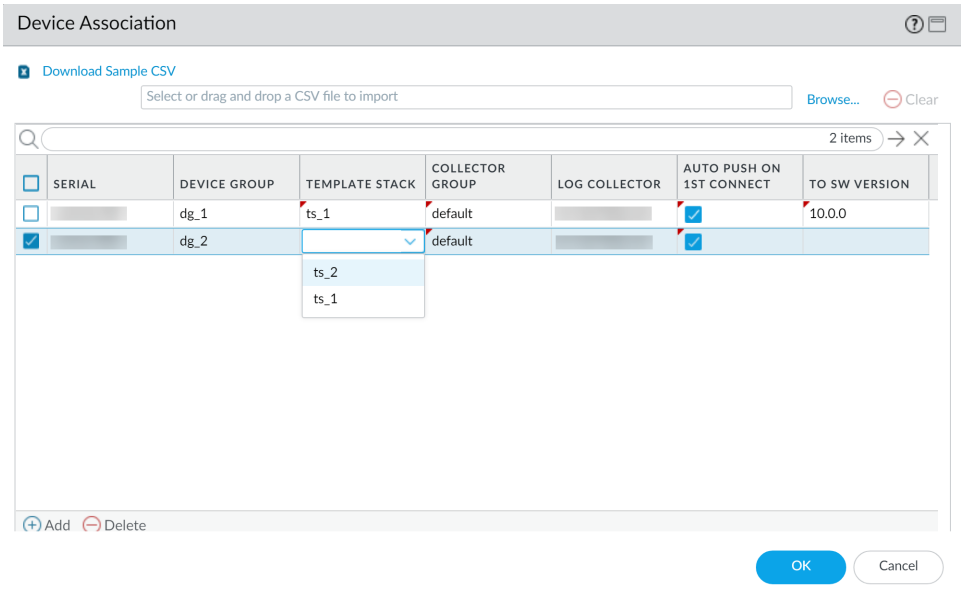
© 2019 Palo Alto Networks, Inc.



4. 根据需要，从每列的下拉列表中分配 **Device Group**（设备组）、**Template Stack**（模板堆栈）、**Collector Group**（收集器组）和 **Log Collector**（日志收集器）。
5. 启用 **Auto Push on 1st connect**（在第一次连接时自动推送）复选框，以在其成功连接到 Panorama 时自动将设备组和模板堆栈配置推送到新设备。

   仅运行 *PAN-OS 8.1* 或更高版本的防火墙支持 *Auto Push on 1st Connect*（在第一次连接时自动推送）选项。`commit all` 作业将从 *Panorama* 对运行 *PAN-OS 8.1* 及更高版本的受管设备执行 。
6. （可选）在 **To SW Version**（到 **SW** 版本）列中选择一个 PAN-OS 发行版本，以在成功连接到 Panorama 后，开始将受管防火墙自动升级到指定的 PAN-OS 发行版本。

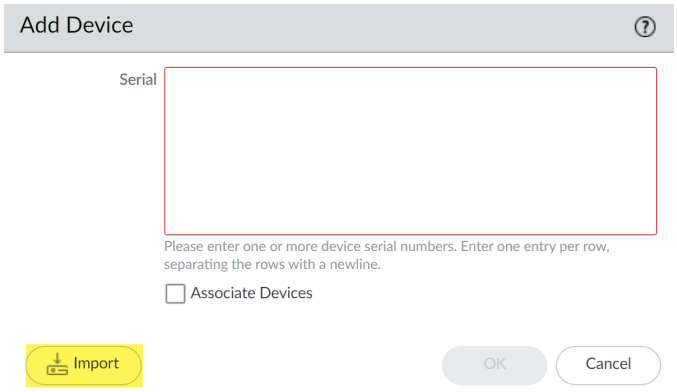
   如果不想要自动升级受管防火墙，请将此列留空。
7. 单击 **OK**（确定）以添加设备。



- 使用逗号分隔值 (CSV) 文件批量导入多个防火墙。

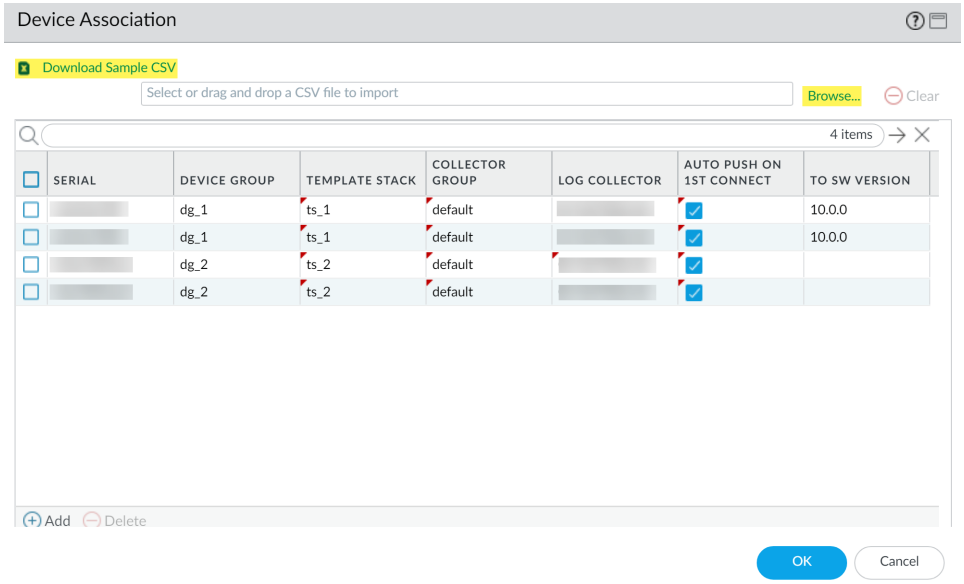
  1. 添加新的受管设备（**Panorama** > **Managed Devices**（受管设备） > **Summary**（摘要））。
  2. 单击 **Import**（导入）。

© 2019 Palo Alto Networks, Inc.



3. **Download Sample CSV**（下载样本 **CSV**），并使用您正在添加的防火墙编辑下载的 CSV 文件。您可以选择将防火墙从 CSV 分配到设备组、模板堆栈、收集器组，或仅输入防火墙序列号并从 Web 界面进行分配。编辑结束后，保存 CSV。
4. **Browse**（浏览）并选择您在前述步骤中编辑的 CSV 文件。
5. 如果尚未在 CSV 中进行分配，则根据需要，从每列的下拉列表中为防火墙分配 **Device Group**（设备组）、**Template Stack**（模板堆栈）、**Collector Group**（收集器组）和 **Log Collector**（日志收集器）。
6. 如果尚未在 CSV 中启用，则启用 **Auto Push on 1st connect**（在第一次连接时自动推送）复选框，以在其成功连接到 Panorama 时自动将设备组和模板堆栈配置推送到新设备。
7. （可选）在 **To SW Version**（到 **SW** 版本）列中选择一个 PAN-OS 发行版本，以在成功连接到 Panorama 后，开始将受管防火墙自动升级到指定的 PAN-OS 发行版本。

   如果不想要自动升级受管防火墙，请将此列留空。
8. 单击 **OK**（确定）以添加设备。



STEP 3 | （可选）添加 **Tag**（标记）。标记可让您在大列表中轻松找到防火墙；可以帮助您动态筛选和调整所显示的防火墙列表。例如，如果添加了名为“分支机构”的标记，则可以筛选整个网络中的所有分支机构防火墙。

1. 选择每个防火墙，并单击 **Tag**（标记）。
2. 单击 **Add**（添加），输入最多可包含 31 个字符的字符串（不能包含空格），然后单击 **OK**（确定）。

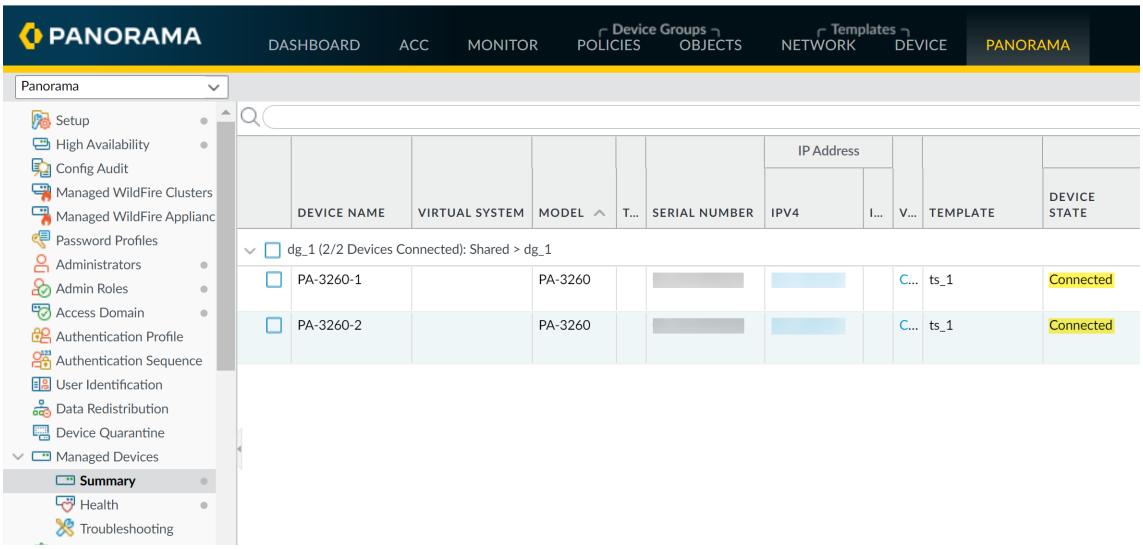
© 2019 Palo Alto Networks, Inc.

STEP 4 | 如果您的部署使用自定义证书在 Panorama 和受管设备之间进行身份验证，请部署自定义客户端设备证书。有关更多信息，请参阅使用自定义证书设置身份验证和添加新客户端设备。

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

STEP 6 | 验证防火墙已经连接上 Panorama。

1. 单击 **Panorama** > **Managed Devices**（受管设备）> **Summary**（摘要）。
2. 确认新设备的 **Device State**（设备状态）显示为 `Connected`。



© 2019 Palo Alto Networks, Inc.

为受管防火墙安装设备证书

在 PAN-OS 10.0 和更高版本中，您必须在受管防火墙上安装设备证书以成功对受管防火墙进行身份验证，继而才能使用 Palo Alto Networks 云服务（如设备遥测、IoT 和企业数据丢失防护 (DLP)）。您可以同时为单个或多个受管防火墙安装设备证书。



要在本地安装防火墙设备证书，请参阅设备证书。

- 为一个受管防火墙安装设备证书
- 为多个受管防火墙安装设备证书

为一个受管防火墙安装设备证书

在 PAN-OS 10.0 和更高版本中，您必须从 Panorama 管理服务器为一个受管防火墙安装设备证书。受管防火墙必须能够访问互联网才能成功安装设备证书。

STEP 1 | 注册 Panorama 和受管防火墙以及 Palo Alto Networks 客户支持门户 (CSP)。

STEP 2 | 登录到 Panorama Web 界面 作为管理员用户。

STEP 3 | 配置网络时间协议 (NTP) 服务器。

需要 NTP 服务器来验证设备证书到期日期，确保设备证书不会提前过期或失效。

1. 选择 **Device**（设备）> **Setup**（设置）> **Services**（服务），然后选择 **Template**（模板）。
2. 根据您的平台选择以下项之一：
   - 对于多虚拟系统平台，请选择 **Global**（全局）并编辑“服务”部分。
   - 对于单个虚拟系统平台，请编辑“服务”部分。
3. 选择 **NTP**，然后输入主机名 `pool.ntp.org` 作为 **Primary NTP Server**（主 NTP 服务器）或输入主 NTP 服务器的 IP 地址。
4. （可选）输入 **Secondary NTP Server**（辅助 NTP 服务器）地址。
5. （可选）要对 NTP 服务器中的时间更新进行身份验证，对于 **Authentication Type**（身份验证类型），请为每个服务器选择以下其中一个选项。
   - **None**（无）（默认）— 禁用 NTP 身份验证。
   - **Symmetric Key**（对称式密钥）— 防火墙使用对称式密钥交换（共享密钥）对时间更新进行身份验证。
     - **Key ID**（密钥 **ID**）— 输入密钥 ID (1-65534)
     - **Algorithm**（算法）— 选择要用于 NTP 身份验证的算法（**MD5** 或 **SHA1**）
6. 单击 **OK**（确定）保存您的配置更改。
7. 选择 **Commit**（提交），然后 **Commit and Push**（提交并推送）配置更改到受管防火墙。

STEP 4 | 选择 **Panorama** > **Managed Devices**（受管设备）> **Summary**（摘要），并选择一个受管防火墙。

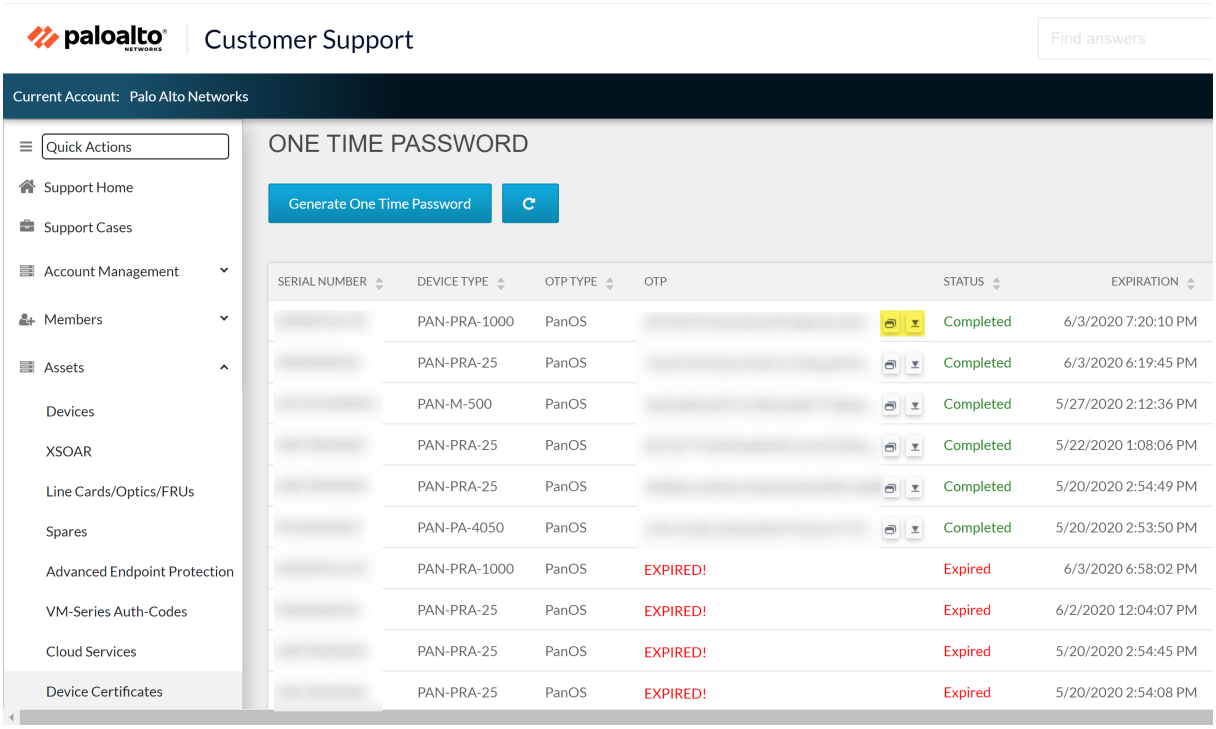
STEP 5 | 选择 **Request OTP From CSP**（向 **CSP** 请求 **OTP**）> **Custom selected devices**（自定义已选设备）。

STEP 6 | 复制整个 OTP 请求令牌。

© 2019 Palo Alto Networks, Inc.

STEP 7 | 为受管防火墙生成一次性密码 (OTP)。

1. 登录到客户支持门户。
2. 选择 **Assets**（资产）> **Device Certificates**（设备证书）和 **Generate OTP**（生成 **OTP**）。
3. 对于 **Device Type**（设备类型），选择 **Generate OTP for Panorama managed firewalls**（为 **Panorama** 受管防火墙生成 **OTP**）。
4. 粘贴在上一步中复制的 OTP 请求，然后 **Generate OTP**（生成 **OTP**）。
5. 单击 **Done**（完成），然后等待几分钟以便成功生成 OTP。如果未显示新 OTP，您可以刷新页面。
6. **Copy to Clipboard**（复制到剪贴板）或 **Download**（下载）OTP。



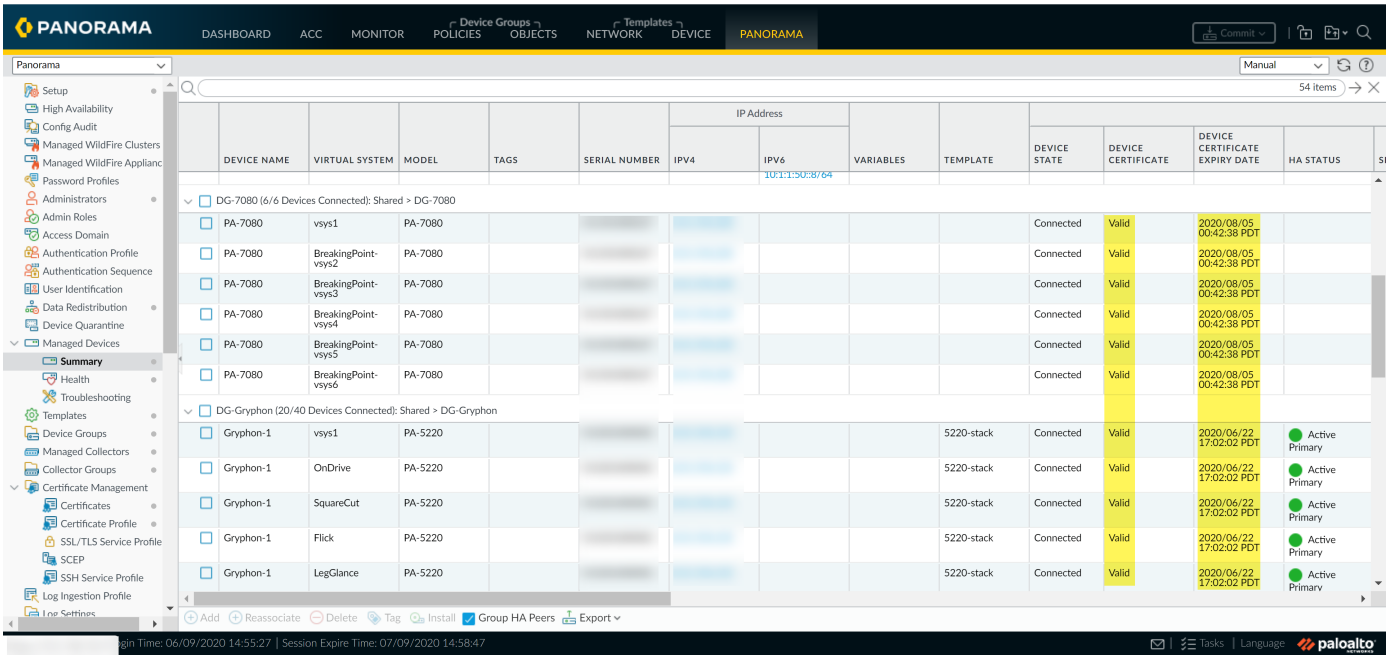
STEP 8 | 登录到 Panorama Web 界面 作为管理员用户。

STEP 9 | 选择 **Panorama** > **Managed Devices**（受管设备）> **Summary**（摘要），并 **Upload OTP**（上传 **OTP**）。

STEP 10 | 粘贴生成的 OTP，然后单击 **Upload**（上传）。

STEP 11 | 验证 **Device Certificate**（设备证书）列显示为 `Valid`（有效），且 **Device Certificate Expiry Date**（设备证书到期日）显示了一个到期日期。

© 2019 Palo Alto Networks, Inc.



为多个受管防火墙安装设备证书

在 PAN-OS 10.0 和更高版本中，您必须从 Panorama 管理服务器为受管防火墙安装设备证书。受管防火墙必须能够访问互联网才能成功安装设备证书。

STEP 1 | 注册 Panorama 和受管防火墙以及 Palo Alto Networks 客户支持门户 (CSP)。

STEP 2 | 登录到 Panorama Web 界面 作为管理员用户。

STEP 3 | 配置网络时间协议 (NTP) 服务器。

需要 NTP 服务器来验证设备证书到期日期，确保设备证书不会提前过期或失效。

1. 选择 **Device**（设备）> **Setup**（设置）> **Services**（服务），然后选择 **Template**（模板）。
2. 根据您的平台选择以下项之一：
   - 对于多虚拟系统平台，请选择 **Global**（全局）并编辑“服务”部分。
   - 对于单个虚拟系统平台，请编辑“服务”部分。
3. 选择 **NTP**，然后输入主机名 `pool.ntp.org` 作为 **Primary NTP Server**（主 NTP 服务器）或输入主 NTP 服务器的 IP 地址。
4. （可选）输入 **Secondary NTP Server**（辅助 NTP 服务器）地址。
5. （可选）要对 NTP 服务器中的时间更新进行身份验证，对于 **Authentication Type**（身份验证类型），请为每个服务器选择以下其中一个选项。
   - **None**（无）（默认）— 禁用 NTP 身份验证。
   - **Symmetric Key**（对称式密钥）— 防火墙使用对称式密钥交换（共享密钥）对时间更新进行身份验证。
     - **Key ID**（密钥 **ID**）— 输入密钥 ID (1-65534)
     - **Algorithm**（算法）— 选择要用于 NTP 身份验证的算法（**MDS** 或 **SHA1**）
6. 单击 **OK**（确定）保存您的配置更改。
7. 选择 **Commit**（提交），然后 **Commit and Push**（提交并推送）配置更改到受管防火墙。

STEP 4 | 选择 **Panorama** > **Managed Devices**（受管设备）> **Summary**（摘要）。

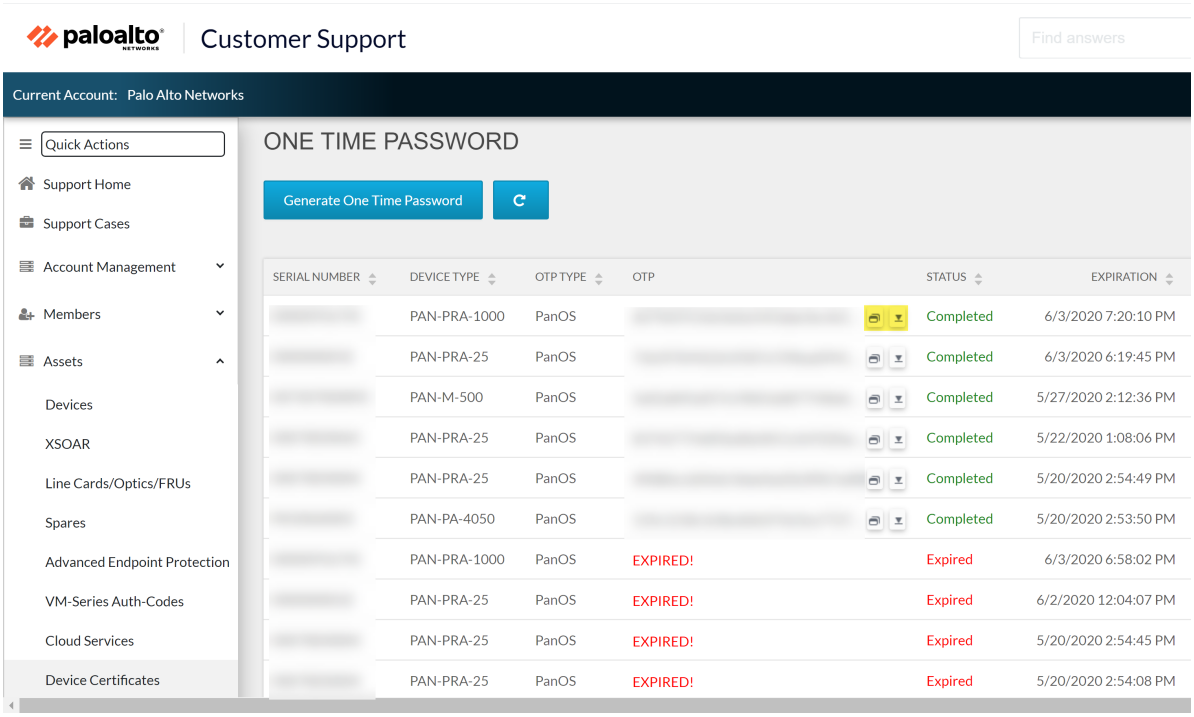
© 2019 Palo Alto Networks, Inc.

STEP 5 | 选择 **Request OTP from CSP**（向 CSP 请求 OTP）> **Select all devices without a certificate**（选择所有不带证书的设备）。

STEP 6 | 复制整个 OTP 请求令牌。

STEP 7 | 为受管防火墙生成一次性密码 (OTP)。

1. 登录到客户支持门户。
2. 选择 **Assets**（资产）> **Device Certificates**（设备证书）和 **Generate OTP**（生成 OTP）。
3. 对于 **Device Type**（设备类型），选择 **Generate OTP for Panorama managed firewalls**（为 Panorama 受管防火墙生成 OTP）。
4. 粘贴在上一步中复制的 OTP 请求，然后 **Generate OTP**（生成 OTP）。
5. 单击 **Done**（完成），然后等待几分钟以便成功生成 OTP。如果未显示新 OTP，您可以刷新页面。
6. **Copy to Clipboard**（复制到剪贴板）或 **Download**（下载）OTP。



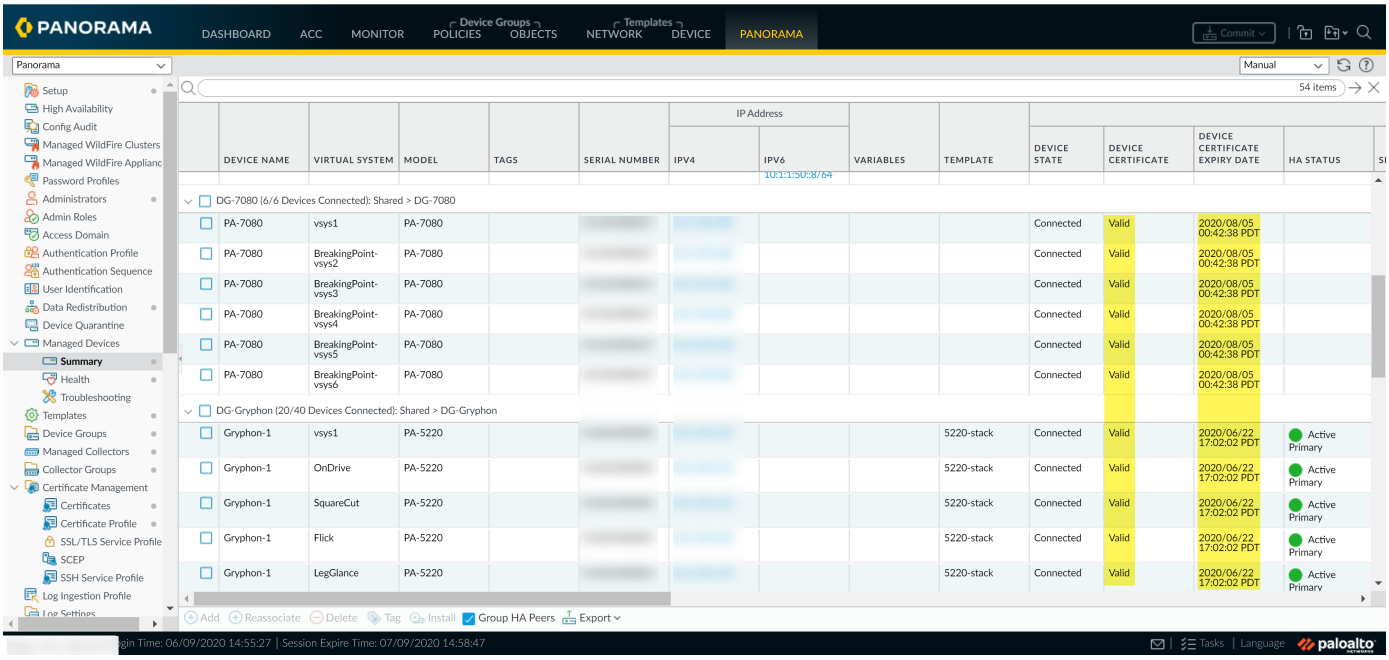
STEP 8 | 登录到 Panorama Web 界面 作为管理员用户。

STEP 9 | 选择 **Panorama** > **Managed Devices**（受管设备）> **Summary**（摘要），并 **Upload OTP**（上传 OTP）。

STEP 10 | 粘贴生成的 OTP，然后单击 **Upload**（上传）。

STEP 11 | 验证 **Device Certificate**（设备证书）列显示为 `Valid`（有效），且 **Device Certificate Expiry Date**（设备证书到期日）显示了一个到期日期。

© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

设置零接触配置

设置零接触配置 (ZTP) 可自动化新受管防火墙登入流程，无需网络管理员手动配置防火墙，从而简化初始防火墙部署。

要成功利用 *ZTP* 服务，请在升级到 *PAN-OS 10.0.0* 或更高版本之前，为 *ZTP* 防火墙装载出厂默认的 *PAN-OS* 版本。

PAN-OS 10.0.1 和更高版本支持 *ZTP*。

- ZTP 概述
- 安装 ZTP 插件
- 配置 ZTP 安装程序管理员帐户
- 添加 ZTP 防火墙到 Panorama
- 使用 CLI 进行 ZTP 任务
- 卸载 ZTP 插件

ZTP 概述

进一步了解零接触配置 (ZTP) 插件及其配置元素。

- 关于 ZTP
- ZTP 配置元素

关于 *ZTP*

零接触配置 (ZTP) 旨在简化和自动化将新防火墙登入到 Panorama™ 管理服务器的流程。ZTP 允许网络管理员直接将受管防火墙发送到其分支并在 ZTP 防火墙成功连接到 Palo Alto Networks ZTP 服务后自动将防火墙添加到 Panorama，因此简化了防火墙初始部署流程。该插件无需 IT 管理员手动配置新受管防火墙，从而让企业在分支位置部署新防火墙时可以节省时间和资源。成功登入后，Panorama 可提供配置和管理 ZTP 配置和防火墙的工具。

查看和订阅 ZTP Service Status（ZTP 服务状态）事件，以获得有关已计划维护窗口、中断和解决方法的通知。

下列运行 PAN-OS 9.1.3 及更高版本的 ZTP 防火墙支持 ZTP：

- PA-220-ZTP 和 PA-220R-ZTP
- PA-820-ZTP 和 PA-850-ZTP
- PA-3220-ZTP、PA-3250-ZTP 和 PA-3260-ZTP

ZTP 配置元素

以下元素共同作用，使您可以通过使用 ZTP 服务将防火墙自动添加到 Panorama 管理服务器来快速登录新部署的 ZTP 受管防火墙。

- **ZTP Plugin**（**ZTP** 插件）— ZTP 插件允许 Panorama 连接到 ZTP 服务并声明 ZTP 防火墙以简化登入。
- **Customer Support Portal**（客户支持门户，**CSP**）— Palo Alto Networks 客户支持门户用于注册您的 Panorama 以连接至 CSP，从而自动注册新添加的 ZTP 防火墙。
- **One-time Password**（一次性密码，**OTP**）— 一次性密码由 Palo Alto Networks 提供，用于在 Panorama 上检索和安装证书，以便其与 CSP 和 ZTP 服务通信。
- **Installer**（安装程序）— 使用 `installeradmin` 管理员角色创建的管理员用户，用于 ZTP 防火墙登入。该管理员用户对 Panorama Web 界面的访问权有限，仅允许输入 ZTP 防火墙序列号和断言密钥来在

© 2019 Palo Alto Networks, Inc.

CSP 和 Panorama 上注册防火墙。可以在 Panorama 上创建，也可以使用 RADIUS、SAML 或 TACACS+ 等远程身份验证来创建安装程序管理员。

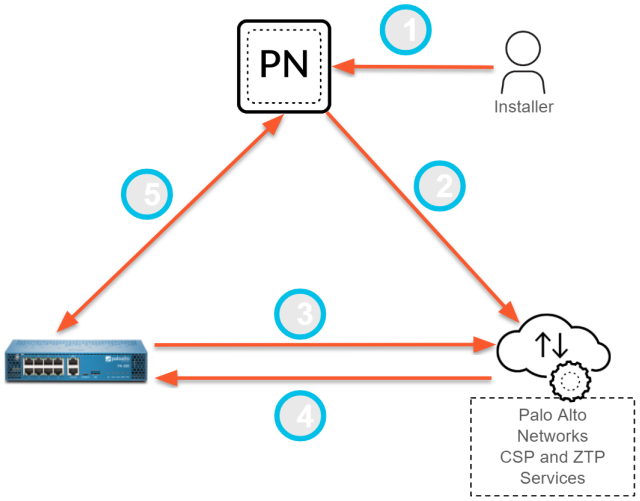
- **Claim Key**（断言密钥）— 物理附加到 ZTP 防火墙的 8 位数密钥，用于向 CSP 注册 ZTP 防火墙。
- **To-SW-Version**（至 **SW** 版本）— 指定 ZTP 防火墙的 PAN-OS 软件版本（**Panorama** > **Managed Devices**（受管设备）> **Summary**（摘要））。选择目标 PAN-OS 版本，并且，如果防火墙运行的是指定版本之前的版本，则防火墙将开始升级循环，直到成功安装目标版本。

Panorama 只能管理运行的 *PAN-OS* 版本与其上安装的版本相同或更旧的防火墙。

在 Panorama 上成功安装 ZTP 插件并向 ZTP 服务注册 Panorama 后，ZTP 登入流程将按以下方式继续：

1. 安装程序或 IT 管理员通过使用防火墙序列号和断言密钥将防火墙添加到 Panorama，从而注册 ZTP 防火墙。
2. Panorama 向 CSP 注册防火墙。成功注册防火墙后，防火墙与 ZTP 服务中同于 Panorama 的 ZTP 租户相关联。

   向 ZTP 服务注册成功的 ZTP 防火墙自动添加为 Panorama 上的受管防火墙（**Panorama** > **Managed Devices**（受管设备））。
3. 当防火墙连接到互联网时，ZTP 防火墙从 CSP 请求设备证书以连接到 ZTP 服务。
4. ZTP 服务将 Panorama IP 或 FQDN 推送到 ZTP 防火墙。
5. ZTP 防火墙连接到 Panorama，且设备组和模板配置从 Panorama 被推送到 ZTP 防火墙。



安装 ZTP 插件

在您的 Panorama™ 管理服务器上安装 ZTP 插件以向 ZTP 服务注册 Panorama，从而为简化登入流程声明 ZTP 防火墙。

如果您的 Panorama 为高可用性 (HA) 配置，则安装 ZTP 插件，并向 ZTP 服务注册两个 Panorama HA 对等。

- 在 Panorama 上安装 ZTP 插件
- 向 ZIP 服务注册 Panorama

在 *Panorama* 上安装 *ZTP* 插件

通过在 Panorama 管理服务器上安装 ZTP 插件来简化 ZTP 防火墙的登入和管理。

STEP 1 | 安装 Panorama 设备证书。

© 2019 Palo Alto Networks, Inc.

STEP 2 | 以拥有 Panorama 插件访问权限的超级用户或 Panorama 管理员登录到 Panorama Web 界面（**Panorama** > **Plugins**（插件））。

STEP 3 | 选择 **Panorama** > **Plugins**（插件），然后搜索 `ztp` 插件。

STEP 4 | **Download**（下载）并 **Install**（安装）最新版 ZTP 插件。

向 *ZIP* 服务注册 *Panorama*

为新的和现有部署向 ZIP 服务注册 Panorama™ 管理服务器。

- 为新部署向 ZTP 服务注册 Panorama
- 为现有部署向 ZIP 服务注册 Panorama

为新部署向 **ZTP** 服务注册 **Panorama**

在 Panorama™ 管理服务器上安装 ZTP 插件后，您必须向 ZTP 服务注册 Panorama，以使 ZTP 服务能够将防火墙与 Panorama 相关联。在 ZTP 新部署的注册过程中会自动生成将 ZTP 防火墙连接到 ZTP 服务所需的设备组和模板配置。在自动生成设备组和模板之后，您必须将 ZTP 防火墙添加到设备组和模板，这样 ZTP 防火墙在首次连接到 Panorama 之后就可以连接到 ZTP 服务。

STEP 1 | 安装 Panorama 设备证书。

STEP 2 | 登录到 Palo Alto Networks 客户支持门户 (CSP)。

STEP 3 | 在 Palo Alto Networks CSP 上将您的 Panorama 与 ZTP 服务相关联。

ZTP 服务仅支持与高可用性 (HA) 配置中的最多两个 Panorama 相关联。如果 Panorama 不在 HA 配置中，则只能关联单个 Panorama。

1. 选择 **Assets**（资产）> **ZTP Service**（**ZTP** 服务）和**Associate Panorama(s)**（关联 **Panorama**）。
2. 选择管理 ZTP 防火墙的 Panorama 的序列号。
3. （仅限 HA）选择 Panorama HA 对端的序列号。
4. 单击 **OK**（确定）。

STEP 4 | 登录到 Panorama Web 界面。

STEP 5 | 选择 **Panorama** > **Zero Touch Provisioning**（零接触配置）> **Setup**（设置），然后编辑 **General**（常规）ZTP 设置。

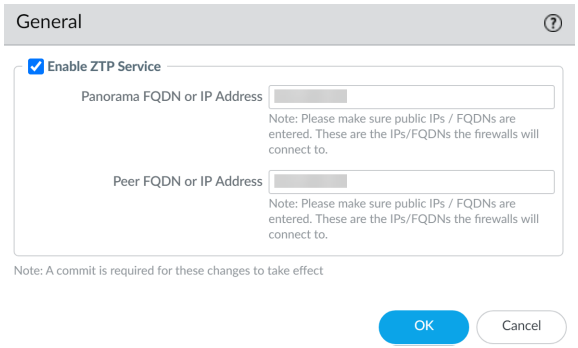
STEP 6 | 向 ZIP 服务注册 Panorama。

1. **Enable ZTP Service**（启用 **ZTP** 服务）。
2. 输入 **Panorama FQDN or IP Address**（**Panorama FQDN** 或 **IP** 地址）。

   这是安装 ZTP 插件以及 CSP 推送到 ZTP 防火墙的 Panorama 的 FQDN 或公共 IP 地址。
3. （仅限 HA）输入 **Peer FQDN or IP Address**（对端 **FQDN** 或 **IP** 地址）。

   这是发生故障转移时安装 ZTP 插件以及 CSP 推送到 ZTP 防火墙的 Panorama 对端的 FQDN 或公共 IP 地址。
4. 单击 **OK**（确定）保存您的配置更改。

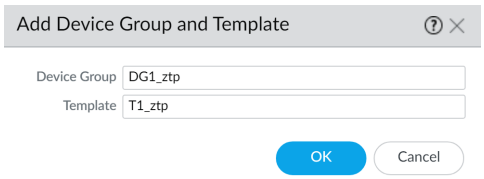
© 2019 Palo Alto Networks, Inc.



STEP 7 | 创建默认设备组和模板来自动生成将 ZTP 防火墙连接到 Panorama 所需的配置。

添加设备组和模板会自动生成一个新设备组和模板，其中包含连接 Panorama 和 ZTP 防火墙的默认配置。

1. **Add Device Group and Template**（添加设备组和模板）。
2. 输入 **Device Group**（设备组）名称。
3. 输入 **Template**（模板）名称。
4. 单击 **OK**（确定）保存您的配置更改。



STEP 8 | 将 ZTP 防火墙添加至在上一步中指定的设备组和模板。

1. 选择 **Panorama** > **Device Groups**（设备组），然后选择已自动创建的设备组。
2. 选择 ZTP **Devices**（设备）。
3. 单击 **OK**（确定）保存您的配置更改。
4. 选择 **Panorama** > **Templates**（模板），然后 **Add Stack**（添加堆栈）。
5. 在 **Templates**（模板）部分，**Add**（添加）已自动生成的模板。
6. 选择 ZTP **Devices**（设备）。
7. 单击 **OK**（确定）保存您的配置更改。

STEP 9 | 验证所需设备组和模板配置是否已成功生成。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网），并选择您在上一步中创建的 **Template**（模板）。
2. 验证 `ethernet1/1` 是否已配置 IP 地址、虚拟路由器和安全区。
3. 选择 **Network**（网络）> **Interfaces**（接口）> **Loopback**（回环），并选择您在上一步中创建的 **Template**（模板）。
4. 验证 `loopback.900` 接口是否已成功创建。
5. 选择 **Policies**（策略）> **Security**（安全性）> **Pre Rules**（预规则），然后选择您在上一步中创建的 **Device Group**（设备组）。
6. 验证 `rule1` 是否已成功创建。
7. 选择 **Policies**（策略）> **NAT** > **Pre Rules**（预规则），然后选择您在上一步中创建的 **Device Group**（设备组）。
8. 验证 `ztp-nat` 是否已成功创建。

STEP 10 | 根据需要修改您的设备组和模板。

© 2019 Palo Alto Networks, Inc.

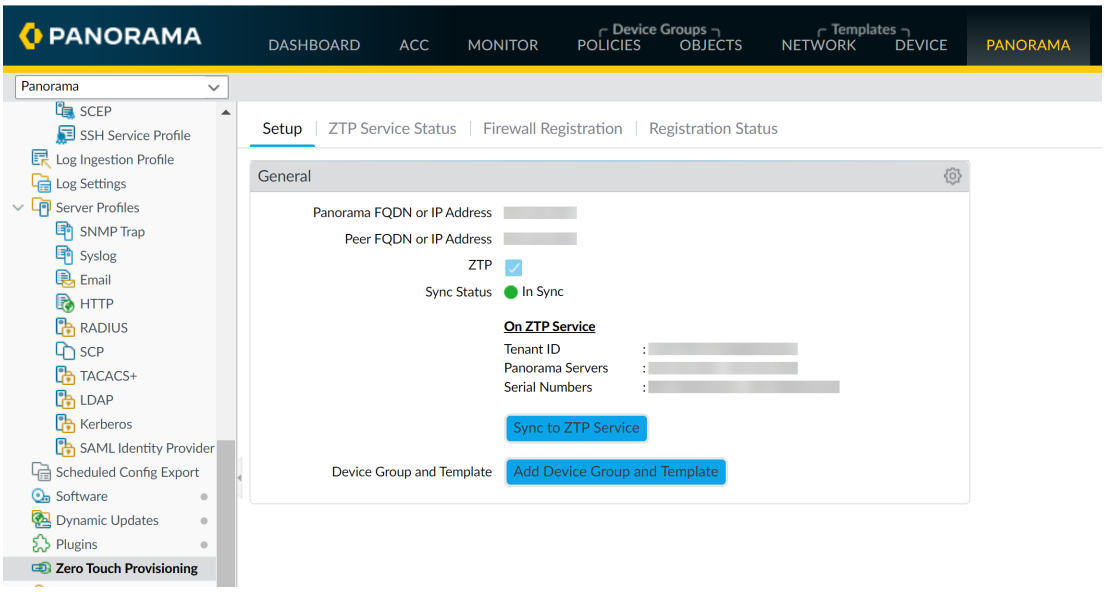
创建和配置新的或现有的设备组和模板以完成您的部署。

在考虑设备组层级和模板堆栈中的模板优先级时，请确保包含所需 ZTP 配置（允许 ZTP 防火墙和 Panorama 通信）的设备组和模板具有优先级，这样在存在冲突配置时不会覆盖配置。

请勿修改 *ethernet1/1* 接口、*loopback.900* 回环接口、*rule1* 安全策略规则或 *ztp-nat NAT* 策略规则的 *IP* 地址、虚拟路由器和安全区。这些是将 *ZTP* 防火墙连接至 *Panorama* 所需的配置。

STEP 11 | 单击 **Commit**（提交）和 **Commit to Panorama**（提交至 **Panorama**）

STEP 12 | **Sync to ZTP Service**（同步至 **ZTP** 服务）并验证 Panorama 同步状态显示为 **In Sync**（同步中）。



为现有部署向 **ZIP** 服务注册 **Panorama**

在 Panorama™ 管理服务器上安装 ZTP 插件后，您必须向 ZTP 服务注册Panorama，以使 ZTP 服务能够将防火墙与 Panorama 关联。作为注册过程中的一部分，在您的 ZTP 防火墙首次连接到 Panorama 之后，将它们添加至其中包含了连接 ZTP 防火墙和 ZTP 服务所需的 ZTP 配置的设备组和模板。

STEP 1 | 安装 Panorama 设备证书。

STEP 2 | 登录到 Palo Alto Networks 客户支持门户 (CSP)。

STEP 3 | 在 Palo Alto Networks CSP 上将您的 Panorama 与 ZTP 服务相关联。

ZTP 服务仅支持与高可用性 (HA) 配置中的最多两个 Panorama 相关联。如果 Panorama 不在 HA 配置中，则只能关联单个 Panorama。

1. 选择 **Assets**（资产）> **ZTP Service**（**ZTP** 服务）和 **Modify Association**（修改关联）。
2. 选择管理 ZTP 防火墙的 Panorama 的序列号。
3. （仅限 HA）选择 Panorama HA 对端的序列号。
4. 单击 **OK**（确定）。

STEP 4 | 登录到 Panorama Web 界面。

© 2019 Palo Alto Networks, Inc.

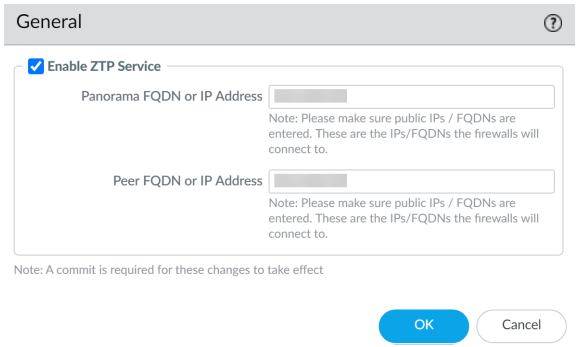
STEP 5 | 选择 **Panorama** > **Zero Touch Provisioning**（零接触配置）> **Setup**（设置），然后编辑 **General**（常规）ZTP 设置。

STEP 6 | 向 ZIP 服务注册 Panorama。

1. **Enable ZTP Service**（启用 **ZTP** 服务）。
2. 输入 **Panorama FQDN or IP Address**（**Panorama FQDN** 或 **IP** 地址）。

   这是安装 ZTP 插件以及 CSP 推送到 ZTP 防火墙的 Panorama 的 FQDN 或公共 IP 地址。
3. （仅限 HA）输入 **Peer FQDN or IP Address**（对端 **FQDN** 或 **IP** 地址）。

   这是发生故障转移时安装 ZTP 插件以及 CSP 推送到 ZTP 防火墙的 Panorama 对端的 FQDN 或公共 IP 地址。
4. 单击 **OK**（确定）保存您的配置更改。



STEP 7 | 将 ZTP 防火墙添加到包含所需 ZTP 配置的设备组和模板。

1. 选择 **Panorama** > **Device Group**（设备组），然后选择将包含所需 ZTP 配置的设备组。
2. 选择 ZTP **Devices**（设备）。
3. 单击 **OK**（确定）保存您的配置更改。
4. 选择 **Panorama** > **Templates**（模板），然后选择模板堆栈，该模板堆栈包含将具备所需 ZTP 配置的模板。
5. 选择 ZTP **Devices**（设备）。
6. 单击 **OK**（确定）保存您的配置更改。

STEP 8 | 根据需要修改您的设备组和模板。

在考虑设备组层级和模板堆栈中的模板优先级时，请确保包含所需 ZTP 配置（允许 ZTP 防火墙和 Panorama 通信）的设备组和模板具有优先级，这样在存在冲突配置时不会覆盖配置。

1. 配置 Ethernet1/1 接口。
   1. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网），然后选择 **Template**（模板）以包含您的 ZTP 配置并选择 **ethernet1/1**。
   2. 对于 **Interface Type**（接口类型），请选择 **Layer3**（第 3 层）。
   3. 选择 **Config**（配置），然后配置 **Virtual Router**（虚拟路由器），再将 **Security Zone**（安全区）设置为 **Untrust**（不信任）。
   4. 单击 **IPv4**；对于 **Type**（类型），选择 **DHCP Client**（**DHCP** 客户端）。

      ZTP 防火墙需要一个 *DHCP* 客户端来与 *ZTP* 服务通信。
   5. 按 **OK**（确定）保存您的配置更改。
2. 创建回环接口

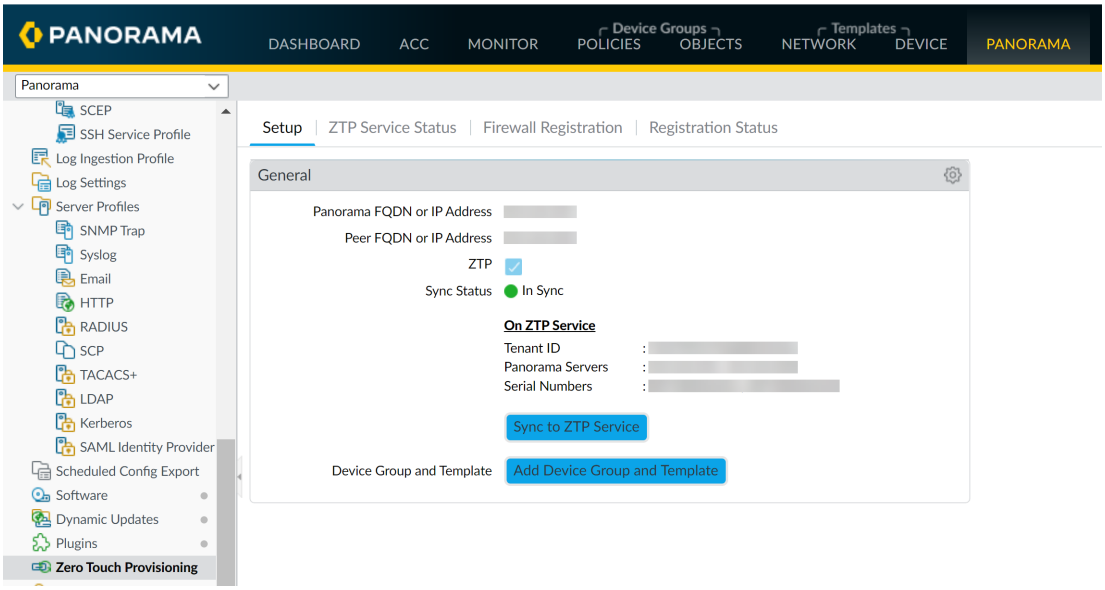
© 2019 Palo Alto Networks, Inc.

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Loopback**（回环），然后选择 **Template**（模板）以包含您的 ZTP 配置并 **Add**（添加）一个回环接口。
2. 对于 **Interface Name**（接口名称），输入 `loopback` 并输入 `900` 后缀。
3. 选择 **Config**（配置），然后选择 **Virtual Router**（虚拟路由器），再将 **Security Zone**（安全区）设置为 **Trust**（信任）。
4. 按 **OK**（确定）保存您的配置更改。

3. 创建安全策略规则以允许 ZTP 防火墙和 Panorama 通信。
   1. 选择 **Policies**（策略）> **Security**（安全性）> **Pre Rules**（预规则），然后选择 **Device Group**（设备组）来包含您的 ZTP 策略规则，并 **Add**（添加）新规则。
   2. 为策略规则输入描述性 **Name**（名称）。
   3. 选择 **Source**（源）> **Source Zone**（源区），并 **Add**（添加）**Trust**（信任）区。
   4. 选择 **Destination**（目标）> **Destination Zone**（目标区），并**Add**（添加）**Untrust**（不信任）区。
   5. 选择 **Action**（操作）> **Action Settings**（操作设置）> **Action**（操作），并选择 **Allow**（允许）。
4. 创建 NAT 策略规则以允许 ZTP 防火墙和 Panorama 通信。
   1. 选择 **Policies**（策略）> **NAT** > **Pre Rules**（预规则），然后选择 **Device Group**（设备组）来包含您的 ZTP 策略规则，并 **Add**（添加）新规则。
   2. 为策略规则输入描述性 **Name**（名称）。
   3. 选择 **Original Packet**（原始包）并配置下列项：
      1. 对于 **Source Zone**（源区），**Add**（添加）**Trust**（信任）区。
      2. 对于 **Destination Zone**（目标区），选择 **Untrust**（不信任）区。
      3. 对于 **Destination Interface**（目标接口），选择 **ethernet1/1** 接口。
   4. 单击 **OK**（确定）保存您的配置更改。

STEP 9 | 单击 **Commit**（提交）和 **Commit to Panorama**（提交至 **Panorama**）

STEP 10 | **Sync to ZTP Service**（同步至 **ZTP** 服务）并验证 Panorama 同步状态显示为 `In Sync`（同步中）。



© 2019 Palo Alto Networks, Inc.

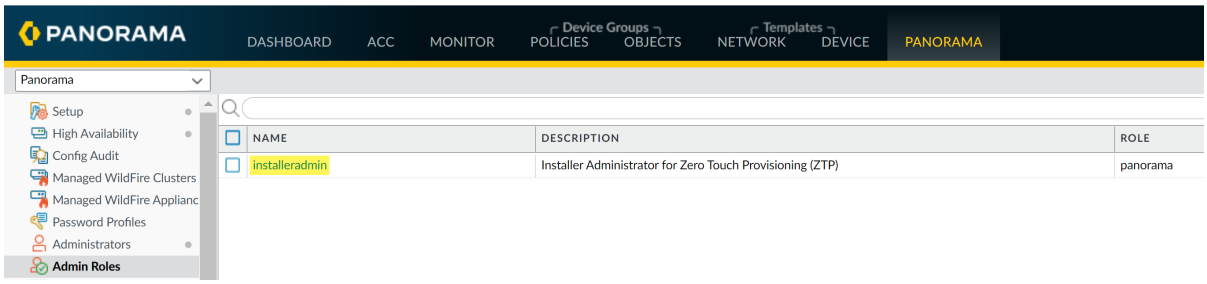
配置 ZTP 安装程序管理员帐户

ZTP 安装程序管理员用户是为非 IT 人员或安装承包商创建的管理员帐户，用于登入新 ZTP 防火墙。安装程序管理员使用一个自动创建的 `installeradmin` 管理员角色来限制 Panorama Web 界面的可见性，并且只允许安装程序在 Panorama 上输入 ZTP 防火墙断言密钥和序列号。

STEP 1 | 登录到 Panorama Web 界面。

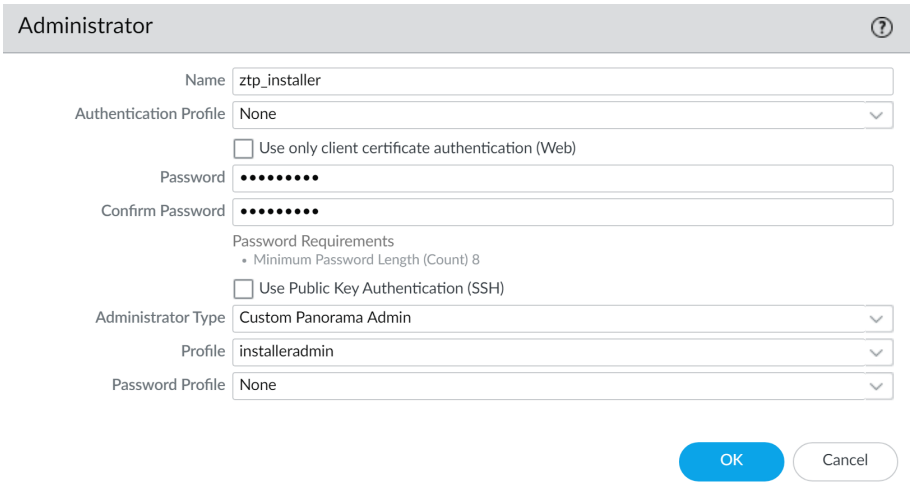
STEP 2 | 选择 **Panorama** > **Admin Roles**（管理员角色），并验证 **`installeradmin`** 管理员角色是否已创建。

当您成功在 Panorama 上安装 ZTP 插件后，就会自动创建 `installeradmin`。



STEP 3 | 配置 ZTP 安装程序管理员用户。

1. 选择 **Panorama** > **Administrators**（管理员），并 **Add**（添加）新管理员用户。
2. 输入 ZTP 安装程序管理员用户的描述性 **Name**（名称）。
3. 输入安全 **Password**（密码）和 **Confirm Password**（确认密码）。
4. 对于 **Administrator Type**（管理员类型），请选择 **Custom Panorama Admin**（自定义 **Panorama** 管理员）。
5. 对于 **Profile**（配置文件），请选择 **installeradmin**
6. 单击 **OK**（确定）保存您的配置更改。



STEP 4 | 选择 **Commit**（提交）和 **Commit to Panorama**（提交到 **Panorama**）。

添加 ZTP 防火墙到 Panorama

您可以添加单个或导入多个 ZTP 防火墙至 Panorama™ 管理服务器。

- 添加 ZTP 防火墙到 Panorama

© 2019 Palo Alto Networks, Inc.

- 导入多个 ZTP 防火墙到 Panorama

添加 *ZTP* 防火墙到 *Panorama*

作为超级用户、Panorama 管理员或 ZTP 安装程序管理员登录到 Panorama™ 管理服务器的 Web 界面以将 ZTP 防火墙添加到 Panorama。如要添加 ZTP 防火墙，必须输入由 Palo Alto Networks 提供的防火墙序列号和断言密钥，然后向 ZTP 服务注册防火墙。通过注册防火墙，可以在客户支持门户帐户中将防火墙声明为您帐户中的资产，并允许 ZTP 服务将防火墙与 Panorama 关联。

当添加 *ZTP* 防火墙到 *Panorama* 时，在步骤 4 中验证防火墙已成功添加到 *Panorama* 之前，不要在 *ZTP* 防火墙上执行任何提交。在 *ZTP* 防火墙上执行本地提交会禁用 *ZTP* 功能，并导致无法成功将防火墙添加至 *Panorama*。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 添加 ZTP 防火墙到 Panorama。

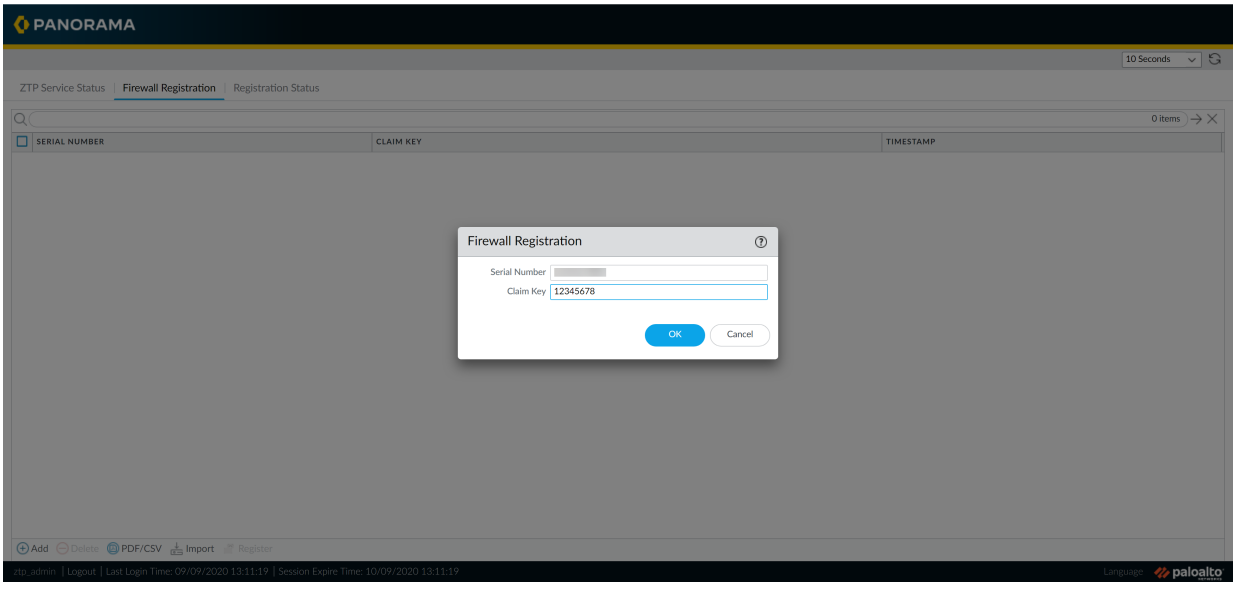
必须连接 *ZTP* 防火墙上的 *Eth1/1* 接口才能成功向 *CSP* 注册 *ZTP* 防火墙并推送策略和网络配置。

1. 选择 **Firewall Registration**（防火墙注册）并 **Add**（添加）新 ZTP 防火墙。
2. 输入该 ZTP 防火墙的 **Serial Number**（序列号）。
3. 输入 Palo Alto Networks 提供的 ZIP 防火墙 **Claim Key**（断言密钥）。

   您从 Palo Alto Networks 接收到的 ZTP 防火墙的背面附有一张物理标签，上面印有 8 位数断言密钥。



4. 单击 **OK**（确定）保存您的配置更改。



STEP 3 | 注册该 ZIP 防火墙。

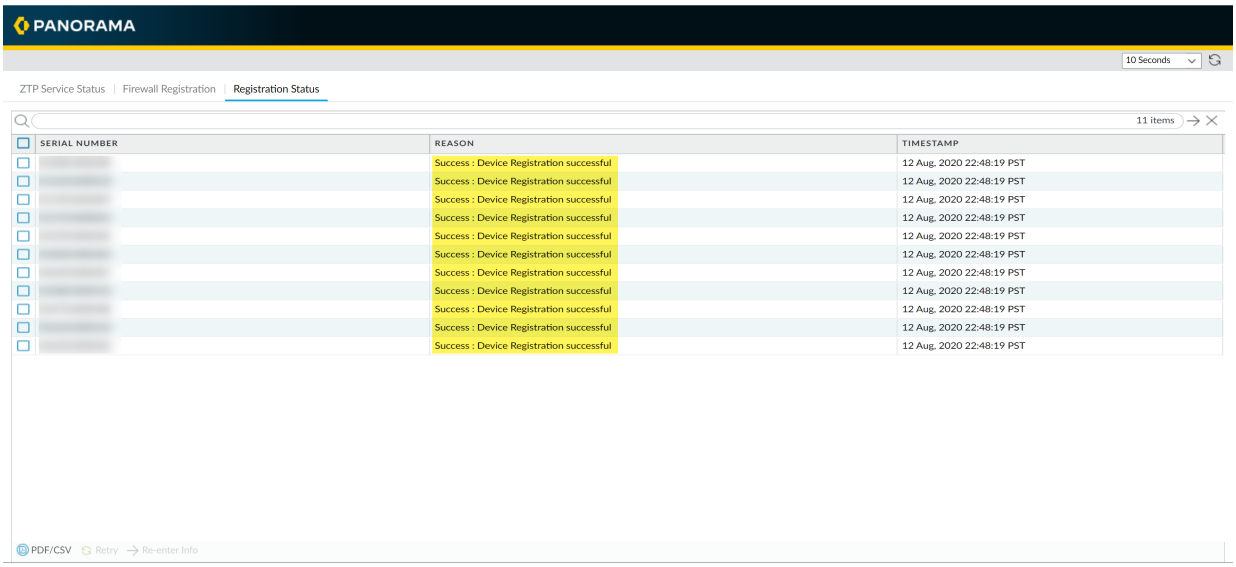
© 2019 Palo Alto Networks, Inc.

1. 选择该新添加的 ZTP 防火墙并 **Register**（注册）该防火墙。
2. 当收到提示时，单击 **Yes**（是）确认注册该 ZTP 防火墙。

STEP 4 | 验证是否成功向 CSP 注册该防火墙。

必须向 *CSP* 成功注册防火墙才能获取设备证书。

1. 选择 **Registration Status**（注册状态）并验证是否已成功向 CSP 注册该 ZTP 防火墙。



2. 登录到 Panorama Web 界面 使用管理员凭据。
3. 选择 **Panorama** > **Managed Devices**（受管设备）> **Summary**（摘要），并验证是否成功将该 ZTP 防火墙添加为受管防火墙。

确保 *To SW Version*（至 *SW* 版本）列被配置为正确 *PAN-OS* 版本，这样防火墙才不会无意间升级或降级。只有 *PAN-OS 10.0.1* 及更高版本才支持 *ZTP* 功能。此外，*PAN-OS* 版本必须与 *Panorama*上运行的 *PAN-OS* 版本相同或是更早版本。

有关详细信息，请参阅升级 ZTP 防火墙。

STEP 5 | 将该 ZTP 防火墙添加到设备组和模板堆栈。

必须将该 ZTP 防火墙添加到设备组和模板堆栈才能让防火墙显示为 `Connected`（已连接），以推送策略和网络配置。

1. 登录到 Panorama Web 界面 使用管理员凭据。
2. 选择 **Panorama** > **Device Groups**（设备组），添加一个设备组，然后将 ZTP 防火墙添加到该设备组。

   添加设备组以创建和配置新设备组，使其包含 ZTP 防火墙的策略对象和规则。
3. 选择 **Panorama** > **Templates**（模板），配置一个模板堆栈，然后将 ZTP 防火墙添加到该模板堆栈。

   配置模板堆栈以创建和配置新模板堆栈，使其包含 ZTP 防火墙的网络配置。

导入多个 *ZTP* 防火墙到 *Panorama*

作为超级用户、Panorama 管理员或 ZTP 安装程序管理员登录到 Panorama™ 管理服务器的 Web 界面以将多个 ZTP 防火墙导入至 Panorama。如要导入多个 ZTP 防火墙，您必须输入包含 Palo Alto Networks 提供的 ZTP 防火墙序列号和相应断言密钥的 CSV 文件，然后向 ZTP 服务注册这些防火墙。通过注册这些防火墙，

© 2019 Palo Alto Networks, Inc.

可以在客户支持门户中将这些防火墙声明为您帐户中的资产，并允许 ZTP 服务将这些防火墙与 Panorama 关联。

当添加 *ZTP* 防火墙到 *Panorama* 时，在步骤 5 中验证防火墙已成功添加到 *Panorama* 之前，不要在 *ZTP* 防火墙上执行任何提交。在 *ZTP* 防火墙上执行本地提交会禁用 *ZTP* 功能，并导致无法成功将防火墙添加至 *Panorama*。

STEP 1 | 收集 ZTP 防火墙的序列号和断言密钥。

您从 Palo Alto Networks 接收到的 ZTP 防火墙的背面附有一张物理标签，上面印有 8 位数断言密钥。



STEP 2 | 创建包含 ZTP 防火墙序列号和断言密钥的 CSV 文件。第一列必须包含序列号，第二列必须包含防火墙相应的断言密钥。请参考以下示例。

	A	B
1	Serial Number	Claim Key
2	abcd1234	123456789
3	xyz7890	987654321

STEP 3 | 将这些 ZTP 防火墙导入至 Panorama。

必须连接 *ZTP* 防火墙上的 *Eth1/1* 接口才能成功向 *CSP* 注册 *ZTP* 防火墙并推送策略和网络配置。

1. 登录到 Panorama Web 界面 使用 ZTP 安装程序管理员凭据。
2. 选择 **Panorama** > **Zero Touch Provisioning**（零接触配置）> **Firewall Registration**（防火墙注册），并 **Import**（导入）这些 ZTP 防火墙。
3. **Browse**（浏览）并选择包含 ZTP 防火墙信息的 CSV 文件，然后点击 **OK**（确定）。

STEP 4 | 注册这些 ZIP 防火墙。

1. 选择这些新添加的 ZTP 防火墙并 **Register**（注册）这些防火墙。
2. 当收到提示时，单击 **Yes**（是）确认注册这些 ZTP 防火墙。

STEP 5 | 验证是否成功向 ZTP 服务注册该防火墙。

1. 选择 **Registration Status**（注册状态）并验证是否成功向 ZTP 服务注册这些 ZTP 防火墙。
2. 登录到 Panorama Web 界面 使用管理员凭据。
3. 选择 **Panorama** > **Managed Devices**（受管设备）> **Summary**（摘要），并验证是否成功向 ZTP 服务注册这些防火墙。

确保 *To SW Version*（至 *SW* 版本）列被配置为正确 *PAN-OS* 版本，这样防火墙才不会无意间升级或降级。只有 *PAN-OS 10.0.1* 及更高版本才支持 *ZTP* 功能。此外，*PAN-OS* 版本必须与 *Panorama* 上运行的 *PAN-OS* 版本相同或是更早版本。

有关详细信息，请参阅升级 ZTP 防火墙。

STEP 6 | 将这些 ZTP 防火墙添加到设备组和模板堆栈。

© 2019 Palo Alto Networks, Inc.

您必须将该 ZTP 防火墙添加到设备组和模板堆栈才能让防火墙显示为 Connected（已连接），以推送策略和网络配置。

1. 登录到 Panorama Web 界面 使用管理员凭据。
2. 选择 **Panorama** > **Device Groups**（设备组），然后将这些防火墙分配至相应设备组。

   添加设备组以创建和配置新设备组，使其包含 ZTP 防火墙的策略对象和规则。
3. 选择 **Panorama** > **Templates**（模板），然后将这些防火墙分配至相应模板堆栈。

   配置模板堆栈以创建和配置新模板堆栈，使其包含 ZTP 防火墙的网络配置。

使用 CLI 进行 ZTP 任务

使用以下 CLI 命令来执行零接触配置 (ZTP) 任务和查看 ZTP 服务状态。

如果您要...	请使用...
从防火墙 **CLI** 管理防火墙	
显示到 ZTP 服务的连接状态。	`> show system ZTP status`
显示到 Panorama 管理服务器的连接状态。	`> show panorama status`
显示 ZTP 型号和防火墙系统信息。	`> show system info`
禁用防火墙上的 ZTP 状态机。 运行此命令不会删除任何现有 ZTP 配置。 在从 *CLI* 禁用防火墙上的 *ZTP* 状态机后，无法再重新启用它。 如要重新启用，必须将防火墙重置为出厂默认设置。	`> request disable ztp`
从 **Panorama** 注册、配置和管理您的 **ZTP** 防火墙	
使用 ZTP 服务在 Eth1/1 接口上创建包含连接受管防火墙和 Panorama 所需配置的设备组或模板。	`> request plugins ztp create dgroup-template device-group <device group name>` `> request plugins ztp create dgroup-template template <template name>`
在防火墙列表中添加一个 ZTP 防火墙，以便将来向 ZTP 服务注册。	`> request plugins ztp firewall-add <serial number> claim-key <claim key>`

© 2019 Palo Alto Networks, Inc.

如果您要...	请使用...
修改已经添加到防火墙列表中的 ZTP 防火墙的序列号，以便将来向 ZTP 服务注册。	`> request plugins ztp firewall-add-modify firewall <old serial number> claim-key <claim key> new-serial <new serial number>`
在防火墙列表中删除一个 ZTP 防火墙，以便将来向 ZTP 服务注册。	`> request plugins ztp firewall-delete firewall <serial number>`
在防火墙列表中添加一个 ZTP 防火墙，以便将来向 ZTP 服务重新注册。 当 ZTP 防火墙最初向 ZTP 服务和需求注册失败时，使用此命令。	`> request plugins ztp firewall-re-enter-info firewall <serial number> claim-key <claim key>`
向 ZIP 服务注册 Panorama™ 管理服务器。	`> request plugins ztp panorama-registration`
向 ZTP 服务注册 ZTP 防火墙。	`> request plugins ztp firewall-registration firewall <serial number> claim-key <claim key>`
向 ZTP 服务重新注册 ZTP 防火墙。 对于向 ZTP 服务最初注册失败的 ZTP 防火墙，使用此命令开始重新注册过程 。	`> request plugins ztp firewall-register-retry firewall <serial number> claim-key <claim key>`
导入 ZTP 防火墙序列号和断言密钥信息。 指定文件必须是 CSV 格式。	`> request plugins ztp ztp-add-import import-path <file path>`
从 **Panorama** 查看 **ZTP** 防火墙信息和 **ZTP** 服务状态	
检索已向 ZTP 服务注册到 Panorama 的 ZTP 防火墙列表。	`> request plugins ztp ztp-service-info` 显示以下详细信息： • `first-firewall-connect-time` — ZTP 防火墙首次连接到 ZTP 服务时的时间戳。 • `last-firewall-connect-time` — ZTP 防火墙最后一次连接到 ZTP 服务时的时间戳。 • `registration-time` — ZTP 防火墙向 ZTP 服务注册时的时间戳。 • `isZTPFirewall` — 防火墙是否为 ZTP 防火墙。 • `created_by` — 添加 ZTP 防火墙的管理用户。

© 2019 Palo Alto Networks, Inc.

如果您要...	请使用...
	• IP Address（IP 地址）— ZTP 防火墙的 IP 地址。
在要向 ZTP 服务注册的防火墙列表中查看 ZTP 防火墙列表。	> show plugins ztp device-add-list
查看 ZTP 防火墙的注册状态。	> show plugins ztp device-reg-status
查看 ZTP 防火墙的 ZTP 服务同步状态。	> request plugins ztp ztp-sync-status
显示完整管理平面 ZTP 连接历史记录。 这有助于对到 ZTP 服务的连接进行故障排除。	> tail follow yes mp-log ms.log

卸载 ZTP 插件

遵循流程从 Panorama™ 管理服务器移除 ZTP 配置和卸载 ZTP 插件。如果 Panorama 为高可用性 (HA) 配置，则在两个 Panorama HA 对上重复这些步骤。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 删除 ZTP 安装程序管理员帐户。

1. 选择 **Panorama** > **Administrators**（管理员），然后选择之前配置的 ZTP 安装程序管理员帐户。
2. **Delete**（删除）ZTP 安装程序管理员帐户。
3. 选择 **Panorama** > **Administrators**（管理员），然后选择 `installeradmin` 管理员角色。
4. **Delete**（删除）`installeradmin` 管理员角色。
5. 选择 **Commit**（提交）和 **Commit to Panorama**（提交到 **Panorama**）。

STEP 3 | 卸载 ZTP 插件

1. 选择 **Panorama** > **Plugins**（插件），然后导航至 Panorama 上安装的 ZTP 插件。
2. 在 Actions（操作）列中，**Remove Config**（移除配置）以从 Panorama 删除 ZTP 相关配置
3. 当系统提示时单击 **OK**（确定）以确认从 Panorama 删除 ZTP 配置。
4. 选择 **Commit**（提交）和 **Commit to Panorama**（提交到 **Panorama**）。
5. **Uninstall**（卸载）ZTP 插件。
6. 当系统提示时单击 **OK**（确定）以从 Panorama 卸载 ZTP 插件。

© 2019 Palo Alto Networks, Inc.

管理设备组

- 添加设备组
- 创建设备组层次
- 创建要在共享或设备组策略中使用的对象
- 还原到继承对象值
- 管理未使用的共享对象
- 管理继承对象的优先级
- 将策略规则或对象移动或克隆到另一设备组
- 在 Panorama 上选择 URL 筛选服务供应商
- 将策略规则推送到防火墙的子集
- 管理规则层次结构

添加设备组

添加防火墙之后（请参阅添加防火墙作为受管设备），您可以将它们划分到设备组（最多 1,024 个），如下所示。请务必将主动-被动高可用性 (HA) 配置中的两个防火墙都分配到同一个设备组中，这样 Panorama 就会将相同的策略规则和对象推送到这些防火墙。PAN-OS 不会跨高可用性对端设备同步推送的规则。若要管理处于您组织中不同管理级别的规则和对象，请创建设备组层次。

STEP 1 | 选择 **Panorama** > **Device Groups**（Panorama > 设备组），然后单击 **Add**（添加）。

STEP 2 | 输入唯一的 **Name**（名称）和 **Description**（说明），以标识设备组。

STEP 3 | 在 Devices（设备）部分中，选择复选框以将防火墙分配到设备组。若要搜索大量的防火墙，请使用筛选器。



您可以将任何防火墙都只分配给一个设备组。您可以将防火墙上的每一个虚拟系统都分配给另一个设备组。

STEP 4 | 在引用模板部分，**Add**（添加）任何具有设备组配置所引用对象的模板或模板堆栈。

您必须为设备组分配适当的模板或模板堆栈参考，以便能成功将模板或模板堆栈关联到设备组。这让您能够引用模板或模板堆栈中配置的对象，无需将不相关的设备添加到模板堆栈。

如果设备组配置未引用模板或模板堆栈内配置的任何对象，则跳过此步骤。

STEP 5 | （可选）对于本身就是高可用性对端设备的防火墙，请选择 **Group HA Peers**（组高可用性对端设备）。

您只能对同一设备组中的受管防火墙 HA 对端设备进行分组。



主动或被动-辅助对端设备的防火墙名称显示在括号中。对 *HA* 对端设备分组是一种视觉变化，并不会产生配置更改。

STEP 6 | 选择将处于您在设备组层次结构中所创建的设备组正上方的 **Parent Device Group**（父设备组）（默认为 **Shared**（共享））。

STEP 7 | 如果您的策略规则将引用用户和用户组，则分配 **Master**（主）防火墙。

在 Panorama 从其中收集用户和用户名的设备组中，这将是唯一的防火墙。

STEP 8 | 单击 **OK**（确定）保存更改。

© 2019 Palo Alto Networks, Inc.

STEP 9 | 选择 **Commit**（提交）> **Commit and Push**（提交并推送），然后将更改 **Commit and Push**（提交并推送）到 Panorama 配置和您所添加的设备组。

创建设备组层次

STEP 1 | 计划设备组层次。

1. 确定设备组级别，以及您将把哪些防火墙和虚拟系统分配到每个设备组和 Shared 位置。您可以将任何一个防火墙或虚拟系统 (vsys) 都只分配给一个设备组。如果某个设备组将仅仅是其他较低级别设备组的组织容器，则您不必向其分配防火墙。
2. 如果防火墙或 vsys 系统分配并不适合您的规划层次，则将这些分配从现有设备组中移除。
   1. 选择 **Panorama** > **Device Groups**（Panorama > 设备组），然后选择设备组。
   2. 在 Devices（设备）部分中，取消勾选您想要移除的防火墙和虚拟系统的复选框，然后单击 **OK**（确定）。
3. 必要时，可添加更多您将向设备组分配的防火墙，请参阅添加防火墙作为受管设备。
4. 如果您使用多个 Panorama 插件来执行端点监视，则包含部署在特定管理程序中的防火墙的设备组不能是包含部署在其他管理程序中的防火墙的设备组的子级或父级。有关详细信息，请参阅设备组层次结构。

STEP 2 | 对于每一个顶层级别的设备组，添加设备组。

1. 在 **Panorama** > **Device Groups**（Panorama > 设备组）页面，单击 **Add**（添加），然后输入**Name**（名称）以标识设备组。
2. 在 Devices（设备）部分中，勾选复选框以将防火墙和虚拟系统分配到设备组。
3. 让 **Parent Device Group**（父设备组）选项保持为 **Shared**（配置）（默认），然后单击 **OK**（确定）。

STEP 3 | 对于每一个较低级别的设备组，添加设备组。

- 对于处于各较低级别的新设备组，重复之前的步骤，但将 **Parent Device Group**（父设备组）设置为处于下一级别之上的设备组。
- 对于每一个现有的设备组，在 **Device Groups**（设备组）页面中，选择要编辑的设备组，选择 **Parent Device Group**（父设备组），然后单击 **OK**（确定）。



如果您将一个设备组移动到另一个父设备组，则其后代设备组也将连同与该设备组及其后代关联的所有防火墙、策略规则和对象，一起随其移动。如果新父设备组位于另一个访问域中，则移动设备组将不再是原访问域的成员。如果新访问域具有父设备组的读写访问权限，则它也将具有移动设备组的读写访问权限。如果新访问域具有父设备组的只读访问权限，则它将不具有移动设备组的任何访问权限。若要重新配置设备组的访问权限，请参阅配置访问域。

STEP 4 | 按照需要配置、移动和复制对象和策略规则以考虑设备组层次中的继承。

- 创建要在共享或设备组策略中使用的对象，或编辑现有对象。

您只能在对象的所处位置（即作为对象分配目的地的设备组）编辑它们。后代设备组将继承来自该位置的对象的只读实例。但是，您可以选择查看步骤覆盖继承的对象值。

- 创建或编辑策略。
- 将策略规则或对象移动或克隆到另一设备组。

STEP 5 | 覆盖继承的对象值。

此操作仅在特定设备组中的对象值必须与继承自祖先设备组的值不同时适用。

覆盖对象后，您可以在后代设备组中再次覆盖它。但是，您无法覆盖共享或预定义（默认）对象。

© 2019 Palo Alto Networks, Inc.

在 **Objects**（对象）选项卡中，继承的对象都具有一个位于 Name（名称）列中的绿色图标，而 Location（位置）列则显示了祖先设备组。

1. 在 **Objects**（对象）选项卡中，选择对象类型（例如 **Objects** > **Addresses**（对象 > 地址））。
2. 选择将具有覆盖实例的 **Device Group**（设备组）。
3. 选择对象，然后单击 **Override**（覆盖）。
4. 编辑各值。您无法编辑 **Name**（名称）或 **Shared**（共享）设置。
5. 单击 **OK**（确定）。Name（名称）列将为对象显示一个黄色与绿色重叠的图标，以表明该对象已被覆盖。



必要时，您可以在稍后还原到继承对象值。

STEP 6 | 保存并提交更改。



在对层次进行任何更改后，提交到 *Panorama* 并推送到设备组。

如果模板引用设备组中的对象（例如接口引用地址），并且分配到模板的防火墙因为层次更改而不再分配到该设备组，则您还必须将更改推送到模板。

选择 **Commit**（提交）> **Commit and Push**（提交并推送），然后将更改 **Commit and Push**（提交并推送）到 Panorama 配置和您所添加或更改的设备组。

创建要在共享或设备组策略中使用的对象

您可以将对象用于任何处于 Shared 位置中、处于该对象所在同一设备组中或处于该设备组后代中的策略规则（有关详细信息，请参阅设备组对象）。



如果您打算利用动态地址组来创建自动适应您网络中更改的策略，请参阅在策略中使用动态地址组以确认 *Panorama* 上受支持的注册 *IP* 地址数。

- 创建共享对象。

  在本例中，我们将添加 URL 筛选类别的共享对象，我们希望针对这些类别来触发警报。

  1. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **URL Filtering**（URL 筛选）选项卡，然后单击 **Add**（添加）。

     Objects（对象）选项卡仅会在您 添加设备组（至少一个设备组）之后出现。
  2. 输入 **Name**（名称）和 **Description**（说明）。
  3. 选择 **Shared**（共享）。
  4. 默认情况下，**Disable Override**（禁用覆盖）选项处于未选择状态，这意味着您可以覆盖所有设备组中对象的继承实例。若要禁用对象覆盖，请勾选此复选框。
  5. 在 **Categories**（类别）选项卡中，选择您希望为之获得通知的每一个类别。
  6. 在 **Action**（操作）列中，选择 **Alert**（警报）。
  7. 单击 **OK**（确定）保存对对象所作的更改。
  8. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

- 创建设备组对象。

  在本例中，我们将为网络上特定的 Web 服务器添加地址对象。

© 2019 Palo Alto Networks, Inc.

1. 选择 **Objects** > **Addresses**（对象 > 地址），然后选择您将在其中使用该对象的 **Device Group**（设备组）。
2. 单击 **Add**（添加）并输入 **Name**（名称）以标识对象。
3. 请务必使 **Shared**（共享）选项处于未选择状态。
4. 默认情况下，**Disable Override**（禁用覆盖）选项处于未选择状态，这意味着您可以覆盖本身就是所选 **Device Group**（设备组）后代的设备组中的对象的继承实例。要禁用对象的覆盖，请选择 **Disable Override**（禁用覆盖）选项。
5. 选择地址对象的 **Type**（类型）以及相关的值。例如，选择 **IP Range**（IP 范围），然后输入 Web 服务器的 IP 地址范围。
6. 单击 **OK**（确定）保存对对象所作的更改。
7. 选择 **Commit**（提交）> **Commit and Push**（提交并推送），然后将更改 **Commit and Push**（提交并推送）到 Panorama 配置和您添加对象的设备组。

- 查看 Panorama 中的共享对象和设备组对象。

  在 **Objects**（对象）选项卡中，Location（位置）列指明了对象是共享对象还是某个设备组的专属对象。

  1. 在 **Objects**（对象）选项卡中，选择对象类型（本例中操作为 **Objects** > **Addresses**（对象 > 地址））。
  2. 选择您已向其添加对象的 **Device Group**（设备组）。

     Objects（对象）选项卡将仅显示处于所选 *Device Group*（设备组）中的或继承自祖先设备组或共享位置的对象。
  3. 验证设备组对象已显示。请注意，Location（地址）列中的设备组名称与 **Device Group**（设备组）下拉列表中的选项一致。

还原到继承对象值

在覆盖设备组对象从祖先设备组继承的值之后，您可以随时将该对象还原到其祖先值。在 **Objects**（对象）选项卡中，覆盖的对象都具有一个位于 Name（名称）列中的黄色与绿色重叠的图标 ()。

如果您想要将祖先值推送到所有覆盖对象，而不是还原特定对象，请参阅管理继承对象的优先级。

有关用于覆盖值的步骤，请参阅步骤5

有关对象继承和覆盖的详细信息，请参阅 设备组对象。

STEP 1 | 在 **Objects**（对象）选项卡中，选择对象类型（例如 **Objects** > **Addresses**（对象 > 地址）），然后选择具有对象覆盖实例的 **Device Group**（设备组）。

STEP 2 | 选择对象，单击 **Revert**（还原），然后单击 **Yes**（是）。Name（名称）列将为对象显示一个绿色图标，指明该对象现在已继承了来自祖先设备组的所有值。

STEP 3 | 选择 **Commit**（提交）> **Commit and Push**（提交并推送），然后将更改 **Commit and Push**（提交并推送）到 Panorama 配置和您还原对象的设备组。

管理未使用的共享对象

当您推送配置更改时设备组，默认情况下，Panorama 会向防火墙推送所有共享对象，而不论任何共享或设备组策略规则是否引用这些对象。但是，您可以将 Panorama 配置为仅推送规则会在设备组中引用的共享对象。**Share Unused Address and Service Objects with Devices**（与设备共享未使用的地址和服务对象）选择可让您限制 Panorama 推送到受管防火墙的对象。

© 2019 Palo Alto Networks, Inc.

禁用 *Share Unused Address and Service Objects with Devices*（与设备共享未使用的地址和服务对象）时，*Panorama* 会在您将策略规则推送到防火墙的子集时忽略 *Target*（目标）防火墙。这意味着，任何规则引用的所有对象都将被推送到设备组内所有防火墙。

要限制推送到一组受管防火墙的对象数，请添加策略规则到子设备组，并根据需要引用共享对象。有关创建子设备组的更多信息，请参阅 创建设备组层次 。

在低端型号上（如 PA-200），请考虑仅将相关的共享对象推送到受管防火墙。这是因为低端型号上可以存储的对象数量比中端或高端型号可以存储的数量少很多。同时，如果您有很多未使用的地址和服务，清除 **Share Unused Address and Service Objects with Devices**（与设备共享未使用的地址和服务对象）选项可以明显缩短防火墙上的提交时间，因为推送到每个防火墙的配置小了很多。但是，禁用此选项可能会增加 Panorama 上的提交时间，因为 Panorama 必须动态检查策略规则是否引用特定对象。

STEP 1 | 选择 **Panorama** > **Setup**（设置）> **Management**（管理），然后 Edit（编辑）Panorama 设置。

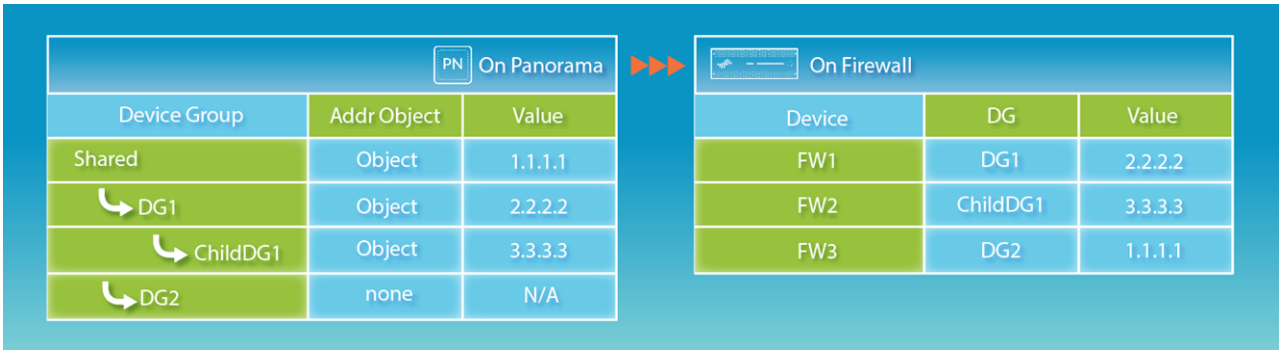
STEP 2 | 清除 **Share Unused Address and Service Objects with Devices**（与设备共享未使用的地址和服务对象）选项以仅推送规则引用的共享对象，或选择此选项以重新启用推送所有共享对象。

STEP 3 | 单击 **OK**（确定）保存更改。

STEP 4 | 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

管理继承对象的优先级

默认情况下，当 设备组层次结构 中多层级上的设备组具有一个名称相同但值不同（例如因覆盖所致）的对象时，后代设备组中的策略规则将使用该后代内的对象值，而不是使用从祖先设备组继承的对象值。或者，您也可以颠倒此优先级测序，将值从包含了对象的最高级祖先推送到所有后代设备组。启用此选项后，下次将配置更改推送到设备组时，继承对象的值会替换后代设备组中任何重写对象的值。下图显示的是设备组内继承对象的优先级：



如果防火墙拥有一个在本地定义的对象，且该对象与从 *Panorama* 推送的共享或设备组对象名称相同，则提交将会失败。

如果您想要将特定覆盖对象还原到其祖先值，而不是将祖先值推送到所有覆盖对象，请参阅还原到继承对象值。

STEP 1 | 选择 **Panorama** > **Setup**（设置）> **Management**（管理），然后Edit（编辑）Panorama 设置。

STEP 2 | 如果您想要颠倒优先级的默认次序，请选择 **Objects defined in ancestors will take higher precedence**（在祖先中定义的对象将具有更高优先级）。对话框随后会显示 **Find Overridden**

© 2019 Palo Alto Networks, Inc.

Objects（查找覆盖对象）链接，该链接提供了一个选项，让您能够查看提交此更改之后有多少覆盖（遮蔽）对象将具有祖先值。您可以将鼠标悬停在数量消息上以显示对象名称。

如果您想要恢复优先级的默认次序，请清除 **Objects defined in ancestors will take higher precedence**（在祖先中定义的对象将具有更高优先级）。

Find Overridden Objects（查找替代对象）仅检测与设备组内其他对象共享名称的共享设备组对象。

STEP 3 | 单击 **OK**（确定）保存更改。

STEP 4 | 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

STEP 5 | （可选）如果您选择 **Objects defined in ancestors will take higher precedence**（在祖先中定义的对象将具有更高的优先级），在您将配置更改推送到设备组之前 Panorama 不会推送祖先对象：选择 **Commit**（提交）> **Push to Devices**（推送到设备），并 **Push**（推送）更改。

将策略规则或对象移动或克隆到另一设备组

在 Panorama 上，如果您将要从设备组移动或克隆的策略规则或对象引用了在目标设备组（**Destination**（目标））中不可用的对象，您必须在操作中同时移动或克隆被引用的对象和引用规则或对象。请记住，在设备组层次中，被引用的对象可能会通过继承而变得可用。例如，共享设备在所有设备组中都可用。您可以执行全局查找来检查引用。如果您移动或克隆某个覆盖对象，请确保已为 **Destination**（目标）的父设备组中的该对象启用了覆盖功能（请参阅创建要在共享或设备组策略中使用的对象）。

复制多个策略规则时，选择规则的顺序将决定它们复制到设备组的顺序。例如，如果您有规则 *1-4*，并且您的选择顺序为 *2-1-4-3*，则复制这些规则的设备组将按照您选择的相同顺序显示规则。但是，一旦成功复制，您可以按照您的意愿重新组织规则。

STEP 1 | 登录到 Panorama，然后选择规则库（例如 **Policy** > **Security** > **Pre Rules**（策略 > 安全 > 前导规则）或对象类型（例如 **Objects** > **Addresses**（对象 > 地址））。

STEP 2 | 选择 **Device Group**（设备组），然后选择一个或多个规则或对象。

STEP 3 | 执行以下步骤之一：

- （仅限规则）**Move**（移动）> **Move to other device group**（移动到另一设备组）
- （仅限对象）**Move**（移动）
- （规则或对象）**Clone**（克隆）

STEP 4 | 在 **Destination**（目标）下拉列表中，选择新设备组或 **Shared**（共享）。默认为上一步中所选择的 **Device Group**（设备组）。

STEP 5 | （仅限规则）选择 **Rule order**（规则次序）：

- **Move top**（置顶）（默认）— 此规则将位于所有其他规则的之前。
- **Move bottom**（置底）— 此规则将位于所有其他规则的之后。
- **Before rule**（前导规则）— 在相邻下拉列表中，选择所选规则之后的规则。
- **After rule**（后继规则）— 在相邻下拉列表中，选择所选规则之前的规则。

STEP 6 | 默认情况下，**Error out on first detected error in validation**（验证时检测到首个错误即停止检查）复选框处于勾选状态，这意味着 Panorama 将显示它发现的第一个错误并停止检查更多的错误。例如，如果 **Destination**（目标）设备组不含您所移动的规则中所引用的对象，则会发生

© 2019 Palo Alto Networks, Inc.

错误。如果您一次移动或克隆多个项目，勾选此复选框可以简化故障排除。如果您取消勾选此复选框，Panorama 将会查找所有错误，然后显示它们。无论是否启用此设置，在您修复所有选定项目的所有错误之前，Panorama 都不会移动或克隆任何项目。

STEP 7 | 单击 **OK**（确定）开始执行错误验证。如果 Panorama 发现了错误，请修复它们，然后重新尝试执行移动或克隆操作。如果 Panorama 未发现错误，它会执行上述操作。

STEP 8 | 选择 Push Scope（推送范围）中的 **Commit**（提交）> **Commit and Push**（提交并推送），**Edit Selections**（编辑选择），选择 **Device Groups**（设备组），选择原始和目标设备组，单击 **OK**（确定），然后将更改 **Commit and Push**（提交并推送）到 Panorama 配置和设备组。

在 Panorama 上选择 URL 筛选服务供应商

URL 筛选可让防火墙监控和控制用户的 Web 访问。配置用于控制 Web 访问的策略规则（安全性、QoS、强制网络门户和解密）会引用 URL 类别。您可以在 Panorama 上选择 URL 筛选服务供应商，以确定可以引用添加到设备组和推送到防火墙的规则中的 URL 类别。

在默认情况下，Panorama 使用 PAN-DB，这是紧密集成到 PAN-OS 和 Palo Alto Networks Threat Intelligence Cloud 的 URL 筛选数据库。PAN-DB 提供高性能本地缓存，最大化 URL 查找的内联性能。其他供应商选项是 Brightcloud，第三方 URL 数据库。



与防火墙不同，*Panorama* 不下载 *URL* 数据库，因此不需要 *URL* 筛选许可证。

以下主题描述了如何在 Panorama 或同时在 Panorama 和受管防火墙上更改 URL 筛选服务供应商。您还可以仅在防火墙上更改 URL 筛选服务供应商。

- Panorama 和防火墙是否必须有匹配的 URL 筛选服务供应商？
- 在高可用性 Panorama 上更改 URL 筛选服务供应商
- 在非高可用性 Panorama 上更改 URL 筛选服务供应商
- 将 Panorama 和高可用性防火墙从 BrightCloud 迁移到 PAN-DB
- 将 Panorama 和非高可用性防火墙从 BrightCloud 迁移到 PAN-DB

Panorama 和防火墙是否必须有匹配的 *URL* 筛选服务供应商？

在任何一台 Panorama 管理服务器或防火墙上，只能激活一个 URL 筛选服务供应商：PAN-DB 或 BrightCloud。当为 Panorama 选择供应商时，您必须考虑供应商和受管防火墙的 PAN-OS 版本：

- PAN-OS 5.0.x 及更早版本 — Panorama 和防火墙需要匹配 URL 筛选服务供应商。
- PAN-OS 6.0 或更新版本 — Panorama 和防火墙不需要匹配 URL 筛选服务供应商。如果检测到供应商不匹配，则防火墙会将从 Panorama 收到的 URL 筛选配置文件和规则中的 URL 类别映射到与在防火墙上启用的供应商匹配的 URL 类别。

因此，对于其中有一部分防火墙运行 PAN-OS 6.0 或更高版本而另一部分防火墙则运行较早版本 PAN-OS 的部署，Panorama 必须使用与运行较早版本的 PAN-OS 的防火墙相同的 URL 筛选服务供应商。例如，如果运行 PAN-OS 5.0 的防火墙使用 PAN-DB，而运行 PAN-OS 7.0 的防火墙使用 BrightCloud，则 Panorama 必须使用 PAN-DB。

在高可用性 *Panorama* 上更改 *URL* 筛选服务供应商

在高可用性 (HA) 部署中，更改 URL 筛选服务供应商时，每个 Panorama 对端设备必须处于非功能状态。因此，为了避免干扰 Panorama 操作，在被动 Panorama（此例中为 Panorama2）上更改 URL 筛选服务供应商，然后触发故障转移后再在主动 Panorama（此例中为 Panorama1）更改供应商。

© 2019 Palo Alto Networks, Inc.

STEP 1 | 在每个 Panorama 高可用性对端设备上更改 URL 筛选服务供应商。

在 *Panorama2*（被动对端设备）中完成此任务，再在 *Panorama1*（主动对端设备）上执行。

1. 登录到 Panorama Web 界面。
2. 选择 **Panorama** > **High Availability**（Panorama > 高可用性），**Suspend local Panorama**（挂起本地 Panorama）。

   您在 Panorama1 上执行此步骤时会触发故障转移，Panorama2 变成主动设备。
3. 选择 **Panorama** > **Setup** > **Management**（Panorama > 设置 > 管理），然后编辑“General Settings（常规设置）”。
4. 选择 **URL Filtering Database**（**URL** 筛选数据库）供应商：**paloaltonetworks** (PAN-DB) 或 **brightcloud**。
5. 选择 **Panorama** > **High Availability**（Panorama > 高可用性），**Make local Panorama functional**（运行本地 Panorama）。

   当您在两个高可用性对端设备上都启用 preemption（默认设置）的 Panorama1 上执行此步骤时，Panorama1 自动恢复为主动状态，Panorama2 恢复为被动状态。

STEP 2 | 验证这些 URL 类别是否可用于在策略中引用。

1. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **URL Filtering**（**URL** 筛选）。
2. 单击 **Add**（添加），然后验证 URL Filtering profile（URL 筛选配置文件）对话框的 **Categories**（类别）选项卡是否显示了与所选供应商关联的 URL 类别。

在非高可用性 *Panorama* 上更改 *URL* 筛选服务供应商

在未部署在高可用性 (HA) 配置中的 Panorama 管理服务器上执行此程序更改 URL 筛选服务供应商。

STEP 1 | 更改 URL 筛选服务供应商。

1. 选择 **Panorama** > **Setup** > **Management**（Panorama > 设置 > 管理），然后编辑“General Settings（常规设置）”。
2. 选择 **URL Filtering Database**（**URL** 筛选数据库）供应商：**paloaltonetworks** (PAN-DB) 或 **brightcloud**。

STEP 2 | 验证这些 URL 类别是否可用于在策略中引用。

1. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **URL Filtering**（**URL** 筛选）。
2. 单击 **Add**（添加），然后验证 URL Filtering profile（URL 筛选配置文件）对话框的 **Categories**（类别）选项卡是否显示了与所选供应商关联的 URL 类别。

将 *Panorama* 和高可用性防火墙从 *BrightCloud* 迁移到 *PAN-DB*

当防火墙部署在高可用性 (HA) 配置中时，执行此程序在 Panorama 和防火墙上，将 URL 筛选服务供应商从 BrightCloud 迁移到 PAN-DB。在本例中，主动（或主动-主要）防火墙的名称为 fw1，而被动（或主动-辅助）防火墙的名称为 fw2。此迁移会自动将 BrightCloud URL 类别映射到 PAN-DB URL 类别。

STEP 1 | 确定哪些防火墙需要新的 PAN-DB URL 筛选许可证。

1. 登录到 Panorama，然后选择 **Panorama** > **Device Deployment** > **Licenses**（Panorama > 设备部署 > 许可证）。
2. 检查 URL 列，确定哪些防火墙具有 PAN-DB 许可证，这些许可证是有效还是过期。

   防火墙可以同时拥有 BrightCloud 和 PAN-DB 的有效许可证，但只能激活一个许可证。

© 2019 Palo Alto Networks, Inc.

如果您不确定 *PAN-DB URL* 筛选许可证是否激活，访问防火墙 *Web* 界面，选择 *Device* > *Licenses*（设备 > 许可证），验证 *PAN-DB URL Filtering*（*PAN-DB URL* 筛选）部分中的 *Active*（激活）字段是否显示 *Yes*（是）。

3. 为没有有效 PAN-DB 许可证的每个防火墙购买新许可证。

   在高可用性部署中，每个防火墙对端设备需要不同的 PAN-DB 许可证和授权码。Palo Alto Networks 会发送一封包含您购买的许可证的对应激活代码的电子邮件。如果找不到此电子邮件，请联系客户支持部门，然后再继续操作。

STEP 2 | 在 Panorama 上将 URL 筛选服务供应商更改为 PAN-DB。

访问 Panorama Web 界面，然后执行以下任务之一：

- 在高可用性 Panorama 上更改 URL 筛选服务供应商
- 在非高可用性 Panorama 上更改 URL 筛选服务供应商

STEP 3 | 在两个防火墙高可用性对端设备上配置 TCP 会话设置，确保尚未同步的会话将在您挂起一个对端设备时进行故障转移。

登录到 CLI（每个防火墙），运行以下命令：

```
> set session tcp-reject-non-syn no
```

STEP 4 | 在每个防火墙高可用性对端设备上将 URL 筛选服务供应商迁移到 PAN-DB。

在 *fw2*（被动或主动-辅助对端设备）上完成此任务，再在 *fw1*（主动或主动-主要对端设备）上完成。

1. 访问防火墙 Web 界面，选择 **Device** > **High Availability** > **Operational Commands**（设备 > 高可用性 > 操作命令），然后单击 **Suspend local device**（挂起本地设备）。

   触发故障转移到 fw2 时，在 fw1 上执行此步骤。
2. 选择 **Device**（设备）> **Licenses**（许可证）。
3. 在 License Management（许可证管理）部分中，选择 **Activate feature using authorization code**（使用授权代码激活功能），输入 **Authorization Code**（身份验证代码），并单击 **OK**（确定）。

   激活 PAN-DB 许可证会使 BrightCloud 许可证自动停用。
4. 在 PAN-DB URL Filtering（PAN-DB URL 筛选）部分中，**Download**（下载）种子文件，选择所在区域，单击 **OK**（确定）。
5. 提交并推送配置更改：
   1. 访问 Panorama Web 界面。
   2. 选择 **Commit**（提交）> **Commit and Push**（提交并推送）和 Push Scope（推送范围）中的 **Edit Selections**（编辑选择）。
   3. 选择 **Device Groups**（设备组），选择防火墙，然后单击 **OK**（确定）。
   4. 将更改 **Commit and Push**（提交并推送）到 Panorama 配置和设备组。
6. 访问防火墙 Web 界面，选择 **Device** > **High Availability** > **Operational Commands**（设备 > 高可用性 > 操作命令），然后单击 **Make local device functional**（使本地设备正常运行）。

   当您在两个防火墙上都启用 preemption（默认设置）的 fw1 上执行此步骤时，fw1 自动恢复为主动（或主动-主要）状态，fw2 恢复为被动（或主动-辅助）状态。

STEP 5 | 将两个防火墙高可用性对端设备还原为原始 TCP 会话设置。

在各防火墙的 CLI 中运行以下命令：

© 2019 Palo Alto Networks, Inc.

```
> set session tcp-reject-non-syn yes
```

将 *Panorama* 和非高可用性防火墙从 *BrightCloud* 迁移到 *PAN-DB*

当防火墙未部署在高可用性 (HA) 配置中时，执行此程序在 Panorama 和防火墙上，将 URL 筛选服务供应商从 BrightCloud 迁移到 PAN-DB。此迁移会自动将 BrightCloud URL 类别映射到 PAN-DB URL 类别。

STEP 1 | 确定哪些防火墙需要新的 PAN-DB URL 筛选许可证。

1. 登录到 Panorama，然后选择 **Panorama** > **Device Deployment** > **Licenses**（Panorama > 设备部署 > 许可证）。
2. 检查 URL 列，确定哪些防火墙具有 PAN-DB 许可证，这些许可证是有效还是过期。

   防火墙可以同时拥有 BrightCloud 和 PAN-DB 的有效许可证，但只能激活一个许可证。

   如果您不确定 *PAN-DB URL* 筛选许可证是否激活，访问防火墙 *Web* 界面，选择 *Device* > *Licenses*（设备 > 许可证），验证 *PAN-DB URL Filtering*（*PAN-DB URL* 筛选）部分中的 *Active*（激活）字段是否显示 *Yes*（是）。
3. 为没有有效 PAN-DB 许可证的防火墙购买新的许可证。

   Palo Alto Networks 会发送一封包含您购买的许可证的对应激活代码的电子邮件。如果找不到此电子邮件，请联系客户支持部门，然后再继续操作。

STEP 2 | 在 Panorama 上将 URL 筛选服务供应商更改为 PAN-DB。

访问 Panorama Web 界面，然后执行以下任务之一：

- 在高可用性 Panorama 上更改 URL 筛选服务供应商
- 在非高可用性 Panorama 上更改 URL 筛选服务供应商

STEP 3 | 在每个防火墙上将 URL 筛选服务供应商迁移到 PAN-DB。

1. 访问防火墙 Web 界面，然后选择 **Device**（设备）> **Licenses**（许可证）。
2. 在 License Management（许可证管理）部分中，选择 **Activate feature using authorization code**（使用授权代码激活功能），输入 **Authorization Code**（身份验证代码），并单击 **OK**（确定）。

   激活 PAN-DB 许可证会使 BrightCloud 许可证自动停用。
3. 在 PAN-DB URL Filtering（PAN-DB URL 筛选）部分中，**Download**（下载）种子文件，选择所在区域，单击 **OK**（确定）。
4. 提交并推送配置更改：
   1. 访问 Panorama Web 界面。
   2. 选择 **Commit**（提交）> **Commit and Push**（提交并推送）和 Push Scope（推送范围）中的 **Edit Selections**（编辑选择）。
   3. 选择 **Device Groups**（设备组），选择防火墙，然后单击 **OK**（确定）。
   4. 将更改 **Commit and Push**（提交并推送）到 Panorama 配置和设备组。

将策略规则推送到防火墙的子集

策略目标可让您在设备组中指定将作为策略规则推送目的地的防火墙。它可让您排除一个或多个防火墙或虚拟系统，或者仅将规则应用到设备组中的特定防火墙或虚拟系统。

随着规则库的发展以及将新建或修改过的规则推送到防火墙时，如果未在创建或修改规则时存档，更改和审核信息会随时间的推移而丢失。使用审核注释存档查看选中规则的审核注释以及配置日志历史记录，并比较两个策略规则版本以查看如何发生更改的规则。从 Panorama 推送的规则审核注释历史记录仅可通过 Panorama 管理服务器查看。但是，您可以在从受管防火墙转发到 Panorama 的配置日志中查看审核注释。

© 2019 Palo Alto Networks, Inc.

但是，无法从防火墙本地创建或修改的规则上查看审核注释存档。要确保在创建或修改规则时捕获审核注释，请实施策略规则、说明、标记和审核注释。

定位规则的功能使您可以将策略集中在 Panorama 上。目标规则允许您在 Panorama 上定义规则（作为共享或设备组前导规则和后续规则）（有关详细信息，请参阅设备组策略），并提高管理规则的可见性和效率。通过审核注释存档，您可以跟踪策略规则如何以及为什么随时间发生变化，从而提升可见性，以便您可以在规则生命周期内审核规则演变。

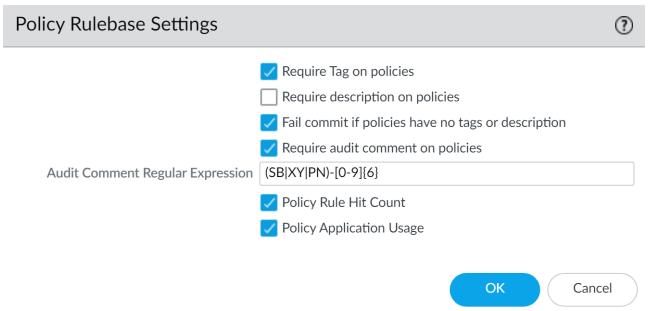
STEP 1 | （最佳实践）对策略规则实施审核注释。

虽然此步骤是可选的，但也是针对策略规则实施审核注释的最佳做法，确保您能捕获创建或修改规则的原因。此外，这一操作还有助于维护用于审核的规则历史记录准确性。

1. 选择 **Panorama** > **Setup**（设置）> **Management**（管理），然后编辑策略规则库设置。
2. 启用 **Require audit comment on policies**（策略所需审核注释）选项。
3. 配置审核注释正则表达式，以规定审核注释格式。

   创建或修改规则时，通过指定字母和数字表达式，要求审核遵循基于业务和审核需求的特定格式。例如，您可以使用此设置指定正则表达式，以匹配您的票据号格式：

   - **[0-9]{<Number of digits>}** — 要求审核注释包含从 0 到 9 的最小位数。例如，**[0-9]{6}** 需要至少 6 位数值（数字 0 到 9）表达式。按需配置所需的最小位数。
   - **<Letter Expression>** — 要求审核注释包含字母表达式。例如，**Reason for Change-**要求管理员使用此字母表达式作为审核注释的开头。
   - **<Letter Expression>-[0-9]{<Number of digits>}**— 要求审核注释包含一组最小位数（0 到 9）的字符串前缀。例如，**SB-[0-9]{6}** 要求审核注释格式以**SB-** 开头，后跟一个最小 6 位（0 到 9 的数字）的数值表达式，例如 **SB-012345**。
   - **(<Letter Expression>)|(<Letter Expression>)|-[0-9]{<Number of digits>}** — 要求审核注释包含使用所配置的其中一组最小位数（0 到 9 的数字）的字母表达式的前缀。例如，**(SB|XY|PN)-[0-9]{6}** 要求审核注释格式以 **SB--**、**XY-** 或 **PN-** 开头，后跟一个最小 6 位（从 0 到 9 的数字）的数值表达式，例如 **SB-012345**、**XY-654321** 或 **PN-012543**。
4. 点击 **OK**（确定）以应用新的策略规则库设置。



5. 选择 **Commit**（提交）和 **Commit to Panorama**（提交到 **Panorama**）。

STEP 2 | 创建规则。

在本例中，我们将在安全性策略规则库中定义一项允许内部网络中用户访问 DMZ 中服务器的前导规则。

1. 选择 **Policies**（策略）选项卡，然后选择您想要为其定义规则的 **Device Group**（设备组）。
2. 选择规则库。对于本例，选择 **Policies** > **Security** > **Pre-Rules**（策略 > 安全 > 前导规则），然后 **Add**（添加）规则。
3. 在 **General**（常规）选项卡上，输入规则的描述性 **Name**（名称），然后，输入 **Audit Comment**（审核注释）。
4. 在 **Source**（源）选项卡中，将 **Source Zone**（源区域）设置为 **Trust**（信任）。
5. 在 **Destination**（目标）选项卡中，将 **Destination Zone**（目标区域）设置为 **DMZ**。

© 2019 Palo Alto Networks, Inc.

6. 在 **Service/URL Category**（服务/URL 类别）选项卡中，将 **Service**（服务）设置为**application-default**。
7. 在 **Actions**（操作）选项卡中，将 **Action**（操作）设置为 **Allow**（允许）。
8. 为所有其他选项集保留默认值。

STEP 3 | 对规则进行定向以包含或排除防火墙的子集。

若要将规则应用到选定防火墙集：

1. 在“策略规则”对话框中选择 **Target**（目标）选项卡。
2. 选择要为其使用规则的防火墙。

   如果您未选择要定向的防火墙，则策略将会添加到设备组中的所有（未勾选）防火墙。

   默认情况下，虽然设备组内虚拟系统复选框为禁用状态，除非您选择一个或多个您想为其使用规则的虚拟系统，否则，所有虚拟系统都将在提交时继承规则。
3. （可选）要从继承规则中排除防火墙子集，请 **Install on all but specified devices**（在除指定设备以外的所有设备上安装），并选择想要排除的防火墙。

   如果您选择了 *Install on all but specified devices*（在除指定设备以外的所有设备上安装）且没有选择任何防火墙，则规则将不会添加到设备组中的任何防火墙。
4. 单击 **OK**（确定）以添加规则。

STEP 4 | 提交并推送配置更改。

1. 选择 **Commit**（提交）> **Commit and Push**（提交并推送）和推送范围中的 **Edit Selections**（编辑选择）。
2. 选择 **Device Groups**（设备组），选择您添加规则的设备组，然后单击 **OK**（确定）。
3. 将更改 **Commit and Push**（提交并推送）到 Panorama 配置和设备组。

STEP 5 | 排除策略规则流量匹配问题验证规则是否如预期一样允许和拒绝流量。

管理规则层次结构

策略规则的次序对您网络的安全而言至关重要。在任何策略层级（共享、设备组或本地定义规则）和规则库（例如共享安全前导规则）内，防火墙会按照规则在 **Policies**（策略）选项卡的页面中所出现的次序从上到下地对这些规则进行评估。防火墙将根据符合所定义的条件的第一个规则匹配数据包，并忽略后继规则。因此，若要执行最特别的匹配，应将较特别的规则移动到较普通的规则之上。

若要了解防火墙在设备组层次分层级和分类型（前导规则、后继规则和默认规则）地评估规则时所遵循的次序，请参阅设备组策略。

STEP 1 | 查看每个规则库的规则层次结构。

1. 选择 **Policies**（策略）选项卡，然后单击 **Preview Rules**（预览规则）。
2. 按 **Rulebase**（规则库）（例如 **Security**（安全）或 **QoS**）筛选预览。
3. 筛选预览以显示特定 **Device Group**（设备组）的规则和该设备组从 Shared 位置和祖先设备组继承的规则。您必须选择已具有分配防火墙的设备组。
4. 按 **Device**（设备）筛选预览以显示其在本地定义的规则。
5. 单击绿色箭头图标，将您的筛选选项应用到预览（请参阅设备组策略）。
6. 完成对规则的预览之后，关闭“Combined Rules Preview（组合规则预览）”对话框。

STEP 2 | 必要时，删除或禁用规则。

© 2019 Palo Alto Networks, Inc.

若要确定防火墙当前未使用哪些规则，请在 *Panorama* 上的 *Context*（上下文）下拉列表中选择该防火墙，选择规则库（例如 *Policies* > *Security*（策略 > 安全）），然后勾选 *Highlight Unused Rules*（突出显示未使用的规则）复选框。橙色的虚线背景指明了防火墙未使用的规则。

1. 选择包含了您将删除或禁用的规则的规则库（例如 **Policies** > **Security** > **Pre Rules**（策略 > 安全 > 前导规则））。
2. 选择包含了该规则的 **Device Group**（设备组）。
3. 选择该规则，然后按需要单击 **Delete**（删除）或 **Disable**（禁用）。禁用的规则将以斜体字体显示。

STEP 3 | 必要时，在规则库内重新定位规则。

若要在防火墙上重新定位本地规则，应在执行本步骤之前，通过在 *Context*（上下文）下拉列表中选择该防火墙以访问其 *Web* 界面。

1. 选择包含了您将移动的规则的规则库（例如 **Policies** > **Security** > **Pre Rules**（策略 > 安全 > 前导规则））。
2. 选择包含了该规则的 **Device Group**（设备组）。
3. 选择该规则，选择 **Move**（移动），然后选择：
   - **Move Top**（置顶）— 将该规则移动到设备组中所有其他规则之上（但不在继承自 Shared 或祖先设备组的规则之上）。
   - **Move Up**（上移）— 将该规则移动到其前面那一条规则之上（但不在继承自 Shared 或祖先设备组的规则之上）。
   - **Move Down**（下移）— 将该规则移动到其后面那一条规则之下。
   - **Move Bottom**（置底）— 将该规则移动到所有其他规则之下。
   - **Move to other device group**（移动到其他设备组）— 请参阅将策略规则或对象移动或克隆到另一设备组。

STEP 4 | 如果您已修改规则，请提交并推送更改。

1. 选择 **Commit**（提交）> **Commit and Push**（提交并推送）和推送范围中的 **Edit Selections**（编辑选择）。
2. 选择 **Device Groups**（设备组），选择包含您已更改或删除的规则的设备组，然后单击 **OK**（确定）。
3. 将更改 **Commit and Push**（提交并推送）到 Panorama 配置和设备组。

© 2019 Palo Alto Networks, Inc.

管理模板和模板堆栈

使用模板和模板堆栈可定义使防火墙能够在您网络中运行的通用基本配置。在您决定要将哪些防火墙添加到哪些模板时、命令堆栈中的模板管理通用及防火墙组别特定设置时以及使用防火墙特定值覆盖模板设置时，请参阅模板和模板堆栈以从总体上了解您应当考虑的问题。



若要删除模板，您必须首先在防火墙上通过本地方式禁用/删除模板设置。只有具备超级用户角色的管理员才能禁用模板。

- 模板功能和例外
- 添加模板
- 配置模板堆栈
- 配置模板或模板堆栈变量
- 导入和覆盖现有模板堆栈变量
- 覆盖模板设置
- 禁用/删除模板设置

模板功能和例外

您可以使用模板和模板堆栈来定义一系列的设置，但您只能通过本地方式在每个受管防火墙上执行以下任务：

- 配置设备阻止列表。
- 清除日志。
- 启用正常模式、multi-vsys 模式、或 FIPS-CC 模式等操作模式。
- 配置高可用性对中防火墙的 IP 地址。
- 配置主密钥和诊断。
- 比较配置文件（配置审核）。



若要为防火墙管理许可证和更新（软件或内容），应使用 *Panorama* > *Device Management*（设备管理）选项卡选项；请勿使用模板。

- 在多虚拟系统防火墙上重命名虚拟系统。

添加模板

您必须首先添加至少一个模板，这样 Panorama™ 才会显示在定义防火墙的网络设置和设备配置时所必需的 **Device**（设备）和 **Network**（网络）选项卡。Panorama 最多支持 1,024 个模板。每个受管防火墙都必须归属于一个模板堆栈。虽然模板包含受管设备配置，但模板堆栈允许您管理模板配置，并将其推送到分配给模板堆栈的所有受管防火墙。



将模板组合到模板堆栈中以避免在模板之间复制多个配置（请参阅模板和模板堆栈以及配置模板堆栈）。

STEP 1 | 添加模板。

1. 选择 **Panorama** > **Templates**（模板）。
2. 单击 **Add**（添加），然后输入唯一的 **Name**（名称）以标识该模板。
3. （可选）输入模板的 **Description**（说明）。
4. 单击 **OK**（确定）保存模板。

© 2019 Palo Alto Networks, Inc.

5. 如果该模板具有一个包含了您想要 Panorama 推送给不支持虚拟系统的防火墙的多项配置（例如接口）的虚拟系统 (vsys)，则选择您创建的模板，然后从 **Default VSYS**（默认虚拟系统）下拉列表中选择该虚拟系统，最后单击 **OK**（确定）。
6. 选择 **Commit**（提交）> **Commit and Push**（提交并推送），然后将更改 **Commit and Push**（提交并推送）到 Panorama 配置和模板。

STEP 2 | 验证模板可用。

当您添加第一个模板之后，Panorama 将会显示 **Device**（设备）和 **Network**（网络）选项卡。这些选项卡将显示 **Template**（模板）下拉列表。检查该下拉列表是否显示了您刚才添加的模板。

STEP 3 | 配置模板堆栈，然后将模板添加到模板堆栈。

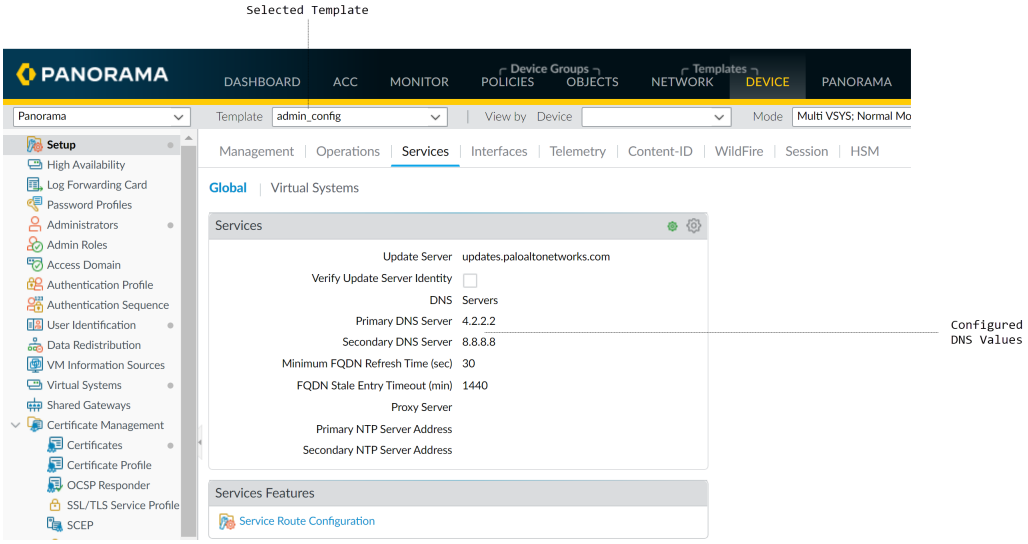
STEP 4 | 使用该模板，将配置更改推送到防火墙。

只有在本地防火墙上才允许重命名 *vsys*，而不是在 *Panorama* 上，结果是获得全新的 *vsys* 或新的 *vsys* 名称被映射到防火墙上错误的 *vsys*。

例如，让我们为该模板中的防火墙定义一个主要域名系统 (DNS) 服务器。

您还可以配置模板或模板堆栈变量，以将设备特定值推送到受管设备。

1. 在 **Device**（设备）选项卡中，从下拉列表中选择 **Template**（模板）。
2. 选择 **Device** > **Setup** > **Services** > **Global**（设备 > 设置 > 服务 > 全局），然后编辑“Services（服务）”部分。
3. 输入 **Primary DNS Server**（主 **DNS** 服务器）的 IP 地址。

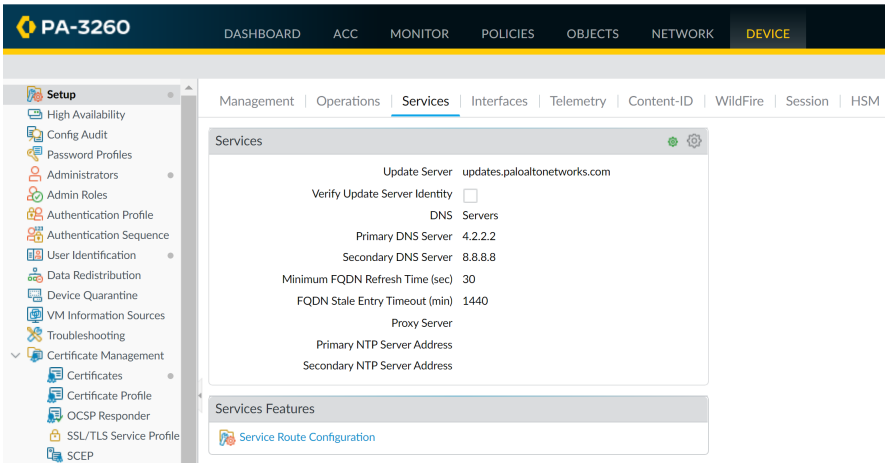


4. 选择 **Commit**（提交）> **Commit and Push**（提交并推送），然后将更改 **Commit and Push**（提交并推送）到 Panorama 配置和模板。

STEP 5 | 验证该防火墙已配置有您之前从 Panorama 推送的模板设置。

1. 在 **Context**（上下文）下拉列表中，选择您已向其推送了模板设置的防火墙之一。
2. 选择**Device**（设备）> **Setup**（设置）> **Services**（服务）> **Global**（全局）。您之前从模板推送的 IP 地址随即将会显示。Services（服务）部分标头会显示一个模板图标（ ），指明该部分中的设置具有推送自模板的值。

© 2019 Palo Alto Networks, Inc.



STEP 6 | 排除网络资源连接问题确认防火墙可以访问您的网络资源。

配置模板堆栈

模板堆栈是可配置的，并允许您合并多个模板，以将整个配置推送到您的受管防火墙。虽然模板是您的防火墙配置的模块化部分，可以在多个堆栈中重复使用，但您还可以配置模板堆栈，以填充需要在分配给堆栈的所有防火墙之间应用的剩余配置。Panorama 最多支持 1,024 个模板堆栈，每个堆栈最多可分配 8 个模板。您可以从模板堆栈所属的模板中应用模板堆栈内配置的对象。如果模板堆栈和堆栈中的模板在值方面发生冲突，将推送模板堆栈中配置的值。有关详细信息和规划，请参阅模板和模板堆栈。

添加模板以配置接口、*VLAN*、虚拟线路、*IPSec* 隧道、*DNS* 代理和虚拟系统。必须配置这些对象，并从模板（而非模板堆栈）推送。一旦从模板推送，您就可以覆盖模板堆栈中除虚拟系统以外的所有对象。

STEP 1 | 规划模板及其在堆栈中的次序。

添加模板，这是您计划分配给模板堆栈的模板。

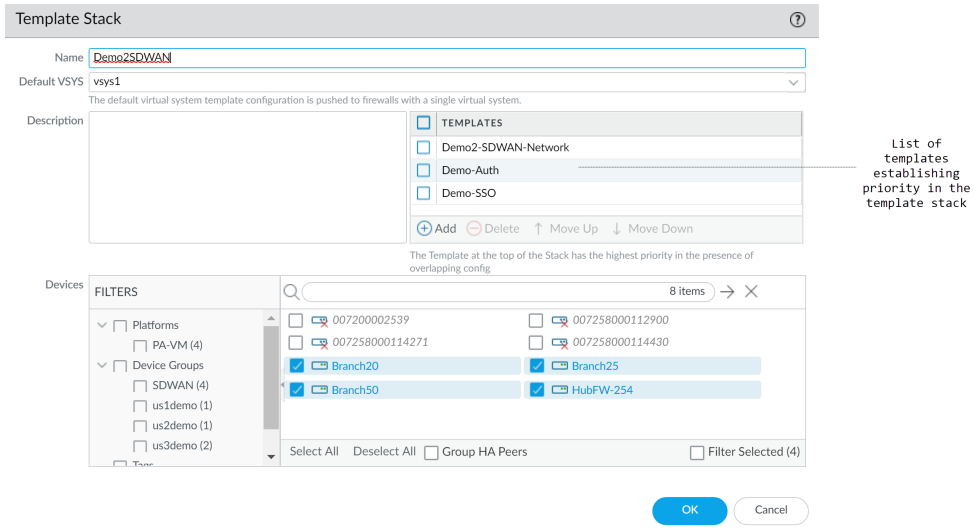
在您规划堆栈内模板的优先级次序（以重叠设置）时，必须检查次序以防止配置错误。例如，假设有一个堆栈，其中 *ethernet1/1* 接口在模板 *A* 中为 *Layer 3* 类型，但在模板 *B* 中则为带有 *VLAN* 的 *Layer 2* 类型。如果模板 *A* 具有更高的优先级，则 *Panorama* 会将 *ethernet1/1* 作为 *Layer 3* 类型推送，但将其分配到 *VLAN*。

亦请注意，即使两个模板都在同一堆栈中，其中一个模板的配置也无法引用另一个模板中的配置。例如，模板 A 中的区域配置无法引用模板 B 中的区域保护配置文件。

STEP 2 | 创建模板堆栈。

1. 选择 **Panorama** > **Templates**（模板），然后 **Add Stack**（添加堆栈）。
2. 输入唯一的**Name**（名称）以标识该堆栈。
3. 对于将合并在堆栈中的每一个堆栈（最多为 8 个），**Add**（添加），然后选择该模板。对话框将按照与重复设置有关的优先级次序列出添加的模板，其中较高优先级模板中的值将覆盖较低优先级模板的值。要更改顺序，选择模板，然后 **Move Up**（向上移）或 **Move Down**（向下移）。

© 2019 Palo Alto Networks, Inc.



4. 在设备部分中，选择防火墙以将其分配到堆栈。对于具有多个虚拟系统的防火墙，您不能分配单个虚拟系统，只能分配整个防火墙。您可以将任何防火墙都只分配给一个模板堆栈。

   每当您将新的受管防火墙添加到 *Panorama* 时，必须将其分配给相应的模板堆栈；*Panorama* 不会自动分配新的防火墙至模板或模板堆栈。当将配置更改推送到模板时，*Panorama* 会将配置推送到已分配给模板堆栈的每个防火墙。

5. （可选）选择 **Group HA Peers**（组高可用性对端设备）以显示高可用性 (HA) 配置中防火墙的复选框。图标将指明高可用性状态：绿色代表主动；黄色代表被动。辅助对端设备的防火墙名称显示在括号中。

   对于主动/被动高可用性，将两个对端设备都添加到同一个模板，这样两者便都将接收配置。对于主动/主动高可用性，您是否将两个对端设备都添加到同一个模板取决于每个对端设备是否都需要相同的配置。有关 PAN-OS 在高可用性对端设备间所同步的配置的列表，请参阅高可用性同步。

6. 单击 **OK**（确定）以保存模板堆栈。

STEP 3 | （可选）配置模板或模板堆栈变量。

STEP 4 | 必要时，编辑 **Network**（网络）和 **Device**（设备）设置。

只有在本地防火墙上才允许重命名 *vsys*。如果您在 *Panorama* 上重命名虚拟系统，您将创建一个全新的虚拟系统，或者新的虚拟系统名称可能会映射到防火墙上的错误虚拟系统。

在单个防火墙上下文中，您可以采用与您覆盖推送自模板的设置时相同的方法来覆盖 Panorama 从堆栈推送的设置：请参阅覆盖模板或模板堆栈值。

1. 筛选选项卡，以仅显示您想要编辑的模式特定设置：

   虽然 *Panorama* 只会将模式特定设置推送到支持这些模式的防火墙，但这种选择性的推送并不会调整模式特定值。例如，如果某个模板既拥有联邦信息处理标准 *(FIPS)* 模式下的防火墙，又拥有采用非 *FIPS* 算法的 *IKE Crypto* 配置文件，那么模板推送将会失败。若要避免此类错误，请使用 *Network*（网络）和 *Device*（设备）选项卡中的 *Mode*（模式）下拉列表以筛选模式特定功能和值选项。

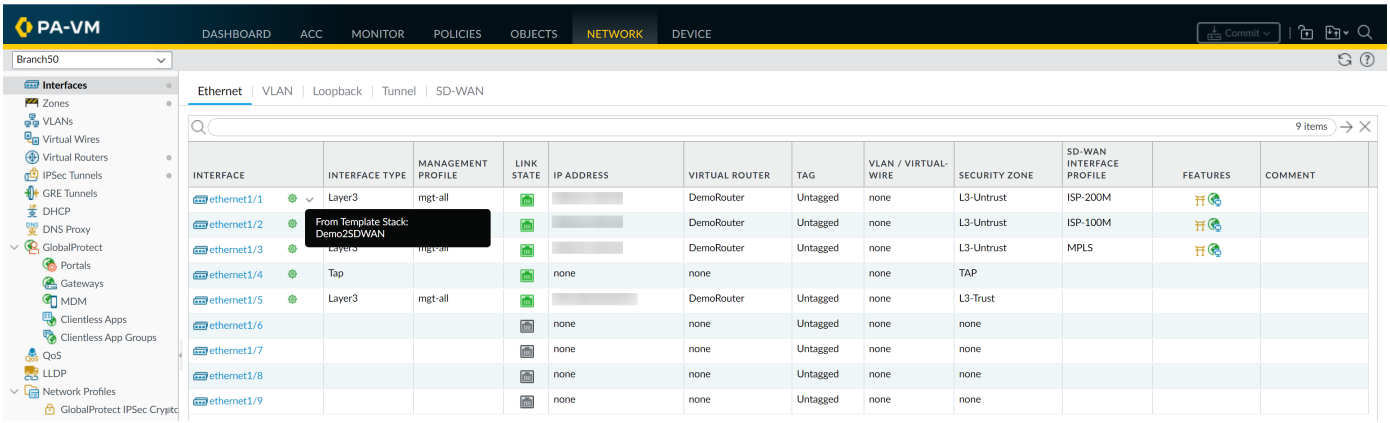
   - 在 **Mode**（模式）下拉列表中，选择或清除 **Multi VSYS**（多虚拟系统）、**Operational Mode**（操作模式）和 **VPN Mode**（VPN 模式）筛选选项。
   - 通过在 **Device**（设备）下拉列表中选择特定防火墙，将所有 **Mode**（模式）选项设置为显示该防火墙的模式配置。

© 2019 Palo Alto Networks, Inc.

2. 建立您的接口和网络连接。例如，配置区域和接口，以对您的网络进行分段，从而管理和控制通过您的防火墙的通信。
3. 按需要编辑设置。
4. 选择推送范围中的 **Commit**（提交）> **Commit and Push**（提交并推送），**Edit Selections**（编辑选择），选择 **Templates**（模板），选择要分配给模板堆栈的防火墙，然后将更改 **Commit and Push**（提交并推送）到 Panorama 配置和模板堆栈。

STEP 5 | 验证模板堆栈工作与预期相符。

1. 从 **Context**（上下文）下拉列表中选择分配给模板堆栈的设备。
2. 选择选项卡，以便通过模板堆栈推送配置更改。
3. 推送自模板堆栈的值会显示一个模板图标（ ），指明该部分中的设置具有推送自模板的值。将鼠标悬停在堆栈上，以查看是哪个模板堆栈推送的值。



STEP 6 | 排除网络资源连接问题确认防火墙可以访问您的网络资源。

配置模板或模板堆栈变量

要更轻松地重用模板或模板堆栈，您可以使用模板和模板堆栈变量替换您的配置中的 IP 地址、组 ID 和接口。模板变量在模板或模板堆栈级别定义，您可以使用这些变量替换 IKE、VPN 和 HA 配置中的 IP 地址、IP 范围、FQDN 和接口，以及组 ID。因为模板配置的优先级高于模板堆栈配置，因此，模板中定义的变量会覆盖模板堆栈中定义的变量。通过变量，您可以减少需要管理的模板和模板堆栈总数，同时保留任何特定于防火墙或设备的值。例如，您的模板堆栈拥有基本配置，则可以使用变量创建不可用于模板或模板堆栈中所有防火墙的值。这允许您管理和推送来自少量模板和模板堆栈的配置，同时考虑任何特定于防火墙或设备的值。在您能够创建新模板或模板堆栈前，这些值为必备项。

要创建模板或模板堆栈变量：

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 创建模板和模板堆栈。

1. 添加模板
2. 配置模板堆栈。

STEP 3 | 选择 **Panorama** > **Templates**（模板），然后 **Manage**（管理）（变量列）想要创建变量的模板或模板堆栈。

STEP 4 | **Add**（添加）新变量。

变量的名称必须以美元 ($) 符号开头。

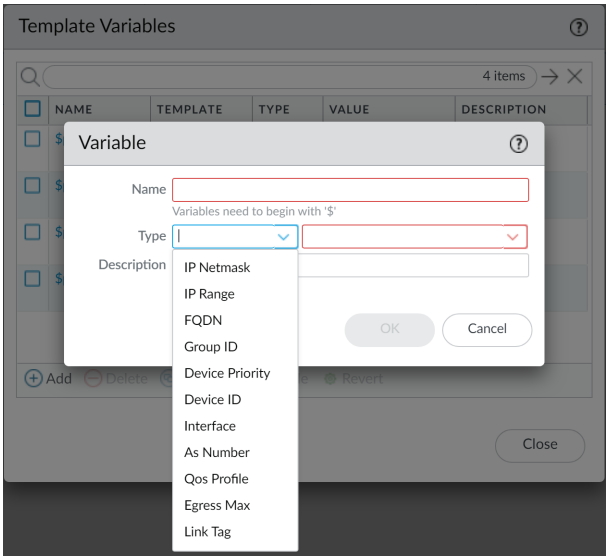
1. 命名新变量。在此示例中，变量名为 `$DNS-primary` 和 `$DNS-secondary`。

© 2019 Palo Alto Networks, Inc.

2. 选择变量 **Type**（类型），并为所选变量类型输入相应的值。

   在此示例中，选择 **IP Netmask**（**IP** 网络掩码）。
3. （可选）为变量输入描述。
4. 单击 **OK**（确定）和 **Close**（关闭）。

还可以在支持变量的位置在线创建变量。



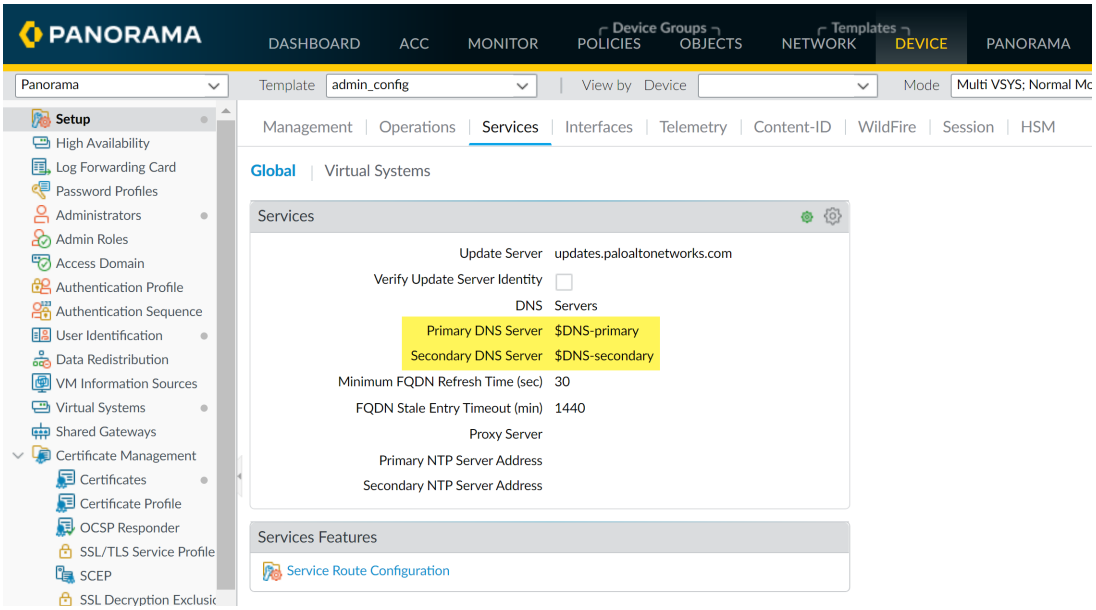
STEP 5 | 从 **Template**（模板）下拉列表选择变量所属的模板或模板堆栈。

STEP 6 | 在适当的位置输入变量。

对于此例，请参考向前定义的 DNS 值。

1. 选择 **Device**（设备）> **Setup**（设置）> **Services**（服务），并编辑服务。
2. 输入 **`$DNS-primary`**，或从 **Primary DNS Server**（主 **DNS** 服务器）下拉列表中选择它。
3. 输入 **$DNS-secondary**，然后从 **Secondary DNS Server**（辅助 **DNS** 服务器）下拉列表中选择它。
4. 单击 **OK**（确定）。

© 2019 Palo Alto Networks, Inc.

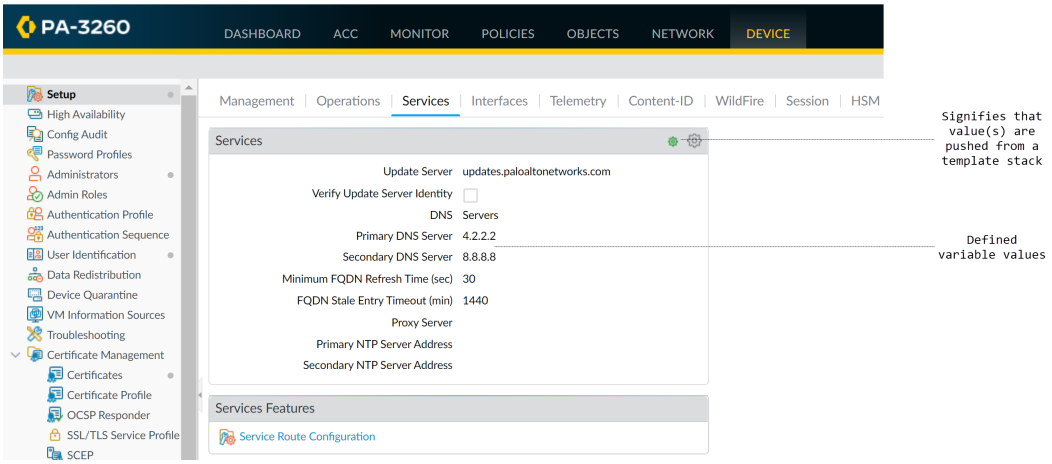


STEP 7 | 单击 **Commit**（提交），**Commit and Push**（提交并推送）您的更改至受管防火墙。

通过引用模板或模板堆栈变量推送设备组配置时，您必须 *Edit Selections*（编辑选择），并 *Include Device and Network Templates*（包括设备和网络模板）。

STEP 8 | 检验是否所有变量值均已推送至受管设备。

1. 从 **Context**（上下文）下拉列表中选择属于创建变量模板堆栈的防火墙。
2. 选择**Device**（设备）> **Setup**（设置）> **Services**（服务）。
3. 模板符号 (.) 用于指示模板或模板堆栈定义的设置（带值）。将鼠标悬停在指示器上，以查看变量定义所属的模板或模板堆栈。从防火墙上下文进行查看时，变量将显示为您为该变量配置的 IP 地址。



STEP 9 | 排除网络资源连接问题确认防火墙可以访问您的网络资源。

导入和覆盖现有模板堆栈变量

使用模板堆栈变量更换防火墙配置中的 IP 地址、IP 范围、FQDN、接口或组 ID。通过变量，您可以减少需要管理的模板和模板堆栈总数，同时保留任何特定于防火墙的值。

© 2019 Palo Alto Networks, Inc.

通过导入模板堆栈变量，您可以覆盖多个现有变量值，并且在导入时不能创建新的模板堆栈变量。关于如何创建新模板或模板堆栈变量的更多信息，请参阅配置模板或模板堆栈变量。

STEP 1 | 登录到 Panorama Web 界面。

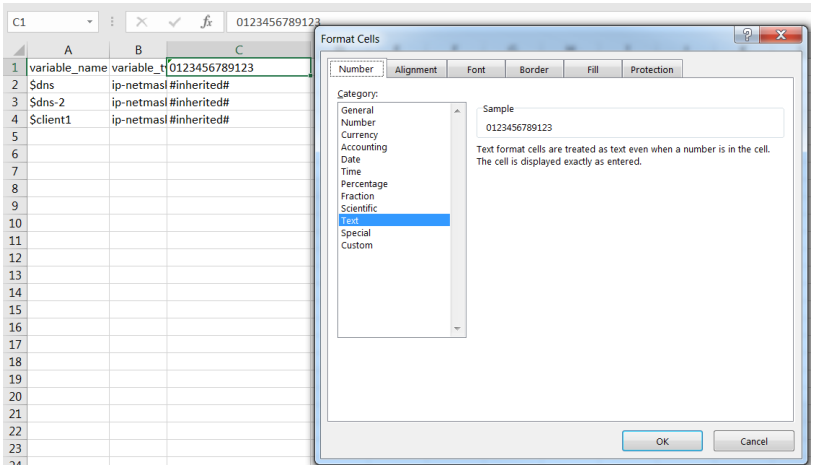
STEP 2 | 导出现有模板堆栈变量。

1. 选择 **Panorama** > **Templates**（模板），然后选择模板或模板堆栈。
2. 选择 **Variable CSV**（变量 **CSV**）> **Export**（导出）。配置的模板堆栈变量作为 CSV 文件下载到本地。
3. 打开导出的 CSV。

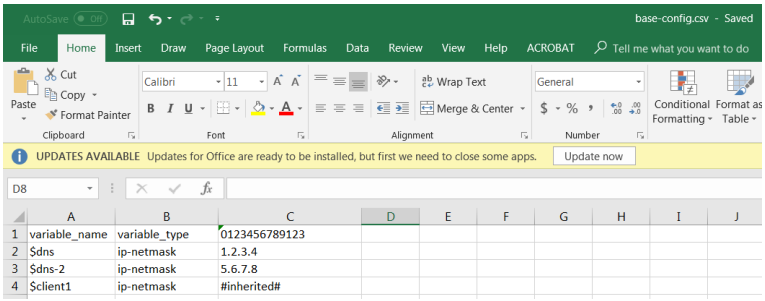
STEP 3 | 编辑包含模板堆栈变量的 CSV 文件，以便按下列格式导入到 Panorama：

显示为 `#inherited#` 的值是在模板堆栈中定义的值。

1. 更正包含防火墙序列号的单元数量。对 CSV 文件中所有防火墙重复此步骤。
   1. 右键单击包含防火墙序列号的单元格，然后选择 **Format Cells**（格式化单元格）。
   2. 选择 **Number**（编号）> **Text**（文本），然后单击 **OK**（确定）。
   3. 在序列号开头处添加一个 **0**。



2. 输入所需模板变量的新值。
3. 选择 **File**（文件）> **Save As**（另存为），然后以 **CSV UTF-8** 格式保存文件。



STEP 4 | 将 CSV 文件导入到模板堆栈。

1. 登录到 Panorama Web 界面。
2. 选择 **Panorama** > **Templates**（模板），并选择在步骤 2 中导出变量的模板堆栈。
3. 选择 **Variable CSV**（变量 **CSV**）> **Import**（导入）并 **Browse**（浏览）步骤 3 中编辑的 CSV 文件。
4. 单击 **OK**（确定）以导入模板堆栈变量。

© 2019 Palo Alto Networks, Inc.

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

STEP 6 | 在适当位置输入变量。

STEP 7 | 单击 **Commit**（提交），**Commit and Push**（提交并推送）您的更改至受管防火墙。

通过引用模板或模板堆栈变量推送设备组配置时，您必须 *Edit Selections*（编辑选择），并 *Include Device and Network Templates*（包括设备和网络模板）。

覆盖模板或模板堆栈值

虽然模板和模板堆栈可让您向多个防火墙应用基本配置，但您仍可能希望配置不一定适用于模板或模板堆栈中所有防火墙的防火墙特定设置。相反，您可能想要覆盖模板设备，以创建一个能将其用作您所有受管防火墙基本配置的模板堆栈配置。模板覆盖可让例外或修改满足您的配置需求。例如，如果您使用模板创建了基本配置，但测试实验室环境中的少数防火墙需要域名系统 (DNS) 服务器 IP 地址或网络时间协议 (NTP) 服务器的不同设置，则您可以覆盖这些模板和模板堆栈设置。

如果您想要禁用或删除防火墙上的所有模板或堆栈设置，而不是覆盖单个值，请参阅禁用/删除模板设置。

您可以通过以下方式之一覆盖模板或模板堆栈值：

- 覆盖防火墙的模板值 或 使用变量覆盖模板或模板堆栈值—有两种方法可以覆盖推送自模板或模板堆栈的值。第一种方法是本地确定防火墙上的值，以覆盖推送自模板或模板堆栈的值。第二种方法是确定特定防火墙变量，以覆盖推送自模板或模板堆栈的值。
- 使用模板堆栈覆盖模板值—确定模板堆栈上的值或变量，以覆盖推送自模板的值。

覆盖防火墙模板值

覆盖本地防火墙上推送自模板或模板堆栈的设置，以创建特定防火墙配置。为此，您可以管理 Panorama™ 的基本模板或模板堆栈配置，同时保留任何不适用于其他防火墙的特定防火墙配置。

STEP 1 | 访问防火墙 Web 界面。

在浏览器的 URL 字段中输入防火墙的 IP 地址以直接访问该防火墙，或在 Panorama 中使用 **Context**（上下文）下拉列表以切换至防火墙上下文。

STEP 2 | 覆盖推送自模板或模板堆栈的值。

在本例中，您将覆盖您之前利用添加模板中的模板而分配的 DNS 服务器 IP 地址。

1. 选择 **Device**（设备）> **Setup**（设置）> **Services**（服务），并编辑服务部分。
2. 单击 **Primary DNS Server**（主要 **DNS** 服务器）的模板图标 ( ) 以启用对字段的覆盖。
3. 输入 **Primary DNS Server**（主要 **DNS** 服务器）的新 IP 地址。模板覆盖符号 ( ) 表明，模板值已被覆盖。
4. 单击 **OK**（确定）并 **Commit**（提交）更改。

使用模板堆栈覆盖模板值

您可以使用模板堆栈值覆盖从模板推送至受管防火墙的配置，以创建您可以用于管理 Panorama™ 受管防火墙基本配置的模板堆栈配置。为此，您可以利用 Panorama 的管理能力将配置更改从单个位置推送至多个设备。在此示例中，您可以使用模板堆栈覆盖推送自模板且名为 `$DNS` 的主要 DNS 服务器 IP 地址变量。

© 2019 Palo Alto Networks, Inc.

Panorama 支持使用模板堆栈覆盖模板中配置的接口，聚合接口的第 *2* 层子接口除外。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 从 **Template**（模板）下拉列表中选择将覆盖模板配置的模板堆栈。

STEP 3 | 覆盖已推送的模板配置。

1. 选择 **Device**（设备）> **Setup**（设置）> **Services**（服务），并编辑服务部分。
2. 配置带 IP 地址的 **Primary DNS**（主要 **DNS**）以覆盖已推送的模板配置，然后单击 **OK**（确定）。

STEP 4 | **Commit and Push**（提交并推送）配置更改。

使用模板堆栈变量覆盖模板值

您可以使用模板堆栈值和变量覆盖从模板推送至受管防火墙的配置，以创建您可以用于管理 Panorama™ 受管防火墙基本配置的模板堆栈配置。为此，您可以利用 Panorama 的管理能力将配置更改从单个位置推送至多个防火墙。在此示例中，您可以通过覆盖推送自模板且名为 `$DNS` 的主要 DNS 服务器 IP 地址变量创建模板堆栈变量。

Panorama 支持使用模板堆栈覆盖模板中配置的接口，聚合接口的第 *2* 层子接口除外。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 覆盖模板变量。

1. 选择 **Panorama** > **Templates**（模板）。
2. **Manage**（管理）（变量列）包含所需覆盖模板的模板堆栈。
3. 查找并选择 **$DNS**变量。
4. 选择 **Override**（覆盖）。
5. 输入新的变量值，并单击 **OK**（确定）。

STEP 3 | **Commit and Push**（提交并推送）更改。

使用变量覆盖模板或模板堆栈值

您可以使用特定防火墙变量来覆盖从模板或模板堆栈推送至受管防火墙的变量，从而创建特定防火墙配置。为此，您可以管理基本模板或模板堆栈配置，同时保留任何不适用于其他所有来自 Panorama™ 的防火墙的特定防火墙配置 。这使您能够利用 Panorama 管理能力的同时考虑单个防火墙所需的任何特定配置。在此示例中， 推送自模板且名为 `$DNS` 的主要 DNS 服务器 IP 地址变量将被覆盖，以创建特定防火墙变量。

您可以覆盖尚未被覆盖的模板或模板堆栈变量。如果模板或模板堆栈变量已被覆盖，则 *Revert*（恢复）覆盖以创建特定防火墙变量。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 覆盖模板或模板堆栈变量。

1. 选择 **Panorama** > **Managed Devices**（受管设备）> **Summary**（摘要）。
2. **Edit**（编辑）（变量列）包含需要覆盖的变量的防火墙。
3. 查找并选择 **$DNS**变量。
4. 选择 **Override**（覆盖）。
5. 输入特定防火墙新 IP 地址，然后单击 **OK**（确定）。

© 2019 Palo Alto Networks, Inc.

STEP 3 | **Commit and Push**（提交并推送）更改。

禁用/删除模板设置

如果您希望停止使用模板或模板堆栈来管理受管防火墙上的配置，则可以禁用模板或堆栈。禁用模板/堆栈时，您可以将模板/堆栈值复制到防火墙的本地配置，或者删除这些值。



如果您想要覆盖单个设置，而不是禁用或删除每一个模板或堆栈设置，请参阅覆盖模板设置。

有关如何使用模板和模板堆栈来管理防火墙的详细信息，请参阅模板和模板堆栈。

STEP 1 | 以具有超级用户角色的管理员身份访问受管防火墙的 Web 界面。您可以通过在浏览器 URL 字段中输入其 IP 地址，或者在 Panorama 中选择 **Context**（上下文）下拉列表中的防火墙直接访问防火墙。

STEP 2 | 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后 Edit（编辑）Panorama 设置。

STEP 3 | 单击 **Disable Device and Network Template**（禁用设备和网络模板）。

STEP 4 | （可选）选择 **Import Device and Network Template before disabling**（在禁用之前导入设备和网络模板）可在防火墙上保存本地配置设置。如果不选择此选项，PAN-OS 将会从防火墙删除 Panorama 推送的所有设置。

STEP 5 | 单击 **OK**（确定）两次，然后 **Commit**（提交）更改。

© 2019 Palo Alto Networks, Inc.

从 Panorama 管理主密钥

Panorama、防火墙、日志收集器、以及 WF-500 设备使用主密钥加密配置中的敏感元素，且具有用于加密密码和配置元素的默认主密钥。

作为标准安全实践的一部分，您应替换默认主密钥，并在其到期之前更改每个单独防火墙、日志收集器、WildFire 设备、和 Panorama 上的密钥。您必须部署相同的主密钥到所有受管设备，且必须在 Panorama 上配置主密钥，以成功将配置从 Panorama 推送到受管设备。为确保密钥部署的统一，直接通过 Panorama 在多个防火墙、日志收集器、和 WF-500 设备上部署新的主密钥，或续订过期主密钥。有关配置主密钥的详细信息，请参阅配置主密钥。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | （最佳实践）选择 **Commit**（提交），然后**Commit and Push**（提交并推送）任何暂挂的配置更改。

Panorama 必须使用新主密钥重新加密数据。要确保所有配置元素均使用新主密钥进行加密，您应在部署新主密钥之前提交所有暂挂更改。

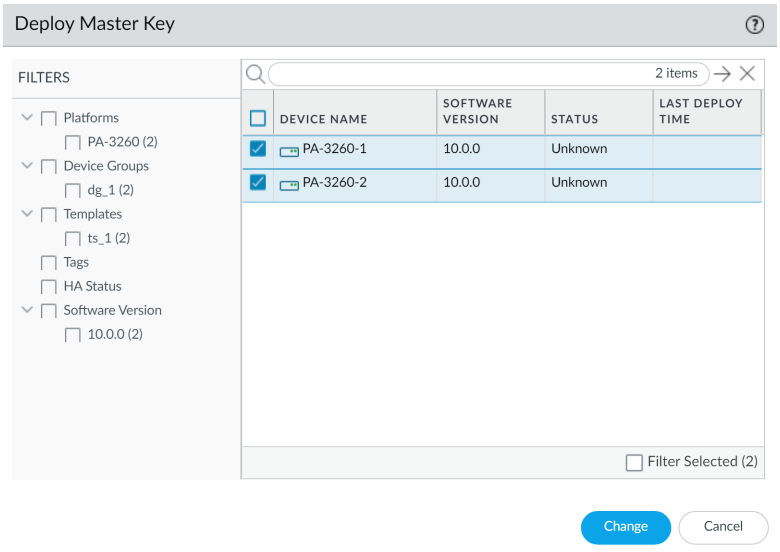
STEP 3 | 配置防火墙、日志收集器、和 WildFire 设备的主密钥，以在密钥生命周期到期之后自动续订同一主密钥。

通过自动续订主密钥，如果密钥在维护窗口之前过期，则您可以使配置保持加密状态，但是，这不能用作在密钥生命周期过期后部署新主密钥的替代方法。配置主密钥在其生命周期结束后自动续订密钥时，请考虑距离下一个可用维护窗口的天数。

1. 选择 **Device**（设备）> **Master Key and Diagnostics**（主密钥和诊断），然后编辑主密钥部分。
2. 将 Panorama 配置为 **Auto Renew with Same Master Key**（将相同主密钥自动续订）指定天数或小时数。

STEP 4 | 部署主密钥到受管防火墙。

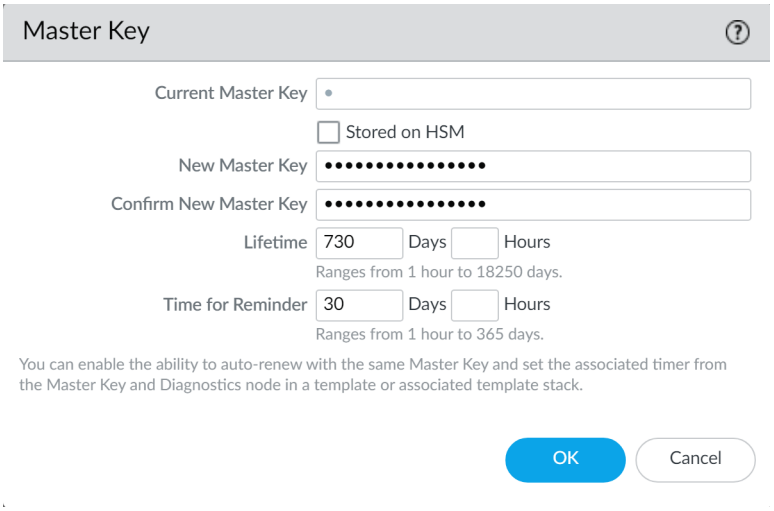
1. 选择 **Panorama** > **Managed Devices**（受管设备）> **Summary**（摘要）和 **Deploy Master Key**（部署主密钥）。
2. 选择所有设备，并 **Change**（更改）主密钥。



3. 配置主密钥：

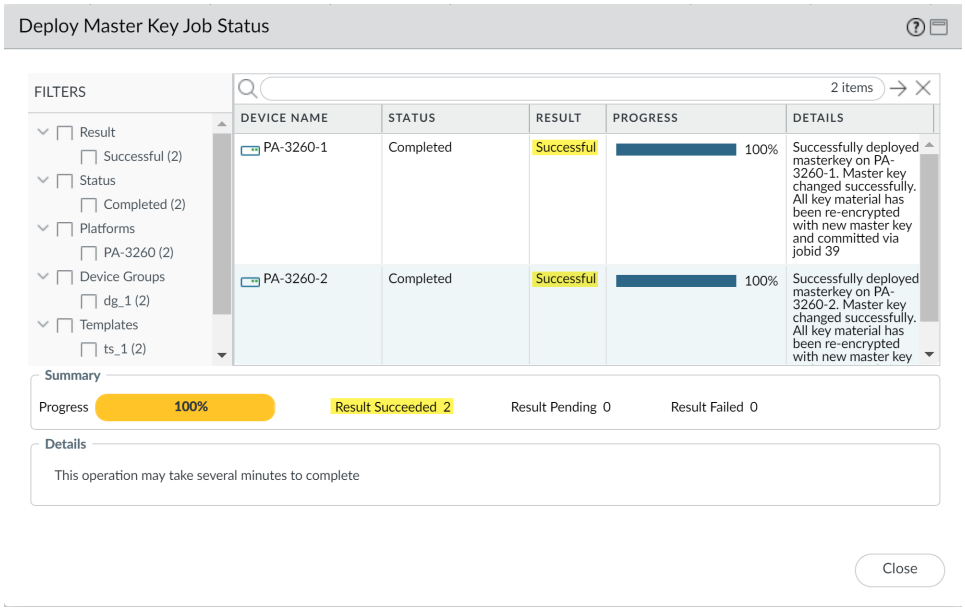
© 2019 Palo Alto Networks, Inc.

1. 如果续订主密钥，则输入 **Current Master Key**（当前主密钥）。如果使用新的主密钥更换默认主密钥，请勿指定 **Current Master Key**（当前主密钥）。
2. 指定 **New Master Key**（新主密钥），并 **Confirm Master Key**（配置主密钥）。
3. 配置主密钥 **Lifetime**（生命周期）和 **Time for Reminder**（提醒时间）。
4. 单击 **OK**（确定）。



4. 验证是否已将主密钥成功部署到所有选定设备。

   从 Panorama 部署新主密钥时，会生成系统日志。



STEP 5 | 部署主密钥到日志收集器。此主密钥必须与您在步骤 3中部署的密钥一致。

1. 选择**Panorama** > **Managed Devices**（受管设备）和 **Deploy Master Key**（部署主密钥）。
2. 选择所有设备，并 **Change**（更改）主密钥。
3. 配置主密钥：
   1. 如果续订主密钥，则输入 **Current Master Key**（当前主密钥）。如果使用新的主密钥更换默认主密钥，请勿指定 **Current Master Key**（当前主密钥）。
   2. 指定 **New Master Key**（新主密钥），并 **Confirm Master Key**（配置主密钥）。
   3. 配置主密钥 **Lifetime**（生命周期）和 **Time for Reminder**（提醒时间）。

© 2019 Palo Alto Networks, Inc.

4. 单击 **OK**（确定）。

4. 验证是否已将主密钥成功部署到所有选定设备。

   从 Panorama 部署新主密钥时，会生成系统日志。

STEP 6 | 部署主密钥到受管 WildFire 设备。此主密钥必须与您在步骤 3中部署的密钥一致。

1. 选择 **Panorama** > **Managed WildFire Appliances**（受管 **WildFire** 设备）和 **Deploy Master Key**（部署主密钥）。
2. 选择所有设备，并 **Change**（更改）主密钥。
3. 配置主密钥：
   1. 如果续订主密钥，则输入 **Current Master Key**（当前主密钥）。如果使用新的主密钥更换默认主密钥，请勿指定 **Current Master Key**（当前主密钥）。
   2. 指定 **New Master Key**（新主密钥），并 **Confirm Master Key**（配置主密钥）。
   3. 配置主密钥 **Lifetime**（生命周期）和 **Time for Reminder**（提醒时间）。
   4. 单击 **OK**（确定）。
4. 验证是否已将主密钥成功部署到所有选定设备。

   从 Panorama 部署新主密钥时，会生成系统日志。

STEP 7 | 在 Panorama 上配置主密钥。此主密钥必须与在步骤 3 到步骤 5 中部署到防火墙、日志收集器、和 WildFire 设备上的密钥一致。

1. 选择**Panorama** > **Master Key and Diagnostics**（主密钥和诊断），然后编辑主密钥。
   1. 如果续订主密钥，则输入 **Current Master Key**（当前主密钥）。如果使用新的主密钥更换默认主密钥，请勿指定 **Current Master Key**（当前主密钥）。
   2. 配置 **New Master Key**（新主密钥），并 **Confirm Master Key**（配置主密钥）。
   3. 配置主密钥 **Lifetime**（生命周期）和 **Time for Reminder**（提醒时间）。
   4. 单击 **OK**（确定）。
2. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

© 2019 Palo Alto Networks, Inc.

设置企业数据丢失防护 (DLP)

使用企业数据丢失防护 (DLP) 来执行组织的数据安全标准，以防止意外的数据滥用、丢失或被盗。

- 企业数据丢失防护 (DLP) 概述
- 企业数据丢失防护 (DLAP) 支持什么？
- 预定义数据筛选配置文件
- 安装企业数据丢失防护 (DLP) 插件
- 创建数据模式
- 创建数据筛选配置文件
- 启用企业数据丢失防护 (DLP)
- 查看企业数据丢失防护 (DLP) 日志详情
- 编辑企业数据丢失防护 (DLP) 设置
- 启用现有数据模式和筛选配置文件
- 卸载企业数据丢失防护 (DLP) 插件

企业数据丢失防护 (DLP) 概述

数据丢失防护 (DLP) 是一组工具和进程，允许您保护敏感信息免遭未经授权访问、滥用、提取和共享。DLP 插件安装在 Panorama 管理服务器上，您可以在其中集中管理强制执行组织数据安全标准的数据模式和数据筛选配置文件，并防止受管防火墙在移动用户和远程网络中丢失敏感数据。数据模式和数据筛选配置文件设计用于在运行 PAN-OS 10.0.2 和更高版本的所有受支持 Panorama 和防火墙型号上工作，以跨所有位置提供一致的数据安全性。要利用企业 DLP，Panorama 和受管防火墙必须具有互联网连接。

企业 DLP 是一项基于云的服务，使用受监督的机器学习算法将敏感文档分类为财务、法律、医疗保健和其他类别，以进行文档分类，从而防止暴露、数据丢失和数据泄露。这些模式可以识别流经网络的流量中的敏感信息，并保护它们免遭暴露。

企业 DLP 允许您通过以下方式保护敏感数据：

- 防止文件上传被泄露到未经批准的 **Web** 应用程序 — 发现并有条件地阻止敏感数据被泄露到不可信的 Web 应用程序。
- 监视到经批准 **Web** 应用程序的上传 — 发现并监视上传到经批准企业应用程序的敏感数据。

为帮助您检查内容并在正确的上下文中分析数据，以便您可以准确地识别敏感数据并进行保护以防止发生事故，企业 DLP 通过云服务启用。企业 DLP 支持 380 多个数据模式和许多预定义数据筛选配置文件。企业 DLP 在新模式和配置文件被添加到云服务后，立即自动使其在安全策略规则中可用。使用以下工具配置企业 DLP：

- Data Patterns（数据模式）— 帮助您检测敏感内容，以及如何在网络上共享和访问该内容。

  预定义数据模式和内置设置让您可以轻松保护包含特定文件属性（如文档标题或作者）、信用卡号、不同国家监管信息（如驾照编号）和第三方 DLP 标签的文件。要提高组织中敏感数据的检测率，您可以创建特定于您的内容检测和数据保护要求的自定义数据模式，作为预定义数据模式的补充。在自定义数据模式中，您还可以定义正则表达式和文件属性，以在文件的自定义或扩展属性中查找元数据或属性，并在数据筛选配置文件中使用。
- Data Filtering Profiles（数据筛选配置文件）— 支持数据分类并监视受管防火墙上可用的功能，以防止数据丢失并减少业务风险。

  数据筛选配置文件是数据模式的集合，这些数据模式被重新分组在一起以扫描特定的对象或内容类型。为执行内容分析，预定义数据筛选配置文件具有包括行业标准数据标识符、关键字和内置逻辑（以机器学习、正则表达式以及法律和财务数据模式校验和的形式）的数据模式。当您在安全策略规则中使用数据筛选配置文件时，防火墙可以检测流量以查找匹配项并采取操作。

© 2019 Palo Alto Networks, Inc.

在利用数据模式（无论是预定义还是自定义）后，您可以从 Panorama 管理数据筛选配置文件。您可以使用预定义数据筛选配置文件，或创建新配置文件，然后向其添加数据模式。然后创建安全策略，并将您添加的配置文件应用到创建的策略。如果用户上传一个文件，文件中的数据匹配策略中的标准，则受管防火墙会创建一个警报通知或阻止文件上传。

当您将一个数据筛选配置文件应用到安全策略规则时，受管防火墙会产生数据筛选日志，其中包含有关匹配数据筛选配置文件中一个或多个数据模式的流量的详情。日志详情可让您验证上传的文件是生成了警报通知还是被阻止，从而进行取证。

您可在数据筛选日志中查看代码段。默认情况下，受管防火墙使用数据掩码部分屏蔽代码段，以防止泄露敏感数据。您可以将受管防火墙配置为完全屏蔽敏感信息、不屏蔽代码段或禁用代码段提取和查看。

要提高检测准确性并减少误报，您还可以指定：

- 邻近关键 — 当关键字在表达式的 200 个字符距离内时，会为资产分配较高的准确性概率。如果一个文档的 `Visa` 后紧跟一个 16 位数，这很可能是一个信用卡号。但如果 Visa 是文本的标题，16 位数位于这个 22 页文档的最后一页，则不太可能是一个信用卡号。

  您还可以在一个关键字组中使用多个关键字，并包括或排除关键字，以查找特定单词是否出现在表达式的 200 个字符之内。
- 置信级 — 置信级与邻近关键字一起让您可以指定一个模式匹配中邻近关键字出现的概率。当置信级为 **Low**（低）时，受管防火墙不会使用邻近关键字来识别匹配项；当置信级为 **High**（高）时，受管防火墙在将文件中的数据模式视为匹配项之前，会在模式中正则表达式的 200 个字符内查找邻近关键字。
- 基本和加权正则表达式 — 正则表达描述如何搜索特定文本模式，在找到模式匹配项时显示匹配出现次数。有两种类型的正则表达式 — *basic*（基本）和 *weighted*（加权）。
  - 基本正则表达式搜索特定文本模式。当找到模式匹配项时，服务会显示匹配出现次数。
  - 加权正则表达式会向文本条目分配一个分数。当超过分数阈值时，服务会返回模式的一个匹配项。

    为减少误报和最大化正则表达式的搜索性能，您可以在创建数据模式时使用加权正则表达式生成器分配分数，以查找对您而言重要的信息并为其计算分数。评分采用一个匹配阈值，当超过分数阈值时，例如，当一个模式的足够多表达式匹配一项资产时，该资产将被表示为该模式的匹配项。

    如需更多信息，包括用例和最佳实践，请参阅《Prisma SaaS 管理员指南》中的配置正则表达式。

企业数据丢失防护 (DLAP) 支持什么？

除运行 PAN-OS 10.0.2 或更高版本且具有最低应用程序和威胁内容版本 8334-6362 的 CN 系列防火墙外，所有基于硬件的防火墙和 VM-Series 防火墙均支持企业数据丢失防护 (DLP)。

以下是可以与企业数据丢失防护 (DLP) 结合使用的受支持应用程序和操作参数。

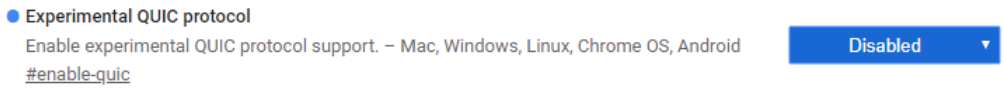
Web 应用程序	PDF	doc/docx	ppt/pptx	xls/xlsx	rtf	Csv	多文件上传	文件大小
Web 浏览	是	是	是	是	是	是	是	20MB
Onedrive Web 应用	是	是	是	是	是	是	是	20MB
Sharepoint Web 应用	是	是	是	是	是	是	是	20MB

© 2019 Palo Alto Networks, Inc.

Web 应用程序	PDF	doc/docx	ppt/pptx	xls/xlsx	rtf	Csv	多文件上传	文件大小
Gmail Web 应用	是	是	是	是	是	是	是	20MB
Box Web 应用	是	是	是	是	是	是	是	20MB
Slack Web 应用	是	是	是	是	是	是	是	20MB

- 应用程序 — 您可以为以下应用程序的基于 Web（基于 HTTP 或 HTTPS）的上传执行 DLP：
  - Box（App-ID 为 boxnet-uploading）
  - Gmail（App-ID 为 gmail-uploading）

    要使用 *Gmail*，您必须禁用 *QUIC* 协议。*Palo Alto Networks* 建议在 *Chrome* 中禁用 *QUIC*。要执行此操作，请在 *Chrome* 的 *URL* 栏中指定 `chrome://flags/`，找到 *Experimental QUIC Protocol*（实验性 *QUIC* 协议），然后选择 *Disabled*（禁用）。

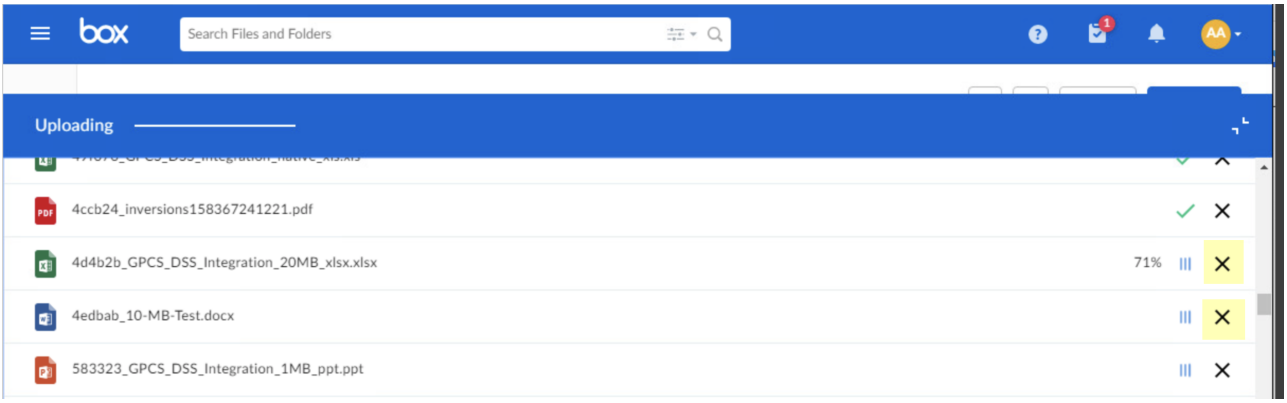
    

  - Microsoft OneDrive（App-ID 为 sharepoint-online-uploading）
  - Microsoft SharePoint（App-ID 为 sharepoint-online-uploading）
  - Slack（App-ID 为 slack-uploading）
  - Web 浏览（App-ID 为 web-browsing）
- 文件操作 — 您可以使用采用 HTTP/1.1 的 HTTP 和 HTTPS（非 FTP 或 SMTP）上传文件。

  一些应用程序（如 *SharePoint* 和 *OneDrive*）默认使用 *HTTP/2*。要组合使用 *HTTP/2* 文件和 *HTTP/1.1*，您需要创建一个解密配置文件和安全策略，去除 *ALPN* 标头。有关详细信息，请参阅启用企业数据丢失防护 (DLP)。
- 数据流 — 支持文件上传（不支持下载）。
- 并发文件上传 — 支持 25 个并发文件上传。
- 文件大小 — 支持最大 20 MB 的文件。

  如果您使用 Box 上传多个文件，且其中一个或多个文件大于 20 MB，则将无法上传全部文件。如要继续，请找出 Box 中大于 20 MB 的文件，单击 **X** 以停止上传这些文件。

© 2019 Palo Alto Networks, Inc.



- 文件类型 — Microsoft Office（.doc、.docx、.ppt、.pptx、.xls、.xlsx）、.csv、.pdf 和 .rtf。
- 响应 — 对 HTTP 和 HTTPS 文件支持 Block（阻止）和 Alert（警报）操作。Block（阻止）页不会显示受管防火墙阻止的文件的名称。
- 数据模式和数据筛选配置文件 — 使用预定义数据模式和数据筛选配置文件，或创建您自己的数据模式和数据筛选配置文件。当前不支持数据模式克隆；但是，如果要在现有配置文件中添加、移除或修改数据标识符，则可以克隆预定义数据筛选配置文件。

  对于每个数据筛选配置文件，企业 DLP 最多允许将 10 个数据模式用于 Block（阻止）规则，50 个数据模式用于 Alert（警报）规则。

  预定义数据模式对扫描的文件进行基于机器学习或正则表达式的检测。企业 DLP 对最高达 1MB 的扫描文件返回以下基于预定义机器学习的数据模式的判定：

  - 银行 – 破产申请
  - 银行 – 对账单
  - 财务 – 财务会计
  - 财务 – 通用
  - 财务 – 发票
  - 财务 – 个人财务
  - 健康 – 通用
  - 法律 – 通用
  - 法律 – 法律诉讼
  - 法律 – 并购
  - 法律 – 专利申请
  - 法律 – 标准商业协议
  - 源代码– `Cfamily`
  - 源代码– 通用
  - 源代码– `java`
  - 源代码– `javascript`
  - 源代码– `perl`
  - 源代码– `powershell`
  - 源代码– `python`
  - 源代码– `r`
  - 源代码– `ruby`
  - 源代码– `vbs`
  - 源代码– `verilog`
  - 源代码– `vhdl`
  - 源代码– `x86_assembly`

© 2019 Palo Alto Networks, Inc.

预定义数据筛选配置文件

下表描述了企业数据丢失防护 (DLP) 随附的预定义数据筛选配置文件：

预定义数据筛选配置文件	扫描
批量 CCN	信用卡号或 Voyager 信用卡号（超过 100）。
CCPA	《加利福尼亚消费者隐私法》合规性。
公司财务文档	财务会计和通用财务信息。
财务信息	银行对账单、银行路由号码、信用卡号（严格检查）、破产申请。
GDPR	驾照编号、税务登记号、居民身份证号、护照号码。
金融服务现代化法 (GLBA)	信用卡号、Voyager 信用卡号、磁条信息、美国税务登记号 (TIN)、美国国民身份证号、社会保险号 (SSN)。
医疗保健	《临床实验室改进修正案》(CLIA) 编号、药品执行管理局 (DEA) 编号和其他医疗文档。
知识产权	源代码、AWS 密钥、访问密钥、公司机密。 有两种类型的知识产权。知识产权 - 基本数据筛选配置文件包含知识产权数据筛选配置文件中包含的数据模式的子集。
法律	法律文档，包括法律诉讼、企业并购、标准商业协议、专利、破产申请。
恶意软件	所有 Microsoft Office 文档、PDF 和可迁移的可执行文件，以及针对 WildFire 的已知威胁。判定基于哈希，这是文件的唯一指纹。
个人可识别信息 (PII)	税务登记号、国民身份证号、护照号码和驾照编号。
猥亵语言	被审查、个人、包括/排除、憎恶同性恋的、性向。
自我伤害	自杀意图。
敏感内容	国民身份证号、银行信息、AWS 密钥或访问密钥、公司机密、CCN。
U.K.PIOCP	税务登记号或国民身份证号。

安装企业数据丢失防护 (DLP) 插件

要在您的 Panorama™ 管理服务器和受管防火墙上安装企业数据丢失防护 (DLP) 插件，您必须从 Palo Alto Networks 客户支持门户下载该插件，将插件上传到 Panorama，然后才能安装插件。您必须在 Panorama 和受管防火墙上安装该插件才能使用企业 DLP。

在 *Panorama* 上成功安装企业 *DLP* 插件后，您的现有数据模式（*Objects*（对象）> *Custom Objects*（自定义对象）> *Data Patterns*（数据模式））和数据筛选配置文件（*Objects*（对象）> *Security Profiles*（安全配置文件）> *Data Filtering*（数据筛选））将自动隐藏。要显示现有数据模式和筛选配置文件，请参阅 启用现有数据模式和筛选配置文件。

© 2019 Palo Alto Networks, Inc.

STEP 1 | 向 Palo Alto Networks 客户支持门户 (CSP) 注册您的 Panorama 和受管防火墙。

STEP 2 | 在 Panorama 上安装设备证书。

STEP 3 | 为受管防火墙安装设备证书。

您必须在利用企业 DLP 的所有受管防火墙上安装设备证书。

STEP 4 | 在 Panorama 上安装插件。

1. 登录到 Panorama Web 界面。
2. 选择 **Panorama** > **Plugins**（插件），然后搜索 dlp 插件的最新版本。
3. 在 Panorama 上 **Download**（下载）并 **Install**（安装）企业 DLP 插件。

STEP 5 | 在受管防火墙上安装插件。

1. 选择 **Panorama** > **Device Deployment**（设备部署）> **Plugins**（插件），然后搜索企业 DLP 插件的最新版本。
2. 在受管防火墙上 **Download**（下载）并 **Install**（安装）企业 DLP 插件。
3. 选择要安装插件的 **Devices**（设备）。
4. 单击 **OK**（确定）安装插件。

STEP 6 | 提交并推送到受管防火墙以完成企业 DLP 插件安装。

要让企业 DLP 数据筛选配置文件名称显示在数据筛选日志中，必须进行此步骤。



尽管支持执行 *Commit and Push*（提交并推送），但不建议对企业 *DLP* 配置更改执行，您需要在“推送范围选择”中手动选择受影响的模板和受管防火墙。

1. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）配置更改。
2. 选择 **Commit**（提交）> **Push to Devices**（推送到设备）和 **Edit Selections**（编辑选择）。
3. 选择 **Device Groups**（设备组），并选择 **Include Device and Network Templates**（包含设备和网络模板）。
4. 单击 **OK**（确定）。
5. 将您的配置更改 **Push**（推送）到受管防火墙。

STEP 7 | 在 Palo Alto Networks 客户支持门户 (CSP) 上激活您的企业 DLP 许可证。

为利用企业 DLP 的所有防火墙重复此步骤。

1. 登录到 Palo Alto Networks 客户支持门户。
2. 选择 **Assets**（资产）> **Devices**（设备），然后在 Actions（操作）列中单击编辑按钮（ ）。
3. 在 Device Licenses（设备许可证）窗口中，选择 **Activate Auth-Code**（激活授权代码）并输入 **Authorization Code**（授权代码）。

   在您购买企业 DLP 插件许可证后，Palo Alto Networks 会自动向您发送一封电子邮件，提供该授权代码。
4. 单击 **Agree and Submit**（同意并提交）。

STEP 8 | 创建 Palo Alto Networks 支持票证以在防火墙之间启用企业 DLP 许可证转移。

通过请求企业 DLP 许可证可转让，允许您将 DLP 许可证转移到其他受管防火墙。

在支持票证中，包含以下信息：

- 为企业 DLP 许可证请求防火墙转移。
- 您的 CSP 帐户 ID 以及与 CSP 帐户关联的电子邮件。

© 2019 Palo Alto Networks, Inc.

- 受管防火墙序列号。如果您在多个受管防火墙上激活了企业 DLP 许可证，则在单个支持票证中包含所有受管防火墙序列号。
- 用于在受管防火墙上激活企业 DLP 许可证的授权代码。
- （可选）如果您有属于另一 CSP 帐户的受管防火墙，请提供这些受管防火墙关联的 CSP 帐户 ID。

STEP 9 | 请确认 Panorama 和受管防火墙属于同一 CSP 帐户。

Panorama 和托管防火墙必须属于同一 CSP 帐户，这可让您共享数据配置文件以实现一致的安全策略执行。

1. 登录到 Palo Alto Networks 客户支持门户。
2. 选择 **Assets**（资产）> **Devices**（设备）并找到您的 Panorama 和受管防火墙。

STEP 10 | 在受管防火墙上激活企业 DLP 插件。

1. 选择 **Panorama** > **Device Deployment**（设备部署）> **License**（许可证），然后 **Activate**（激活）企业 DLP 插件。
2. 为目标受管防火墙输入 **Auth Code**（授权代码）。

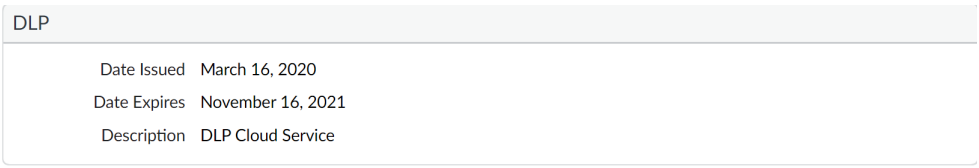
   在您购买企业 DLP 插件许可证后，Palo Alto Networks 会自动向您发送一封电子邮件，提供该授权代码。
3. 在受管防火墙上 **Activate**（激活）企业 DLP 插件许可证。

STEP 11 | 选择 **Objects**（对象）> **DLP** > **DLP Data Filtering**（DLP 数据筛选），并确认显示了预定义数据筛选配置文件。

当 Panorama 成功连接到 DLP 云服务时，Panorama 会自动填充预定义数据筛选配置文件。

STEP 12 | 验证已在您的受管防火墙上成功激活企业 DLP 许可证。

1. 启动防火墙 Web 界面。
2. 选择 **Device**（设备）> **Licenses**（许可证），验证是否已成功激活许可证。



创建数据模式

数据模式可让您使用正则表达式、文件属性或代表网络上敏感信息的关键字来指定匹配标准和标识模式。创建的所有数据模式均跨所有设备组共享。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 选择 **Objects**（对象）> **DLP** > **DLP Data Patterns**（DLP 数据模式），然后指定 **Device Group**（设备组）。

STEP 3 | **Add**（添加）新数据模式。

STEP 4 | 指定数据模式的 **Type**（类型）和标准，并为其提供 **Name**（名称）。

使用以下数据模式类型：

- **Regular Expression**（正则表达式）— 创建要在数据模式中使用的正则表达式。

© 2019 Palo Alto Networks, Inc.

您可以选择 **Basic**（基本）或 **Advanced**（高级）数据模式。使用 **Advanced**（高级）数据模式来创建基本或加权正则表达式。使用加权正则表达式时，会为每个文本条目分配一个分数，当超过分数阈值时，例如，当一个模式的足够多表达式匹配一项资产时，该资产将被表示为该模式的匹配项。

然后使用 **Regular Expressions**（正则表达式）区域中的查询生成器来添加表达式，可以是常规（**Basic**（基本））或加权（**Advanced**（高级））正则表达式。

您可以输入一个或多个 **Proximity Keywords**（邻近关键字）与数据筛选模式结合使用。在具有高置信级的数据筛选配置文件中使用邻近关键字。当您上传文件时，受管防火墙在将文件中的指定数据模式视为匹配项之前，会在正则表达式的 200 个字符内查找您指定的邻近关键字。

- **File Property**（文件属性）— 添加要匹配的文件属性模式。

  对于数据治理和信息保护，如果您在 MS Office 和 PDF 文档中使用分类标签或嵌入标记以包含更多信息用于审计和跟踪，您可以创建文件属性数据模式来匹配属于文件中自定义或扩展属性的元数据或属性。无论您使用的是 Titus 之类的自动分类机制，还是要求用户添加标记，都可以指定一个名称-值对，以匹配文件中嵌入的自定义或扩展属性。

  企业 DLP 支持 MS Office 和 PDF 文档中的文件属性数据模式。OLE (.doc/.ppt) 和 XML (.docx/.pptx) 格式的 MS Office 均受支持。

  然后添加 **Tag Name**（标记名称）和 **Tag Value**（标记值）。

  Tag Name（标记名称）和 **Tag Value**（标记值）是一个关联对，用于指定您想要查找的属性（例如，您可以将 **Tag Name**（标记名称）指定为 **Label**（标签），将 **Tag Value**（标记值）指定为 **Confidential**（机密））。您可以添加任意数量的文件属性。当您之后在数据筛选配置文件中引用文件属性数据模式时，匹配标准中使用布尔“或”匹配。

STEP 5 | 单击 **OK**（确定）以保存数据模式。

STEP 6 | 提交配置更改并将其推送到利用企业 DLP 的受管防火墙。



尽管支持执行 *Commit and Push*（提交并推送），但不建议对企业 *DLP* 配置更改执行，您需要在“推送范围选择”中手动选择受影响的模板和受管防火墙。

1. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）配置更改。
2. 选择 **Commit**（提交）> **Push to Devices**（推送到设备）和 **Edit Selections**（编辑选择）。
3. 选择 **Device Groups**（设备组），并选择 **Include Device and Network Templates**（包含设备和网络模板）。
4. 单击 **OK**（确定）。
5. 将您的配置更改 **Push**（推送）到受管防火墙。

STEP 7 | 创建数据筛选配置文件 使用一个或多个数据模式。

创建数据筛选配置文件

创建数据筛选配置文件以添加多个数据模式并指定匹配项和置信级。所有预定义和自定义数据筛选配置文件均跨所有设备组可用。

在使用预定义数据模式创建数据筛选配置文件时，请考虑预定义数据模式使用的检测类型，因为这决定了企业 DLP 如何对已扫描文件作出判定。例如，当您创建包括三个基于机器学习的数据模式和 7 个基于正则表达式的数据模式的数据筛选配置文件时，如果扫描的文件超过 1MB，则企业 DLP 将基于 7 个基于正则表达式的模式返回判定。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | （可选）创建一个或多个数据模式。

© 2019 Palo Alto Networks, Inc.

STEP 3 | 选择 **Objects**（对象） > **DLP** > **DLP Data Filters**（**DLP** 数据筛选器），然后指定 **Device Group**（设备组）。

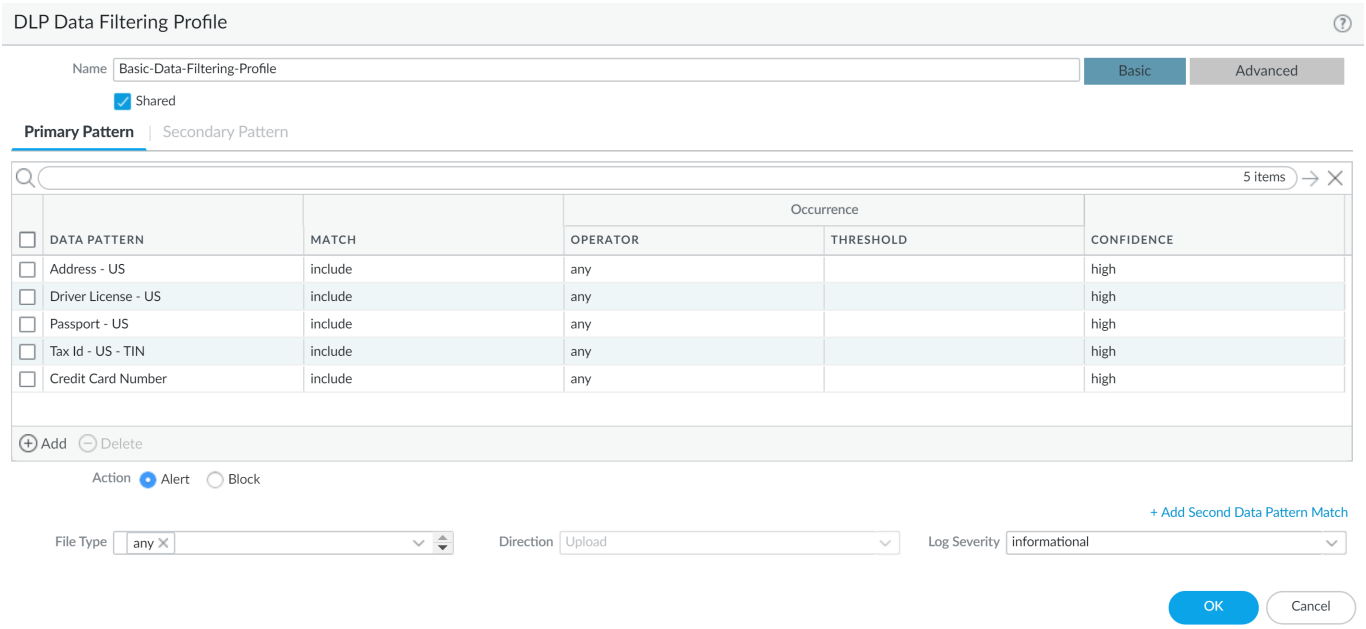
STEP 4 | **Add**（添加）新数据筛选配置文件。

STEP 5 | 为数据筛选配置文件配置主要模式。

- 如果选择 **Basic**（基本）选项，请配置以下设置：
  - **Primary Pattern**（主要模式）— **Add**（添加）一个或多个数据模式以指定为匹配标准。

    如果您指定多个数据模式，受管防火墙会在匹配标准中使用布尔“或”匹配。
  - **Match**（匹配）— 选择您指定的模式应当匹配（包括）还是不匹配（排除）指定标准。
  - **Operator**（运算符）— 选择与 **Threshold**（阈值）参数结合使用的运算符。指定 **Any**（任何）以忽略阈值。
  - **Threshold**（阈值）— 指定与您指定的 **Operator**（运算符）结合使用的值。

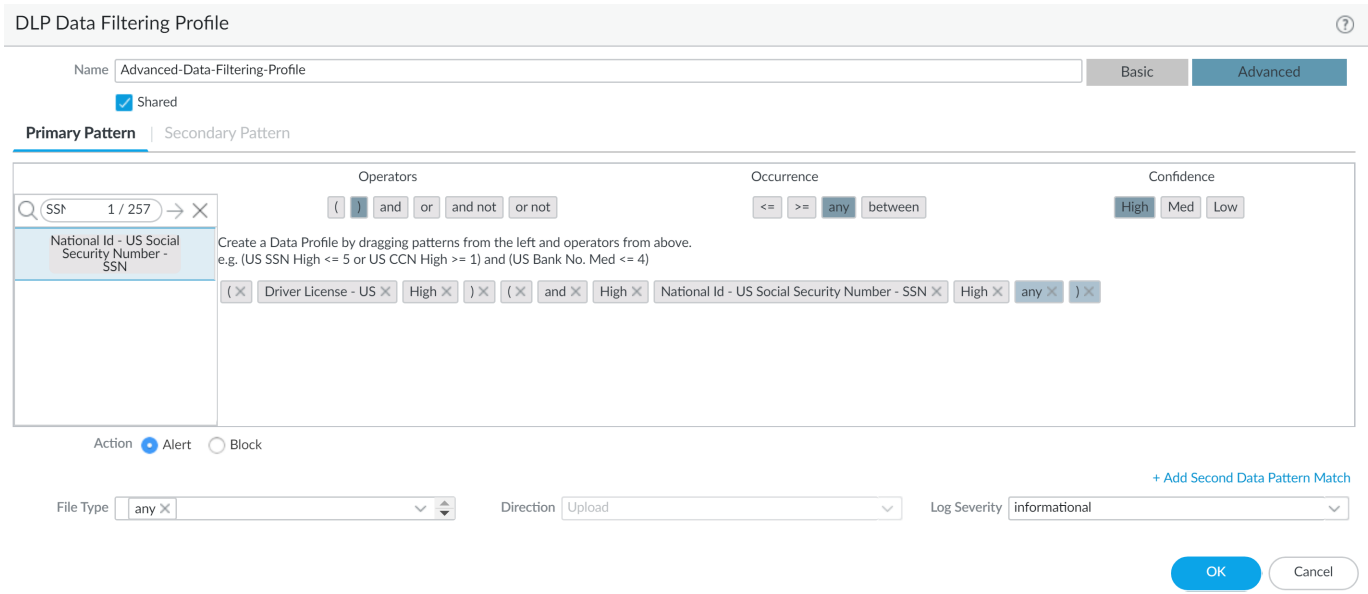
    例如，要匹配一个在文件中出现 3 次或以上的模式，请选择 **Operator**（运算符）**more_than_or_equal_to** 和 **Threshold**（阈值）**3**。
  - **Confidence**（置信）— 将此项与您在创建的数据模式中指定的邻近关键字结合使用。将置信级指定为 **Low**（低）意味着受管防火墙不使用邻近关键字。将置信级指定为 **High**（高）意味着受管防火墙在将文件中的数据模式视为匹配项之前，会在模式中正则表达式的 200 个字符内查找模式中的邻近关键字。



- 如果您选择 **Advanced**（高级）选项，则通过将数据模式、**Confidence**（置信）级、**Operators**（运算符）和 **Occurrence**（发生次数）值拖放到页面中心的字段中来创建表达式。

  指定值以便其显示在以下截图中（数据模式、**Confidence**（置信）和 **Operator**（运算符）或 **Occurrence**（发生次数）值）。

© 2019 Palo Alto Networks, Inc.



STEP 6 | 选择要在文件上执行的 **Action**（操作）（**Alert**（警报）或 **Block**（阻止））。

STEP 7 | 指定 **File Type**（文件类型）。

将文件类型保留为 **any**（任何）以匹配任何受支持的文件类型。

STEP 8 | 选择上传的 **Direction**（方向）。

不支持下载。

STEP 9 | （可选）设置与此规则匹配的文件记录的 **Log Severity**（日志严重性）。

默认严重性为 **Informational**（信息性）。

STEP 10 | 单击 **OK**（确定）保存您的配置更改。

STEP 11 | 将数据筛选配置文件附加至安全策略规则。

1. 选择 **Policies**（策略）> **Security**（安全），然后指定 **Device Group**（设备组）。
2. 选择您想要向其添加数据筛选配置文件的安全策略规则。
3. 选择 **Actions**（操作）并将 **Profile Type**（配置文件类型）设置为 **Profiles**（配置文件）。
4. 选择您之前创建的 **Data Filtering**（数据筛选）配置文件。
5. 单击 **OK**（确定）保存您的配置更改。

STEP 12 | 提交配置更改并将其推送到利用企业 DLP 的受管防火墙。

尽管支持执行 *Commit and Push*（提交并推送），但不建议对企业 *DLP* 配置更改执行，您需要在“推送范围选择”中手动选择受影响的模板和受管防火墙。

1. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）配置更改。
2. 选择 **Commit**（提交）> **Push to Devices**（推送到设备）和 **Edit Selections**（编辑选择）。
3. 选择 **Device Groups**（设备组），并选择 **Include Device and Network Templates**（包含设备和网络模板）。

© 2019 Palo Alto Networks, Inc.

4. 单击 **OK**（确定）。
5. 将您的配置更改 **Push**（推送）到受管防火墙。

启用企业数据丢失防护 (DLP)

完成以下步骤以成功配置您的受管防火墙利用企业数据丢失防护 (DLP)。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | （仅限硬件防火墙）创建服务路由以启用防火墙连接到互联网。

必须配置服务路由才能为这些防火墙平台成功利用企业 DLP。



为运行 *PAN-OS 10.0* 和更高版本的所有受支持防火墙型号创建服务路由。

1. 选择 **Device**（设备）> **Setup**（设置）> **Services**（服务），然后选择包含企业 DLP 配置的模板
2. 单击 **Service Features**（服务功能）中的 **Service Route Configuration**（服务路由配置），然后选择 **Customize**（自定义）。
3. 单击 **Dataplane**（数据平面），然后配置 **Source Interface**（源接口）和 **Source Address**（源地址）。

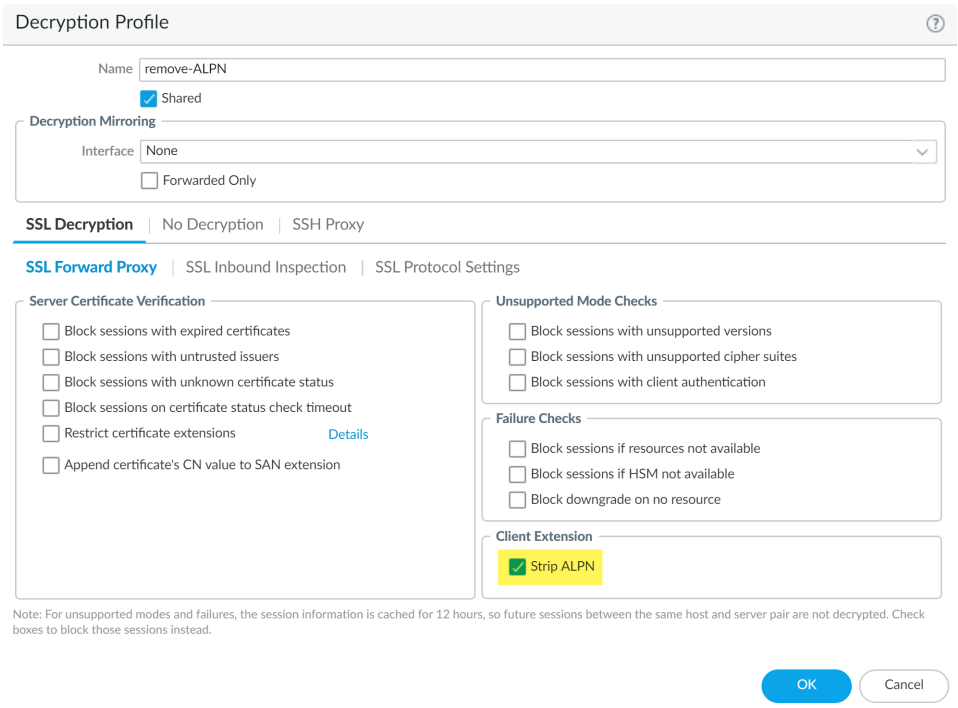
   源接口必须具有互联网连接。请参阅配置接口和创建地址对象以获取更多有关创建源接口和地址的信息。
4. 选择（选中）**Dataplane**（数据平面），然后单击 **OK**（确定）保存您的配置更改。
5. 选择 **Device**（设备）> **Setup**（设置）> **Content-ID**（内容 **ID**），然后复制 **Service URL Setting**（服务 **URL** 设置）部分中的 **Public Cloud Server**（公共云服务器）FQDN。
6. 选择 **Policies**（策略）> **Security**（安全），然后 **Add**（添加）一个允许流量从源接口到公共云服务器 FQDN 的安全策略规则。

STEP 3 | 创建解密配置文件以从上传的文件中移除应用程序层协议协商 (ALPN) 标头。

企业 DLP 支持 HTTP/1.1。一些应用程序（如 SharePoint 和 OneDrive）默认支持 HTTP/2 进行上传。要让从使用 HTTP/2 的应用程序上传的文件与企业 DLP 兼容，请完成以下步骤：

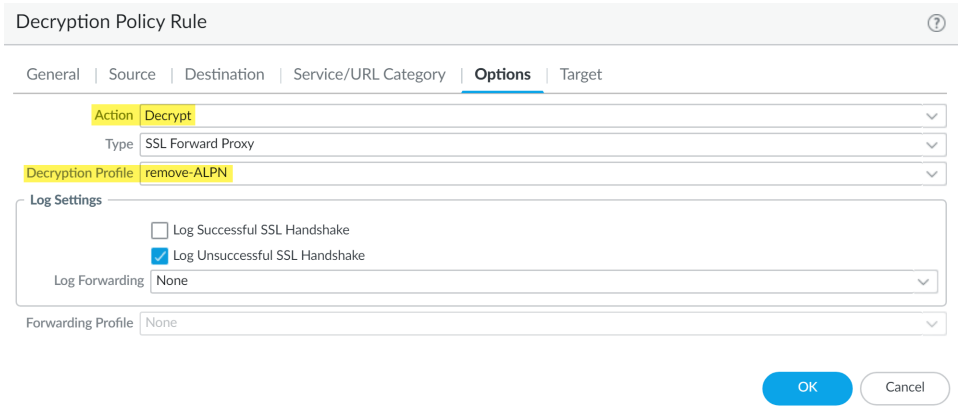
1. 选择 **Objects**（对象）> **Decryption**（解密）> **Decryption Profile**（解密配置文件），然后指定 **Device Group**（设备组）。
2. **Add**（添加）新解密配置文件。
3. 输入描述性的 **Name**（名称）。
4. （可选）启用（选中）**Shared**（共享）以使该解密配置文件跨所有设备组可用。
5. 选择 **SSL Decryption**（**SSL** 解密）> **SSL Forward Proxy**（**SSL** 转发代理），然后启用（选中）**Client Extension**（客户端扩展）中的 **Strip ALPN**（剥离 **ALPN**）
6. 单击 **OK**（确定）保存您的配置更改。

© 2019 Palo Alto Networks, Inc.



STEP 4 | 创建策略规则以从已上传文件中移除 ALPN 标头。

1. 选择 **Policies**（策略）> **Decryption**（解密），然后指定 **Device Group**（设备组）。
2. **Add**（添加）一个新解密策略规则，并根据需要进行配置。
3. 选择**Options**（选项）。
4. 针对 **Action**（操作），选择 **Decrypt**（解密）。
5. 选择您创建的 **Decryption Profile**（解密配置文件）。
6. 单击 **OK**（确定）保存您的配置更改。



STEP 5 | 禁用 QUIC 协议以拒绝端口 80 和 443 上的流量。

许多受支持的 Web 应用程序（如 Gmail）要求您禁用 QUIC 协议，如此企业 DLP 才能够正确运作。

1. 选择 **Policies**（策略）> **Security**（安全），然后指定 **Device Group**（设备组）。
2. **Add**（添加）一个拒绝使用 **quic** 应用程序的流量的安全策略规则。
3. 选择 **Objects**（对象）> **Services**（服务），然后指定 **Device Group**（设备组）。
4. **Add**（添加）两个服务：一个用于端口 80 上的 UDP，一个用于端口 443 上的 UDP。

© 2019 Palo Alto Networks, Inc.

QUIC 的较新版本可能被错误识别为 **unknown-udp**。对此，Palo Alto Networks 建议为 UDP 端口 80 和 UDP 端口 443 添加服务，并创建额外的安全策略来拒绝这些端口上的 UDP 流量。

5. 选择 **Policies**（策略）> **Security**（安全），然后指定 **Device Group**（设备组）。
6. **Add**（添加）一个安全策略规则，其中包括您创建用于拒绝到 UDP 端口 80 和 443 的流量的服务。

   完成后，您将有两个安全策略：一个阻止 QUIC 协议，一个阻止 UDP 端口 80 和 443 上的流量。

STEP 6 | 创建数据模式。

STEP 7 | 创建数据筛选配置文件。

STEP 8 | 将数据筛选配置文件附加至安全策略规则。

请参阅创建安全策略规则以获取更多有关创建新安全策略规则的信息。



要将您的 *Panorama* 管理服务器降级到之前的 *PAN-OS* 版本，您必须移除安全策略规则中引用的所有企业 *DLP* 数据模式和数据筛选配置文件。在创建和组织引用企业 *DLP* 数据模式和筛选配置文件的策略规则时，请考虑到这一点。

例如，创建一个包含所有安全策略规则的设备组，其中包含对企业 *DLP* 数据模式和筛选配置文件的引用。这样，当您需要降级 *Panorama PAN-OS* 版本时，您可以快速修改相关策略规则。

1. 选择 **Policies**（策略）> **Security**（安全）> **Pre Rules**（前导规则），然后指定 **Device Group**（设备组）。
2. 选择您想要向其添加数据筛选配置文件的安全策略规则。
3. 选择 **Actions**（操作）并将 **Profile Type**（配置文件类型）设置为 **Profiles**（配置文件）。
4. 选择您创建的 **Data Filtering**（数据筛选）配置文件。
5. 单击 **OK**（确定）保存您的配置更改。

STEP 9 | 提交配置更改并将其推送到利用企业 DLP 的受管防火墙。



尽管支持执行 *Commit and Push*（提交并推送），但不建议对企业 *DLP* 配置更改执行，您需要在“推送范围选择”中手动选择受影响的模板和受管防火墙。

1. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）配置更改。
2. 选择 **Commit**（提交）> **Push to Devices**（推送到设备）和 **Edit Selections**（编辑选择）。
3. 选择 **Device Groups**（设备组），并选择 **Include Device and Network Templates**（包含设备和网络模板）。
4. 单击 **OK**（确定）。
5. 将您的配置更改 **Push**（推送）到受管防火墙。

查看企业数据丢失防护 (DLP) 日志详情

如果受管防火墙在文件上传期间检测到敏感内容，且您已创建 Alert（警报）或 Block（阻止）操作，则会生成数据筛选日志。您可以筛选和查看检测到的流量的详细日志数据，如策略规则信息、流量的源和目标，以及与数据模式关联的数据配置文件。此外，详细日志视图会显示流量匹配的特定数据模式，并显示数据模式匹配项的总唯一次数和总出现次数。仅可在 Panorama 上查看详细日志。

当受管防火墙在文件上传期间检测到敏感内容，且您已创建 Alert（警报）或 Block（阻止）操作时，它将生成日志。然后，您可以从数据筛选日志中查看敏感内容，称为 *snippet*（代码段）。代码段是与模式匹配项关联的证据或可识别信息。例如，如果您指定了“信用卡号”数据模式，则受管防火墙将返回用户的社会保险号作为匹配的代码段。默认情况下，受管防火墙会返回代码段。

© 2019 Palo Alto Networks, Inc.

受管防火墙使用数据掩码来屏蔽代码段中的数据。默认情况下，数据筛选日志以明文显示值的后四位数（部分屏蔽）。例如，数据筛选日志将信用卡号的代码段显示为 `XXXX-XXXX-XXXX-1234`。您还可以指定以明文完整显示数据，或完全屏蔽数据以隐藏所有值。

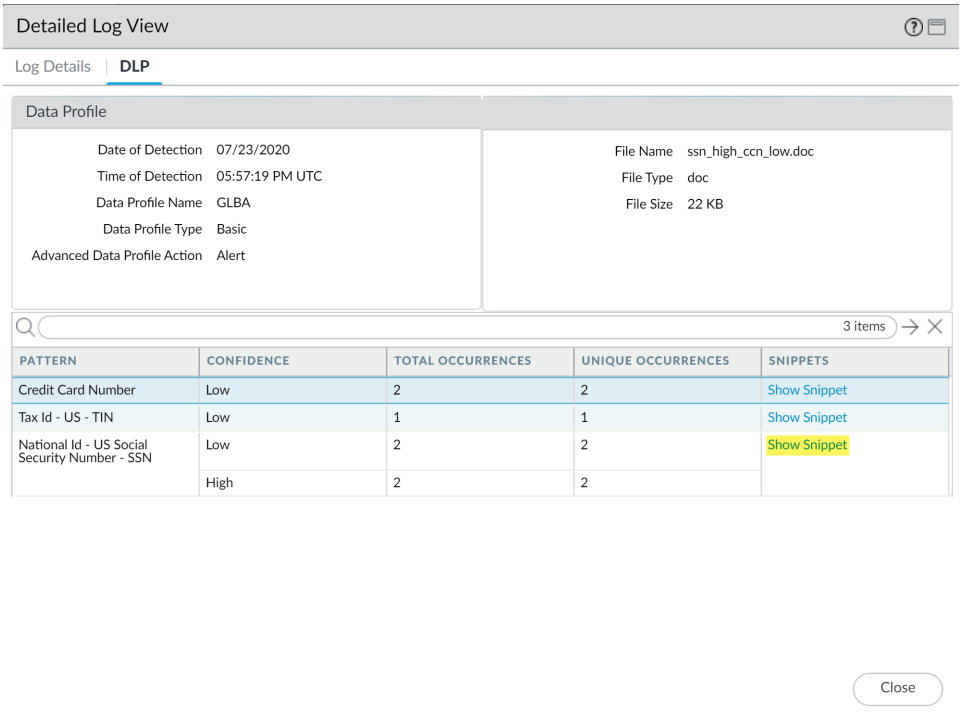
要查看特定于 DLP 的日志，包括文件代码段，请完成以下步骤。

STEP 1 | 启用企业数据丢失防护 (DLP)。

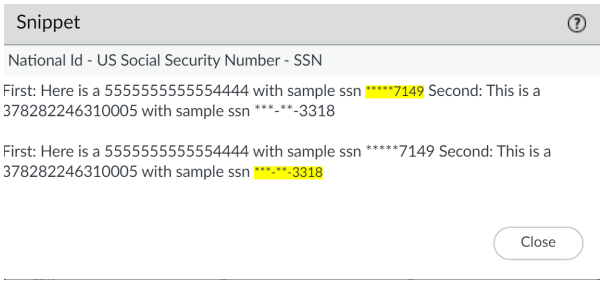
STEP 2 | 选择 **Monitor**（监视器）> **Logs**（日志）> **Data Filtering**（数据筛选），然后通过输入 **(subtype eq dlp) Filter**（筛选）数据筛选日志。

STEP 3 | 查看有关文件的更多详情，包括文件代码段。

1. 单击您想要查看更多详情的特定日志条目左边的放大镜 ()。
2. 选择 **DLP** 以查看模式详情。
3. 选择 **Show Snippet**（显示代码段）以查看匹配特定数据模式的数据的代码段。



4. 查看屏蔽的代码段以了解检测到什么数据。



启用现有数据模式和筛选配置文件

成功安装企业数据丢失防护 (DLP) 插件后，现有数据模式和筛选配置文件将不再显示，但仍可以在安全策略规则中引用。如果您已经配置了数据筛选模式和配置文件，需要在安装企业 DLP 插件后进行编辑，您可以重新将其显示在 Panorama Web 界面中。

© 2019 Palo Alto Networks, Inc.

STEP 1 | 登录到 Panorama 命令行界面。

STEP 2 | 启用现有数据模式和筛选配置文件。

```
admin> request plugins dlp hide-old-config no
```

Panorama 返回 `pass` 以确认现有数据模式和筛选配置文件现已显示。



输入以下命令以不再显示现有数据模式和筛选配置文件。

```
admin> request plugins dlp hide-old-config yes
```

STEP 3 | 登录到 Panorama Web 界面。

STEP 4 | 编辑现有数据模式和筛选配置文件。

1. 选择 **Objects**（对象）> **Custom Objects**（自定义对象）> **Data Patterns**（数据模式），然后编辑您的数据模式。
2. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **Data Filtering**（数据筛选），然后编辑您的数据筛选配置文件。

STEP 5 | 选择 **Policies**（策略）> **Security**（安全），然后选择 **Device Group**（设备组）以根据需要修改安全策略规则。

STEP 6 | 提交配置更改并将其推送到利用企业 DLP 的受管防火墙。



尽管支持执行 *Commit and Push*（提交并推送），但不建议对企业 *DLP* 配置更改执行，您需要在“推送范围选择”中手动选择受影响的模板和受管防火墙。

1. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）配置更改。
2. 选择 **Commit**（提交）> **Push to Devices**（推送到设备）和 **Edit Selections**（编辑选择）。
3. 选择 **Device Groups**（设备组），并选择 **Include Device and Network Templates**（包含设备和网络模板）。
4. 单击 **OK**（确定）。
5. 将您的配置更改 **Push**（推送）到受管防火墙。

编辑企业数据丢失防护 (DLP) 设置

编辑企业数据丢失防护 (DLP) 设置，以编辑文件扫描的云内容设置、配置数据筛选设置以及配置在 DLP 代码段中屏蔽多少敏感数据。

- 编辑云内容设置
- 编辑企业数据丢失防护 (DLP) 数据筛选设置
- 编辑企业数据丢失防护 (DLP) 代码段设置

编辑云内容设置

默认情况下，企业数据丢失防护 (DLP) 配置有云内容完全限定域名 (FQDN)，其会自动解析到私密云服务服务器来扫描您的企业 DLP 文件。如果您有特定的数据驻留要求，则可以通过编辑云内容 FQDN 来指定区域性云服务服务器，以发送企业数据丢失防护 (DLP) 文件进行扫描。

STEP 1 | 登录到 Panorama Web 界面。

© 2019 Palo Alto Networks, Inc.

STEP 2 | 选择 **Device**（设备）> **Setup**（设置）> **Content-ID**（内容 **ID**），然后选择与利用企业 DLP 的受管防火墙关联的 **Template**（模板）。

STEP 3 | 编辑云内容 FQDN。

1. 编辑 **Cloud Content Settings**（云内容设置）。
2. 根据您的数据驻留要求修改 **Public Cloud Server**（公共云服务器）。
   - **APAC** — `apac.hawkeye.services-edge.paloaltonetworks.com`
   - 欧洲 — `eu.hawkeye.services-edge.paloaltonetworks.com`
   - 美国—`us.hawkeye.services-edge.paloaltonetworks.com`
3. 单击 **OK**（确定）保存您的配置更改。

STEP 4 | 提交配置更改并将其推送到利用企业 DLP 的受管防火墙。



尽管支持执行 *Commit and Push*（提交并推送），但不建议对企业 *DLP* 配置更改执行，您需要在"推送范围选择"中手动选择受影响的模板和受管防火墙。

1. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）配置更改。
2. 选择 **Commit**（提交）> **Push to Devices**（推送到设备）和 **Edit Selections**（编辑选择）。
3. 选择 **Device Groups**（设备组），并选择 **Include Device and Network Templates**（包含设备和网络模板）。
4. 单击 **OK**（确定）。
5. 将您的配置更改 **Push**（推送）到受管防火墙。

编辑企业数据丢失防护 *(DLP)* 数据筛选设置

为扫描到企业数据丢失防护 (DLP) 云服务的文件配置网络设置，并指定利用企业 DLP 的防火墙采取的操作。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 选择 **Device**（设备）> **Setup**（设置）> **DLP**，然后选择与利用企业 DLP 的受管防火墙关联的 **Template**（模板）。

STEP 3 | 编辑数据筛选设置。

1. 针对文件上传，为防火墙采取的操作指定 **Max Latency (sec)**（最大延迟（秒））。
2. 指定当扫描以存储到 DLP 云服务的文件达到配置的 **Max Latency**（最大延迟）时，防火墙采取的 **Action on Max Latency**（达到最大延迟时的操作）（**Block**（阻止）或 **Allow**（允许））。

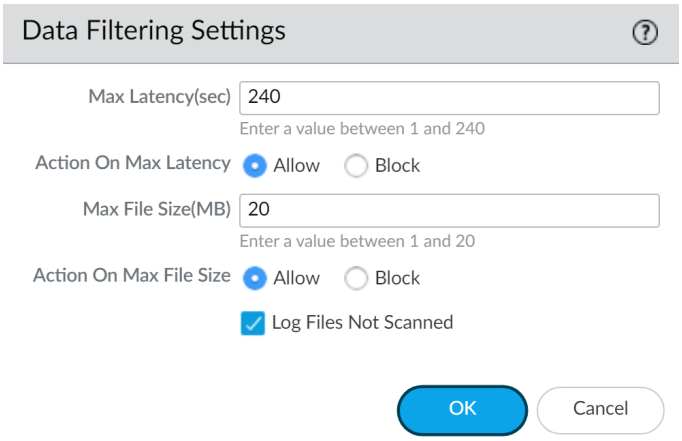
   

   选择 *Block*（阻止）仅应用至配置为阻止文件的企业 DLP 数据筛选配置文件。此设置不会影响配置为在扫描到包含敏感数据的流量时发出警报的企业 *DLP* 筛选配置文件。
3. 指定 **Max File Size (MB)**（最大文件大小 **(MB)**）以对存储在 DLP 云服务中的文件强制执行最大文件大小。
4. 指定当扫描到 DLP 云服务的文件达到配置的 **Max File Size**（最大文件大小）时，防火墙采取的 **Action on Max Latency**（达到最大文件大小时的操作）（**Block**（阻止）或 **Allow**（允许））。

   选择 *Block*（阻止）仅应用至配置为阻止文件的企业 DLP 数据筛选配置文件。此设置不会影响配置为在扫描到包含敏感数据的流量时发出警报的企业 *DLP* 筛选配置文件。
5. 选中（启用）**Log Files Not Scanned**（日志文件未扫描）以在无法将文件扫描到 DLP 云服务时在数据筛选日志中生成警报。
6. 单击 **OK**（确定）保存您的配置更改。

© 2019 Palo Alto Networks, Inc.



STEP 4 | 提交配置更改并将其推送到利用企业 DLP 的受管防火墙。

尽管支持执行 *Commit and Push*（提交并推送），但不建议对企业 *DLP* 配置更改执行，您需要在“推送范围选择”中手动选择受影响的模板和受管防火墙。

1. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）配置更改。
2. 选择 **Commit**（提交）> **Push to Devices**（推送到设备）和 **Edit Selections**（编辑选择）。
3. 选择 **Device Groups**（设备组），并选择 **Include Device and Network Templates**（包含设备和网络模板）。
4. 单击 **OK**（确定）。
5. 将您的配置更改 **Push**（推送）到受管防火墙。

编辑企业数据丢失防护 *(DLP)* 代码段设置

配置防火墙以将匹配企业 DLP 数据模式的敏感数据代码段存储在 DLP 云服务中，以及配置在存储的情况下如何屏蔽敏感数据。

STEP 1 | 登录到 Panorama Web 界面。

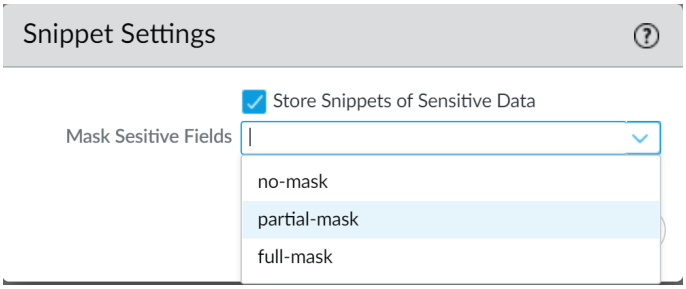
STEP 2 | 选择 **Panorama** > **DLP** > **Configuration**（配置），然后编辑 Snippet Settings（代码段设置）。

STEP 3 | 选中（启用）**Store Snippets of Sensitive Data**（存储敏感数据代码段）以将匹配企业 DLP 数据模式的敏感数据代码段存储在 DLP 云服务中。

STEP 4 | 为 DLP 云服务中的存储配置如何屏蔽敏感字段。

- **no-mask**（不屏蔽）— 当存储在 DLP 云服务中时，匹配的敏感数据代码段不会被屏蔽且完全可见。
- **partial-mask**（部分屏蔽）— 当存储在 DLP 云服务中时，匹配的敏感数据代码段会被部分屏蔽，只显示四个字符。
- **full-mask**（完全屏蔽）— 当存储在 DLP 云服务中时，匹配的敏感数据代码段被完全屏蔽。

© 2019 Palo Alto Networks, Inc.



STEP 5 | 单击 **OK**（确定）保存您的配置更改。

STEP 6 | 提交配置更改并将其推送到利用企业 DLP 的受管防火墙。

尽管支持执行 *Commit and Push*（提交并推送），但不建议对企业 *DLP* 配置更改执行，您需要在“推送范围选择”中手动选择受影响的模板和受管防火墙。

1. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）配置更改。
2. 选择 **Commit**（提交）> **Push to Devices**（推送到设备）和 **Edit Selections**（编辑选择）。
3. 选择 **Device Groups**（设备组），并选择 **Include Device and Network Templates**（包含设备和网络模板）。
4. 单击 **OK**（确定）。
5. 将您的配置更改 **Push**（推送）到受管防火墙。

卸载企业数据丢失防护 (DLP) 插件

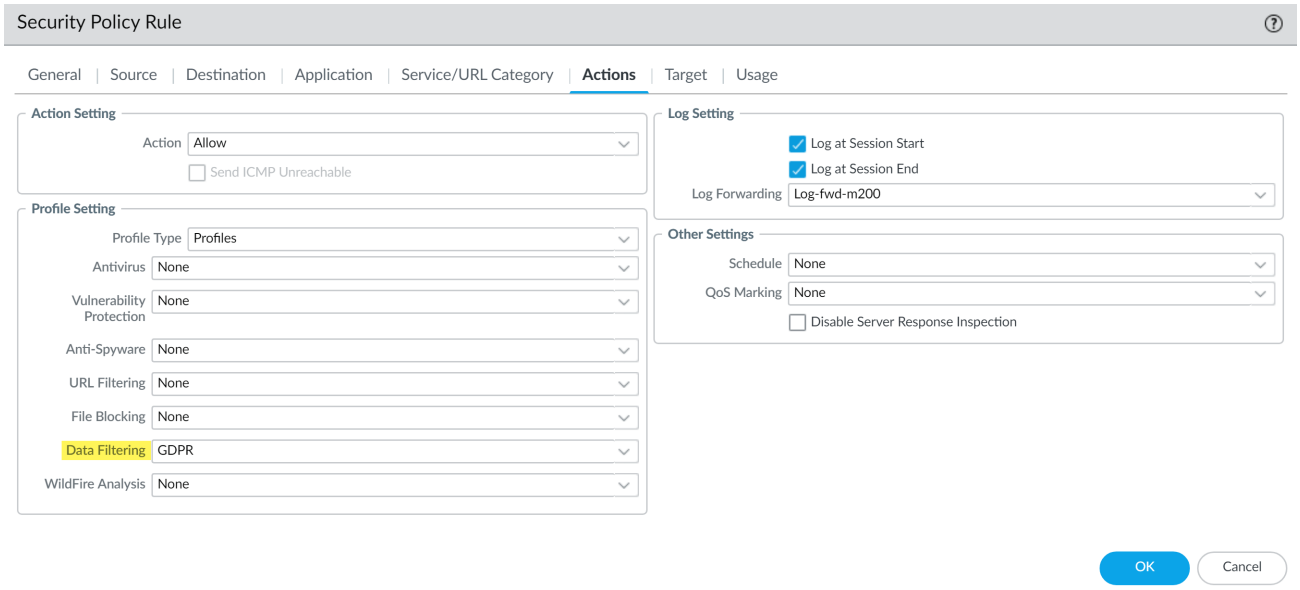
要卸载企业数据丢失防护 (DLP) 插件，必须先从所有安全策略规则中删除所有企业数据丢失防护 (DLP) 数据筛选配置文件引用，然后才能在 Panorama™ 管理服务器和受管防火墙上卸载该插件。成功卸载插件后，您可以继续降级 Panorama 和受管防火墙。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 选择 **Policies**（策略）> **Security**（安全），然后从安全策略规则移除所有企业 DLP 数据筛选配置文件。

需要完成此步骤才能成功卸载企业 DLP 插件。

© 2019 Palo Alto Networks, Inc.



STEP 3 | 提交配置更改并将其推送到利用企业 DLP 的受管防火墙。

尽管支持执行 *Commit and Push*（提交并推送），但不建议对企业 *DLP* 配置更改执行，您需要在“推送范围选择”中手动选择受影响的模板和受管防火墙。

1. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）配置更改。
2. 选择 **Commit**（提交）> **Push to Devices**（推送到设备）和 **Edit Selections**（编辑选择）。
3. 选择 **Device Groups**（设备组），并选择 **Include Device and Network Templates**（包含设备和网络模板）。
4. 单击 **OK**（确定）。
5. 将您的配置更改 **Push**（推送）到受管防火墙。

STEP 4 | 从受管防火墙卸载企业 DLP 插件。

1. 访问受管防火墙 CLI。
2. 使用以下命令卸载企业 DLP 插件：

```
admin> request plugins uninstall dlp
```

当系统提示时输入 **y** 以确认卸载企业 DLP 插件。

STEP 5 | 从 Panorama 卸载企业 DLP 插件。

1. 登录到 Panorama Web 界面。
2. 选择 **Panorama** > **Plugins**（插件），然后 **Uninstall**（卸载）企业 DLP 插件。

STEP 6 | 提交配置更改并将其推送到利用企业 DLP 的受管防火墙。

尽管支持执行 *Commit and Push*（提交并推送），但不建议对企业 *DLP* 配置更改执行，您需要在“推送范围选择”中手动选择受影响的模板和受管防火墙。

1. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）配置更改。
2. 选择 **Commit**（提交）> **Push to Devices**（推送到设备）和 **Edit Selections**（编辑选择）。

© 2019 Palo Alto Networks, Inc.

3. 选择 **Device Groups**（设备组），并选择 **Include Device and Network Templates**（包含设备和网络模板）。
4. 单击 **OK**（确定）。
5. 将您的配置更改 **Push**（推送）到受管防火墙。

© 2019 Palo Alto Networks, Inc.

重新分发数据到受管防火墙

要确保所有执行策略和生成报告的防火墙都具有适用于策略规则的所需数据和身份验证时间戳，您可以利用 Panorama 基础架构重新分发映射和时间戳。

- 配置 Panorama 管理服务器以重新分发数据。
  1. 将防火墙、虚拟系统或 Windows User-ID 代理作为重新分发代理添加到 Panorama：
     1. 选择 **Panorama** > **Data Redistribution**（数据重新分发）并 **Add**（添加）每个重新分发代理。
     2. 输入 **Name**（名称）以标识重新分发代理。
     3. 确认代理 **Enabled**（已启用）。
     4. 输入防火墙上 MGT 接口的 **Host**（主机）名或 IP 地址。
     5. 输入防火墙将侦听数据重新分发查询的 **Port**（端口）号（默认为 5007）。
     6. 如果重新分发代理为防火墙或虚拟系统，请输入 **Collector Name**（收集器名称）和 **Collector Pre-Shared Key**（收集器预共享密钥）。
     7. 选择您想要重新分发的 **Data type**（数据类型）。您可以选择所有数据类型，但您必须选择以下数据类型中的至少一个：
        - **IP** 用户映射
        - **IP** 标记
        - 用户标记
        - **HIP**
        - 隔离列表
     8. 单击 **OK**（确定）保存配置。
  2. 启用 Panorama MGT 接口以响应来自防火墙的数据重新分发查询：

     如果 *Panorama* 管理服务器具有高可用性 *(HA)* 配置，请在每个 *HA* 对端设备上执行此步骤作为最佳做法，以便在 *Panorama* 进行故障转移时继续进行重新分发。

     1. 选择 **Panorama** > **Setup**（设置）> **Interfaces**（接口），然后选择 **Management**（管理）。
     2. 选择 Network Services（网络服务）部分中的 **User-ID**，然后单击 **OK**（确定）。
  3. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**）以激活对 Panorama 所作的更改。

- 配置防火墙以接收 Panorama 重新分发的数据。
  1. 选择 **Device**（设备）> **Data Redistribution**（数据重新分发）> **Agents**（代理），然后选择要向其分配防火墙的 **Template**（模板）。
  2. **Add**（添加）代理并输入 **Name**（名称）。
  3. 选择想要添加代理的方式：
     - **Serial Number**（序列号）— 从列表中选择您想要使用的 Panorama 的 **Serial Number**（序列号）：
       - **panorama** — 主动或单独 Panorama
       - **panorama2** —（仅限 HA）被动 Panorama
     - **Host and Port**（主机和端口）— 指定以下信息：
       - 选择防火墙上 MGT 接口的 **Host**（主机）名或 IP 地址。
       - 选择主机是否为 **LDAP Proxy**（**LDAP** 代理）。
       - 输入防火墙将侦听数据重新分发查询的 **Port**（端口）号（默认为 5007）。
       - 如果重新分发代理为防火墙或虚拟系统，请输入 **Collector Name**（收集器名称）和 **Collector Pre-Shared Key**（收集器预共享密钥）。

© 2019 Palo Alto Networks, Inc.

- 选择您想要重新分发的 **Data type**（数据类型）。

4. 确认代理被 **Enabled**（启用），然后单击 **OK**（确定）以保存配置。
5. 选择 **Commit**（提交）> **Commit and Push**（提交并推送）以激活对 Panorama 所作的更改并将更改推送到防火墙。

- 确认 Panorama 和防火墙能收到重新分发的数据。
  1. 查看代理统计信息（**Panorama** > **Data Redistribution**（数据重新分发）> **Agents**（代理）），然后选择 **Status**（状态）以查看重新分发代理的活动摘要，例如客户端防火墙已收到的映射数。
  2. 确认 User-ID 日志中的 **Source Name**（源名称）（**Monitor**（监控）> **Logs**（日志）> **User-ID**），以验证防火墙是否能从重新分发代理接收映射。
  3. 查看 IP 标记日志（**Monitor**（监视器）> **Logs**（日志）> **IP-Tag**（**IP** 标记））以确认客户端防火墙可以接收数据。
  4. 访问重新分发数据的防火墙或 Panorama 管理服务器的 CLI。
  5. 通过运行以下命令显示所有用户映射：

```
> show user ip-user-mapping all
```

  6. 记录与任何一个用户名关联的 IP 地址。
  7. 访问接收重新分发数据的防火墙或 Panorama 管理服务器的 CLI。
  8. 显示所记录 *<IP-address>* 的映射信息和身份验证时间戳：

```
> show user ip-user-mapping ip <IP-address>
IP address:     192.0.2.0 (vsys1)
User:           corpdomain\username1
From:           UIA
Idle Timeout:   10229s
Max. TTL:       10229s
MFA Timestamp: first(1) - 2016/12/09 08:35:04
Group(s):       corpdomain\groupname(621)
```



此示例输出显示针对身份验证挑战（因素）的响应的时间戳。对于使用多重因素身份验证 (MFA) 的身份验证规则，输出显示多个时间戳。

© 2019 Palo Alto Networks, Inc.

从防火墙过渡到 Panorama Management

如果您已经部署了 Palo Alto Networks 防火墙并将在本地对它们进行了配置，但现在希望使用 Panorama 来集中地管理它们，则必须执行迁移前规划。迁移涉及将防火墙配置导入 Panorama 以及在过渡完成后验证防火墙工作是否符合预期。如果某些设置是单个防火墙所独有的，您可以继续访问防火墙以管理这些独特的设置。您可以通过从 Panorama 推送任何给定防火墙设置的值或者在防火墙上以本地方式配置该设置来管理该设置，但您无法同时使用 Panorama 和防火墙来管理该设置。如果您想要从 Panorama 管理中排除某些防火墙设置，您可以：

- 迁移整个防火墙配置，然后在 Panorama 上删除您将要以本地方式在防火墙上管理的设置。您也可以覆盖模板设置（此模板设置将由 Panorama 推送到防火墙），而不是在 Panorama 上删除该设置。
- 加载一部分防火墙配置，其中只包括您将使用 Panoramato 来管理的设置。



在向 *Panorama* 管理过渡期间，防火墙不会丢失日志。

- 计划向 Panorama 管理的过渡
- 从防火墙迁移到 Panorama 管理
- 从防火墙 HA 对迁移到 Panorama 管理
- 将部分防火墙配置加载到 Panorama 中

计划向 Panorama 管理的过渡

以下任务从较高层次概括了向 Panorama 管理迁移防火墙时所需的规划：

- ❑ 确定要迁移的防火墙。
- ❑ 计划维护窗口并确保 Panorama 或防火墙上没有挂起的配置更改。
- ❑ 在迁移之前保存您已知运行中的 Panorama 和防火墙配置。
  - 导出防火墙的设备状态。
  - 导出正在运行的 Panorama 配置的已命名 Panorama 配置快照。
- ❑ 确定 Panorama 和防火墙的软件及内容版本，并确定您将如何管理许可证和更新。有关重要的详细信息，请参阅Panorama、日志收集器、防火墙和 WildFire 的版本兼容性。
- ❑ 就 URL 筛选数据库（BrightCloud 或 PAN-DB）、日志收集和管理员角色计划您的 Panorama 部署。
- ❑ 计划如何管理共享设置。

  以一种将减少冗余并精简对所有防火墙之间或防火墙集内共享之设置的管理的方式，计划设备组层次结构、模板和模板堆栈。在迁移期间，您可以选择是否将对象从防火墙上的 Shared 位置导入到 Panorama 上的 Shared，但以下情况例外：

  - 如果共享防火墙对象具有与现有共享 Panorama 对象相同的名称和值，则导入排除该防火墙对象。
  - 如果共享防火墙对象的名称或值不同于现有共享 Panorama 对象，则 Panorama 会将防火墙对象导入到为此次导入而创建的每一个新设备组。
  - 如果导入到模板中的配置引用了共享防火墙对象，或者如果共享防火墙对象引用了导入到模板的配置，则不论您是否勾选 **Import devices' shared objects into Panorama's shared context**（将设备的共享对象导入到 **Panorama** 的共享上下文）复选框，Panorama 都会将该对象导入为共享对象。
- ❑ 确定防火墙是否具有您因为 Panorama 早已包含了类似的元素，或者因为这些元素为防火墙所特有（例如时区设置）而且您不会使用 Panorama 来管理它们而不想导入的配置元素（策略、对象和其他设置）。您可以执行全局查找来确定 Panorama 上是否存在类似的元素。
- ❑ 为每个设备组确定通用区域。此项操作包括每个设备组中防火墙和虚拟系统的区域命名策略。例如，如果您有两个名称分别为 Branch LAN 和 WAN 的通用区域，则 Panorama 可以推送引用了这些区域的策略规则，而无需了解端口或介质类型、型号或逻辑寻址方案之间的差异。
- ❑ 创建迁移后测试计划。

© 2019 Palo Alto Networks, Inc.

您将使用测试计划来验证防火墙在迁移之后工作时是否与迁移之前一样有效率。测试计划可能涉及多项任务，例如：

- 在迁移完成之后监控防火墙至少 24 小时。
- 监控 Panorama 和防火墙日志是否出现异常。
- 检查管理员在 Panorama 上的登录。
- 测试来自多个源头的各种类型的流量。例如，检查带宽图形、会话计数和拒绝规则流量日志条目（请参见使用 Panorama 的可视化功能）。测试应涵盖策略配置的代表性样本。
- 与您的网络运营中心 (NOC) 和安全运营中心 (SOC) 一起检查任何用户报告的问题。
- 纳入有助于验证防火墙功能性的任何其他测试标准。

从防火墙迁移到 Panorama 管理

当您导入防火墙配置时，Panorama 会自动地创建模板来容纳导入的网络和设备设置。为了容纳导入的策略和对象，Panorama 会自动地为每个防火墙创建一个设备组，或为多虚拟系统 (vsys) 防火墙中的每个虚拟系统创建一个设备组。

当您执行以下步骤时，Panorama 会导入整个防火墙配置。或者，可将部分防火墙配置加载到 Panorama 中。

Panorama 可以从运行 *PAN-OS 5.0* 或更高版本的防火墙导入配置，可向这些防火墙推送配置。例外情况是，*Panorama 6.1* 及更高版本无法将配置推送到运行 *PAN-OS 6.0.0* 至 *6.0.3* 版本的防火墙。

Panorama 可以从已经是受管设备的防火墙导入配置，但仅限于它们尚未分配到设备组或模板时。

STEP 1 | 计划迁移。

请参阅计划向 Panorama 管理的过渡中的检查清单。

STEP 2 | 将防火墙添加为受管设备。

添加防火墙作为受管设备：

1. 登录到 Panorama，选择 **Panorama** > **Managed Devices**（受管设备）>，然后单击 **Add**（添加）。
2. 输入该防火墙的序列号，然后单击 **OK**（确定）。

   如果您将导入多个防火墙配置，请输入每一个防火墙的序列号（每行输入一个）。或者，您也可以从 *Microsoft Excel* 工作表复制并粘贴这些序列号。
3. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

STEP 3 | 设置从防火墙到 Panorama 的连接。

1. 登录到防火墙，选择 **Device**（设备）> **Setup**（设置），然后编辑 Panorama 设置。
2. 在 **Panorama Servers**（**Panorama** 服务器）字段中，输入 Panorama 管理服务器的 IP 地址。
3. 单击 **OK**（确定）和 **Commit**（提交）。

STEP 4 | 将防火墙配置导入 Panorama。

如果您随后决定重新导入防火墙配置，则首先应将防火墙从您最初导入它们时所在的设备组和模板中删除。如果设备组和模板名称与防火墙主机名一致，则可以在重新导入防火墙配置前删除设备组和模板，或使用 *Device Group Name Prefix*（设备组名称前缀）字段定义重新导入时创建的新设备组和模板名称。此外，当您从设备组或模板删除它们时，防火墙不会丢失日志。

© 2019 Palo Alto Networks, Inc.

1. 在 Panorama 中，选择 **Panorama** > **Setup** > **Operations**（Panorama > 设置 > 操作），单击 **Import device configuration to Panorama**（将设备配置导入 Panorama），然后选择 **Device**（设备）。

   Panorama 无法从已分配给现有设备组或模板的防火墙导入配置。

2. （可选）编辑 **Template Name**（模板名称）。默认值为防火墙名称。您不能使用现有模板或模板堆栈的名称。
3. （可选）编辑 **Device Group**（设备组）名称。对于多 vsys 防火墙，默认情况下每个设备组都具有一个 vsys 名称，因此为每个设备组添加一个字符串作为设备组名称前缀。否则，默认值为防火墙名称。您无法使用现有设备组的名称。

   默认情况下，*Import devices' shared objects into Panorama's shared context*（将设备的共享对象导入 *Panorama* 的共享上下文）处于勾选状态，这意味着 *Panorama* 操作会将属于防火墙中 *Shared*（共享）位置的对象导入到 *Panorama* 中的 *Shared*（共享）。如果导入的对象不在防火墙的 *Shared*（共享）上下文中，则将其应用于正在导入的每个设备组。如果清除该复选框，*Panorama* 副本将不会比较导入的对象，并将所有共享的防火墙对象应用到要导入的设备组中，而不是 *Shared*（共享）。而这样可能会创建重复的对象，因此在大多数情况下，最佳的做法是勾选此复选框。若要了解将共享或重复对象导入 *Panorama* 的后果，请参阅计划如何管理共享设置。
4. 为导入的策略规则选择 **Rule Import Location**（规则导入位置）：**Pre Rulebase**（前导规则库）或 **Post Rulebase**（后继规则库）。无论您的选择怎样，Panorama 都会将默认安全规则（区域内默认和区域间默认）导入后续规则库。

   如果 *Panorama* 拥有名称与所导入的防火墙规则相同的规则，*Panorama* 会同时显示两个规则。在执行 *Panorama* 提交之前，删除规则之一，以防止提交错误。

5. 单击 **OK**（确定）。Panorama 会显示导入状态、结果、您所选项目的详细信息、已导入内容的详细信息以及任何警告。单击 **Close**（关闭）。
6. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

STEP 5 | 将配置从 Panorama 推送到新添加的设备。

要防止出现重复的规则或对象名称，将设备组配置从 Panorama 推送到防火墙，以防止提交错误。

若要成功将防火墙管理迁移到 *Panorama* 管理服务器，则必须执行此步骤。若要成功将防火墙管理迁移到 *Panorama* 管理服务器，则必须执行此步骤。

1. 登录到 Panorama Web 界面 并选择**Panorama** > **Setup**（设置）> **Operations**（操作），然后单击 **Export or push device config bundle**（导出或推送设备配置包）。
2. 单击 **Export or push device config bundle**（导出或推送设备配置包），并从下拉列表中选择 **Device**（设备），然后单击 **OK**（确定）。
3. 选择您从其中导入配置的 **Device**（设备），单击 **OK**（确定），然后单击 **Push & Commit**（推送并提交）。Panorama 将推送该配置包并在防火墙上启动提交。
4. 推送提交成功后，单击 **Close**（关闭）。
5. 为防火墙启动 Web 界面，确保配置已成功提交。如果失败，则在防火墙上本地 **Commit**（提交）更改。
6. 在 Panorama Web 界面上，选择 **Panorama** > **Managed Devices**（受管设备）> **summary**（摘要），并验证设备组和模板对于被动防火墙是否同步。验证被动防火墙上的策略规则，对象和网络设置是否与活动防火墙匹配。在防火墙 Web 界面上，验证配置对象是否显示绿色配置（.），这表示配置对象已从 Panorama 推送。
7. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

STEP 6 | 精细调整导入的配置。

© 2019 Palo Alto Networks, Inc.

1. 在 Panorama 中，选择 **Panorama** > **Config Audit**（Panorama > 配置审核），选择用于比较的 **Running config**（运行配置）和 **Candidate config**（待选配置），单击 **Go**（开始），然后检查输出。
2. 根据配置审核和 Panorama 在导入之后显示的任何警告，按需要更新设备组和模板配置。例如：
   - 删除冗余的对象和策略规则。
   - 将策略规则或对象移动或克隆到另一设备组。
   - 将防火墙移动到不同的设备组或模板。
   - 将 Panorama 在导入期间创建的设备组移动到另一父设备组：选择 **Panorama** > **Device Groups**（Panorama > 设备组），选择您想要移动的设备组，选择新 **Parent Device Group**（父设备组），然后单击 **OK**（确定）。

STEP 7 | 向防火墙推送防火墙配置包，从而将所有策略规则和对象从其本地配置中删除。

此步骤对于预防重复的规则或对象名称而言必不可少，当您在下一步骤将设备组配置从 Panorama 推送到防火墙时，重复的规则或对象名称可能会导致提交错误。

1. 在 Panorama 中，选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。
2. 选择 **Panorama** > **Setup**（设置）> **Operations**（操作），然后单击 **Export or push device config bundle**（导出 **Panorama** 或推送设备配置包）。
3. 选择您从其中导入配置的 **Device**（设备），单击 **OK**（确定），然后单击 **Push & Commit**（推送并提交）。Panorama 将推送该配置包并在防火墙上启动提交。

STEP 8 | 推送设备组和模板配置以完成向集中管理的过渡。

如果您是在迁移多个防火墙，则请在继续操作之前对每一个防火墙执行所有先前步骤（含本步骤）。

1. 选择 **Commit**（提交）> **Commit and Push**（提交并推送）和推送范围中的 **Edit Selections**（编辑选择）。
2. 选择 **Device Groups**（设备组）并选择包含导入的防火墙配置的设备组。
3. 选中 **Merge with Device Candidate Config**（与设备待选配置合并）、**Include Device and Network Templates**（包含设备和网络模板）和 **Force Template Values**（强制模板值）复选框。
4. 单击 **OK**（确定）保存对推送范围所作的更改。
5. **Commit and Push**（提交并推送）更改。

STEP 9 | 合并所有已导入的防火墙配置。

如果您是在迁移多个防火墙，则必须执行此操作。

1. 导入所有防火墙配置之后，按需要更新设备组和模板，以消除冗余并精简配置管理：请参阅精细调整导入的配置。（您不必再次推送防火墙配置包。）
2. 配置任何防火墙特定设置。

   如果防火墙将具有本地区域，则您必须创建它们，然后才能执行设备组或模板提交；Panorama 无法就区域名称或区域配置来轮询防火墙。如果您使用本地防火墙规则，请确保它们的名称是唯一的（与 Panorama 中的名称不重复）。必要时，您可以使用防火墙特定值来覆盖模板或模板堆栈值。
3. 提交并推送更改：
   1. 选择 **Commit**（提交）> **Commit and Push**（提交并推送）和推送范围中的 **Edit Selections**（编辑选择）。
   2. 选择 **Device Groups**（设备组），选择您更改的设备组，然后选择 **Include Device and Network Templates**（包含设备和网络模板）。
   3. 单击 **OK**（确定）保存对推送范围所作的更改。
   4. **Commit and Push**（提交并推送）更改。

STEP 10 | 执行迁移后测试计划。

© 2019 Palo Alto Networks, Inc.

执行您在规划迁移期间设计的验证任务，以确认防火墙在采用 Panorama 推送的配置运行时与采用其原始本地配置运行时一样高效：请参阅创建迁移后测试计划。

从防火墙 HA 对迁移到 Panorama 管理

如果您希望使用 Panorama 管理 HA 配置中的防火墙对，则可以选择将本地配置的本地配置导入 Panorama，而无需重新创建任何配置或策略。您将首先将防火墙配置导入 Panorama，然后将其创建为设备组和模板。您将执行将设备组和模板推送到防火墙的特殊配置，以覆盖本地防火墙配置并使防火墙与 Panorama 同步。

STEP 1 | 计划迁移。

请参阅计划向 Panorama 管理的过渡中的检查清单。

STEP 2 | 禁用 HA 对端设备之间的配置同步。

对 HA 对中的两个防火墙重复这些步骤。

1. 登录到每个防火墙上的 Web 界面，选择 **Device**（设备）> **High Availability**（高可用性）> **General**（常规），然后编辑 Setup（设置）部分。
2. 清除 **Enable Config Sync**（启用配置同步），并单击 **OK**（确定）。
3. 在每个防火墙上 **Commit**（提交）配置更改。

STEP 3 | 将每个防火墙连接到 Panorama。

如果 *Panorama* 已经从这些防火墙接收日志，则不需要执行此步骤。继续步骤 5。

对 HA 对中的两个防火墙重复这些步骤。

1. 登录到每个防火墙上的 Web 界面，选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后编辑Panorama 设置部分。
2. 在 **Panorama Servers**（**Panorama** 服务器）字段中，输入 Panorama 管理服务器的 IP 地址，确认已启用 **Panorama Policy and Objects**（**Panorama** 策略和对象）和 **Device and Network Template**（设备和网络模板），然后选择 **OK**（确定）。
3. 在每个防火墙上 **Commit**（提交）配置更改。

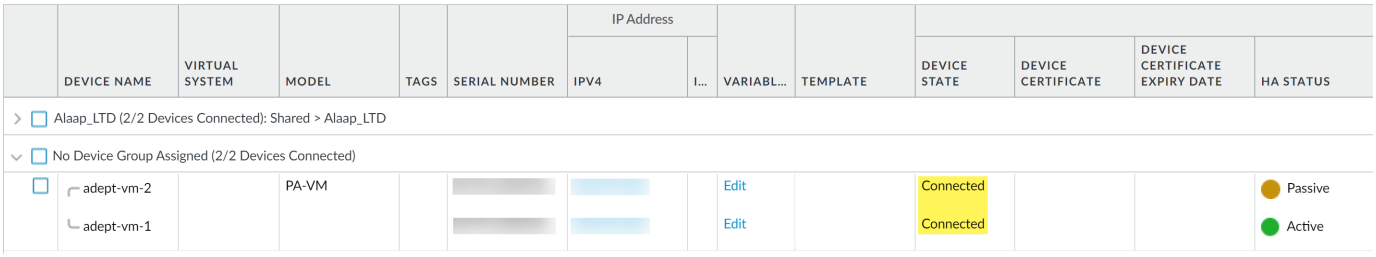
STEP 4 | 将每个防火墙添加为受管设备。

如果 *Panorama* 已经从这些防火墙接收日志，则不需要执行此步骤。继续步骤 5。

添加防火墙作为受管设备。

1. 登录到 Panorama Web 界面，选择 **Panorama** > **Managed Devices**（Panorama > 受管设备），然后单击 **Add**（添加）。
2. 输入每个防火墙的序列号，然后单击 **OK**（确定）。
3. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。
4. 核实每个防火墙的 Device State（设备状态）为 Connected（已连接）。

© 2019 Palo Alto Networks, Inc.



	DEVICE NAME	VIRTUAL SYSTEM	MODEL	TAGS	SERIAL NUMBER	IP Address IPV4	I...	VARIABL...	TEMPLATE	DEVICE STATE	DEVICE CERTIFICATE	DEVICE CERTIFICATE EXPIRY DATE	HA STATUS
>	Alaap_LTD (2/2 Devices Connected): Shared > Alaap_LTD												
v	No Device Group Assigned (2/2 Devices Connected)												
	adept-vm-2		PA-VM					Edit		Connected			Passive
	adept-vm-1							Edit		Connected			Active

STEP 5 | 将每个防火墙配置导入 Panorama。

在此步骤中，不要将任何设备组或模板堆栈配置推送到受管防火墙。在此步骤推送设备组和模板堆栈配置会擦除后续步骤中的本地防火墙 *HA* 配置。

如果您随后决定重新导入防火墙配置，则首先应将防火墙从您最初导入它们时所在的设备组和模板中删除。如果设备组和模板名称与防火墙主机名一致，则可以在重新导入防火墙配置前删除设备组和模板，或使用 *Device Group Name Prefix*（设备组名称前缀）字段输入重新导入时创建的新设备组和模板名称。此外，当您从设备组或模板删除它们时，防火墙不会丢失日志。

1. 在 Panorama 中，选择 **Panorama** > **Setup** > **Operations**（Panorama > 设置 > 操作），单击 **Import device configuration to Panorama**（将设备配置导入 Panorama），然后选择 **Device**（设备）。

   Panorama 无法从已分配给现有设备组或模板的防火墙导入配置。

2. （可选）编辑 **Template Name**（模板名称）。默认值为防火墙名称。您不能使用现有模板或模板堆栈的名称。
3. （可选）编辑 **Device Group**（设备组）名称。对于多 vsys 防火墙，默认情况下每个设备组都具有一个 vsys 名称，因此为每个设备组添加一个字符串作为设备组名称前缀。否则，默认值为防火墙名称。您无法使用现有设备组的名称。

   默认情况下，*Import devices' shared objects into Panorama's shared context*（将设备的共享对象导入 *Panorama* 的共享上下文）处于勾选状态，这意味着 *Panorama* 操作会将属于防火墙中 *Shared*（共享）位置的对象导入到 *Panorama* 中的 *Shared*（共享）。如果导入的对象不在防火墙的 *Shared*（共享）上下文中，则将其应用于正在导入的每个设备组。如果清除该复选框，*Panorama* 副本将不会比较导入的对象，并将所有共享的防火墙对象应用到要导入的设备组中，而不是 *Shared*（共享）。而这样可能会创建重复的对象，因此在大多数情况下，最佳的做法是勾选此复选框。若要了解将共享或重复对象导入 *Panorama* 的后果，请参阅计划如何管理共享设置。
4. **Commit to Panorama**（提交到 **Panorama**）。
5. 选择 **Panorama** > **Setup**（设置）> **Operations**（操作），然后单击 **Export or push device config bundle**（导出 **Panorama** 或推送设备配置包）。选择 **Device**（设备），并选择 **OK**（确定），然后 **Push & Commit**（推送并提交）配置。

   在推送设备组和模板堆栈前，必须清除步骤 2 中两个防火墙上的"启用配置同步"设置。

6. 为防火墙 HA 对启动 Web 界面，确保已成功提交上一步中推送的配置。如果失败，则在防火墙上本地 **Commit**（提交）更改。
7. 在第二个防火墙上重复步骤 1-6。该过程将为每个防火墙创建设备组和模板堆栈。

STEP 6 | 将 HA 防火墙对添加到相同的设备组和模板堆栈中。

如果 HA 防火墙对处于主动/主动配置中，请跳过此步骤。

1. 选择 **Panorama** > **Device Group**（设备组），选择第二个防火墙的设备组并 **Delete**（删除）。

© 2019 Palo Alto Networks, Inc.

2. 选择第一个防火墙的设备组，选择第二个防火墙，单击 **OK**（确定）和 **Commit to Panorama**（提交到 **Panorama**）将其添加到与 HA 对端设备相同的设备组。
3. 选择 **Panorama** > **Templates**（模板），选择第二个防火墙的模板并 **Delete**（删除）。
4. 选择第一个防火墙的模板，添加第二个防火墙，选择 **OK**（确定）和 **Commit to Panorama**（提交到 **Panorama**）将其添加到与 HA 对端设备相同的模板。
5. 在与新迁移的防火墙关联的模板中移除 HA 设置。
   1. 选择 **Device**（设备）> **Setup**（设置）> **High Availability**（高可用性）
   2. 选择 **Remove All**（全部移除）。
   3. **Commit to Panorama**（提交到 **Panorama**）。
6. 将设备组和模板堆栈配置推送到受管防火墙。

   先将设备组和模板堆栈配置推送到被动 *HA* 对，然后推送到主动 *HA* 对。

   1. 选择 **Commit**（提交）> **Push to Devices**（推送到设备）和 **Edit Selections**（编辑选择）。
   2. 启用（选择）**Merge Device Candidate Config**（合并设备待选配置）、**Include Device and Network Templates**（包含设备和网络模板）以及 **Force Template Values**（强制模板值）复选框。
   3. 单击 **OK**（确定）。
   4. **Push**（推送）到您的受管防火墙。
   5. 在主动对上，启动 Web 界面，然后选择 **Device**（设备）> **High Availability**（高可用性）> **Operational Commands**（操作命令），之后单击 **Suspend local device**（挂起本地设备）。

      在修改主动 HA 对前故障转移到被动 HA 对，以便在完成配置迁移时保持安全状态。
   6. 为现在的被动 HA 对重复步骤 1-4。
   7. 在现在的主动对上，启动 Web 界面，然后选择 **Device**（设备）> **High Availability**（高可用性）> **Operational Commands**（操作命令），之后单击 **Suspend local device**（挂起本地设备）。

      这会还原原始主动/被动 HA 对角色。
7. 选择 **Panorama** > **Managed Devices**（受管设备）> **Summary**（摘要），并验证设备组和模板对于被动防火墙是否同步。验证被动防火墙上的策略规则，对象和网络设置是否与活动防火墙匹配。

STEP 7 | 启用 HA 对端设备之间的配置同步。

如果您计划维护需要同步的本地配置，请对 HA 对中的两个防火墙重复这些步骤。

1. 登录到每个防火墙上的 Web 界面，选择 **Device**（设备）> **High Availability**（高可用性）> **General**（常规），然后编辑 Setup（设置）部分。
2. 选择 **Enable Config Sync**（启用配置同步），并单击 **OK**（确定）。
3. 在每个防火墙上 **Commit**（提交）配置更改。

将部分防火墙配置加载到 Panorama 中

如果某个防火墙上一些配置设置与其他防火墙上的配置相同，则您可以将这些特定设置加载到 Panorama 中，然后将它们推送到所有其他防火墙或特定设备组和模板中的防火墙。

将配置加载到 Panorama 管理服务器需要完整提交，并且必须由超级用户执行。在执行恢复和加载配置快照等特定 Panorama 操作时需要完整提交，而自定义管理员角色配置文件不支持完整提交。

STEP 1 | 计划向 Panorama 的过渡。

请参阅计划向 Panorama 管理的过渡中的检查清单。

STEP 2 | 决定如何管理重复的设置，即那些名称在 Panorama 中与在防火墙中相同的设置。

© 2019 Palo Alto Networks, Inc.

在您加载部分防火墙配置之前，Panorama 和该防火墙可能已经具有重复的设置。加载防火墙配置也可能会将与其他受管防火墙中设置重复的设置添加到 Panorama 中。

如果 *Panorama* 中的策略规则或对象具有与防火墙上策略规则或对象相同的名称，则提交错误会在您尝试向该防火墙推送设备组设置时发生。如果 *Panorama* 中的模板设置具有与防火墙上模板设置相同的名称，则其模板值将在推送该模板时覆盖防火墙上的模板值。

1. 在 Panorama 上，执行全局查找以确定是否存在重复的设置。
2. 如果您将使用 Panorama 来管理设置，则删除或重命名防火墙上的重复设置，或者如果您将使用防火墙来管理设置，则删除或重命名 Panorama 上的重复设置。如果您将使用防火墙来管理设备或网络设置，而非删除或重命名 Panorama 上的重复设置，您也可以从 Panorama 推送这些设置（步骤 6），然后在防火墙上使用防火墙特定值覆盖模板或模板堆栈值。

STEP 3 | 将整个防火墙配置导出到您的本地计算机。

1. 在防火墙上，选择 **Device**（设备）> **Setup**（设置）> **Operations**（操作）。
2. 单击 **Save named configuration snapshot**（保存已命名配置快照），输入 **Name**（名称）以标识该配置，然后单击 **OK**（确定）。
3. 单击 **Export named configuration snapshot**（导出已命名配置快照），选择您刚才所保存配置的 **Name**（名称），然后单击 **OK**（确定）。防火墙会将该配置导出为 XML 文件。

STEP 4 | 将防火墙配置快照导入 Panorama。

1. 在 Panorama 上，选择 **Panorama** > **Setup** > **Operations**（Panorama > 设置 > 操作）。
2. 单击 **Import named Panorama configuration snapshot**（导入已命名 **Panorama** 配置快照），**Browse**（浏览）到您已导出到计算机上的防火墙配置，然后单击 **OK**（确定）。

使用此选项导入防火墙配置文件之后，您可以不能使用 *Panorama Web* 界面来加载它。正如下一步骤中所述，您必须使用 *XML API* 或 *CLI*。

STEP 5 | 将所需的部分防火墙配置加载到 Panorama 中。

若要指定一部分配置（例如所有应用程序对象），您必须标识：

- 源 xpath — 防火墙配置文件中的 XML 节点，您的加载起始于此。
- 目标 xpath — Panorama 配置中的节点，您的加载结束于此。

使用 XML API 或 CLI 以标识和加载部分配置：

1. 使用防火墙 XML API 或 CLI 以标识源 xpath。

   例如，防火墙的 vsys1 中应用程序对象的 xpath 为：

```
/config/devices/entry[@name='localhost.localdomain']/vsys/
entry[@name='vsys1']/application
```

2. 使用 Panorama XML API 或 CLI 以标识目标 xpath。

   例如，将应用程序对象加载到名为 US-West 的设备组中时，xpath 为：

```
/config/devices/entry[@name='localhost.localdomain']/device-group/
entry[@name='US-West']/application
```

3. 使用 Panorama CLI 以加载配置并提交更改：

```
# load config partial mode [append|merge|replace] from-xpath <source-
xpath> to-xpath <destination-xpath> from <filename>
```


© 2019 Palo Alto Networks, Inc.

```
# commit
```

例如，输入以下命令，以将应用程序对象从名为 fw1-config.xml 的导入防火墙配置上的 vsys1 加载到 Panorama 上名为 US-West 的设备组：

```
# load config partial mode merge from-xpath devices/
entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/application
 to-xpath /config/devices/entry[@name='localhost.localdomain']/device-
group/entry[@name='US-West']/application from fw1-config.xml
# commit
```

STEP 6 | 将部分配置从 Panorama 送到防火墙，以完成向集中管理的过渡。

1. 在防火墙上，删除任何与 Panorama 中规则或对象具有相同名称的规则或对象。如果该防火墙的设备组具有其他防火墙，且这些防火墙含有与 Panorama 中规则或对象重复的规则或对象，则还应在这些防火墙上执行本步骤。有关详细信息，请参阅步骤 2。
2. 在 Panorama 上，将部分配置推送到防火墙。
   1. 选择 **Commit**（提交）> **Commit and Push**（提交并推送）和推送范围中的 **Edit Selections**（编辑选择）。
   2. 选择 **Device Groups**（设备组）并选择包含导入的防火墙配置的设备组。
   3. 选中 **Merge with Device Candidate Config**（与设备待选配置合并）、**Include Device and Network Templates**（包含设备和网络模板）和 **Force Template Values**（强制模板值）复选框。
   4. 单击 **OK**（确定）保存对推送范围所作的更改。
   5. **Commit and Push**（提交并推送）更改。
3. 如果该防火墙具有您不希望使用 Panorama 来管理的设备或网络设置，则在防火墙上覆盖模板或模板堆栈值。

STEP 7 | 执行迁移后测试计划。

执行您在规划迁移期间设计的验证任务，以确认防火墙在采用 Panorama 推送的配置进行工作时与采用其原始本地配置进行工作时一样有效率：请参阅创建迁移后测试计划。

© 2019 Palo Alto Networks, Inc.

在 Panorama 上监控设备

添加防火墙并配置策略规则后，您可以监控运行状况，确保防火墙在健康的参数内运行。对于策略规则，监控流量规则匹配情况，以确定符合您流量实施需求的规则。

- 监控设备运行状况
- 监控策略规则使用情况

监控设备运行状况

监控受管防火墙的运行状况信息，以便在影响您的网络安全之前识别并解决硬件问题。Panorama™ 和受管防火墙均必须运行 PAN-OS® 8.1 或更高版本，但防火墙无须成为设备组或模板堆栈的一部分，从而监控其摘要会话、日志记录、资源和环境性能。Panorama 可存储您的受管防火墙近九十 (90) 天的运行状况监控统计数据，因此，当您选择防火墙时，您可以查看会话、环境、接口、日志记录、资源以及高可用性性能的时间趋势图和表。Panorama 通过七 (7) 天的平均值和标准偏差计算每个指标的基准性能，从而确定特定防火墙的正常操作范围。除了跟踪基准性能并对时间趋势性能进行对比外，您还可以查看哪些防火墙具有偏差指标，且能在影响您的网络之前隔离性能相关的问题。一旦 Panorama 发现指标超出正常操作范围，就会标记指标，并使用偏差防火墙填充偏差设备选项卡。

运行状况监控数据存储在 Panorama 上，并在删除防火墙时予以保存。当防火墙从 Panorama 管理中移除时，将不再显示运行状况监控数据，但会保留九十 (90) 天。九十 (90) 天后，所有已移除防火墙的所有运行状况监控数据均从 Panorama 删除。如果将防火墙添加回 Panorama 管理，则显示自防火墙移除时最新的运行状况监控数据。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 选择 **Panorama** > **Managed Devices**（受管设备）> **Health**（运行状况），以监控受管防火墙的运行状况。

查看 **All Devices**（所有设备），以查看所有受管防火墙列表和已监控的运行状况指标。选择单个防火墙，以通过时间趋势图和受监控指标表查看详细设备视图。

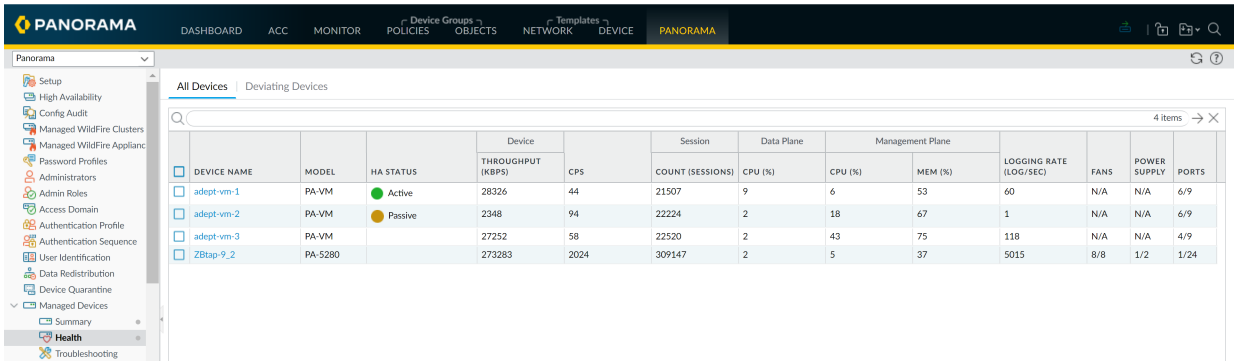


图 **12:** 受管防火墙运行状况监控

© 2019 Palo Alto Networks, Inc.

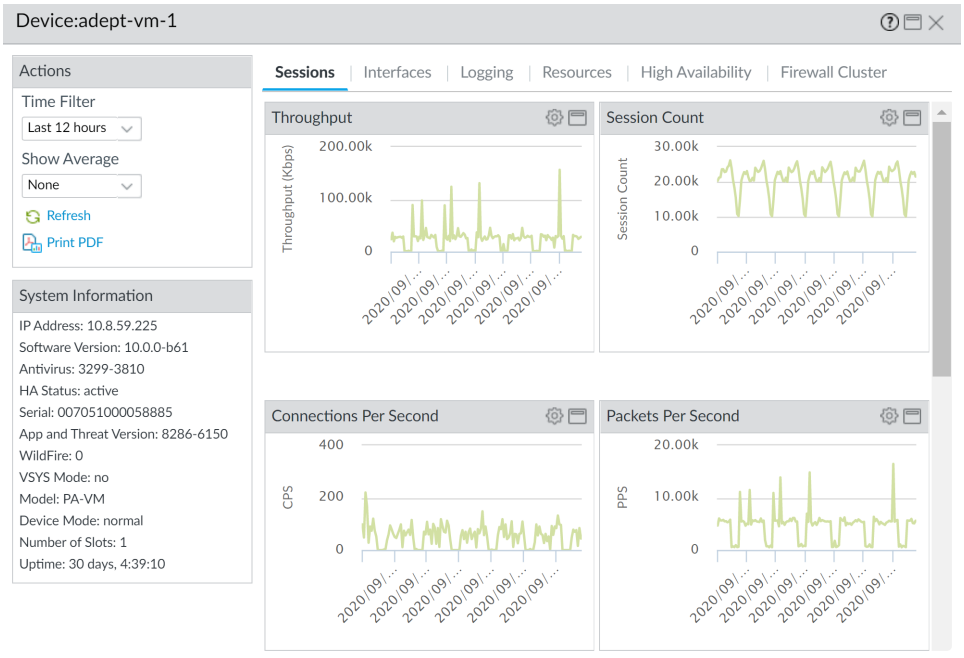
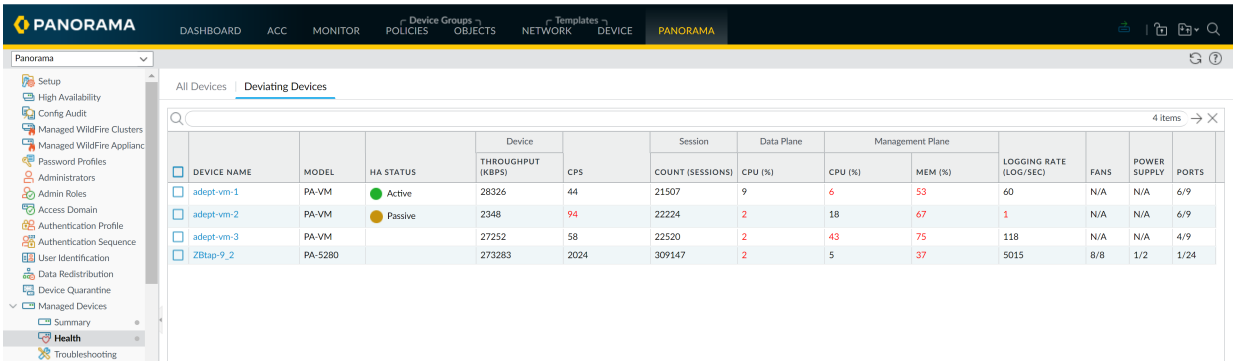


图 13: 详细设备视图

STEP 3 | 选择 **Deviating Devices**（偏差设备）以查看其运行状况指标已偏离计算基准的防火墙。

Panorama 列出报告其指标已偏离计算基准的所有防火墙，并以红色显示偏差指标。



监控策略规则使用情况

当您的策略发生变化时，跟踪 Panorama 的规则使用情况有助于您评估您的策略实施是否继续符合您的实施需求。这种可见性使您能够识别并删除未使用的规则，从而降低安全风险，保持您的策略规则库的有序性。此外，跟踪规则使用情况还可以快速验证新规则的添加和规则的更改情况，以及监控操作和故障排除任务的规则使用情况。您可以在 Panorama 上查看您向其推送策略的设备组中防火墙的规则使用情况，从而确定是否所有、部分或没有防火墙具有匹配的流量，而不是只能监控设备组中所有防火墙的总规则命中次数。您可以在自定义时间范围内利用 Created（创建）和 Modified（修改）日期等规则使用情况数据来快速筛选规则。所显示的规则使用信息在重启、数据面板重启和升级期间持续存在。

您可以在 Panorama 上查看运行 PAN-OS 8.1 或更高版本的受管防火墙的规则使用详情，其中已启用策略规则命中次数（默认），并且您已经使用设备组为其定义并推送策略规则。Panorama 无法检索防火墙上本地配置的策略规则的规则使用详情，因此，您必须登录到防火墙才能查看本地配置规则的规则使用信息。

筛选策略规则库后，管理员可以直接从策略优化器中执行删除、禁用、启用和标记策略规则等操作。例如，您可以筛选未使用的规则，然后进行标记以供检查，从而确定是否需要在规则库中安全删除这些规则，或是

© 2019 Palo Alto Networks, Inc.

将其继续保留在规则库中。通过让管理员直接从策略优化器执行操作，您可以减少用于进一步协助简化规则生命周期管理工作的管理开销，确保您的防火墙不会过度配置。

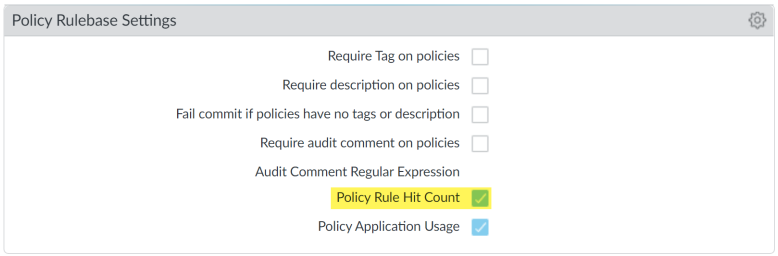
使用策略优化器优化首先迁移或清理的规则时，策略规则使用数据可能会很有用。

要查看任何共享规则的规则使用情况，或特定设备组的规则使用情况：

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 验证 **Policy Rule Hit Count**（策略规则命中次数）是否启用。

1. 导航至策略规则库设置（**Panorama** > **Setup**（设置） > **Management**（管理））。
2. 验证 **Policy Rule Hit Count**（策略规则命中次数）是否启用。



STEP 3 | 选择 **Policies**（策略） > *<policy rule>* 以查看规则。

STEP 4 | 更改设备组上下文为 **Shared**（共享），或是更改为想要查看的特定设备组。

STEP 5 | 确定是否正在使用该规则（规则使用情况）。策略规则使用情况出现以下其中一种状态：

启用策略规则使用情况的防火墙必须运行 PAN-OS 8.1 或更新版本，以便 Panorama 确定规则使用情况。

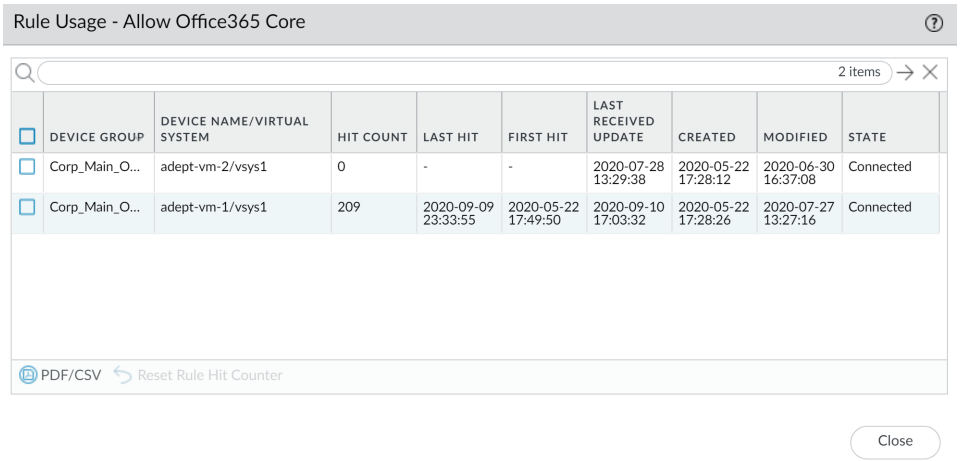
- 已使用—当设备组中推送策略规则的所有防火墙均有匹配策略规则的流量时。
- 部分使用—当设备组中推送策略规则的一些防火墙拥有匹配策略规则的流量时。
- 未使用—当设备组中推送策略规则的防火墙不具有匹配策略规则的流量时。
- **Em-dash (—)**—当设备组中推送策略规则的防火墙未启用策略规则点击数时，或不可用于 Panorama 确定规则使用情况时。
- 修改时间 — 最后一次修改策略规则的日期和时间。
- 创建时间 — 策略规则创建的日期和时间。

如果在 *Panorama* 运行 *PAN-OS 8.1* 且 *Policy Rule Hit Count*（策略规则命中次数）设置启用的情况下创建该规则，则在升级到 *PAN-OS 9.0* 或更高版本时，*First Hit*（第一次命中）日期和时间将用作 *Created*（创建）日期和时间。如果该规则在 *Policy Rule Hit Count*（策略规则命中次数）设置被禁用时创建于 *PAN-OS 8.1* 中，或该规则在 *Panorama* 运行 *PAN-OS 8.0* 或更早版本时创建，则 *Panorama* 成功升级到 *PAN-OS 9.0* 或更高版本的日期和时间将用作规则 *Created*（创建）日期。

© 2019 Palo Alto Networks, Inc.

Rule Usage		DAYS WITH NO NEW APPS	MODIFIED	CREATED
RULE USAGE	APPS SEEN			
Used	6	150	2020-06-24 10:34:...	2020-04-09 11:34:03
Unused	0	-	2020-06-24 10:34:...	2020-04-16 11:42:46
Used	11	57	2020-06-24 10:34:...	2020-04-16 11:42:46
Partially Used	3	111	2020-06-24 10:34:...	2020-05-22 17:26:44
Unused	0	-	2020-06-24 10:34:...	2020-05-22 22:45:53

STEP 6 | 单击 Rule Usage（规则使用情况）状态以查看使用该规则的防火墙列表以及与每个防火墙上该规则相匹配的流量点击次数数据。



STEP 7 | （可选）查看设备组中单个防火墙的策略规则命中次数数据。

1. 单击 **Preview Rules**（预览规则）。
2. 从设备上下文选择想要查看策略规则使用情况数据的防火墙。

STEP 8 | 选择 **Policies**（策略），然后在 Policy Optimizer（策略优化器）对话框中查看 **Rule Usage**（规则使用情况）筛选器。

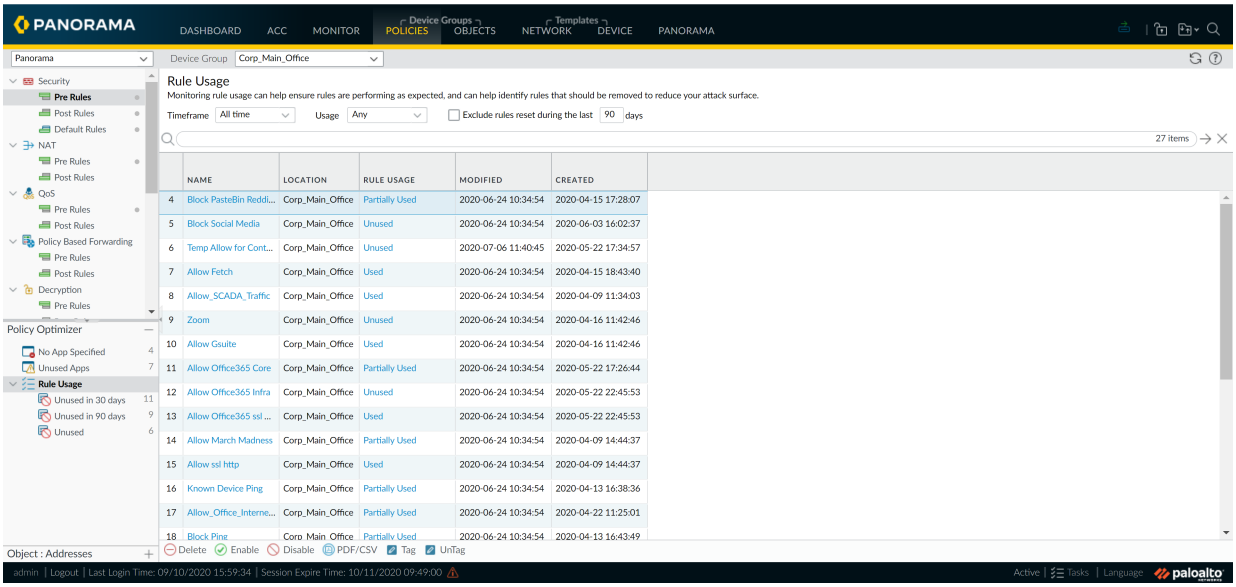
STEP 9 | 筛选选中规则库中的规则。

您可以对从 Panorama 推送到防火墙的规则执行规则使用情况筛选。Panorama 无法对防火墙上本地配置的规则执行规则使用情况筛选。

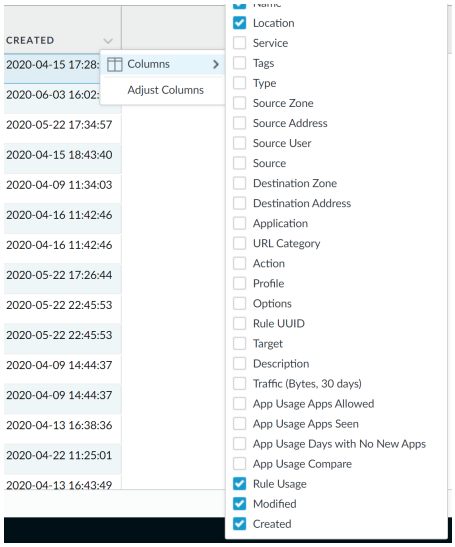
使用规则使用情况筛选器评估指定时间段内的规则使用情况。例如，筛选选定规则库中最近 *30* 天内未使用的规则。您还可以使用 *Created*（创建）和 *Modified*（修改）日期等其他规则属性评估规则使用情况，从而可以筛选出正确的规则组以供查看。使用此数据有助于您管理规则生命周期，并确定是否需要删除规则，以减小您的网络攻击面。

1. 选择想要筛选的 **Timeframe**（时间段），或者指定 **Custom**（自定义）时间段。
2. 选择您想要筛选的规则 **Usage**（使用情况）。
3. （可选）如果已重置任何规则的规则使用情况数据，请检查排除最近 *<number of days>* 天内的规则重置，并决定何时根据规则重置以来指定的天数排除规则。筛选结果仅包含指定天数之前重置的规则。

© 2019 Palo Alto Networks, Inc.

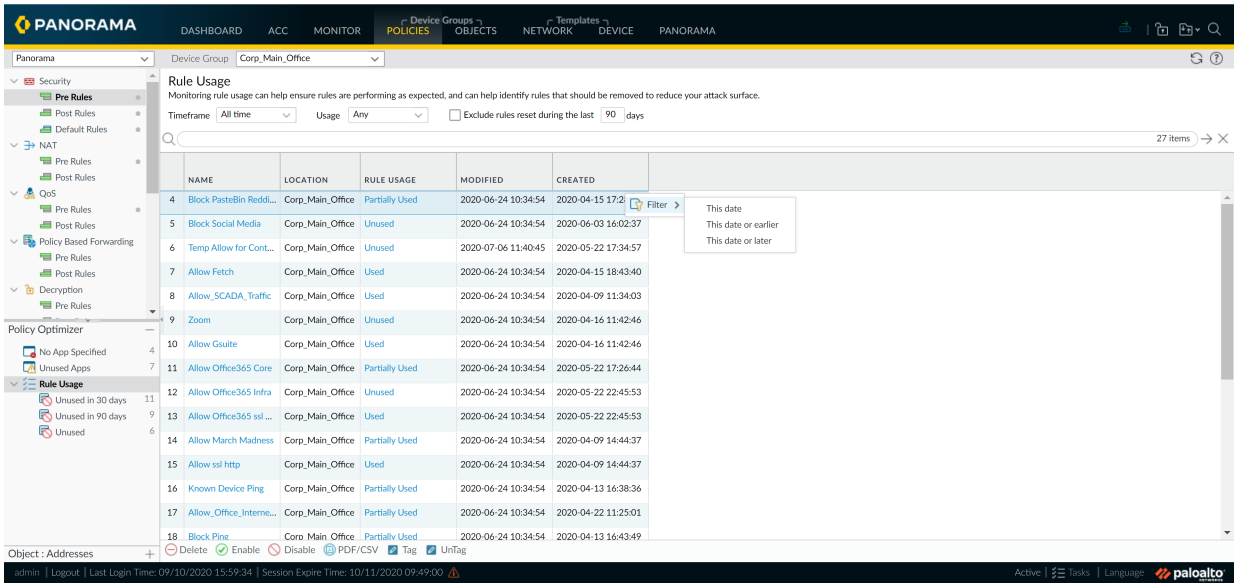


4. （可选）根据除规则使用情况之外的其他规则数据指定搜索筛选器。
   1. 将鼠标悬停于列标题上，并从下拉列表中选择 **Columns**（列）。
   2. 添加想要筛选或显示的任何其他列。



   3. 将鼠标悬停于想要筛选的列数据上，并从下拉列表中选择 **Filter**（筛选）。对于包含日期的数据，选择是否使用 **This date**（此日期）、**This date or earlier**（此日期或更早日期）或 **This date or later**（此日期或更晚日期）进行筛选。
   4. 单击 **Apply Filter**（应用筛选器）（→）。

© 2019 Palo Alto Networks, Inc.



STEP 10 | 对一个或多个未使用的策略规则执行操作。

1. 选择一个或多个未使用的策略规则。
2. 然后执行以下操作之一：
   - **Delete**（删除）— 删除所选的一个或多个策略规则。
   - **Enable**（启用）— 启用所选的一个或多个策略规则（若已禁用）。
   - **Disable**（禁用）— 禁用所选的一个或多个策略规则（若已启用）。
   - **Tag**（标记）— 将一个或多个组标记应用于所选的一个或多个策略规则。若要标记策略规则，组标记必须已经存在。
   - **Untag**（取消标记）— 取消所选的一个或多个策略规则中的组标记。
3. 选择 **Commit**（提交），然后 **Commit and Push**（提交并推送）您的更改。

© 2019 Palo Alto Networks, Inc.

用例：使用 Panorama 配置防火墙

假设您希望在高可用性配置中使用 Panorama 来管理网络中的十二个防火墙：六个防火墙部署在六个分支机构中，两个数据中心的高可用性配置中各有两个防火墙，两个区域性总部中各有一个防火墙。

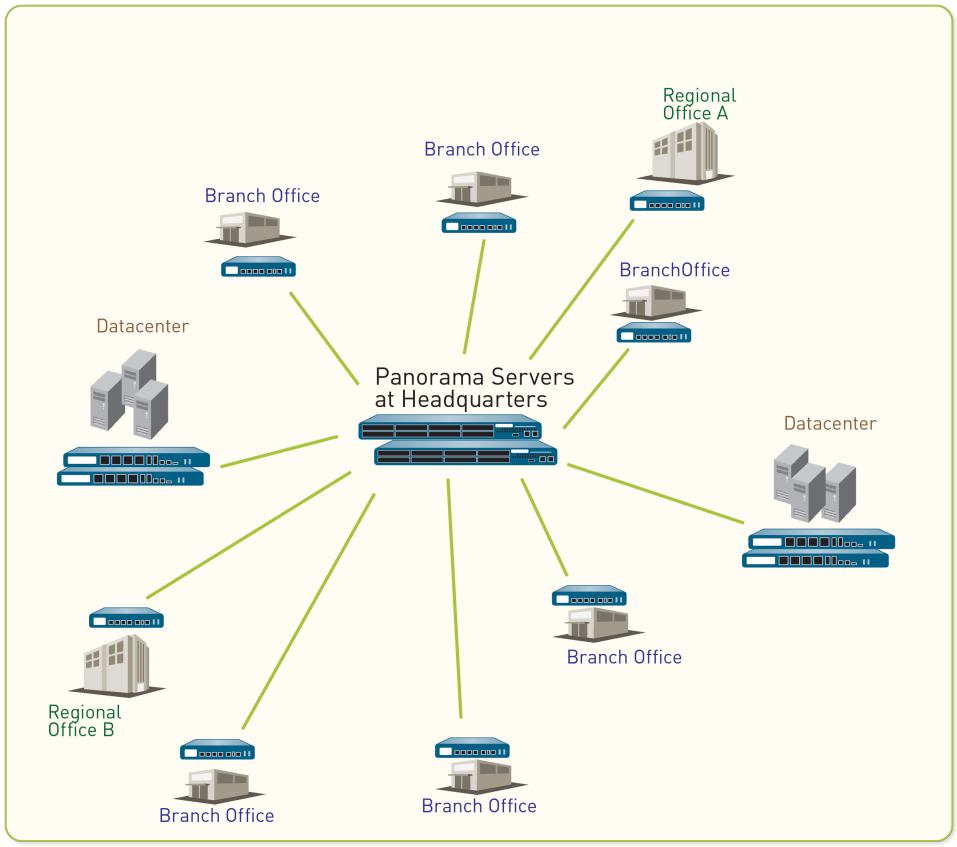


图 14: 防火墙分发示例

创建集中管理策略的第一步是确定如何将防火墙分组到设备组和模板，以便有效地从 Panorama 推送配置。您可以根据防火墙的业务功能、地理位置或管理域进行分组。在本例中，您已创建两个设备组和三个模板来使用 Panorama 管理防火墙：

- 本用例中的设备组
- 本用例中的模板
- 设置集中配置和策略

本用例中的设备组

在用例：使用 Panorama 配置防火墙中，我们需要根据防火墙将要执行的功能定义两个设备组：

- DG_BranchAndRegional，集合了在分支机构和区域总部用作安全网关的防火墙。我们将分支机构防火墙和区域总部防火墙放到相同的设备组中，是因为功能相似的防火墙需要相似的策略规则库。
- DG_DataCenter，集合了在数据中心保护服务器的防火墙。

我们随后可以管理两个设备组中之间的共享策略规则，还可以为区域机构和分支机构组来管理不同的设备组规则。为了提高灵活性，区域或分支机构中的本地管理员可以创建与特定资源、目标和服务流程相匹配的本地规则，以便访问该机构所需的应用程序和服务。在本例中，我们针对安全规则创建了以下层次结构；您可以针对任何其他规则库使用相似的方法。

© 2019 Palo Alto Networks, Inc.

Device Groups	DG_BranchAndRegional		DG_DataCenter
Rules	**Regional**	**Branch**	**Datacenter**
Shared pre-rule	Allow DNS and SNMP services.		
	Acceptable use policy that denies access to specified URL categories and peer-to-peer traffic that is of risk level 3, 4, and 5.		
Device Group pre-rule	Allow Facebook to all users in the marketing group in the regional offices only.		Allow access to the Amazon cloud application for the specified hosts/servers in the datacenter.
Local rules on a device	None		
Device Group post-rule	None		
Shared post-rule	To enable logging for all Internet-bound traffic on your network, create a rule that allows or denies all traffic from the trust zone to the untrust zone.		

图 **15:** 安全规则层次

本用例中的模板

当为模板分组防火墙时，我们必须考虑网络配置的差异。例如，如果接口配置不同 — 接口在类型方面不同，或者使用的接口在编号方案和链路容量方面不同，或者区域到接口的映射不同 — 防火墙就必须在不同的模板中。此外，配置防火墙访问网络资源的方式可能不尽相同，因为防火墙在地理范围方面是分布式的，例如，它们所访问的 DNS 服务器、syslog 服务器和网关可能不同。因此，考虑到最佳基本配置，在用例：使用 Panorama 配置防火墙中必须将防火墙安排到单独的模板中，如下所示：

- T_Branch 用于分支机构防火墙
- T_Regional 用于区域总部防火墙
- T_DataCenter 用于数据中心防火墙

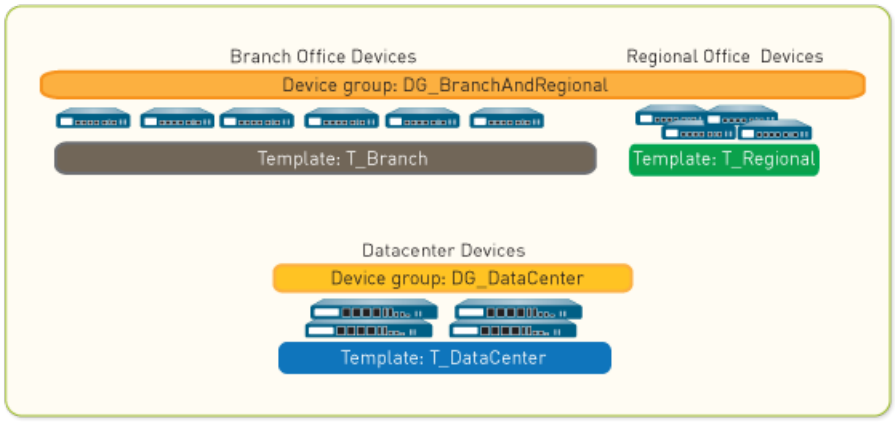


图 **16:** 设备组示例

© 2019 Palo Alto Networks, Inc.

如果您计划在主动/主动高可用性配置中部署防火墙，请将高可用性对中的每个防火墙分配到单独的模板。这样做可以针对每个对端设备灵活地设置单独的网络配置。例如，您可以针对每个对端设备在单独的模板中管理网络配置，以便于每个对端设备都可以连接到不同的北向绑定和南向绑定路由器，并且可以具有不同的 *OSPF* 或 *BGP* 对等配置。

设置集中配置和策略

在用例：使用 Panorama 配置防火墙中，我们需要执行以下任务集中部署和管理防火墙：

- 添加受管防火墙并部署更新
- 使用模板来管理基础配置
- 使用设备组来推送策略规则
- 预览规则和提交更改

添加受管防火墙并部署更新

用例：使用 Panorama 配置防火墙中的第一个任务是添加防火墙作为受管设备，并将内容更新和 PAN-OS 软件更新部署到这些防火墙。

STEP 1 | 对于 Panorama 将要管理的每个防火墙，添加防火墙作为受管设备。

在本例中，添加 12 个防火墙。

STEP 2 | 将内容更新部署到防火墙。如果您购买了威胁防御订阅，则将会为您提供内容和防病毒数据库。首先安装 **Applications**（应用程序）或 **Applications and Threats**（应用程序和威胁）数据库，然后安装 **Antivirus**（防病毒软件）。

要查看 *Panorama* 上执行的所有任务的状态和进度，请参阅使用 Panorama 任务管理器。

1. 选择 **Panorama** > **Device Deployment** > **Dynamic Updates**（Panorama > 设备部署 > 动态更新）。
2. 单击 **Check Now**（立即检查）以检查最新更新。如果 Action（操作）列中的值为 **Download**（下载），这表明更新可用。
3. 单击 **Download**（下载）。下载完成后，Action（操作）列中的值将更改为 **Install**（安装）。
4. 在 **Action**（操作）列中，单击 **Install**（安装）。使用筛选器或用户定义的标记选择您想要安装此更新的受管防火墙。
5. 单击 **OK**（确定），然后监控每个防火墙的内容更新的状态、进度和结果。**Result**（结果）列将显示安装的成功或失败状况。

STEP 3 | 将软件更新部署到防火墙。

1. 选择 **Panorama** > **Device Deployment** > **Software**（Panorama > 设备部署 > 软件）。
2. 单击 **Check Now**（立即检查）以检查最新更新。如果 Action（操作）列中的值为 **Download**（下载），这表明更新可用。
3. 找到各种硬件型号所需的版本，然后单击 **Download**（下载）。下载完成后，Action（操作）列中的值将更改为 **Install**（安装）。
4. 在 Action（操作）列中，单击 **Install**（安装）链接。使用筛选器或用户定义的标记选择要安装此版本的受管防火墙。
5. 选中 **Reboot device after install**（安装后重新启动设备）或 **Upload only to device (do not install)**（仅上传到设备（不安装））复选框，然后单击 **OK**（确定）。**Results**（结果）列显示安装的成功或失败状况。

© 2019 Palo Alto Networks, Inc.

使用模板来管理基础配置

用例的第二个任务：使用 Panorama 配置防火墙中的第二个任务是创建将基本配置推送到防火墙所需的模板。

STEP 1 | 对于您将使用的每个模板，添加模板并为其分配相应的防火墙。

在本例中，创建名为 T_Branch、T_Regional 和 T_DataCenter 的模板。

STEP 2 | 定义 DNS 服务器、NTP 服务器、Syslog 服务器和登录条幅。对每个模板重复执行此步骤。

1. 在 **Device**（设备）选项卡中，从下拉列表中选择 **Template**（模板）。
2. 配置 DNS 和 NTP 服务器：
    1. 选择 **Device** > **Setup** > **Services** > **Global**（设备 > 设置 > 服务 > 全局），然后编辑“Services（服务）”。
    2. 在 **Services**（服务）选项卡中，输入 **Primary DNS Server**（主要 **DNS** 服务器）的 IP 地址。

    如果任何防火墙具有多个虚拟系统 *(vsys)*，则对于每个虚拟系统，向模板添加 DNS 服务器配置文件（*Device*（设备）> *Server Profiles*（服务器配置文件）> *DNS*）。
    3. 在 **NTP** 选项卡中，输入 **Primary NTP Server**（主要 **NTP** 服务器）的 IP 地址。
    4. 单击 **OK**（确定）保存更改。
3. 添加登录横幅：选择 **Device** > **Setup** > **Management**（设备 > 设置 > 管理），然后编辑“General Setting（常规设置）”部分，输入 **Login Banner**（登录横幅）的文本，然后单击 **OK**（确定）。
4. 配置 Syslog 服务器配置文件（**Device** > **Server Profiles** > **Syslog**（设备 > 服务器配置文件 > Syslog））。

STEP 3 | 启用对受管防火墙的管理界面的 HTTPS、SSH 和 SNMP 访问权限。对每个模板重复执行此步骤。

1. 在 **Device**（设备）选项卡中，从下拉列表中选择 **Template**（模板）。
2. 选择 **Setup** > **Management**（设置 > 管理），然后编辑“Management Interface Settings（管理界面设置）”。
3. 勾选 Services（服务）下的 **HTTPS**、**SSH** 和 **SNMP** 复选框，然后单击 **OK**（确定）。

STEP 4 | 在数据中心模板 (T_DataCenter) 中为防火墙创建区域保护配置文件。

1. 选择 **Network**（网络）选项卡，然后选择 **Template**（模板）下拉列表中的 T_DataCenter。
2. 选择 **Network Profiles** > **Zone Protection**（网络配置文件 > 区域保护），然后单击 **Add**（添加）。
3. 在本例中，根据 SYN Flood 攻击启用保护 — 在泛滥攻击保护选项卡中，选中 **SYN** 复选框，并将操作设置为 **SYN Cookie**、将警报数据包/秒设置为 **100**、将激活数据包/秒设置为 **1000**，以及将最大数据包/秒设置为 **10000**。
4. 在本例中，启用警报 — 在 **Reconnaissance Protection**（侦测保护）选项卡中，选中 **TCP Port Scan**（**TCP** 端口扫描）、**Host Sweep**（主机扫描）和 **UDP Port Scan**（**UDP** 端口扫描）的 **Enable**（启用）复选框。确保将 Action（操作）值设置为 **alert**（警报）（默认值）。
5. 单击 **OK**（确定）以保存区域保护配置文件。

STEP 5 | 在数据中心模板 (T_DataCenter) 中配置接口和区域设置，然后附加您刚才创建的区域保护配置文件。



在执行此步骤之前，您必须在防火墙上配置本地接口。对于每个接口，您至少必须定义接口类型，并将其分配到虚拟路由器（如果需要），然后附加安全区域。

1. 选择 **Network**（网络）选项卡，然后选择 **Template**（模板）下拉列表中的 T_DataCenter。
2. 选择 **Network** > **Interface**（网络 > 接口），然后在“Interface（接口）”列中单击接口名称。

© 2019 Palo Alto Networks, Inc.

3. 从下拉列表中选择 **Interface Type**（接口类型）。
4. 在 **Virtual Router**（虚拟路由器）下拉列表中，单击 **New Virtual Router**（新建虚拟路由器）。在确定路由器时，确保 **Name**（名称）与在防火墙上定义的名称相匹配。
5. 在 **Security Zone**（安全区域）下拉列表中，单击 **New Zone**（新建区域）。在定义区域时，确保 **Name**（名称）与在防火墙上定义的名称相匹配。
6. 单击 **OK**（确定）保存对接口所作的更改。
7. 选择 **Network** > **Zones**（网络 > 区域），然后选择刚创建的区域。验证已经将正确的接口连接到区域。
8. 在 **Zone Protection Profile**（区域保护配置文件）下拉列表中，选择您所创建的配置文件，然后单击 **OK**（确定）。

STEP 6 | 推送您的模板更改。

1. 选择 **Commit**（提交）> **Commit and Push**（提交并推送）和推送范围中的 **Edit Selections**（编辑选择）。
2. 选择 **Templates**（模板）并选择分配给您进行更改的模板的防火墙。
3. **Commit and Push**（提交并推送）对 Panorama 配置和模板的更改。

使用设备组来推送策略规则

用例的第三个任务：使用 Panorama 配置防火墙中的第三个任务是创建设备组来管理防火墙上的策略规则。

STEP 1 | 创建设备组并为每个设备组分配相应的防火墙：请参阅添加设备组。

在本例中，创建名为 DG_BranchAndRegional 和 DG_DataCenter 的设备组。

在配置 DG_BranchAndRegional 设备组中，您必须分配一个 **Master**（主）防火墙。它是设备组中的唯一防火墙，用于收集用户和组映射信息进行策略评估。

STEP 2 | 创建共享的前导规则可以支持 DNS 和 SNMP 服务。

1. 创建用于 DNS 和 SNMP 服务的共享应用程序组。
    1. 选择 **Objects**（对象）> **Application Group**（应用程序组），然后单击 **Add**（添加）。
    2. 输入 **Name**（名称），并勾选 **Shared**（共享）复选框以创建共享应用程序组对象。
    3. 单击添加，键入 **DNS**，然后从列表中选择 **dns**。针对 SNMP 重复以上操作，并选择 **snmp**、**snmp-trap**（**snmp** 陷阱）。
    4. 单击 **OK**（确定）以创建应用程序组。
2. 创建共享规则。
    1. 选择 **Policies**（策略）选项卡，然后选择 **Device Group**（设备组）下拉列表中的 **Shared**（共享）。
    2. 选择 **Security** > **Pre-Rules**（安全 > 前导规则）规则库。
    3. 单击 **Add**（添加），然后输入安全规则的 **Name**（名称）。
    4. 在规则的 **Source**（源）和 **Destination**（目标）选项卡中，单击 **Add**（添加）并输入流量的 **Source Zone**（源区域）和 **Destination Zone**（目标区域）。
    5. 在 **Applications**（应用程序）选项卡中，单击 **Add**（添加），键入刚创建的应用程序组对象的名称，然后从下拉列表中选择该名称。
    6. 在 **Actions**（操作）选项卡中，将 **Action**（操作）设置为 **Allow**（允许），然后单击 **OK**（确定）。

STEP 3 | 为所有办事处定义企业可接受的使用策略。在本例中，创建既能限制访问某些 URL 类别，又能拒绝访问风险等级为 3、4 或 5 的点对点流量的共享规则。

1. 选择 **Policies**（策略）选项卡，然后选择 **Device Group**（设备组）下拉列表中的 **Shared**（共享）。
2. 选择 **Security** > **Pre-Rules**（安全 > 先导规则），然后单击 **Add**（添加）。

© 2019 Palo Alto Networks, Inc.

3. 在 **General**（常规）选项卡上，输入安全规则的 **Name**（名称）。
4. 在 **Source**（源）和 **Destination**（目标）选项卡中，单击 **Add**（添加），然后为 **Source Zone**（源区域）和 **Destination Zone**（目标区域）流量选择 **any**（任何）。
5. 在 **Application**（应用程序）选项卡中，定义应用程序筛选器：
    1. 单击 **Add**（添加），然后在下拉列表的页脚中单击 **New Application Filter**（新建应用程序筛选器）。
    2. 输入 **Name**（名称），并选中 **Shared**（共享）复选框。
    3. 在 Risk（风险）列中，选择等级 **3**、**4** 和 **5**。
    4. 在 Technology（技术）列中，选择**peer-to-peer**（对等）。
    5. 单击 **OK**（确定）保存新的筛选器。
6. 在 **Service/URL Category**（服务/**URL** 类别）选项卡中，单击 URL Category（URL 类别）部分中的 **Add**（添加），然后选择要阻止的类别（如 **streaming-media**（流媒体）、**dating**（约会）和 **online-personal-storage**（在线个人存储））。
7. 您也可以附加默认 URL 筛选配置文件 — 在 **Actions**（操作）选项卡的 Profile Setting（配置文件设置）部分中选择 **Profile Type**（配置文件类型）选项**Profiles**（配置文件），然后选择 **URL Filtering**（**URL** 筛选）选项 **default**（默认）。
8. 单击 **OK**（确定）保存安全前导规则。

STEP 4 | 只允许区域总部中营销组的所有用户使用 Facebook。

根据用户和用户组启用安全规则包含以下先决任务：

- 在防火墙上设置 User-ID。
- 对于包含了您想要标识的用户的区域，为每一个区域启用 User-ID。
- 为 DG_BranchAndRegional 设备组定义一个主防火墙（请参阅步骤 1）。

1. 选择 **Policies**（策略）选项卡，然后选择 **Device Group**（设备组）下拉列表中的 DG_BranchAndRegional。
2. 选择 **Security** > **Pre-Rules**（安全 > 前导规则）规则库。
3. 单击 **Add**（添加），然后输入安全规则的 **Name**（名称）。
4. 在 **Source**（源）选项卡中，**Add**（添加）包含了营销组用户的源区域。
5. 在 **Destination**（目标）选项卡中，**Add**（添加）目标区域。
6. 在 **User**（用户）选项卡中，将营销用户组 **Add**（添加）到源用户列表。
7. 在应用程序选项卡中，单击添加，键入 `Facebook`，然后从下拉列表中选择它。
8. 在 **Action**（操作）选项卡中，将 **Action**（操作）设置为 **Allow**（允许）。
9. 在 **Target**（目标）选项卡中，选择区域总部防火墙并单击 **OK**（确定）。

STEP 5 | 允许数据中心的指定主机/服务器访问 Amazon 云应用程序。

1. 为数据中心内需要访问 Amazon 云应用程序的服务器/主机创建地址对象。
    1. 选择 **Objects** > **Addresses**（对象 > 地址），然后在 **Device Group**（设备组）下拉列表中选择 DG_DataCenter。
    2. 单击 **Add**（添加），然后输入地址对象的 **Name**（名称）。
    3. 选择 **Type**（类型），然后指定 IP 地址和网络掩码（**IP Netmask**（**IP** 网络掩码）），IP 地址的范围（**IP Range**（**IP** 范围））或 **FQDN**。
    4. 单击 **OK**（确定）保存对象。
2. 创建允许访问 Amazon 云应用程序的安全规则。
    1. 选择 **Policies** > **Security** > **Pre-Rules**（策略 > 安全 > 前导规则），然后在 **Device Group**（设备组）下拉列表中选择 DG_DataCenter。
    2. 单击 **Add**（添加），然后输入安全规则的 **Name**（名称）。
    3. 选择 **Source**（源）选项卡，**Add**（添加）数据中心的源区域，然后 **Add**（添加）您刚才定义的地址对象（源地址）。

© 2019 Palo Alto Networks, Inc.

4. 选择 **Destination**（目标）选项卡，然后 **Add**（添加）目标区域。
5. 选择 **Application**（应用程序）选项卡，单击 **Add**（添加），键入 **amazon**，然后从列表中选择 Amazon 应用程序。
6. 选择 **Action**（操作）选项卡，然后将 **Action**（操作）设置为 **Allow**（允许）。
7. 单击 **OK**（确定）保存规则。

STEP 6 | 要为网络上的所有互联网绑定流量启用日志记录，应创建规则用来将信任区域与不信任区域进行匹配。

1. 选择 **Policies**（策略）选项卡，然后选择 **Device Group**（设备组）下拉列表中的 **Shared**（共享）。
2. 选择 **Security** > **Pre-Rules**（安全 > 前导规则）规则库。
3. 单击 **Add**（添加），然后输入安全规则的 **Name**（名称）。
4. 在规则的 **Source**（源）和 **Destination**（目标）选项卡中，分别将 **trust_zone**和 **untrust_zone** **Add**（添加）为源区域和目标区域。
5. 在 **Action**（操作）选项卡中，将 **Action**（操作）设置为 **Deny**（拒绝），将 **Log Setting**（日志设置）设置为 **Log at Session end**（在会话结束时记录），然后单击 **OK**（确定）。

预览规则和提交更改

用例：使用 Panorama 配置防火墙中的最终任务是查看规则，并将所作的更改提交到 Panorama、设备组和模板。

STEP 1 | 预览规则。

该预览可让您直观评估如何为特殊规则库对规则进行分层。

1. 选择 **Policies**（策略）和 **Preview Rules**（预览规则）。
2. 选择 **Rulebase**（规则库）、**Device Group**（设备组）和 **Device**（设备）。
3. 完毕后，关闭预览对话框。

STEP 2 | 提交并推送您的配置更改。

1. 选择 **Commit**（提交） > **Commit and Push**（提交并推送）和推送范围中的 **Edit Selections**（编辑选择）。
2. 选择 **Device Groups**（设备组），选择您添加的设备组，然后选择 **Include Device and Network Templates**（包含设备和网络模板）。
3. 单击 **OK**（确定）保存对推送范围所作的更改。
4. **Commit and Push**（提交并推送）更改。

STEP 3 | 确认 Panorama 已应用模板和策略配置。

1. 在 Panorama 标题中，将 **Context**（上下文）设置为防火墙以访问其 Web 界面。
2. 查看模板和策略配置以确保您的更改已存在。

© 2019 Palo Alto Networks, Inc.

管理大规模防火墙部署

Panorama™ 提供多个管理大规模防火墙部署的选项。为了合并所有管理功能，在“仅管理”模式下，Panorama 支持使用 M-600 设备管理最多 5,000 个防火墙或使用 Panorama 虚拟设备管理最多 2,500 个防火墙。为了简化用于 5000 个防火墙以上的大规模防火墙部署的部署和操作管理，您可以使用 Panorama Interconnect 插件以通过单个 Panorama 控制器管理多个 Panorama 管理服务器节点。

- 确定大规模防火墙部署最佳解决方案
- 提高 M-600 和 Panorama 虚拟设备的设备管理容量
- Panorama Interconnect

确定大规模防火墙部署最佳解决方案

为了减轻管理大规模防火墙部署配置的操作负担，Palo Alto Networks 提供各种不同的防火墙管理选项来最好地适应您的部署场景。

如果您的大规模防火墙部署由一个或几个 Panorama 管理服务器构成，则可以部署一台最多可管理 5,000 个防火墙的 M-600 设备，或最多可管理 2,500 个防火墙的 Panorama 虚拟设备，以通过单个 Panorama 管理服务器利用所有 Panorama 功能。提高 M-600 和 Panorama 虚拟设备的设备管理容量是纵向扩展部署的理想之选，让您可以通过单个 Panorama 管理服务器管理大量防火墙，而非为了管理少数防火墙而部署多个 Panorama 管理服务器。

如果您的大规模防火墙部署由多个具有类似配置的 Panorama 管理服务器构成，则您可以通过Panorama Interconnect插件从单个 Panorama 控制器管理多个 Panorama 节点。因为可以从 Panorama 控制器对策略和配置进行集中管理，因此，此插件简化了大规模防火墙部署的部署和操作管理。通过 Panorama 控制器，设备组和模板堆栈配置将与 Panorama 节点同步，并被推送到受管设备。Panorama Interconnect 插件是横向扩展防火墙部署的理想之选，具有多个分布式 Panorama 管理服务器。

© 2019 Palo Alto Networks, Inc.

提高 M-600 和 Panorama 虚拟设备的设备管理容量

在“仅管理”模式下，M-600 设备最多可以管理 5,000 个防火墙，而 Panorama 虚拟设备最多可管理 2,500 个防火墙，从而减少了大规模防火墙部署的管理足迹。

- 提高设备管理容量要求
- 部署 Panorama 以提高设备管理容量

提高设备管理容量要求

在“仅管理”模式下，您可以使用一台 M-600 设备最多管理 5,000 个防火墙或者使用一台 Panorama 虚拟设备最多管理 2,500 个防火墙。从单个 Panorama 管理服务器管理此类大型部署可降低配置管理的操作复杂性，并减少管理多个 Panorama 管理服务器所产生的安全和合规风险。

对于日志收集，单个 Panorama 管理服务器是理想之选，因为其提供一个集中位置来查看和分析受管设备的日志数据，而不要求您访问每个单独 Panorama 管理服务器。为了在系统或网络出现故障时提供冗余，Palo Alto Networks 推荐在高可用性 (HA) 配置中部署两台 Panorama 管理服务器。

要生成预定义报告，必须启用 Panorama 以使用用于预定义报告的 Panorama 数据。这样，通过使用 Panorama 或专用日志收集器已收集的日志数据就可以生成预定义报告，这样会减少生成报告耗用的资源。必须启用此设置，否则，Panorama 性能可能会受到影响，且 Panorama 可能会无响应。

要管理多达 5000 个防火墙，Panorama 管理服务器必须满足以下最低要求：

要求	M 系列设备	Panorama 虚拟设备
模型	M-600	所有受支持的 Panorama 管理程序。有关详细信息，请参阅Panorama 型号。
Panorama 模式	仅管理	仅管理
受管防火墙数量	5,000	2，500
系统磁盘	240GB SSD — 用于存储操作系统文件和系统日志。	• 81GB — 用于存储操作系统文件和系统日志。 • 容量至少为 90GB 的其他磁盘。
内核	28（超线程）	28（超线程）
内存	256GB	250GB
日志收集	不支持本地日志收集。 要设置日志收集，请参阅使用专用日志收集器部署 Panorama 。	不支持本地日志收集。 要设置日志收集，请参阅使用专用日志收集器部署 Panorama 。
日志记录和报告	启用 **Use Panorama Data for Pre-Defined Reports**（使用用于预定义报告的 **Panorama** 数据）设置（**Panorama** > **Setup**（设置）>	启用 **Use Panorama Data for Pre-Defined Reports**（使用用于预定义报告的 **Panorama** 数据）设置（**Panorama** > **Setup**（设置）>

© 2019 Palo Alto Networks, Inc.

要求	M 系列设备	Panorama 虚拟设备
	Management（管理）> **Logging and Reporting Settings**（日志记录和报告设置）> **Log Export and Reporting**（日志导出和报告））	**Management**（管理）> **Logging and Reporting Settings**（日志记录和报告设置）> **Log Export and Reporting**（日志导出和报告））

部署 Panorama 以提高设备管理容量

如要部署 Panorama 以提高设备管理容量，请确定部署场景并执行以下步骤：

- 安装 Panorama 以提高设备管理容量
- 升级 Panorama 以提高设备管理容量

安装 *Panorama* 以提高设备管理容量

激活设备管理许可证，以通过单个 M-600 Panorama™ 管理服务器或单台 Panorama 虚拟设备管理 1,000 多个防火墙。

STEP 1 | 要获取能够使您最多管理 5000 个防火墙的 Panorama 设备管理许可证，请联系 Palo Alto Networks 销售代表。

- 如果部署 M-600 设备，可获取 `PAN-M-600-P-1K` 设备管理许可证。
- 如果部署 Panorama 虚拟设备，可获取 `PAN-PRA-1000` 设备管理许可证。

STEP 2 | 重新启动 Panorama 管理服务器。

- （仅限 M-600 设备）设置 M 系列设备。

或者

- 设置 Panorama 虚拟设备。

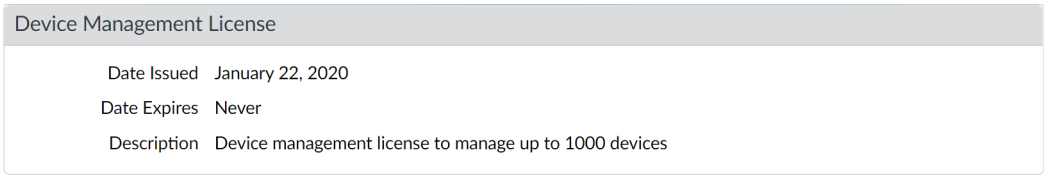
STEP 3 | 如果此模式下的 Panorama 不可用，则将 Panorama 管理服务器更改为“仅管理”模式。

- 从步骤 5 开始在仅管理模式下设置 M 系列设备。
- 在仅管理模式下设置 Panorama 虚拟设备。

STEP 4 | 注册 Panorama 管理服务器，并安装许可证。

1. 注册 Panorama。
2. 激活 Panorama 支持许可证。
3. 激活 Panorama 虚拟服务器上的设备管理许可证。
   - 在 M 系列设备上激活/检索防火墙管理许可证。
   - 在 Panorama 虚拟设备未连接到互联网时激活/检索防火墙管理许可证。
   - 在 Panorama 虚拟设备连接到互联网时激活/检索防火墙管理许可证。

STEP 5 | 选择 **Panorama** > **Licenses**（许可证），并验证设备管理许可证成功激活。



© 2019 Palo Alto Networks, Inc.

如果在 *Panorama* 上激活新的设备管理许可证，则您可以通过 *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 or more`（设备管理许可证可管理多达 `1000` 台设备或更多）。

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 | 增加 Panorama 虚拟设备上的 CPU 和内存 如果 Panorama 虚拟设备尚未满足提高设备管理容量所需的最低资源要求。

请查看提高设备管理容量要求以验证您现有的 Panorama 虚拟设备在升级前是否满足最低要求。

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）从步骤 5 开始至在仅管理模式下设置 M 系列设备。

或者

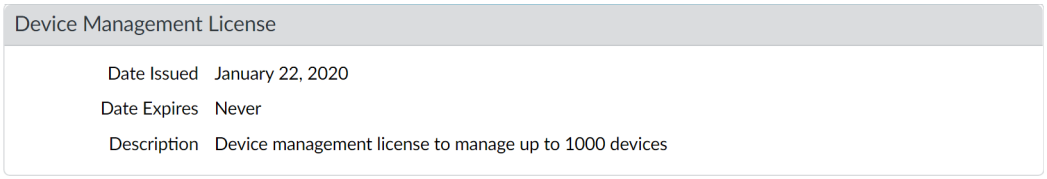
- 在仅管理模式下设置 Panorama 虚拟设备。

STEP 4 | 登录到 Panorama Web 界面。

STEP 5 | 升级 Panorama 管理服务器。

- 使用互联网连接安装 Panorama 更新。
- 未连接互联网时安装 Panorama 更新。
- 在高可用性配置中安装 Panorama 更新。

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）。

© 2019 Palo Alto Networks, Inc.

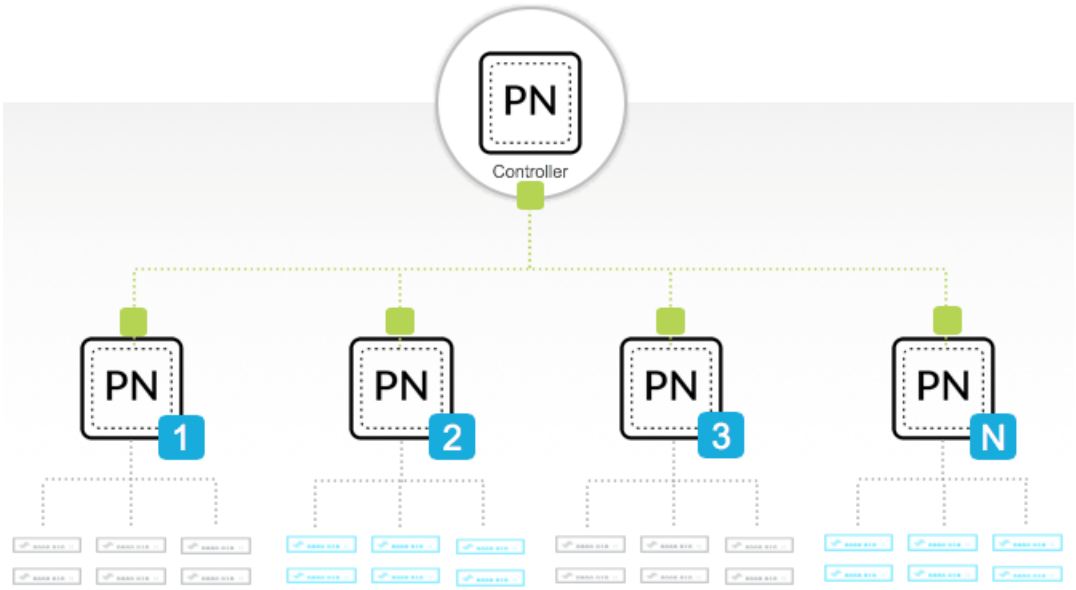
Panorama Interconnect

使用 Panorama™ Interconnect 管理大规模防火墙部署的配置。若要管理多个具有类似配置的 Panorama 管理服务器的配置，Panorama Interconnect 是理想的选择。

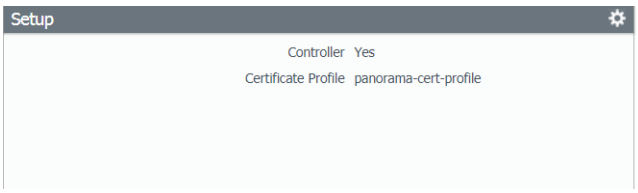
- Panorama Interconnect 概述
- Panorama Interconnect 要求
- 启动 Panorama 控制器和节点之间的身份验证
- 设置 Panorama Interconnect 插件
- 同步 Panorama Interconnect
- 采用 Panorama Interconnect 管理防火墙
- 升级 Panorama Interconnect 插件

Panorama Interconnect 概述

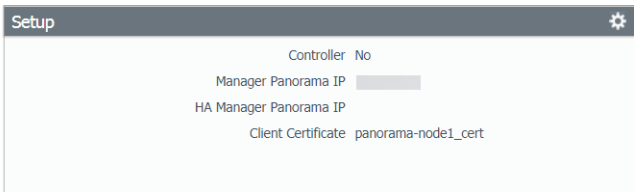
当您在超过单个 Panorama 实例管理容量的大量防火墙之间进行同构配置时，或是如果您已部署多个 Panorama™ 管理服务器时，则可以使用 Interconnect 插件或 Panorama 来减轻操作负担。您可以通过 Interconnect 插件设置用于管理最多 64 个 Panorama 节点的 Panorama 控制器，这样，可以简化网络上 Panorama 设备和受管防火墙的常用配置和策略。例如，您可以将 Panorama 控制器设置为用于管理 Panorama 特定配置（Panorama 节点上的管理员角色）以及推送 Panorama 节点以管理所有防火墙的所有常用模板堆栈和设备组配置之间的中心点。下图所示为 Panorama Interconnect 层次结构，其中，Panorama 控制器管理多个 Panorama 节点，Panorama 节点又反过来管理多个设备。



下图所示为在成功配置 Panorama 控制器和 Panorama 节点后用于这两者的 Panorama Interconnect **Setup**（设置）页面示例。



Panorama Controller



Panorama Node

© 2019 Palo Alto Networks, Inc.

必须完成下列任务以设置 Panorama Interconnect 插件：

任务	详细信息
查看Panorama Interconnect 要求	Panorama 管理服务器和防火墙必须满足系统和操作要求，以便成功部署 Panorama Interconnect 。 这包括安装和激活许可证，注册 Panorama 管理服务器。
启动 Panorama 控制器和节点之间的身份验证	生成或导入证书颁发机构，并为节点颁发证书，然后配置证书配置文件，确保 Panorama 控制器和 Panorama 节点之间通信安全。
设置 Panorama Interconnect 插件	在 Panorama 控制器和 Panorama 节点上下载、安装并设置 Panorama Interconnect 插件。
准备 Panorama 控制器，以便将配置推送到受管防火墙。	在Panorama 控制器上，添加设备组和配置模板堆栈以配置策略规则、对象和设置，从而使防火墙在网络上进行操作。
同步 Panorama Interconnect	将特定于 Panorama 的配置以及模板堆栈和设备组配置从 Panorama 控制器推送到 Panorama 节点。
采用 Panorama Interconnect 管理防火墙	添加一个或多个防火墙，并将同步配置从 Panorama 节点推送到受管设备。

Panorama Interconnect 要求

计划并查看在 Panorama 管理服务器上成功部署 Panorama™ Interconnect 插件的要求。

- 计划您的 Panorama Interconnect 部署
- Panorama Interconnect 的系统要求
- Panorama Interconnect 的证书要求

计划您的 *Panorama Interconnect* 部署

要在 Panorama 管理服务器上成功部署 Panorama™ Interconnect 插件：

- ❑ 查看 Panorama Interconnect 的系统要求。

  确认您的 Panorama 和受管防火墙满足最低资源要求且您的防火墙是单 vsys 防火墙。
- ❑ 为您的 Panorama 节点和受管防火墙计划设备组和模板堆栈配置。

  配置管理集中在 Panorama 控制器上，并复制到 Panorama 控制器管理的所有 Panorama 节点中。确保此配置简单、紧凑，且在所有 Panorama 节点上基本相同。

  互联支持基于设备组和模板的集中配置，其中包括对象、策略、防火墙和网络配置。互联部署中不支持 Panorama 集成插件（如 NSX、SD-WAN 和 Prisma 访问）添加的增量功能。

  Panorama 节点配置只能从 *Panorama* 控制器进行管理。当将 Panorama 节点与 Panorama 控制器同步时，在 *Panorama* 节点上所做的配置更改将被覆盖。
- ❑ 设置 Panorama 控制器和 Panorama 节点为仅管理模式。有关更改 Panorama 管理服务器模式的更多信息，请参阅在仅管理模式下设置 M 系列设备或在仅管理模式下设置 Panorama 虚拟设备。

© 2019 Palo Alto Networks, Inc.

因为管理过程和日志收集过程需要较多的资源，因此，在 *Panorama* 模式下部署 *Panorama* 控制器或 *Panorama* 节点上具有本地日志收集功能的 *Panorama Interconnect* 可能会导致性能下降。

- 注册 Panorama 和安装许可证 Panorama 控制器和 Panorama 节点。
- 部署一个或多个用于日志收集的专用日志收集器。有关在日志收集模式下部署 Panorama 管理服务器的日志存储要求和程序的更多信息，请参阅设置 Panorama。

  仅可从 Panorama 节点进行日志和报告生成。
- 在安装插件之前，Panorama 控制器和 Panorama 节点必须处于操作模式。Panorama Interconnect 插件不支持 FIPS 模式下的 Panorama 管理服务器，可能会导致 Panorama 服务管理器无响应。
- 获取证书颁发机构 (CA) 并生成 Panorama 控制器 CA 签署的 Panorama 节点证书，以确保 Panorama 控制器和 Panorama 节点之间的通信安全。有关详细信息，请参阅启动 Panorama 控制器和节点之间的身份验证。
- 启用 Panorama 控制器、Panorama 节点和受管防火墙上的 HTTPS 访问，以便登录到 Panorama Web 界面和防火墙 Web 界面。Panorama 不支持 CLI 和 API 访问。

Panorama Interconnect 的系统要求

确保 Panorama™ 管理服务器和防火墙符合系统要求，以便成功安装 Panorama Interconnect 插件，并管理大规模的防火墙部署：

- Panorama Interconnect 仅管理单一 VSYS 防火墙

要求	Panorama 控制器和节点	防火墙
模式	仅管理（推荐）	N/A
CPU 和内存	16 个 CPU 和 32GB 内存	N/A
系统磁盘	81GB	N/A
受支持的 OS	PAN-OS 8.1.3 或更高版本	PAN-OS 7.1 或更高版本
受支持的型号	• **M** 系列设备 — M-600 • **Panorama** 虚拟设备 — 关于所有受支持的 Panorama 虚拟设备型号，请参阅Panorama 型号。	• 物理防火墙 — 关于所有受支持的物理防火墙型号，请参阅防火墙型号。 • **VM** 系列防火墙 — 关于所有受支持的 VM 系列防火墙，请参阅VM 系列型号。

Panorama Interconnect 的证书要求

要确保 Panorama™ 控制器和 Panorama节点之间通信的安全，使用的证书必须满足以下要求：

- Panorama 控制器上需要使用负责颁发 Panorama 节点证书的证书颁发机构 (CA)。您可以创建自签名根 CA 证书或导入证书和私钥进行签名。请注意，您必须在 **Panorama** 选项卡中配置 CA 证书，以便设置 Interconnect 插件。
- 要为每个 Panorama 节点导入证书或是生成唯一证书，Panorama 控制器上的 CA 证书必须颁发用于节点的证书。
  - 如果正向 Panorama 节点导入证书，则证书 **Common Name**（通用名）必须是 Panorama 节点的序列号。
  - 此证书必须采用 PKCS12 或 PEM 格式，并应包含私钥，以便 Panorama 节点成功进行身份验证。

© 2019 Palo Alto Networks, Inc.

启动 Panorama 控制器和节点之间的身份验证

创建用于确保 Panorama™ 控制器和 Panorama 节点之间通信安全的证书配置文件。

- 获取 Panorama 控制器 CA 证书
- 生成 Panorama 节点证书
- 创建用于验证 Panorama 节点的证书配置文件

获取 *Panorama* 控制器 *CA* 证书

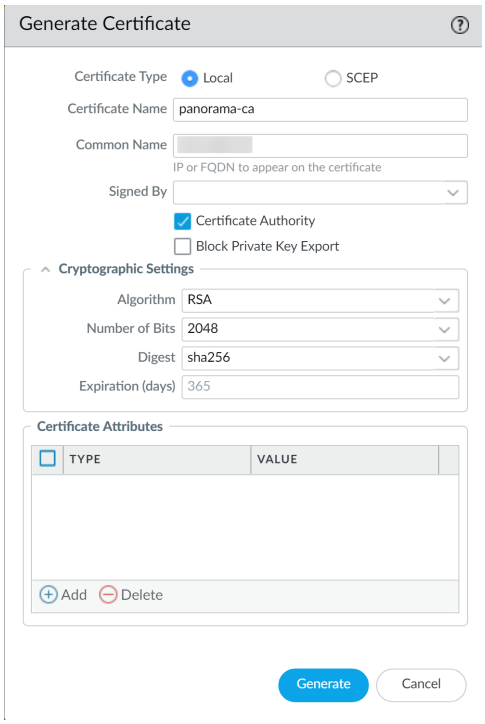
创建一个用于向 Panorama™ 节点颁发证书的受信任的证书颁发机构 (CA)，确保与互联网之间的连接安全。为大规模防火墙部署设置 Panorama 时需要提供受信任的 CA。

STEP 1 | Panorama 控制器的登录到 Panorama Web 界面。

STEP 2 | 创建证书颁发机构证书。

- 生成新 **CA** 证书

1. 选择 **Panorama** > **Certificate Management**（证书管理）> **Certificates**（证书），然后 **Generate**（生成）新的证书。
2. 对于 **Certificate Type**（证书类型），选择 **Local**（本地）。
3. 输入 **Certificate Name**（证书名称），如 **`panorama-ca`**。证书名称区分大小写且最多可包含 31 个字符。它必须是唯一的，且只能使用字母、数字、连字符和下划线。
4. 在 **Common Name**（通用名）字段，输入 Panorama 控制器的 IP 地址或 FQDN。
5. 将 **Signed By**（签名者）字段留空以便将证书指定为自签名。
6. 选中 **Certificate Authority**（证书颁发机构）复选框。
7. **Generate**（生成）CA 证书。

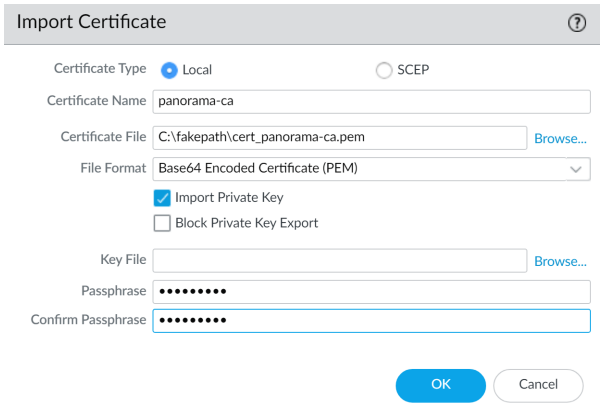


- 导入现有 **CA** 证书

1. 选择 **Panorama** > **Certificate Management**（证书管理）> **Certificates**（证书），然后 **Import**（导入）CA 证书。

© 2019 Palo Alto Networks, Inc.

2. 输入 **Certificate Name**（证书名称），如 **`panorama-CA`**。证书名称区分大小写且最多可包含 31 个字符。它必须是唯一的，且只能使用字母、数字、连字符和下划线。
3. **Browse**（浏览）以查找 **Certificate File**（证书文件）。
4. 选择 **File Format**（数据格式）：
   - **Base64 Encoded Certificate (PEM)**（**Base64** 编码证书 **(PEM)**）— 必须从证书单独导入密钥。选择 **Import Private Key**（导入私钥）复选框，然后 **Browse**（浏览）**Key File**（密钥文件）。
   - **Encrypted Private Key and Certificate (PKCS12)**（加密私钥和证书 **(PKCS12)**）— 常见格式，其中密钥和证书在一个容器（**Certificate File**（证书文件））中。
5. 输入并重新输入（确认）用于密钥加密的 **Passphrase**（密码）。
6. 单击 **OK**（确定）。证书页面现在显示已导入的 CA 证书。



STEP 3 | 单击 **Commit**（提交）和 **Commit to Panorama**（提交到 **Panorama**）。

生成 *Panorama* 节点证书

要使 Panorama™ 控制器对每个 Panorama 节点进行身份验证，请为每个 Panorama 节点创建唯一证书。Panorama 控制器和节点使用基于证书的身份验证确保相互之间的通信安全。生成 Panorama 节点唯一证书之前，获取 Panorama 控制器 CA 证书。

如果您的 Panorama 节点位于高可用性 (HA) 配置中，您必须创建并导入两个 Panorama 节点的 Panorama 节点证书到 HA 配置中的每个对端。

STEP 1 | Panorama 控制器的登录到 Panorama Web 界面。

STEP 2 | 选择 **Panorama** > **Certificate Management**（证书管理）> **Certificates**（证书），然后 **Generate**（生成）新的证书。

1. 对于 **Certificate Type**（证书类型），选择 **Local**（本地）。

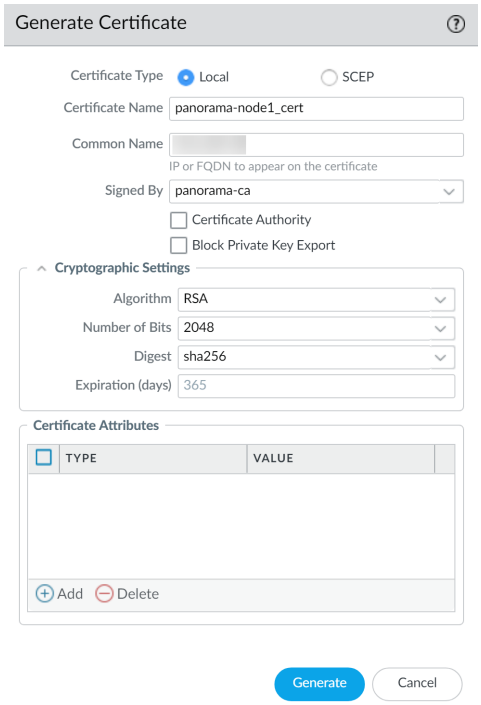
   目前还不支持 *SCEP*。

2. 输入 **Certificate Name**（证书名称），如 **`panorama-node1_cert`**。证书名称区分大小写且最多可包含 31 个字符。它必须是唯一的，且只能使用字母、数字、连字符和下划线。
3. 在 **Common Name**（通用名）字段，输入 Panorama 节点序列号。

   必须在 *Common Name*（通用名）字段内输入序列号，以便对 *Panorama* 控制器和 *Panorama* 节点之间的连接进行验证。如果未在此字段内输入序列号，则 *Panorama* 节点无法连接到 *Panorama* 控制器。

4. 在 **Signed By**（签名者）字段中，选择 CA 证书。
5. **Generate**（生成）证书。

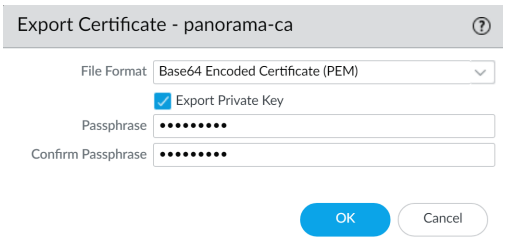
© 2019 Palo Alto Networks, Inc.



STEP 3 | 单击 **Commit**（提交）和 **Commit to Panorama**（提交到 **Panorama**）。

STEP 4 | 导出在步骤 2 中为每个 Panorama 节点生成的证书。

1. 选择 **Panorama** > **Certificate Management**（证书管理）> **Certificates**（证书），然后选择证书，并 **Export Certificate**（导出证书）。
2. 选择 **File Format**（文件格式）：
   - **Base64 Encoded Certificate (PEM)**（**Base64** 编码证书 **(PEM)**）— 允许您分别导出证书和私钥。如果您希望导出的文件包含私钥，请选中 **Export Private Key**（导出私钥）复选框。
   - **Encrypted Private Key and Certificate (PKCS12)**（加密私钥和证书 **(PKCS12)**）— 将证书和私钥导出在单个文件中。
3. 选中 **Export private key**（导出私钥）框。
4. 输入 **Passphrase**（密码）并 **Confirm Passphrase**（确认密码）以加密私钥。此密码是将证书密钥导入 Panorama 节点的密码。
5. 单击 **OK**（确认），将证书/私钥文件保存到您的计算机中。



6. 输入证书的描述性文件名称，这样，您可以轻松标识需要导入的 Panorama 节点，然后 **Save**（保存）证书。

STEP 5 | 将证书导入每个 Panorama 节点。

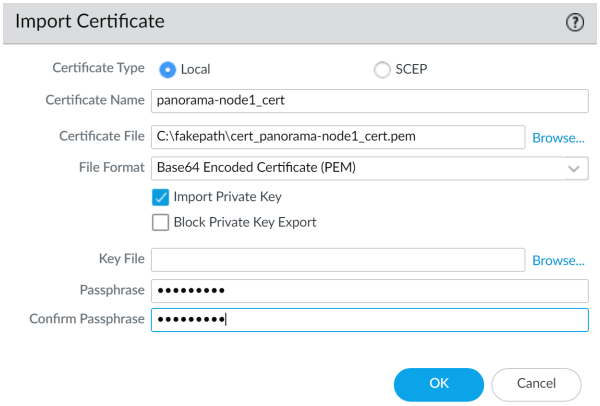
1. 登录到 Panorama Web 界面Panorama 节点。
2. 选择 **Panorama** > **Certificate Management**（证书管理）> **Certificates**（证书），然后 **Import**（导入）证书：

© 2019 Palo Alto Networks, Inc.

1. 对于 **Certificate Type**（证书类型），选择 **Local**（本地）。

   目前还不支持 *SCEP*。

2. 输入相同的 **Certificate Name**（证书名称）。此名称区分大小写且最多可包含 31 个字符。它必须是唯一的，且只能使用字母、数字、连字符和下划线。
3. **Browse**（浏览）在步骤 4 中导入的证书。
4. 选中 **Import private key**（导入私钥）框。
5. 输入用于加密私钥的 **Passphrase**（密码）并 **Confirm Passphrase**（确认密码）。
6. 单击确定以导入证书。



3. 单击 **Commit**（提交）和 **Commit to Panorama**（提交到 **Panorama**）。

创建用于验证 *Panorama* 节点的证书配置文件

证书配置文件定义了要使用哪些证书颁发机构 (CA) 证书来验证用于保护 Panorama™ 控制器与 Panorama 节点之间安全通信和验证 Panorama 节点撤销状态的 Panorama 节点证书。为大规模防火墙部署设置 Panorama 时，需要证书配置文件。

STEP 1 | Panorama 控制器的登录到 Panorama Web 界面。

STEP 2 | 获取 Panorama 控制器 CA 证书。

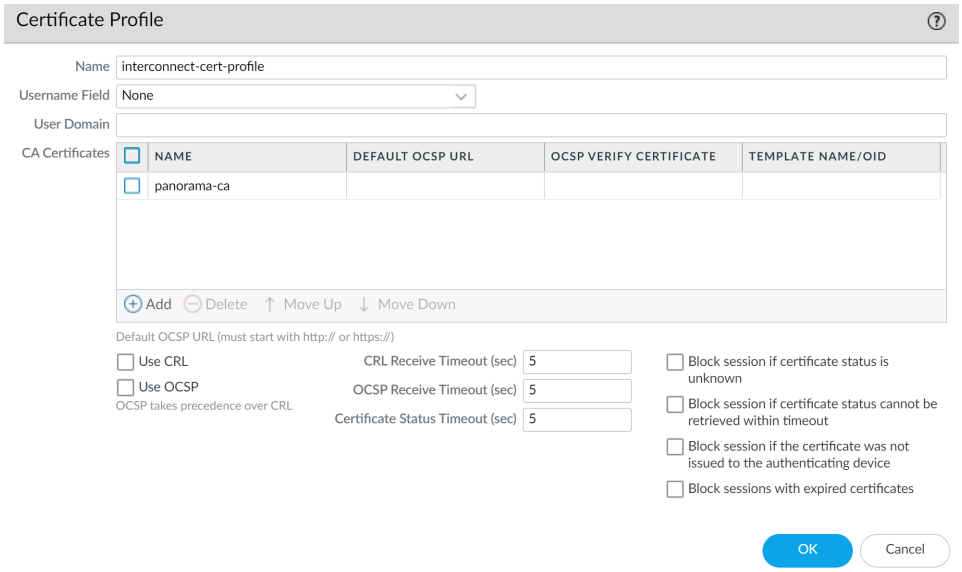
STEP 3 | 生成 Panorama 节点证书用于确保 Panorama™ 控制器和 Panorama 节点之间通信的安全。为所有 Panorama 节点重复执行此步骤。

STEP 4 | 创建证书配置文件。

当前不支持 *CRL* 和 *OCSP*。

1. 选择 **Panorama** > **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件），然后 **Add**（添加）新的证书配置文件。
2. 输入证书配置文件的 **Name**（名称）。
3. **Add**（添加）在步骤 2 中创建的 CA 证书。
4. 单击 **OK**（确定）以完成添加证书配置文件。

© 2019 Palo Alto Networks, Inc.



STEP 5 | 单击 **Commit**（提交）和 **Commit to Panorama**（提交到 **Panorama**）。

设置 Panorama Interconnect 插件

通过 Panorama™ Interconnect 使大规模防火墙部署的模板堆栈和设备组管理集中化，以将重复的配置从 Panorama 控制器推送到 Panorama 节点，从而确保防火墙配置和安全策略之间的一致性。您可以采用 Panorama Interconnect 创建用于管理 Panorama 节点（管理防火墙和推送配置）的 Panorama 管理器。这是您能够从单一位置管理大规模防火墙部署的配置，从而缩短配置多个 Panorama 管理服务器的时间，并在发生配置错误时减少安全漏洞。在 Panorama 管理服务器上设置 Panorama Interconnect 插件之前，请查看Panorama Interconnect 要求。

如果您的 Panorama 节点在高可用性 (HA) 配置中，则必须在两个 Panorama HA 对端上设置 Panorama Interconnect 插件。

STEP 1 | 安装 Panorama Interconnect 插件。必须在 Panorama 控制器和所有 Panorama 节点上安装插件。

1. 登录到 Panorama Web 界面。
2. 选择 **Panorama** > **Plugins**（插件），然后搜索 `Interconnect`。
3. **Download**（下载）并 **Install**（安装）Panorama Interconnect 插件。
4. 单击 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**）以完成安装 Panorama Interconnect 插件。

STEP 2 | 启动 Panorama 控制器和节点之间的身份验证以确保 Panorama 控制器和 Panorama 节点之间的身份验证。

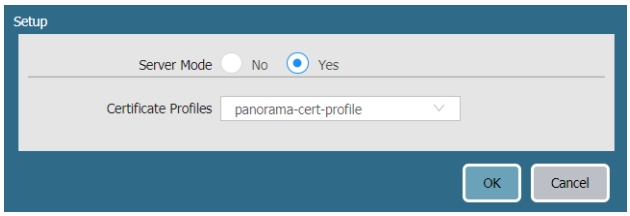
STEP 3 | 在 Panorama 控制器上设置插件。如果 Panorama 控制器处于 HA 配置中，则在高可用性对端设备上重复此步骤。

一旦 *Panorama* 配置为 *Panorama* 控制器，则无法将 *Panorama* 控制器重新配置为 *Panorama* 节点。验证是否正在将正确的 *Panorama* 管理服务器配置为 *Panorama* 控制器，然后再继续。

1. 选择 **Panorama** > **Interconnect** > **Setup**（设置），然后编辑 **Interconnect Plugin Setup**（**Interconnect** 插件设置）：

© 2019 Palo Alto Networks, Inc.

2. 在 **Server Mode**（服务器模式）字段中，选择 **Yes**（是）。
3. 选择您在步骤 2 中创建的 **Certificate Profile**（证书配置文件）。
4. 单击 **OK**（确定）以保存设置。

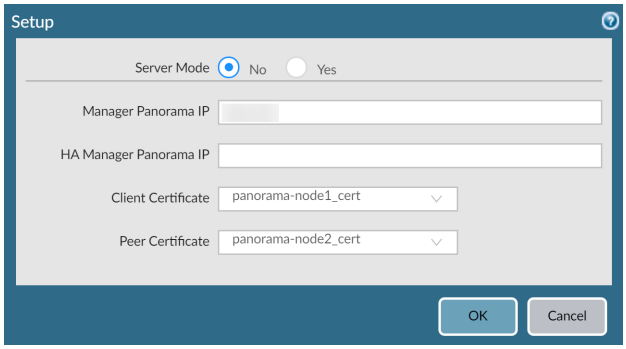


5. 单击 **Commit**（提交）和 **Commit to Panorama**（提交到 **Panorama**）。

STEP 4 | 在 Panorama 节点上设置插件。为所有 Panorama 节点重复执行此步骤。

如果您的 *Panorama* 节点在高可用性 *(HA)* 配置中，则在每个对端上设置 *Panorama Interconnect* 插件时必须选择已导入每个 *Panorama* 节点 *HA* 对端的 *Panorama* 节点证书。

1. 选择 **Panorama** > **Interconnect** > **Setup**（设置），然后编辑 **Interconnect Plugin Setup**（**Interconnect** 插件设置）：
   1. 在 **Server Mode**（服务器模式）字段中，选择 **No**（否）。
   2. **Manager Panorama IP**（管理 **Panorama IP**）— 输入 Panorama 控制器的管理 IP 地址。
   3. **HA Manager IP**（**HA** 管理器 **IP**）— 如果 Panorama 控制器处于高可用性配置，则输入 HA Panorama 控制器对端设备的管理 IP 地址。
   4. 选择在步骤 2 中导入的 Panorama 节点证书。
   5. （仅限 HA）选择在步骤 2 中导入的对端 Panorama 节点证书。
2. 单击 **OK**（确定）以保存设置。



3. 单击 **Commit**（提交）和 **Commit to Panorama**（提交到 **Panorama**）以完成 Panorama 节点上的插件设置。

STEP 5 | 添加 Panorama 节点到 Panorama 控制器。

1. 选择 **Panorama** > **Interconnect** > **Panorama Nodes**（**Panorama** 节点），然后 **Add**（添加）Panorama 节点。
   1. 输入 Panorama 节点的 **Name**（名称）。这无需与 Panorama 管理服务器上设置的设备名称相匹配。

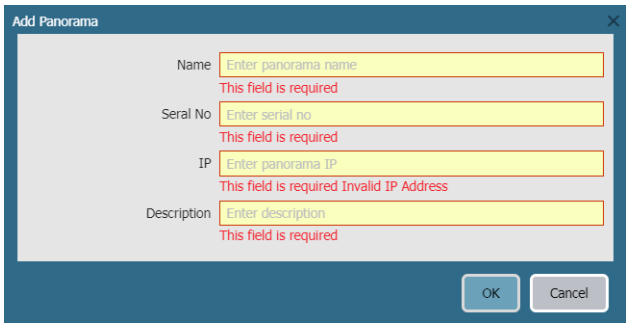
      Panorama 节点 *Name*（名称）中不得包含句点 *(.)*。

   2. 输入 Panorama 节点的 **Serial No**（序列号）。
   3. 输入 Panorama 节点的 **IP**地址。此 IP 地址必须可以访问 Panorama 控制器。

© 2019 Palo Alto Networks, Inc.

4. 输入 Panorama 节点的 **Description**（描述）。

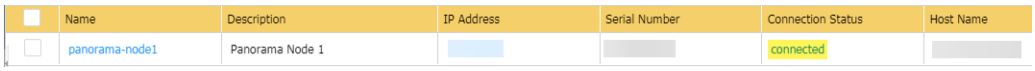
2. 单击 **Ok**（确定）以添加 Panorama 节点。



3. 单击 **Commit**（提交）和 **Commit to Panorama**（提交到 **Panorama**）以完成添加 Panorama 节点。

STEP 6 | 验证新添加的 Panorama 节点是否已连接（显示 **Connected**）。

1. 选择 **Panorama** > **Interconnect** > **Panorama Nodes**（**Panorama** 节点）。
2. 找到添加的 Panorama 节点，并验证连接状态列是否显示 `Connected`。



STEP 7 | 在 Panorama 控制器和 Panorama 节点上成功安装插件后，则执行下一步以完成 Panorama Interconnect 设置：

1. 在 Panorama 控制器上，添加设备组。重复此步骤以根据需要创建任何数量的设备组。
2. 在 Panorama 控制器上，配置模板堆栈。重复此步骤以创建所需数量的模板堆栈。
3. 同步 Panorama Interconnect 以将特定于 Panorama 的配置以及模板堆栈和设备组配置从 Panorama 控制器推送到 Panorama 节点。
4. 在 Panorama 控制器上，添加一个或多个由 Panorama 节点管理的防火墙。
   - 添加防火墙到 Panorama 节点
   - 将多个防火墙导入到 Panorama 节点
5. 将 Panorama 节点配置推送到受管设备。

同步 Panorama Interconnect

要从 Panorama 控制器推送 Panorama™ 模板堆栈和设备组配置，请将 Panorama 节点配置与 Panorama 控制器同步，以同步任何特定于 Panorama 的配置，从而促使 Panorama 节点推送配置到受管设备。

- 将 Panorama 常规配置推送到 Panorama 节点
- 将 Panorama 节点与 Panorama 控制器同步

将 *Panorama* 常规配置推送到 *Panorama* 节点

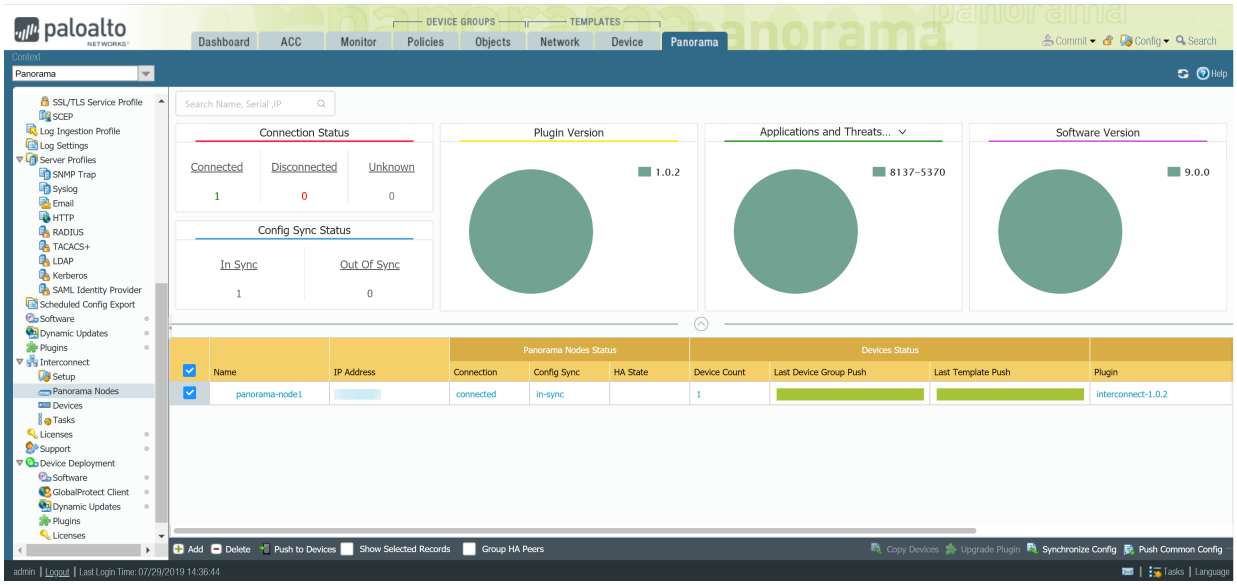
推送 Panorama™ 控制器常规配置到 Panorama 节点，以便将任何特定于 Panorama 的配置应用于 Panorama 节点。要同步模板堆栈和设备组配置以便将其推送到受管设备，请参阅将 Panorama 节点与 Panorama 控制器同步。

STEP 1 | Panorama 控制器的登录到 Panorama Web 界面。

STEP 2 | 选择 **Panorama** > **Interconnect** > **Panorama Nodes**（**Panorama** 节点），并选择用于管理防火墙的 Panorama 节点以推送配置。

STEP 3 | **Push Common Config**（推送常规配置）以便将特定于 Panorama 的配置推送到 Panorama 节点。

© 2019 Palo Alto Networks, Inc.



将 *Panorama* 节点与 *Panorama* 控制器同步

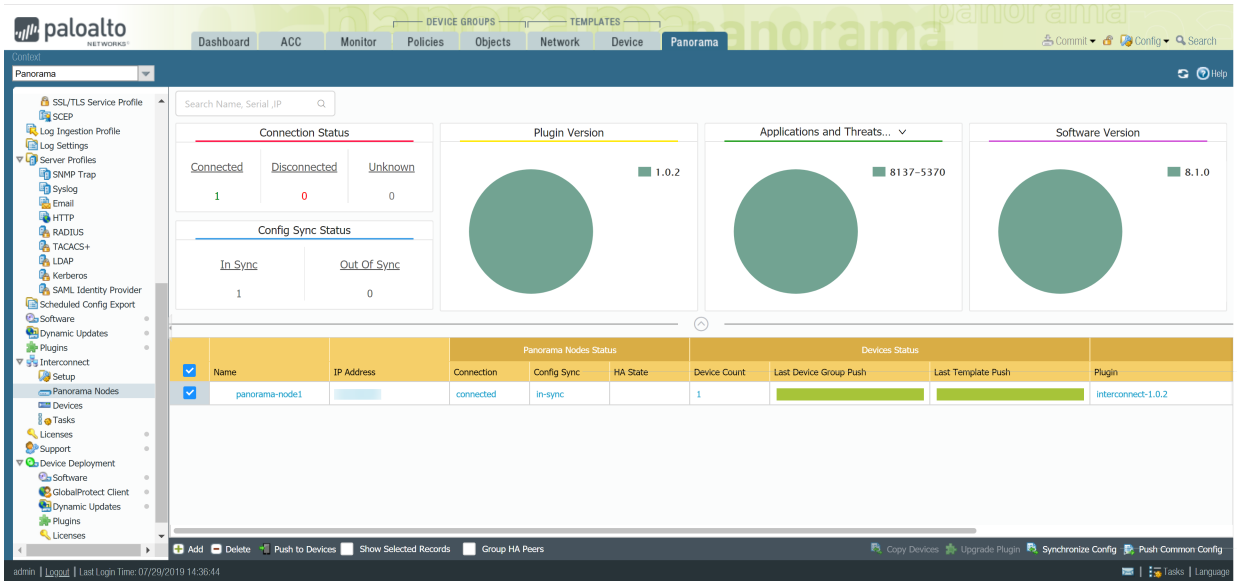
将 Panorama™ 控制器配置与 Panorama 节点同步，这样，Panorama 节点可将任何模板堆栈或设备组配置推送到受管设备。

STEP 1 | Panorama 控制器的登录到 Panorama Web 界面。

STEP 2 | 选择 **Panorama** > **Interconnect** > **Panorama Nodes**（**Panorama** 节点），并选择用于与 Panorama 控制器同步的 Panorama 节点。

STEP 3 | **Synchronize Config**（同步配置），以便将设备组和模板堆栈配置推送到 Panorama 节点。这是将配置推送到受管设备的必备过程。

STEP 4 | 在同步状态列中，验证 Panorama 节点是否同步（显示 **in-sync**）。



© 2019 Palo Alto Networks, Inc.

采用 Panorama Interconnect 管理防火墙

添加单个防火墙或批量导入多个设备，以便由 Panorama™ 节点进行管理。

- 添加防火墙到 Panorama 节点
- 将多个防火墙导入到 Panorama 节点
- 导入模板堆栈变量
- 使用 Panorama Interconnect 管理主密钥
- 将 Panorama 节点配置推送到受管设备

添加防火墙到 *Panorama* 节点

添加一个受 Panorama™ 节点管理的防火墙，以便从集中式 Panorama 控制器管理模板堆栈和设备组配置。要批量导入多个防火墙，请参阅将多个防火墙导入到 Panorama 节点。

STEP 1 | 配置防火墙以便与 Panorama 节点进行通信。

1. 在防火墙上执行初始配置，使其可以访问且能够在网络上与 Panorama 进行通行。
2. 将 Panorama 节点 IP 地址添加到防火墙。
    1. 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后 Edit（编辑）Panorama 设置。
    2. 在第一个字段中输入 Panorama IP 地址。
    3. （可选）如果您已在 Panorama 中设置高可用性对，请在第二个字段中输入辅助 Panorama IP 地址。
    4. 单击 **OK**（确定）。
3. 选择 **Commit**（提交）并 **Commit**（提交）更改。

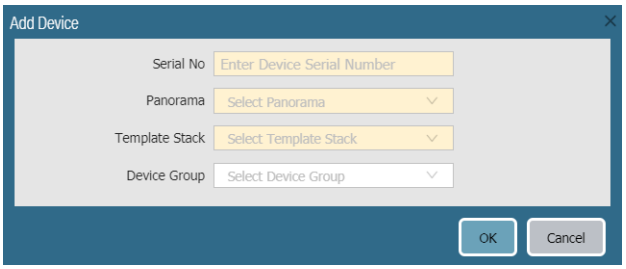
STEP 2 | Panorama 控制器的登录到 Panorama Web 界面。

STEP 3 | 选择 **Panorama** > **Interconnect**（互联）> **Devices**（设备），并 **Add**（添加）防火墙。

STEP 4 | 输入防火墙信息：

- 输入防火墙的 **Serial No**（序列号）。
- 选择用于管理防火墙的 **Panorama** 节点。
- 选择用于管理防火墙配置的 **Template Stack**（模板堆栈）。
- 选择用于与防火墙关联的 **Device Group**（设备组）。

STEP 5 | 单击 **OK**（确定），将防火墙添加为受管设备。



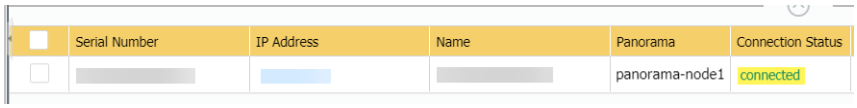
STEP 6 | 单击 **Commit**（提交）和 **Commit to Panorama**（提交到 **Panorama**）以完成添加防火墙。

STEP 7 | 选择 **Panorama** > **Interconnect**（互联）> **Panorama Nodes**（**Panorama** 节点）并 **Synchronize Config**（同步配置）。

STEP 8 | 验证新添加的防火墙是否 `Connected`。

© 2019 Palo Alto Networks, Inc.

1. 选择 **Panorama** > **Interconnect**（互联）> **Devices**（设备）。
2. 找到添加的防火墙，并验证连接状态列是否显示 `Connected`。



将多个防火墙导入到 *Panorama* 节点

您可以使用在导入过程中为您提供的 CSV 模板导入受 Panorama™ 节点管理的多个防火墙。一次性导入多个防火墙允许您快速添加多个防火墙到 Panorama 节点，并将其分配给模板堆栈和设备组，以集中进行配置管理。

导入多个防火墙时，可以将防火墙添加到不同的 Panorama 节点以及不同的模板堆栈和设备组。例如，您已完成 Panorama 节点 A 和 Panorama 节点 B 的部署，每个节点均带有两个模板堆栈和两个设备组。如果导入 100 个防火墙，则可以通过以下方式导入：

- 添加 50 个防火墙到 Panorama 节点 A：
  - 分配 25 个防火墙到模板堆栈 A1 和设备组 A1。
  - 分配 25 个防火墙到模板堆栈 A2 和设备组 A2。
- 添加 50 个防火墙到 Panorama 节点 B：
  - 分配 30 个防火墙到模板堆栈 B1 和设备组 B1。
  - 分配 20 个防火墙到模板堆栈 B2 和设备组 B2。

要添加单个防火墙，请参阅添加防火墙到 Panorama 节点。

STEP 1 | 配置防火墙以便与 Panorama 节点进行通信。

通过互联插件为所有受 Panorama 管理的防火墙执行此步骤。

1. 在防火墙上执行初始配置，使其可以访问且能够在网络上与 Panorama 进行通行。
2. 将 Panorama 节点 IP 地址添加到防火墙。
   1. 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后 Edit（编辑）Panorama 设置。
   2. 在第一个字段中输入 Panorama IP 地址。
   3. （可选）如果您已在 Panorama 中设置高可用性对，请在第二个字段中输入辅助 Panorama IP 地址。
   4. 单击 **OK**（确定）。
3. 选择 **Commit**（提交）并 **Commit**（提交）更改。

STEP 2 | Panorama 控制器的登录到 Panorama Web 界面。

STEP 3 | 单击 **Commit**（提交）和 **Commit to Panorama**（提交到 **Panorama**），将任何暂挂配置更改为 Panorama 控制器。导入多个防火墙要求 Panorama 控制器没有暂挂更改，否则，导入将失败。

STEP 4 | 选择 **Panorama** > **Interconnect** > **Devices**（设备），然后 **Import**（导入）防火墙。

STEP 5 | 单击 **Download Sample CSV**（下载样本 **CSV**）以下载正确格式的 CSV 文件来上传多个防火墙。

STEP 6 | 填写已下载的 CSV。**serial**（序列）、**panorama**、**device-group**（设备组）和 **template-stack**（模板堆栈）字段中输入适当的值。在导入防火墙之前，必须在 Panorama 控制器上完成 Panorama 节点、设备组和模板堆栈的添加和创建，这也是成功添加防护期所需。输入防火墙信息之后，请 **Save**（保持）文件。

© 2019 Palo Alto Networks, Inc.

此外，您还可以分配防火墙到内容调度。防火墙导入则无需执行这些步骤。

不支持更改 *CSV* 列顺序。如果列顺序重新排序，则防火墙导入失败。

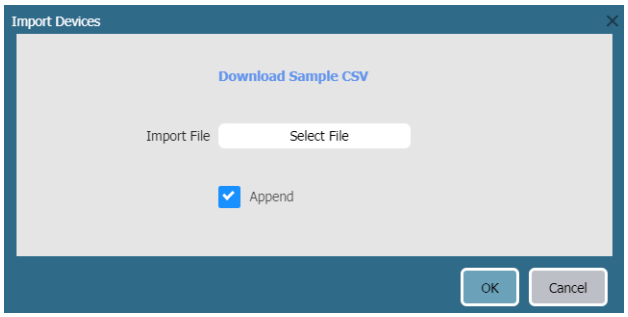
STEP 7 | 返回到 Panorama Web 界面，**Select File**（选择文件）以浏览并选择包含防火墙信息的 CSV 文件。

批量导入缺少必要信息的防火墙会导致整个导入失败。如果遇到错误，系统会发出一条错误信息提示，显示导入文件位置错误。

STEP 8 | **Append**（附加）新设备，以将其添加到 **Devices**（设备）列表的末尾。所有导入设备均必须为新设备。如果导入的任何设备是 Panorama 控制器上运行配置的一部分，则导入失败。

如果想要删除列表中现有设备，只想添加您正在添加的新设备，则取消选择 *Append*（附加）框。

STEP 9 | 单击 **OK**（确定），将防火墙添加为受管设备。

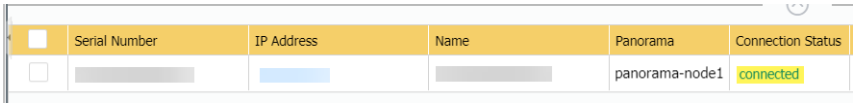


STEP 10 | 单击 **Commit**（提交）和 **Commit to Panorama**（提交到 **Panorama**）以完成添加防火墙。

STEP 11 | 选择 **Panorama** > **Interconnect**（互联）> **Panorama Nodes**（Panorama 节点）并 **Synchronize Config**（同步配置）。

STEP 12 | 验证新导入的防火墙是否 `Connected`。

1. 选择 **Panorama** > **Interconnect**（互联）> **Devices**（设备）。
2. 找到导入的防火墙，并验证连接状态列是否显示 `Connected`。



导入模板堆栈变量

使用模板堆栈变量更换 IP 地址、IP 范围、FQDN、IKE 中的接口、VPN 和 HA通过变量，您可以减少需要管理的模板和模板堆栈总数，同时保留任何特定于防火墙的值。

通过导入模板堆栈变量，您可以覆盖多个现有变量值，并且在导入时不能创建新的模板堆栈变量。关于如何创建新模板或模板堆栈变量的更多信息，请参阅配置模板或模板堆栈变量。

STEP 1 | 导出现有模板堆栈变量。

1. 对于 Panorama 控制器，登录到 Panorama Web 界面。
2. 选择 **Panorama** > **Interconnect** > **Devices**（设备），然后 **Export Variables**（导出变量）。
3. 从下拉菜单中选择模板堆栈 **Name**（名称）。

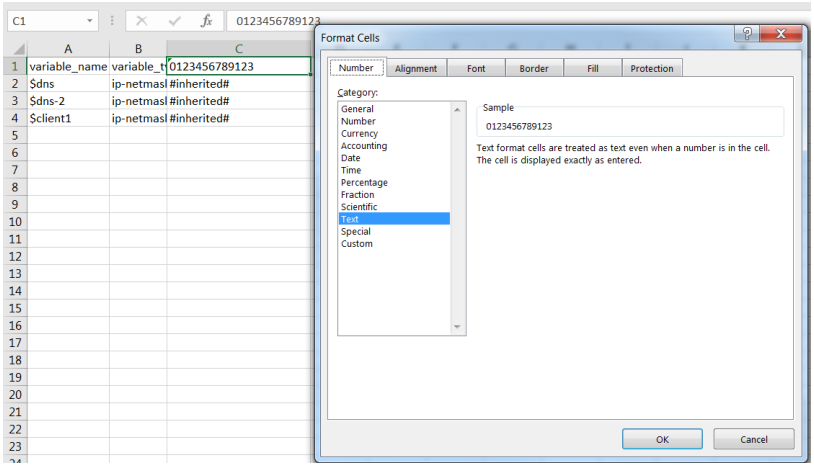
© 2019 Palo Alto Networks, Inc.

4. 单击 **Ok**（确定）并保存 CSV 文件。

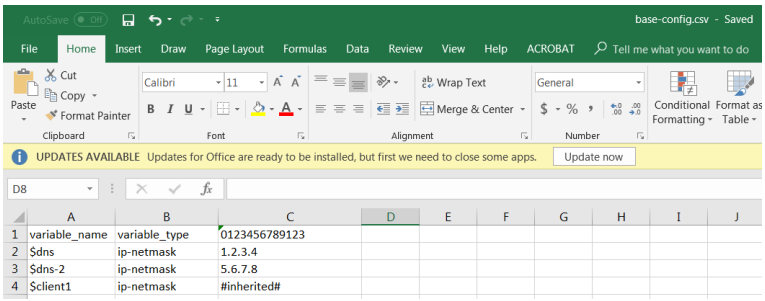
STEP 2 | 编辑包含模板堆栈变量的 CSV 文件，以便按下列格式导入到 Panorama Interconnect ：

显示为 `#inherited#` 的值是在模板堆栈中定义的值。

1. 更正包含防火墙序列号的单元数量。对 CSV 文件中所有防火墙重复此步骤。
   1. 右键单击包含防火墙序列号的单元格，然后选择 **Format Cells**（格式化单元格）。
   2. 选择 **Number**（编号）> **Text**（文本），然后单击 **OK**（确定）。
   3. 在序列号开头处添加一个 **0** 。

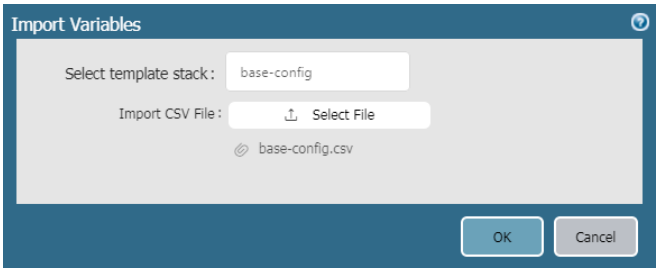


2. 输入所需模板变量的新值。
3. 选择 **File**（文件）> **Save As**（另存为），然后以 **CSV UTF-8** 格式保存文件。



STEP 3 | 将 CSV 文件导入到模板堆栈。

1. 对于 Panorama 控制器，登录到 Panorama Web 界面。
2. 选择 **Panorama** > **Interconnect** > **Devices**（设备），然后 **Import Variables**（导入变量）。
3. 在 **Select template stack**（选择模板堆栈）下拉列表中，选择将变量导入到其中的模板堆栈。
4. 在 **Import CSV File**（导入 **CSV** 文件）中，单击 **Select File**（选择文件），然后选择包含模板堆栈变量的 CSV 文件。
5. 单击 **OK**（确定）以导入模板堆栈变量。



© 2019 Palo Alto Networks, Inc.

6. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

STEP 4 | 将 Panorama 节点与 Panorama 控制器同步。

STEP 5 | 将 Panorama 节点配置推送到受管设备。

使用 *Panorama Interconnect* 管理主密钥

Panorama、防火墙、日志收集器、以及 WF-500 设备使用主密钥加密配置中的敏感元素，且具有用于加密密码和配置元素的默认主密钥。

作为标准安全实践的一部分，您必须在主密钥到期时续订每个单独防火墙、日志收集器、WildFire 设备、和 Panorama 上的主密钥。部署到受管设备的主密钥必须与用于 Panorama 控制器、Panorama 节点和受管设备的主密钥相同，这样才能成功推送配置。为确保密钥部署的统一，直接通过 Panorama 在多个防火墙、日志收集器、和 WF-500 设备上部署新的主密钥，或续订过期主密钥。使用 Panorama Interconnect 时，必须通过单一程序为 Panorama 控制器、Panorama 节点、和受管设备配置并部署相同的主密钥。要部署主密钥到受管设备，必须在每个 Panorama 节点上配置主密钥，并将其部署到受此节点管理的所有设备。有关详细信息，请参阅配置主密钥。

STEP 1 | 在 Panorama 控制器上配置主密钥。

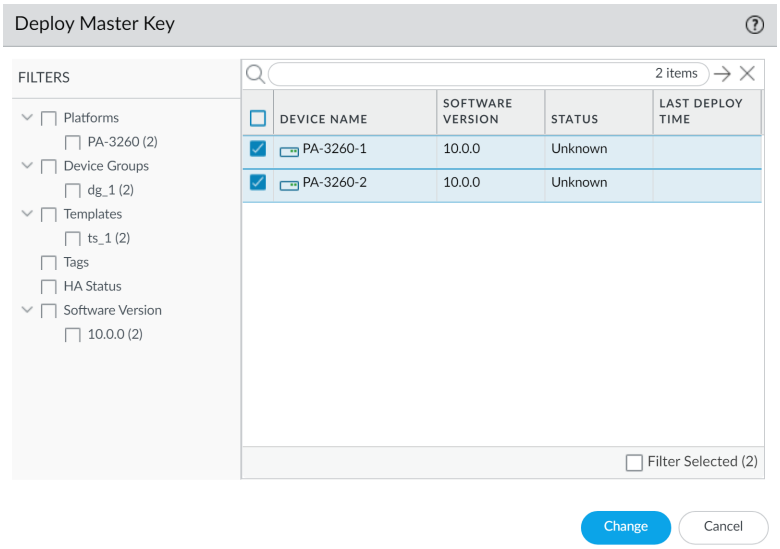
1. 在 Panorama 控制器上，登录到 Panorama Web 界面。
2. 选择**Panorama** > **Master Key and Diagnostics**（主密钥和诊断），然后编辑主密钥。
    1. 如果续订主密钥，则输入 **Current Master Key**（当前主密钥）。如果使用新的主密钥更换默认主密钥，请勿指定 **Current Master Key**（当前主密钥）。
    2. 配置 **New Master Key**（新主密钥），并 **Confirm Master Key**（配置主密钥）。
    3. 配置主密钥 **Lifetime**（生命周期）和 **Time for Reminder**（提醒时间）。
    4. 将 Panorama 控制器配置为：在密钥生命周期到期后，**Auto Renew with Same Master Key**（将相同主密钥自动续订）指定天数。
    5. 单击 **OK**（确定）。
3. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

STEP 2 | 部署主密钥到受 Panorama 节点管理的设备。

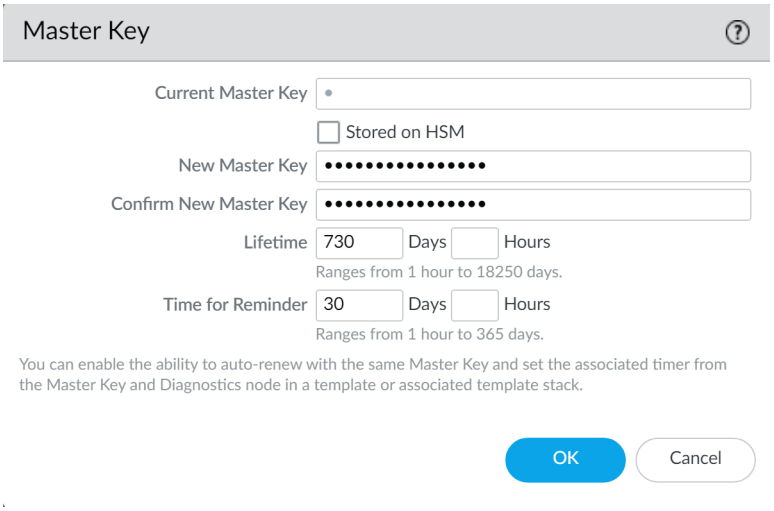
为所有 Panorama 节点重复执行此步骤。

1. 在 Panorama 节点上，登录到 Panorama Web 界面。
2. 选择 **Panorama** > **Master Key and Diagnostics**（主密钥和诊断），并配置主密钥。新主密钥必须与您在步骤 1 中在 Panorama 控制器上配置的密钥一致。
    1. 如果续订主密钥，则输入 **Current Master Key**（当前主密钥）。如果使用新的主密钥更换默认主密钥，请勿指定 **Current Master Key**（当前主密钥）。
    2. 配置 **New Master Key**（新主密钥），并 **Confirm Master Key**（配置主密钥）。
    3. 配置主密钥 **Lifetime**（生命周期）和 **Time for Reminder**（提醒时间）。
    4. 将 Panorama 控制器配置为：在密钥生命周期到期后，**Auto Renew with Same Master Key**（将相同主密钥自动续订）指定天数。
    5. 单击 **OK**（确定）。
3. 选择 **Panorama** > **Managed Devices**（受管设备）> **Summary**（摘要）和 **Deploy Master Key**（部署主密钥）。
4. 选择所有设备，并 **Change**（更改）主密钥。

© 2019 Palo Alto Networks, Inc.



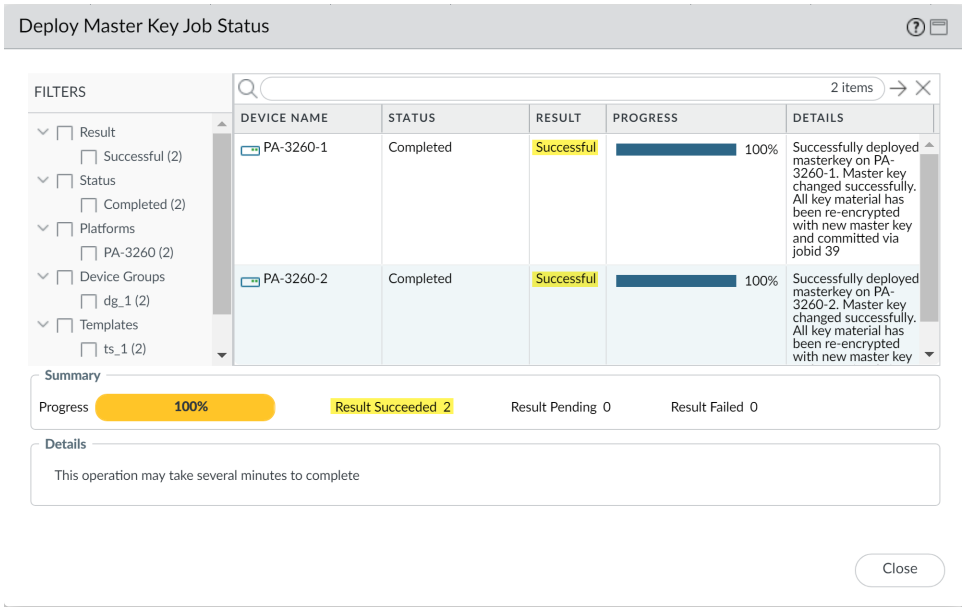
5. 配置主密钥此密钥必须与您在步骤1中配置的密钥一致：
   1. 如果续订主密钥，则输入 **Current Master Key**（当前主密钥）。如果使用新的主密钥更换默认主密钥，请勿指定 **Current Master Key**（当前主密钥）。
   2. 配置 **New Master Key**（新主密钥），并 **Confirm Master Key**（配置主密钥）。
   3. 配置主密钥 **Lifetime**（生命周期）和 **Time for Reminder**（提醒时间）。
   4. 单击 **OK**（确定）。



6. 验证是否已将主密钥成功部署到所有选定设备。

   从 Panorama 部署新主密钥时，会生成系统日志。

© 2019 Palo Alto Networks, Inc.



STEP 3 | 部署主密钥到日志收集器。

为所有 Panorama 节点重复执行此步骤。此新主密钥必须与您在步骤 1中配置的密钥一致。

1. 选择**Panorama** > **Managed Devices**（受管设备）和 **Deploy Master Key**（部署主密钥）。
2. 选择所有设备，并 **Change**（更改）主密钥。
3. 配置主密钥：
    1. 如果续订主密钥，则输入 **Current Master Key**（当前主密钥）。如果使用新的主密钥更换默认主密钥，请勿指定 **Current Master Key**（当前主密钥）。
    2. 指定 **New Master Key**（新主密钥），并 **Confirm Master Key**（配置主密钥）。
    3. 配置主密钥 **Lifetime**（生命周期）和 **Time for Reminder**（提醒时间）。
    4. 单击 **OK**（确定）。
4. 验证是否已将主密钥成功部署到所有选定设备。

    从 Panorama 部署新主密钥时，会生成系统日志。

STEP 4 | 部署主密钥到受管 WildFire 设备。

为所有 Panorama 节点重复执行此步骤。此新主密钥必须与您在步骤 1中配置的密钥一致。

1. 选择 **Panorama** > **Managed WildFire Appliances**（受管 **WildFire** 设备） 和 **Deploy Master Key**（部署主密钥）。
2. 选择所有设备，并 **Change**（更改）主密钥。
3. 配置主密钥：
    1. 如果续订主密钥，则输入 **Current Master Key**（当前主密钥）。如果使用新的主密钥更换默认主密钥，请勿指定 **Current Master Key**（当前主密钥）。
    2. 指定 **New Master Key**（新主密钥），并 **Confirm Master Key**（配置主密钥）。
    3. 配置主密钥 **Lifetime**（生命周期）和 **Time for Reminder**（提醒时间）。
    4. 单击 **OK**（确定）。
4. 验证是否已将主密钥成功部署到所有选定设备。

    从 Panorama 部署新主密钥时，会生成系统日志。

© 2019 Palo Alto Networks, Inc.

将 *Panorama* 节点配置推送到受管设备

将 Panorama 节点与 Panorama 控制器同步、模板堆栈和设备组配置之后，将模板堆栈和设备组配置推送到受管设备。

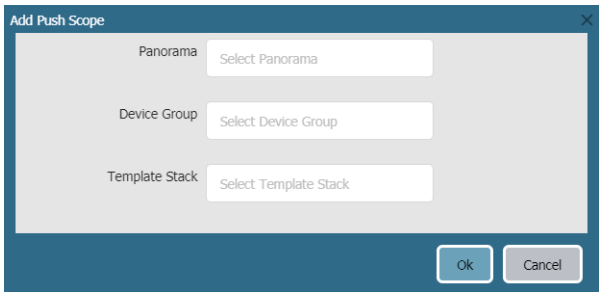
STEP 1 | Panorama 控制器的登录到 Panorama Web 界面。

STEP 2 | 选择 **Panorama** > **Interconnect**（互联）> **Devices**（设备）。

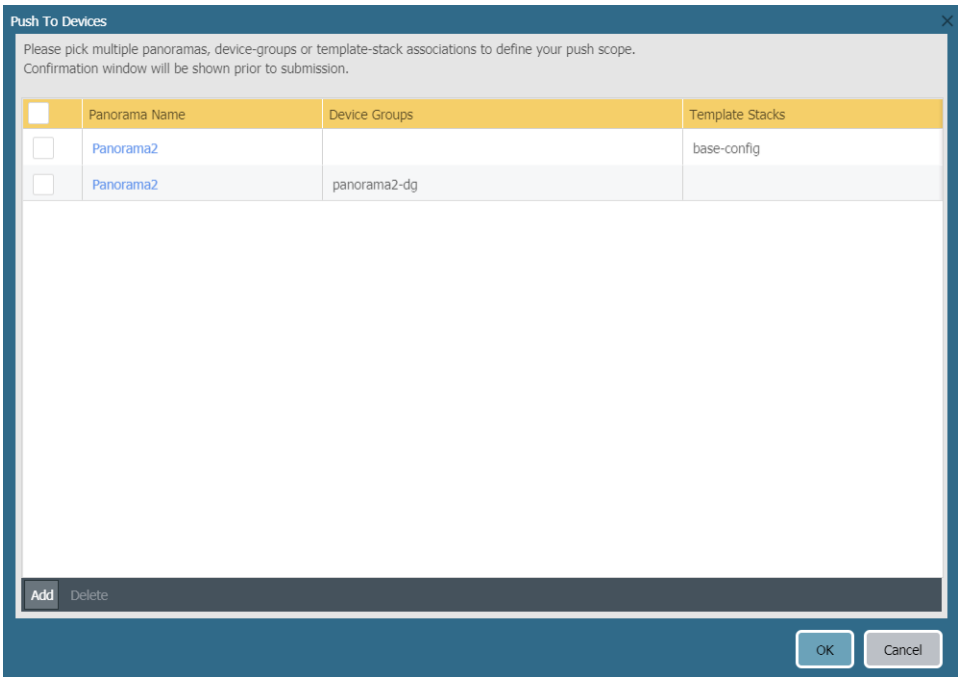
STEP 3 | **Push to Devices**（推送到设备）以将同步配置从 Panorama 节点推送到受管设备。

STEP 4 | **Add**（添加）用于管理设备的 Panorama 节点以推送配置。必要时，重复此步骤以推送至多个 Panorama 节点、设备组或模板：

1. 选择 **Panorama** 节点。
2. 选择 **Device Group**（设备组）以推送设备组和模板堆栈配置，或是选择 **Template Stack**（模板堆栈）以仅推送模板堆栈配置。
3. 单击 **OK**（确定）以完成定义推送范围。



STEP 5 | 单击 **OK**（确定），将配置推送到受管设备。



STEP 6 | 在设备组推送状态列和模板堆栈推送状态列，验证推送是否同步（显示 **in-sync**）。

© 2019 Palo Alto Networks, Inc.

升级 Panorama Interconnect 插件

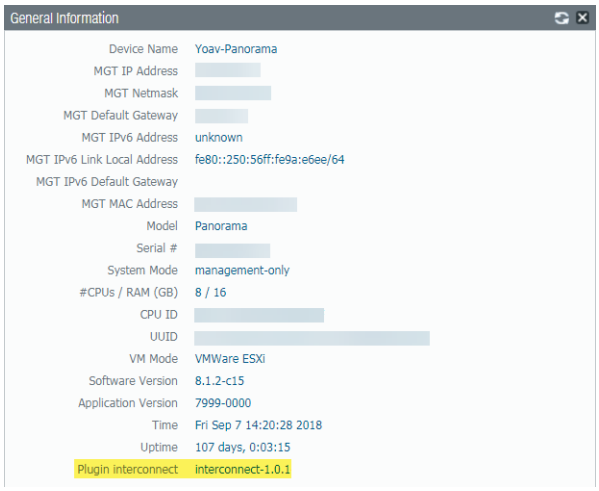
使用下列程序在 Panorama 控制器和 Panorama 节点上升级 Panorama™ Interconnect 插件。升级 Panorama Interconnect 插件时，必须先升级 Panorama 控制器，然后再将 Panorama 节点升级到与控制器相同的插件版本。在 Panorama 节点上下载并安装的新插件版本必须与您在 Panorama 控制器上安装的插件版本一致，确保 Panorama 控制器和所选 Panorama 节点上的插件版本保持同步。

如果这是您第一次安装插件，请参阅设置 Panorama Interconnect 插件。

STEP 1 | Panorama 控制器的登录到 Panorama Web 界面。

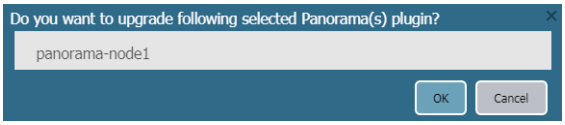
STEP 2 | 在 Panorama 控制器上升级 Panorama Interconnect 插件。

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。

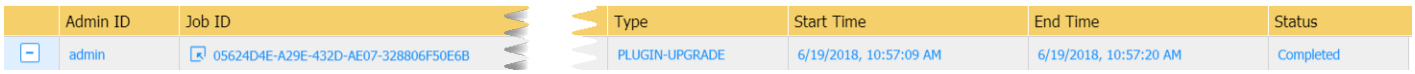


STEP 3 | 在 Panorama 节点上升级 Panorama Interconnect 插件。

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。



© 2019 Palo Alto Networks, Inc.

管理日志收集

所有 Palo Alto Networks 防火墙都可以生成日志，用来提供防火墙活动的审核记录。对于集中式日志记录和报告，必须将防火墙上生成的日志转发到包含 Panorama™ 管理服务器或日志收集器的预置型基础架构，或是发送日志到基于云的 Cortex 数据湖。或者，您可以配置 Panorama 将日志转发到外部日志记录目标（如 syslog 服务器）。

如果您将日志转发到传统模式下的 Panorama 虚拟设备，则不需要执行任何其他任务来启用日志记录。如果您将日志转发到日志收集器，则必须将它们配置为受管收集器并将其分配给收集器组。受管收集器可以是 Panorama 模式下的本地 M 系列设备或 Panorama 虚拟设备。此外，日志收集器模式下的 M 系列设备或 Panorama 虚拟设备可以是专用日志收集器。要确定是部署其中一种还是两种类型的受管收集器，请参阅本地和分布式日志收集。

要管理 Panorama 在本地生成的系统和配置日志，请参阅监视 Panorama。

- 配置受管收集器
- 为专用日志收集器配置身份验证
- 管理收集器组
- 配置 Panorama 的日志转发
- 配置到外部目标的 Syslog 转发
- 转发日志至 Cortex 数据湖
- 验证 Panorama 的日志转发
- 修改日志转发和缓冲默认设置
- 配置从 Panorama 到外部目标的日志转发
- 日志收集部署

配置受管收集器

要启用 Panorama 管理服务器管理日志收集器，您必须将后者添加为受管收集器。您可以添加两种类型的受管收集器：

- 专用日志收集器 — 要将新的 M-600、 M-500、 M-200 设备或 Panorama 虚拟设备设置为日志收集器，或将现有的 M-Series 设备或 Panorama 虚拟设备从 Panorama 模式切换到日志收集器模式，请参阅将 M-Series 设备设置为日志收集器。请记住，从 Panorama 模式切换到日志收集器模式将删除在 Panorama 模式下在 M 系列设备上预定义的本地日志收集器。
- 本地日志收集器 — 日志收集器可以在 Panorama 模式下在 M-600、 M-500、M-200 设备或 Panorama 虚拟设备上本地运行。在 M 系列设备上，已预定义日志收集器；在虚拟设备上，必须添加日志收集器。当 Panorama 管理服务器具有高可用性 (HA) 配置时，每个高可用性对端设备都可以具有一个本地日志收集器。但是，相对于主要 Panorama，辅助 Panorama 上的日志收集器是远程的，而不是本地的。因此，要在辅助 Panorama 上使用日志收集器，必须手动将其添加到主要 Panorama（有关详细信息，请参阅使用本地日志收集器部署 Panorama M 系列设备或使用本地日志收集器部署 Panorama 虚拟设备）。如果删除本地日志收集器，则可以稍后将其添加回来。以下步骤介绍如何添加本地日志收集器。



最佳做法是在 *Panorama* 管理服务器上保留本地日志收集器和收集器组，无论它是否管理专用日志收集器。



如果 *Panorama* 虚拟设备处于传统模式，则必须切换到 *Panorama* 模式以创建日志收集器。有关详情，请参阅使用本地日志收集器设置 Panorama 虚拟设备。

STEP 1 | 记录日志收集器的序列号。

在添加日志收集器作为受管收集器时，您将需要此序列号。

1. 访问 Panorama Web 界面。
2. 选择 **Dashboard**（仪表盘），并记录 General Information（一般信息）部分中的 **Serial #**（序列号）。

STEP 2 | 将日志收集器添加为受管收集器。

1. 选择 **Panorama** > **Managed Collectors**（受管收集器），然后 **Add**（添加）新的日志收集器。
2. 在 **General**（常规）设置中，输入为日志收集器记录的序列号（**Collector S/N**（收集器序列号））。
3. 单击 **OK**（确定）保存更改。
4. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**）。

STEP 3 | （可选）配置日志收集器管理员身份验证。

1. 选择 **Panorama** > **Managed Collectors**（受管收集器），然后通过单击其名称编辑日志收集器。
2. 配置日志收集器管理员密码：
   1. 选择密码 **Mode**（模式）。
   2. 如果选择 **Password**（密码）模式，请输入明文 **Password**（密码），并 **Confirm Password**（确认密码）。如果选择 **Password Hash**（密码哈希）模式，输入最多由 63 个字符组成的哈希密码字符串。
3. 配置管理员登录安全要求：



如果设置 *Failed Attempts*（失败的尝试次数）为除 *0* 以外的一个值，但将 *Lockout Time*（锁定时间）设置为 *0*，那么用户将被无限期锁定，直到其他管理员手动解锁此管理员。如果尚未创建其他管理员，则必须在 *Panorama* 上重新配置 *Failed Attempts*（失败的尝试次数）和 *Lockout Time*（锁定时间），并将此配置更改推送到日

© 2019 Palo Alto Networks, Inc.

志收集器。要确保管理员永远不被锁定，请将 *Failed Attempts*（失败的尝试次数）和 *Lockout Time*（锁定时间）默认设置为 *0*。

1. 输入登录 **Failed Attempts**（失败的尝试次数）值。该范围介于默认值 0 与最大值 10 之间，其中，值 0 表示登录尝试次数不受限制。
2. 输入 **Lockout Time**（锁定时间）值，该值介于默认值 0 和最大值 60 分钟之间。

4. 单击 **OK**（确定）保存更改。

STEP 4 | 启用日志记录硬盘。

1. 选择 **Panorama** > **Managed Collectors**（受管收集器），然后通过单击其名称编辑日志收集器。

   日志收集器名称具有与 Panorama 管理服务器的主机名相同的值。
2. 选择 **Disks**（磁盘），**Add**（添加）每个磁盘对。
3. 单击 **OK**（确定）保存更改。
4. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**）。

STEP 5 | （可选）如果您的部署使用自定义证书在 Panorama 和受管设备之间进行身份验证，请部署自定义客户端设备证书。有关更多信息，请参阅使用自定义证书设置身份验证。

1. 选择 **Panorama** > **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件），然后从下拉列表中选择证书配置文件或单击 **New Certificate Profile**（新建证书配置文件）以创建证书配置文件。
2. 选择 **Panorama** > **Managed Collectors**（受管收集器），并 **Add**（添加）新的日志收集器或选择现有的日志收集器。选择 **Communication**（通信）。
3. 选择 Type（类型）下拉列表中的设备证书类型。
   - 如果您使用本地设备证书，请从各自下拉列表中选择 **Certificate**（证书）和 **Certificate Profile**（证书配置文件）。
   - 如果您使用 SCEP 作为设备证书，请从各自下拉列表中选择 **SCEP Profile**（**SCEP** 配置文件）和 **Certificate Profile**（证书配置文件）。
4. 单击 **OK**（确定）。

STEP 6 | （可选）在日志收集器上配置 **Secure Server Communication**（安全服务器通信）。有关更多信息，请参阅使用自定义证书设置身份验证。

1. 选择 **Panorama** > **Managed Collectors**（受管收集器），然后单击 **Add**（添加）。选择 **Communication**（通信）。
2. 验证 **Custom Certificate Only**（仅允许自定义证书）复选框未选中。这允许您在迁移到自定义证书的同时继续管理所有设备。

   如果选中 *Custom Certificate Only*（仅允许自定义证书）复选框，则日志收集器不会进行身份验证，并且无法使用预定义证书从设备接收日志。
3. 从 **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）下拉列表中选择 SSL/TLS 服务配置文件。此 SSL/TLS 服务配置文件适用于日志收集器和发送日志的设备之间的所有 SSL 连接。
4. 从 **Certificate Profile**（证书配置文件）下拉列表中选择证书配置文件。
5. 选择 **Authorize Client Based on Serial Number**（根据序列号对客户端进行身份验证）让服务器根据受管设备的序列号检查客户端。客户端证书必须将特殊关键字 $UDID 设置为要根据序列号进行授权的 CN。
6. 在 **Disconnect Wait Time (min)**（断开连接等待时间（分钟））中，输入 Panorama 在与其受管设备断开并重新建立连接之前所需的分钟数。该字段默认为空，范围为 0 至 44,640 分钟。

   在您提交新配置之前，断开连接等待时间不会开始倒计时。
7. （可选）配置授权列表。

© 2019 Palo Alto Networks, Inc.

1. 单击 Authorization List（授权列表）下的 **Add**（添加）。
2. 选择 **Subject**（主题）或 **Subject Alt Name**（主题备用名称）作为标识符类型。
3. 输入所选类型的标识符。
4. 单击 **OK**（确定）。
5. 选择 **Check Authorization List**（检查授权列表）以执行授权列表。

8. 单击 **OK**（确定）。
9. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**）。

STEP 7 | 验证您的更改。

1. 核实 **Panorama** > **Managed Collectors**（Panorama > 受管收集器）页面列出了您已添加的日志收集器。Connected（已连接）列显示表明日志收集器已连接到 Panorama 的复选标记。您可能需要等待几分钟，等页面显示更新后的连接状态。

   直到您配置收集器组并将配置更改推送到收集器组，配置状态列显示不同步，运行时间状态列显示已断开连接，以及 *CLI* 命令 ***`show interface all`*** 显示这些接口为 *`down`*。
2. 单击最后一列的 **Statistics**（统计信息）验证是否启用了日志记录磁盘。

STEP 8 | 后续步骤...

您必须执行以下步骤，这样日志收集器随后才可以接收防火墙日志：

1. 配置 Panorama 的日志转发。
2. 配置收集器组 — 在 M 系列设备上，已预定义默认收集器组，并且已经包含本地日志收集器作为成员。在 Panorama 虚拟设备上，您必须添加收集器组并添加本地日志收集器作为成员。在这两种型号上，都将防火墙分配给本地日志收集器以进行日志转发。

© 2019 Palo Alto Networks, Inc.

为专用日志收集器配置身份验证

通过配置具有精细身份验证参数的本地管理用户，以及利用 RADIUS、TACAS+ 或 LDAP 进行授权和身份验证，为您的专用日志收集器创建和配置增强的身份验证。

当您从 Panorama 配置和推送管理员时，将使用您在 Panorama 上配置的管理员覆盖专用日志收集器上的现有管理员。

- 为专用日志收集器配置管理员帐户
- 为专用日志收集器配置 RADIUS 身份验证
- 为专用日志收集器配置 TACACS+ 身份验证
- 为专用日志收集器配置 LDAP 身份验证

为专用日志收集器配置管理员帐户

为您的专用日志收集器创建一个或多个具有精细身份验证参数的管理员，以便从 Panorama™ 管理服务器进行管理。此外，还可以从 Panorama 配置本地管理员，这可以在专用日志收集器的 CLI 上直接进行配置。但是，向专用日志收集器推送新配置更改会使用为专用日志收集器配置的管理员覆盖现有本地管理员。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 配置受管收集器。

STEP 3 | （可选）配置身份验证配置文件以定义身份验证服务，该服务验证访问专用日志收集器 CLI 的管理员的登录凭据。

STEP 4 | 根据需要配置一个或多个管理员帐户。

在 Panorama 上创建的管理员帐户之后会导入到专用日志收集器并从 Panorama 进行管理。

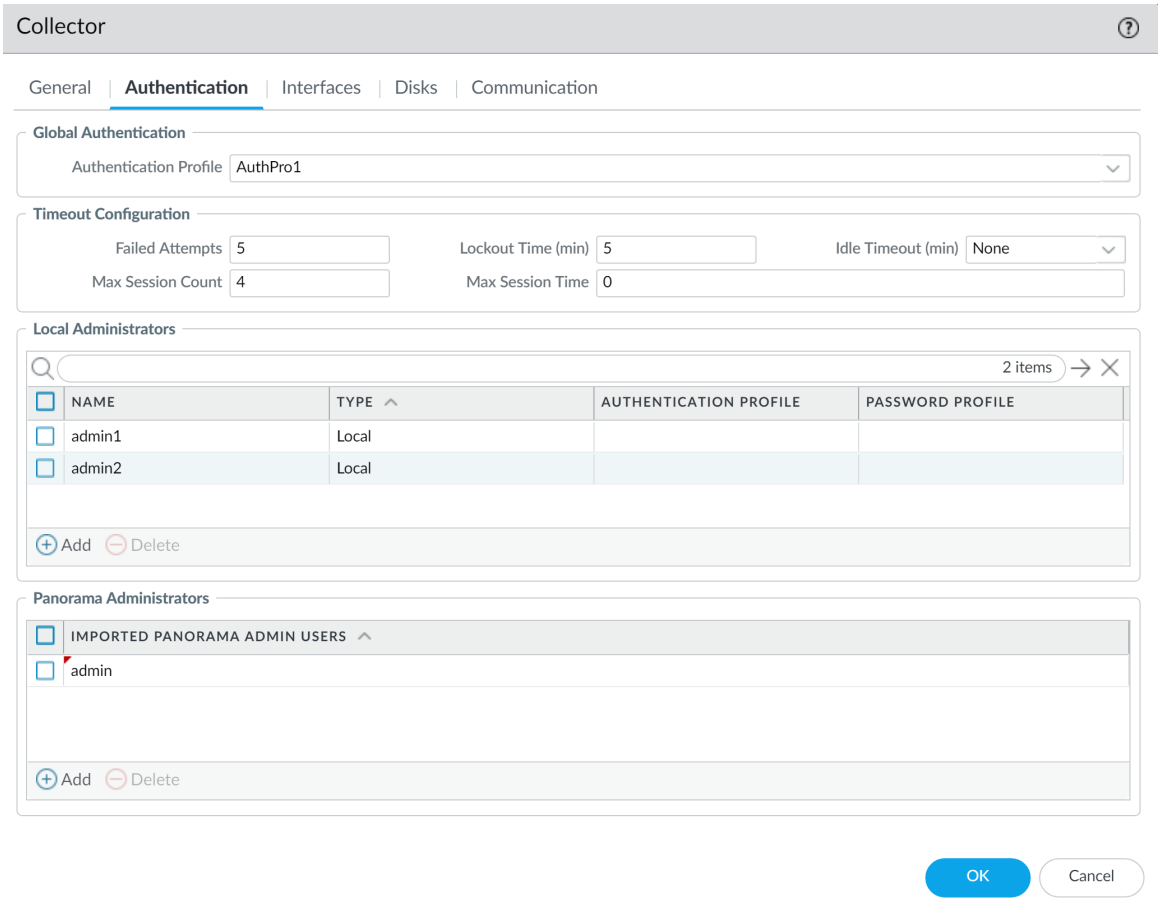
STEP 5 | 为专用日志收集器配置身份验证。

1. 选择 **Panorama** > **Managed Collectors**（受管收集器），然后选择您之前添加的专用日志收集器。
2. （可选）选择您在上一步中配置的 **Authentication Profile**（身份验证配置文件）。
3. 为专用日志收集器配置身份验证 **Timeout Configuration**（超时配置）。
    1. 输入 **Failed Attempt**（失败尝试）次数，在此次数之后用户将被锁定在专用日志收集器 CLI 之外。
    2. 输入 **Lockout Time**（锁定时间）（以分钟为单位），此时间即在用户达到配置的 **Failed Attempts**（失败尝试）次数后，专用日志收集器锁定用户帐户的时间。
    3. 输入 **Idle Timeout**（空闲超时）（以分钟为单位），在此时间之后用户会因为不活动而自动注销。
    4. 输入 **Max Session Count**（最大会话计数）以设置多少用户帐户可以同时访问专用日志收集器。
    5. 输入管理员在自动注销之前可登录的 **Max Session Time**（最长会话时间）。
4. 添加专用日志收集器管理员。

    管理员可以添加为本地管理员或作为导入的 Panorama 管理员 — 但不能同时为二者。不支持将同一管理员同时添加为本地管理员和作为导入的 Panorama 管理员，这会导致 Panorama 提交失败。例如，如果您将 `admin1` 同时添加为本地和 Panorama 管理员，向 Panorama 的提交将会失败。

    1. **Add**（添加）并配置专属于专用日志收集器的新管理员。这些管理员特定于为其创建的专用日志收集器，您可以从此表格管理这些管理员。
    2. **Add**（添加）在 Panorama 上配置的任何管理员。这些管理员在 Panorama 上创建，并导入至专用日志收集器。
5. 单击 **OK**（确定）以保存专用日志收集器身份验证配置。

© 2019 Palo Alto Networks, Inc.



STEP 6 | **Commit**（提交），然后 **Commit and Push**（提交并推送）您的配置更改。

STEP 7 | 使用本地管理员用户登录到 Panorama 命令行界面专用日志收集器以验证您能够成功访问专用日志收集器。

为专用日志收集器配置 RADIUS 身份验证

使用 RADIUS 服务器来验证对专用日志收集器 CLI 的管理访问权限。您也可以在 RADIUS 服务器上定义供应商特定属性 (VSA) 来管理管理员授权。使用 VSA 使您能够通过目录服务来快速更改管理员的角色、访问域和用户组，这通常比在 Panorama™ 管理服务器上重新配置设置更为容易。

您可以将 Palo Alto Networks RADIUS 词典导入到 *RADIUS* 服务器，以定义实现 *Panorama* 和 *RADIUS* 服务器之间通信的身份验证属性。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 配置受管收集器。

STEP 3 | 配置 RADIUS 身份验证。

1. 添加 RADIUS 服务器配置文件。

   配置文件定义了专用日志收集器连接到 RADIUS 服务器的方式。

   1. 选择 **Panorama** > **Server Profiles**（服务器配置文件）> **RADIUS**，并 **Add**（添加）配置文件。

© 2019 Palo Alto Networks, Inc.

2. 输入 **Profile Name**（配置文件名称）以标识服务器配置文件。
3. 输入身份验证请求超时后以秒为单位的 **Timeout**（超时）（默认为 3；范围为 1-20）。
4. 选择专用日志收集器用来对 RADIUS 服务器进行身份验证的 **Authentication Protocol**（身份验证协议）（默认为 **CHAP**）。

   如果 *RADIUS* 服务器支持该协议，请选择 *CHAP*；该协议比 *PAP* 更安全。

5. **Add**（添加）每个 RADIUS 服务器，并输入以下内容：
   1. 标识服务器的 **Name**（名称）。
   2. **RADIUS Server**（**RADIUS** 服务器）IP 地址或 FQDN。
   3. **Secret**（密钥）/**Confirm Secret**（确认密钥）（加密用户名和密码的密钥）。
   4. 用于身份验证请求的服务器 **Port**（端口）（默认为 1812）。
6. 单击 **OK**（确定）保存服务器配置文件。

2. 将 RADIUS 服务器配置文件分配到身份验证配置文件。

   身份验证配置文件定义了一组管理员通用的身份验证设置。

   1. 选择 **Panorama** > **Authentication Profile**（身份验证配置文件），并 **Add**（添加）配置文件。
   2. 输入 **Name**（名称）以标识身份验证配置文件。
   3. 将 **Type**（类型）设置为 **RADIUS**。
   4. 选择您配置的 **Server Profile**（服务器配置文件）。
   5. 选择 **Retrieve user group from RADIUS**（从 **RADIUS** 中检索用户组），以从 RADIUS 服务器上定义的 VSA 收集用户组信息。

      Panorama 与您在身份验证配置文件允许列表中指定的组在组信息方面进行匹配。
   6. 选择 **Advanced**（高级），并在允许列表中 **Add**（添加）允许使用此身份验证配置文件进行身份验证的管理员。
   7. 单击 **OK**（确定）保存身份验证配置文件。

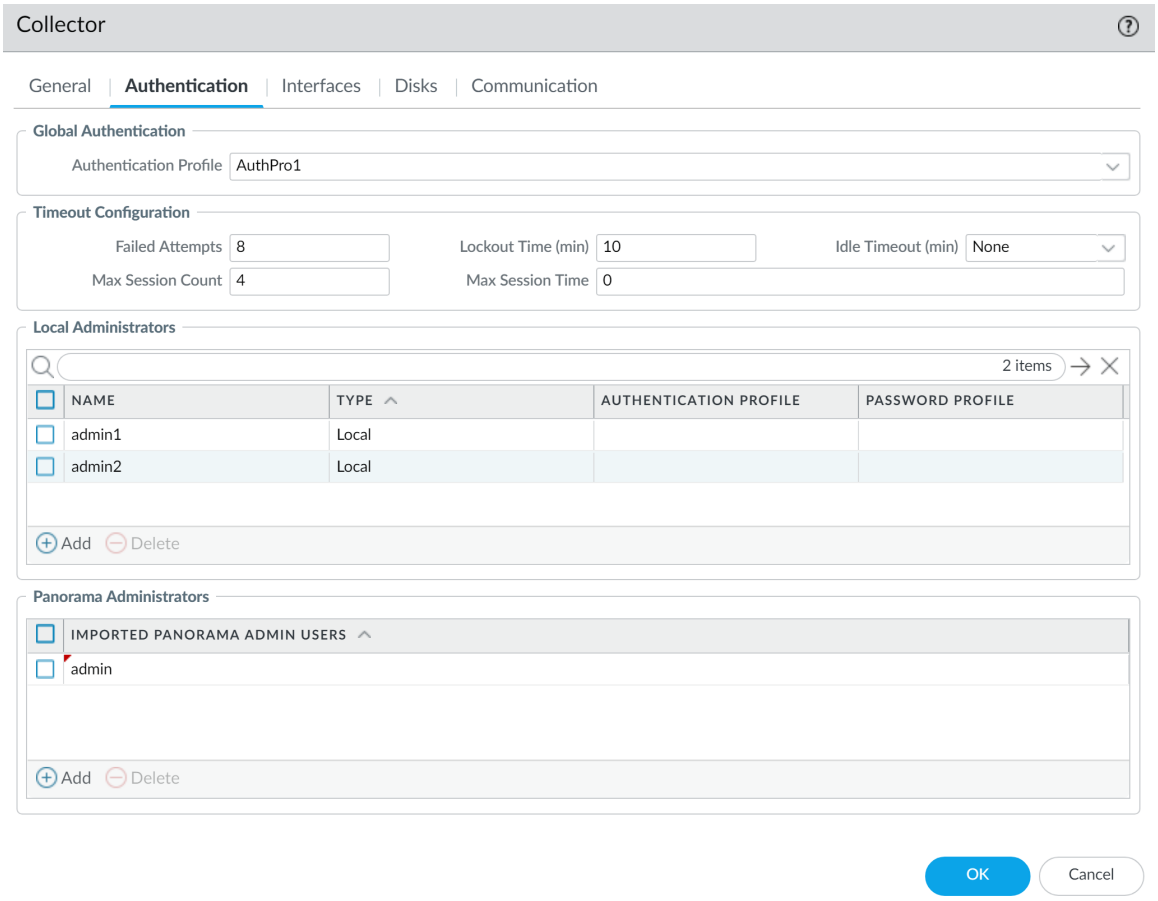
STEP 4 | 为专用日志收集器配置身份验证。

1. 选择 **Panorama** > **Managed Collectors**（受管收集器），然后选择您之前添加的专用日志收集器。
2. 选择您在上一步中配置的 **Authentication Profile**（身份验证配置文件）。

   如果没有分配全局身份验证配置文件，您必须为每个单独的本地管理员分配一个身份验证配置文件才能利用远程身份验证。
3. 为专用日志收集器配置身份验证 **Timeout Configuration**（超时配置）。
   1. 输入 **Failed Attempt**（失败尝试）次数，在此次数之后用户将被锁定在专用日志收集器 CLI 之外。
   2. 输入 **Lockout Time**（锁定时间）（以分钟为单位），此时间即在用户达到配置的 **Failed Attempts**（失败尝试）次数后，专用日志收集器锁定用户帐户的时间。
   3. 输入 **Idle Timeout**（空闲超时）（以分钟为单位），在此时间之后用户会因为不活动而自动注销。
   4. 输入 **Max Session Count**（最大会话计数）以设置多少用户帐户可以同时访问专用日志收集器。
   5. 输入管理员在自动注销之前可登录的 **Max Session Time**（最长会话时间）。
4. 添加专用日志收集器管理员。

   管理员可以添加为本地管理员或作为导入的 Panorama 管理员 — 但不能同时为二者。不支持将同一管理员同时添加为本地管理员和作为导入的 Panorama 管理员，这会导致 Panorama 提交失败。例如，如果您将 `admin1` 同时添加为本地和 Panorama 管理员，向 Panorama 的提交将会失败。
   1. **Add**（添加）并配置专属于专用日志收集器的新管理员。这些管理员特定于为其创建的专用日志收集器，您可以从此表格管理这些管理员。
   2. **Add**（添加）在 Panorama 上配置的任何管理员。这些管理员在 Panorama 上创建，并导入至专用日志收集器。
5. 单击 **OK**（确定）以保存专用日志收集器身份验证配置。

© 2019 Palo Alto Networks, Inc.



STEP 5 | **Commit**（提交），然后 **Commit and Push**（提交并推送）您的配置更改。

STEP 6 | 使用本地管理员用户登录到 Panorama 命令行界面专用日志收集器以验证您能够成功访问专用日志收集器。

为专用日志收集器配置 TACACS+ 身份验证

您可以使用 TACACS+ 服务器来验证对专用日志收集器 CLI 的管理访问权限。您也可以在 TACACS+ 服务器上定义供应商特定属性 (VSA) 来管理管理员授权。使用 SAML 使您能够通过目录服务来快速更改管理员的角色、访问域和用户组，这通常比在 Panorama 上重新配置设置更为容易。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 配置受管收集器。

STEP 3 | 配置 TACACS+ 身份验证。

1. 添加 TACACS+ 服务器配置文件。

   配置文件定义了专用日志收集器连接到 TACACS+ 服务器的方式。

   1. 选择 **Panorama** > **Server Profiles**（服务器配置文件）> **TACACS+**，并 **Add**（添加）配置文件。
   2. 输入 **Profile Name**（配置文件名称）以标识服务器配置文件。
   3. 输入身份验证请求超时后以秒为单位的 **Timeout**（超时）（默认为 3；范围为 1-20）。
   4. 选择 Panorama 用来对 TACACS+ 服务器进行身份验证的 **Authentication Protocol**（身份验证协议）（默认为 **CHAP**）。

© 2019 Palo Alto Networks, Inc.

5. 如果 TACACS+ 服务器支持该协议，请选择 **CHAP**；该协议比 **PAP** 更安全。
6. **Add**（添加）每个 TACACS+ 服务器，并输入以下内容：
    1. 标识服务器的 **Name**（名称）。
    2. **TACACS+ Server**（**TACACS+** 服务器）IP 地址或 FQDN。
    3. **Secret**（密钥）/**Confirm Secret**（确认密钥）（加密用户名和密码的密钥）。
    4. 用于身份验证请求的服务器 **Port**（端口）（默认为 49）。
7. 单击 **OK**（确定）保存服务器配置文件。

2. 将 TACACS+ 服务器配置文件分配到身份验证配置文件。

    身份验证配置文件定义了一组管理员通用的身份验证设置。

    1. 选择 **Panorama** > **Authentication Profile**（身份验证配置文件），并 **Add**（添加）配置文件。
    2. 输入 **Name**（名称）以标识配置文件。
    3. 将 **Type**（类型）设置为 **TACACS+**。
    4. 选择您配置的 **Server Profile**（服务器配置文件）。
    5. 选择 **Retrieve user group from TACACS+**（从 **TACACS+** 中检索用户组），以从 TACACS+ 服务器上定义的 VSA 收集用户组信息。

        Panorama 与您在身份验证配置文件允许列表中指定的组在组信息方面进行匹配。
    6. 选择 **Advanced**（高级），并在允许列表中 **Add**（添加）允许使用此身份验证配置文件进行身份验证的管理员。
    7. 单击 **OK**（确定）保存身份验证配置文件。

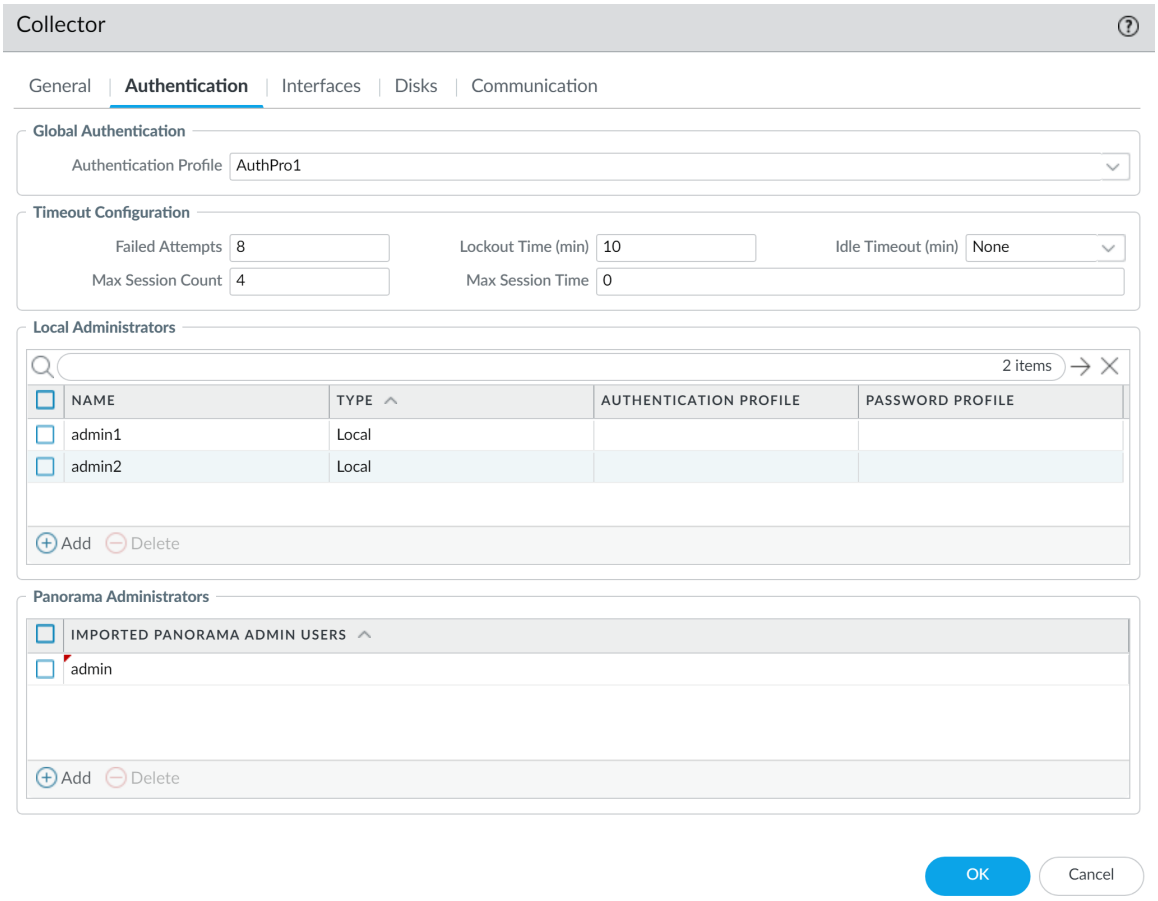
STEP 4 | 为专用日志收集器配置身份验证。

1. 选择 **Panorama** > **Managed Collectors**（受管收集器），然后选择您之前添加的专用日志收集器。
2. 选择您在上一步中配置的 **Authentication Profile**（身份验证配置文件）。

    如果没有分配全局身份验证配置文件，您必须为每个单独的本地管理员分配一个身份验证配置文件才能利用远程身份验证。
3. 为专用日志收集器配置身份验证 **Timeout Configuration**（超时配置）。
    1. 输入 **Failed Attempt**（失败尝试）次数，在此次数之后用户将被锁定在专用日志收集器 CLI 之外。
    2. 输入 **Lockout Time**（锁定时间）（以分钟为单位），此时间即在用户达到配置的 **Failed Attempts**（失败尝试）次数后，专用日志收集器锁定用户帐户的时间。
    3. 输入 **Idle Timeout**（空闲超时）（以分钟为单位），在此时间之后用户会因为不活动而自动注销。
    4. 输入 **Max Session Count**（最大会话计数）以设置多少用户帐户可以同时访问专用日志收集器。
    5. 输入管理员在自动注销之前可登录的 **Max Session Time**（最长会话时间）。
4. 添加专用日志收集器管理员。

    管理员可以添加为本地管理员或作为导入的 Panorama 管理员 — 但不能同时为二者。不支持将同一管理员同时添加为本地管理员和作为导入的 Panorama 管理员，这会导致 Panorama 提交失败。例如，如果您将 `admin1` 同时添加为本地和 Panorama 管理员，向 Panorama 的提交将会失败。
    1. **Add**（添加）并配置专属于专用日志收集器的新管理员。这些管理员特定于为其创建的专用日志收集器，您可以从此表格管理这些管理员。
    2. **Add**（添加）在 Panorama 上配置的任何管理员。这些管理员在 Panorama 上创建，并导入至专用日志收集器。
5. 单击 **OK**（确定）以保存专用日志收集器身份验证配置。

© 2019 Palo Alto Networks, Inc.



STEP 5 | **Commit**（提交），然后 **Commit and Push**（提交并推送）您的配置更改。

STEP 6 | 使用本地管理员用户登录到 Panorama 命令行界面专用日志收集器以验证您能够成功访问专用日志收集器。

为专用日志收集器配置 LDAP 身份验证

您可以使用 LDAP 对访问专用日志收集器 Web 界面的最终用户进行身份验证。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 配置受管收集器。

STEP 3 | 添加 LDAP 服务器配置文件。

配置文件定义了专用日志收集器连接到 LDAP 服务器的方式。

1. 选择 **Panorama** > **Server Profiles**（服务器配置文件）> **LDAP**，然后 **Add**（添加）服务器配置文件。
2. 输入 **Profile Name**（配置文件名称）以标识服务器配置文件。
3. **Add**（添加）LDAP 服务器（最多 4 个）。对于每个服务器，输入 **Name**（名称）（以标识服务器）、**LDAP Server**（**LDAP** 服务器）IP 地址或 FQDN 以及服务器 **Port**（端口）（默认为 389）。

   如果使用 *FQDN* 地址对象来标识服务器，并随后更改地址，则必须提交更改以使新服务器地址生效。
4. 选择服务器 **Type**（类型）。

© 2019 Palo Alto Networks, Inc.

5. 选择 **Base DN**（基本 **DN**）。

   要标识目录的基本 DN，请打开 **Active Directory Domains and Trusts**（活动目录域和信任）Microsoft 管理控制台控制单元，并使用顶级域的名称。
6. 输入 **Bind DN**（绑定 **DN**）和 **Password**（密码）以启用身份验证服务对防火墙进行身份验证。

   绑定 *DN* 账户必须有权读取 *LDAP* 目录。
7. 以秒为单位输入 **Bind Timeout**（绑定超时）和 **Search Timeout**（搜索超时）（默认均为 30）。
8. 输入 **Retry Interval**（重试时间间隔），以秒计（默认为 60）。
9. （可选）如果您希望端点使用 SSL 或 TLS 与目录服务器建立更安全的连接，启用 **Require SSL/TLS secured connection**（需要 **SSL/TLS** 安全连接）选项（默认启用）。端点使用的协议取决于服务器端口：
   - 389（默认）— TLS（具体来说，专用日志收集器使用 StartTLS 操作，这会将初始明文连接升级到 TLS。）
   - 636 — SSL
   - 任何其他端口 — 专用日志收集器首先尝试使用 TLS。如果目录服务器不支持 TLS，则专用日志收集器回退至 SSL。
10. （可选）如需额外的安全性，启用 **Verify Server Certificate for SSL sessions**（验证 **SSL** 会话的服务器证书）选项，使端点验证目录服务器为 SSL/TLS 连接出示的证书。要启用验证，还必须启用 **Require SSL/TLS secured connection**（需要 **SSL/TLS** 安全连接）选项。为了验证成功，证书必须符合以下条件之一：
    - 它位于 Panorama 证书列表中：**Panorama** > **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书）。必要时，将证书导入 Panorama。
    - 证书签发机构位于可信证书授权机构列表中：**Panorama** > **Certificate Management**（证书管理）> **Certificates**（证书）。
11. 单击 **OK**（确定）保存服务器配置文件。

STEP 4 | 为专用日志收集器配置身份验证。

1. 选择 **Panorama** > **Managed Collectors**（受管收集器），然后选择您之前添加的专用日志收集器。
2. 为专用日志收集器配置身份验证 **Timeout Configuration**（超时配置）。
   1. 输入 **Failed Attempt**（失败尝试）次数，在此次数之后用户将被锁定在专用日志收集器 CLI 之外。
   2. 输入 **Lockout Time**（锁定时间）（以分钟为单位），此时间即在用户达到配置的 **Failed Attempts**（失败尝试）次数后，专用日志收集器锁定用户帐户的时间。
   3. 输入 **Idle Timeout**（空闲超时）（以分钟为单位），在此时间之后用户会因为不活动而自动注销。
   4. 输入 **Max Session Count**（最大会话计数）以设置多少用户帐户可以同时访问专用日志收集器。
   5. 输入管理员在自动注销之前可登录的 **Max Session Time**（最长会话时间）。
3. 添加专用日志收集器管理员。

   管理员可以添加为本地管理员或作为导入的 Panorama 管理员 — 但不能同时为二者。不支持将同一管理员同时添加为本地管理员和作为导入的 Panorama 管理员，这会导致 Panorama 提交失败。例如，如果您将 `admin1` 同时添加为本地和 Panorama 管理员，向 Panorama 的提交将会失败。
   - 配置本地管理员。

     配置专属于专用日志收集器的新管理员。这些管理员特定于为其创建的专用日志收集器，您可以从此表格管理这些管理员。
     1. **Add**（添加）一个或多个新本地管理员。
     2. 输入本地管理员的 **Name**（名称）。
     3. 配置一个您之前创建的 **Authentication Profile**（身份验证配置文件）。

© 2019 Palo Alto Networks, Inc.

仅单个本地管理员才支持 *LDAP* 身份验证配置文件。

4. 启用（选中）**Use Public Key Authentication (SSH)**（使用公钥身份验证 **(SSH)**）以导入公钥文件进行身份验证。
5. 选择一个 **Password Profile**（密码配置文件）以设置过期参数。

- 导入现有 Panorama 管理员

  导入在 Panorama 上配置的现有管理员。这些管理员在 Panorama 上配置和管理，并导入至专用日志收集器。

1. **Add**（添加）现有 Panorama 管理员

4. 单击 **OK**（确定）以保存专用日志收集器身份验证配置。

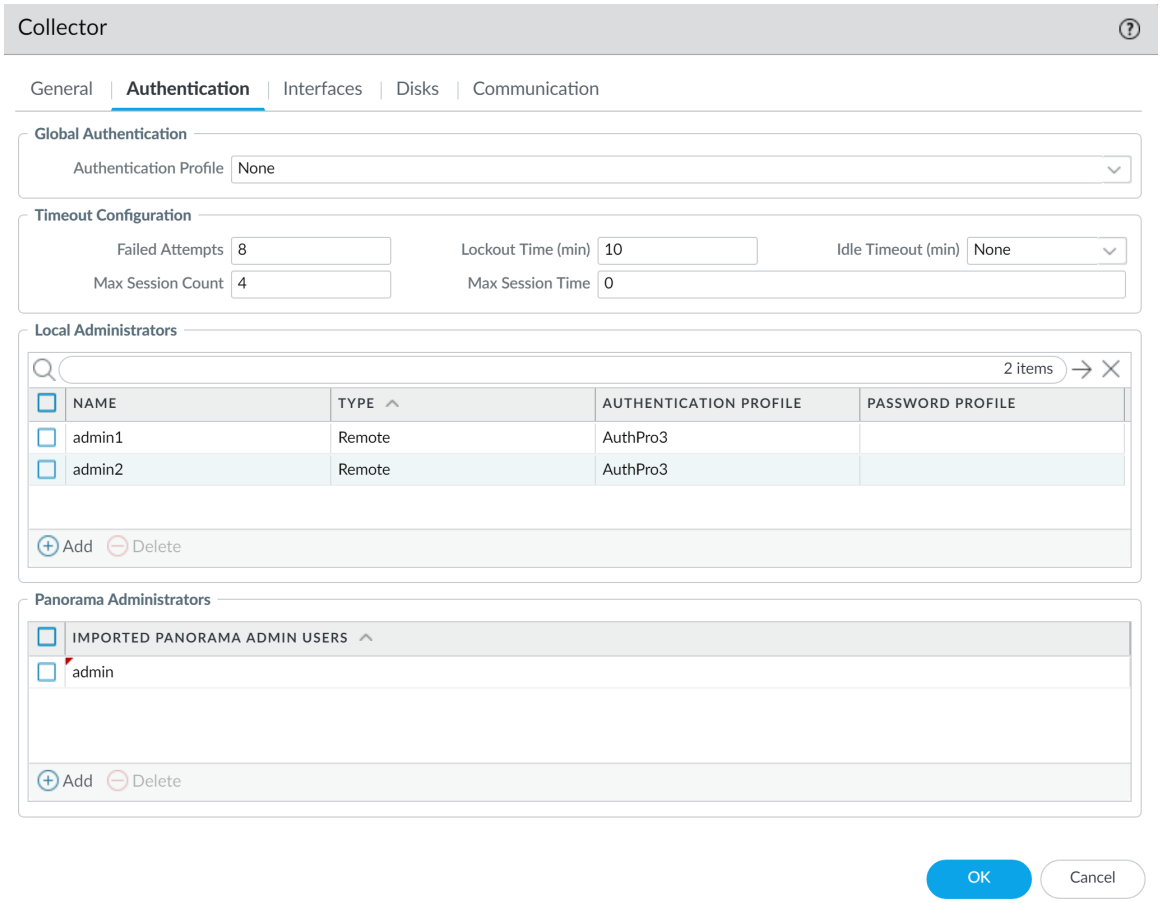
STEP 5 | 为专用日志收集器配置身份验证。

1. 选择 **Panorama** > **Managed Collectors**（受管收集器），然后选择您之前添加的专用日志收集器。
2. 选择您在上一步中配置的 **Authentication Profile**（身份验证配置文件）。
3. 为专用日志收集器配置身份验证 **Timeout Configuration**（超时配置）。
   1. 输入 **Failed Attempt**（失败尝试）次数，在此次数之后用户将被锁定在专用日志收集器 CLI 之外。
   2. 输入 **Lockout Time**（锁定时间）（以分钟为单位），此时间即在用户达到配置的 **Failed Attempts**（失败尝试）次数后，专用日志收集器锁定用户帐户的时间。
   3. 输入 **Idle Timeout**（空闲超时）（以分钟为单位），在此时间之后用户会因为不活动而自动注销。
   4. 输入 **Max Session Count**（最大会话计数）以设置多少用户帐户可以同时访问专用日志收集器。
   5. 输入管理员在自动注销之前可登录的 **Max Session Time**（最长会话时间）。
4. 添加专用日志收集器管理员。

   您必须将管理员 (**admin**) 添加为本地管理员或作为导入的 Panorama 管理员 — 但不能同时为二者。如果没有添加管理员，或者管理员被同时添加为本地管理员和导入的 Panorama 管理员，则会导致推送到受管收集器失败。

   1. **Add**（添加）并配置专属于专用日志收集器的新管理员。这些管理员特定于为其创建的专用日志收集器，您可以从此表格管理这些管理员。
   2. **Add**（添加）在 Panorama 上配置的任何管理员。这些管理员在 Panorama 上创建，并导入至专用日志收集器。
5. 单击 **OK**（确定）以保存专用日志收集器身份验证配置。

© 2019 Palo Alto Networks, Inc.



STEP 6 | **Commit**（提交），然后 **Commit and Push**（提交并推送）您的配置更改。

STEP 7 | 使用本地管理员用户登录到 Panorama 命令行界面专用日志收集器以验证您能够成功访问专用日志收集器。

© 2019 Palo Alto Networks, Inc.

管理收集器组

收集器组是作为单个逻辑日志收集防火墙日志而运作的 1 至 16 个日志收集器。您必须至少将一个日志收集器分配给收集器组，以便防火墙成功将日志发送到日志收集器。如果没有配置收集器组或没有将日志收集器分配给收集器组，则会丢弃防火墙日志。您可以将收集器组配置为具有多个日志收集器，从而确保日志冗余，或适应超过单个日志收集器容量的日志记录速率（请参阅Panorama 型号）。要了解风险和建议的缓解措施，请参阅具有多个日志收集器的收集器组的警告。

Panorama 模式下的 M-600、 M-500 和 M-200 设备具有包含预定义本地日志收集器的预定义收集器组。您可以编辑预定义收集器组的所有设置，但其名称除外（默认）。

如果删除收集器组，将会丢失日志。

Palo Alto Networks 建议在 *Panorama* 管理服务器上保留预定义日志收集器和收集器组，无论 *Panorama* 是否也管理专用日志收集器。

如果将 *M* 系列设备从 *Panorama* 模式切换到日志收集器模式，设备将丢失其预定义收集器组和日志收集器。然后，您必须将 M 系列设备设置为日志收集器，将其作为受管收集器添加到 *Panorama*，并将收集器组配置为包含受管收集器。

- 配置收集器组
- 在日志收集器之间使用自定义证书配置身份验证
- 将日志收集器移动到另一收集器组
- 从收集器组删除防火墙

配置收集器组

在配置收集器组前，决定每个收集器组是只拥有一个日志收集器还是拥有多个日志收集器（最多 16 个）。拥有多个日志收集器的收集器组支持更高的日志记录速率和日志冗余，但具有以下要求：

- 在任何单个收集器组中，所有日志收集器均必须在相同的 Panorama 型号上运行：均为 M-600 设备、均为 M-500 设备、均为 M-200 设备或均为 Panorama 虚拟设备。
- 日志冗余只有在每个日志收集器拥有相同数量的日志记录磁盘时才可用。要将磁盘添加到日志收集器，请参阅增加 M 系列设备上的存储空间。
- （最佳实践）同一收集器组内的所有日志收集器必须位于同一局域网 (LAN) 中。由于网络中断很常见，且可能会导致日志数据丢失，因此，应避免将同一或不同广域网 (WAN) 中的日志收集器添加到同一收集器组。此外，建议同一收集器组内的日志收集器应彼此靠近，以便 Panorama 能在需要时快速查询日志收集器。

STEP 1 | 在配置收集器组之前，应执行以下任务。

1. 对于将要分配到收集器组的每一个防火墙，添加防火墙作为受管设备。
2. 对于将要分配到收集器组的每一个日志收集器，配置受管收集器。

STEP 2 | 添加收集器组。

1. 访问 Panorama Web 界面，选择 **Panorama** > **Collector Groups**（收集器组），然后 **Add**（添加）收集器组或编辑现有的一个收集器组。
2. 如果您正在添加收集器组，请输入该收集器组的 **Name**（名称）。

   您无法重命名现有的收集器组。
3. 输入收集器组将保留防火墙日志的**Minimum Retention Period**（最小保留期）天数（范围为 1 至 2,000）。

   默认情况下，该字段为空，这表示收集器组无限期地保留日志。
4. 将日志收集器（1 至 16 个）**Add**（添加）到收集器组成员列表。

© 2019 Palo Alto Networks, Inc.

5. （推荐）如果要将多个日志收集器添加到单个收集器组，请**Enable log redundancy across collectors**（启用跨收集器记录冗余）。

   冗余可确保当任何一个日志收集器变得无法使用时所有日志都不会丢失。每个日志都将具有两个副本，而且每个副本都将都驻留在不同的日志收集器上。例如，如果在收集器组中有两个日志收集器，则日志会被同时写入这两个日志收集器。

   启用冗余会创建更多日志，因此需要更多存储容量，使得存储容量减半。当收集器组用完容量空间后，将会删除较早的日志。冗余还能将收集器组中的日志处理通信增加一倍，从而将其最大日志记录速率降低一半，因为每个日志收集器均必须分发其收到的每个日志的副本。

STEP 3 | 将日志收集器和防火墙分配到收集器组。

1. 选择 **Device Log Forwarding**（设备日志转发），并 **Add**（添加）防火墙的日志转发首选项列表。

   日志数据将通过单独 TCP 通道转发。通过添加日志转发首选项列表，您可以创建单独 TCP 连接来转发日志数据。

   首选项列表确定日志收集器从防火墙接收日志的顺序。如果未分配日志转发首选项列表，您可能遇到下列情况之一：

   - 如果 *Panorama* 处于“仅管理”模式，则 *Panorama* 会丢弃所有传入日志。
   - 如果本地日志收集器在 *Panorama* 处于 *Panorama* 模式时未被配置为受管收集器，则 *Panorama* 会丢弃所有传入日志。
   - 如果本地日志收集器在 *Panorama* 处于 *Panorama* 模式时被配置为受管收集器，则会接收传入日志，但 *Panorama* 可能会成为瓶颈，因为所有受管防火墙都是先将日志转发到本地日志收集器，然后再重新分发给其他可用日志收集器。

   1. 在 Devices（设备）部分中，**Modify**（修改）防火墙列表，然后单击 **OK**（确定）。
   2. 在 Collectors（收集器）部分中，将日志收集器 **Add**（添加）到首选项列表。

      如果您在步骤 2 中启用了冗余，则建议添加至少两个日志收集器。如果分配多个日志收集器，则第一个日志收集器将为主要日志收集器；当主要日志收集器变成不可用时，防火墙会将日志发送到列表中的下一个日志收集器。要更改日志收集器的优先级，选择日志收集器，然后单击 **Move Up**（上移）（较高优先级）或 **Move Down**（下移）（较低优先级）。
   3. 单击 **OK**（确定）。

STEP 4 | 定义每种日志类型的存储容量（日志配额）和过期期限。

1. 返回到 **General**（常规）选项卡，然后单击 **Log Storage**（日志存储）值。

   如果该字段显示 *0MB*，则验证您是否已为日志记录启用磁盘对并已提交更改（请参阅 *Disks*（磁盘）选项卡下的配置受管收集器）。
2. 输入每种日志类型的日志存储 **Quota**（配额）**(%)**。
3. 输入每种日志类型的 **Max Days**（最大天数）（到期期限），范围为 1 至 2,000。

   默认情况下，该字段留空，这意味着日志永远不会过期。

STEP 5 | 提交并验证您的更改。

1. 选择 **Commit**（提交）> **Commit and Push**（提交并推送），然后将更改 **Commit and Push**（提交并推送）到 Panorama 和配置的收集器组。
2. 选择 **Panorama** > **Managed Collectors**（受管收集器）以验证收集器组中的日志收集器是否：

   - 连接到 **Panorama** — Connected（已连接）列将显示一个复选标记图标，以表明日志收集器已连接上 Panorama。
   - 与 **Panorama** 同步 — Configuration Status（配置状态）列指示日志收集器与 Panorama 是 `In Sync`（绿色图标）还是 `Out of Sync`（红色图标）。

© 2019 Palo Alto Networks, Inc.

STEP 6 | 排除网络资源连接问题确认防火墙已成功连接到日志收集器。

STEP 7 | 后续步骤...

1. 配置 Panorama 的日志转发。

   在您将防火墙配置为转发到 Panorama 之前，收集器组将不会接收防火墙日志。
2. （可选）配置从 Panorama 到外部目标的日志转发。

   您可以将每个收集器组都配置为向单独的目标转发日志（例如 syslog 服务器）。

在日志收集器之间使用自定义证书配置身份验证

完成以下程序，以配置用于日志收集器之间通信的自定义证书。因为服务器和客户端角色为动态选择，因此您必须在收集器组内每个日志收集器上配置安全服务器通信和安全客户端通信。使用自定义证书建立唯一的信任链，以确保您的日志收集器组成员之间的相互身份验证。

更多有关使用自定义证书的信息，请参阅SSL/TLS 连接如何进行相互身份验证？

STEP 1 | 获取每个日志收集器的密钥对和证书颁发机构 (CA) 颁发的证书。

STEP 2 | 导入 CA 证书以验证用于收集器组内每个日志收集器的客户端日志收集器、服务器密钥对、以及客户端密钥对。

1. 选择 **Panorama** > **Certificate Management**（证书管理）> **Certificate**（证书）> **Import**（导入）。
2. 导入 CA 证书、服务器密钥对、以及客户端密钥对。
3. 对每个日志收集器重复步骤。

STEP 3 | 为安全服务器通信配置包含根 CA 和中间 CA 的证书配置文件。此证书配置文件定义日志收集器之间的身份验证。

1. 选择 **Panorama** > **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件）。
2. 配置证书配置文件。

   如果将中间 CA 配置为证书配置文件的一部分，则还必须包含根 CA。

STEP 4 | 配置安全客户端通信的证书配置文件。您可以单独在每个客户端日志收集器上配置此配置文件，也可以将配置从 Panorama™ 推送至受管的日志收集器。



如果您使用 *SCEP* 作为客户端证书，请配置 SCEP 配置文件，而非证书配置文件。

1. 选择 **Panorama** > **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件）。
2. 配置证书配置文件。

STEP 5 | 配置 SSL/TLS 服务配置文件。

1. 选择 **Panorama** > **Certificate Management**（证书管理）> **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）。
2. 配置 SSL/TLS 服务配置文件以定义日志收集器用于 SSL/TLS 服务的证书和协议。

STEP 6 | 在所有日志收集器上部署自定义证书后，执行自定义证书身份验证。

1. 选择 **Panorama** > **Collector Groups**（Panorama > 收集器组），然后选择收集器组。
2. 在常规选项卡上，**Enable secure inter LC Communication**（启用安全的 **LC** 间通信）。

   如果启用安全的 LC 间通信，且收集器组包含本地日志收集器，则会出现一个链接，指示 **Log Collector on local Panorama is using the secure client configuration from Panorama**（本地 **Panorama** 上的日志收集器正在使用来自 **Panorama** 的安全客户端配置）> **Secure Communication Settings**（安

© 2019 Palo Alto Networks, Inc.

全通信设置）。您可以从此处单击此链接，以打开安全通信设置对话框，并为本地日志收集器配置安全服务器和安全客户端设置。

3. 单击 **OK**（确定）。
4. **Commit**（提交）更改。

STEP 7 | 在每个日志收集器上配置安全服务器通信。

1. 为专用日志收集器选择 **Panorama** > **Managed Collectors**（受管收集器）或 **Panorama** > **Setup**（设置）> **Management**（管理），然后**Edit**（编辑）本地日志收集器的安全通信设置。
2. 对于专用日志收集器，单击日志收集器，并选择**Communications**（通信）。
3. 启用**Customize Secure Server Communication**（自定义安全服务器通信）功能。
4. 从 **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）下拉列表中选择 SSL/TLS 服务配置文件。该 SSL/TLS 服务配置文件适用于日志收集器之间的所有 SSL 连接。
5. 从下拉列表中选择 **Certificate Profile**（证书配置文件）。
6. 验证 **Custom Certificate Only**（仅允许自定义证书）是否已禁用（取消选择）。此时，允许日志收集器间通信在配置到自定义证书时通过预定义证书进行执行。
7. 设置日志收集器断开和重新连接至其他日志收集器之前应等待的断开等待时间（以分钟计）。该字段默认为空（范围为 0 至 44,640 分钟）。
8. （可选）配置授权列表。授权列表增加证书身份验证之外的额外安全层。授权列表检查客户证书主题或主题备用名称。如果与客户端证书一起提供的主题或主题备用名称与授权列表上的标识符不匹配，则身份验证被拒绝。
   1. **Add**（添加）授权列表。
   2. 选择在证书配置文件中配置的 **Subject**（主题）或 **Subject Alt Name**（主题备用名称）作为标识符类型。
   3. 如果标识符为 `Subject`，则输入通用名，如果标识符为 `Subject Alt Name`，则输入 IP 地址、主机名或电子邮件。
   4. 单击 **OK**（确定）。
   5. 启用 **Check Authorization List**（检查授权列表）选项，配置 Panorama，以执行授权列表。
9. 单击 **OK**（确定）。
10. **Commit**（提交）更改。

提交这些更改后，断开等待时间将开始倒计时。等待时间结束时，若没有配置证书，则收集器组中的日志收集器无法进行连接。

STEP 8 | 在每个日志收集器上配置安全客户端通信。

1. 为专用日志收集器选择 **Panorama** > **Managed Collectors**（受管收集器）或 **Panorama** > **Setup**（设置）> **Management**（管理），然后**Edit**（编辑）本地日志收集器的安全通信设置。
2. 对于专用日志收集器，单击日志收集器，并选择**Communications**（通信）。
3. 在安全客户端通信中，从相应的下拉列表中选择**Certificate Type**（证书类型）、**Certificate**（证书）和 **Certificate Profile**（证书配置文件）。
4. 单击 **OK**（确定）。
5. **Commit**（提交）更改。

将日志收集器移动到另一收集器组

M-600、M-500、M-200 设备和 Panorama 虚拟设备可以在每个收集器组中拥有一个或多个日志收集器。您可以根据收集器组的日志记录速率和日记存储要求将日志收集器分配到该收集器组。如果收集器组中的日志记录速率和所需存储容量增高，您最好是增加 M 系列设备上的存储容量或者使用额外日志收集器配置收集器组。但是，在某些部署中，在不同收集器组之间转移日志收集器则可能更为经济。

© 2019 Palo Alto Networks, Inc.

当日志收集器位于 *Panorama* 模式下 *M-600*、*M-500* 或 *M-200* 设备的本地时，只有在设备是高可用性 *(HA)* 配置中的被动对时才可以移动日志收集器。*HA* 同步采用与新收集器组相关联的配置。切勿移动位于主动高可用性对端设备本地的日志收集器。

在任何单个收集器组中，所有日志收集器均必须在相同的 *Panorama* 型号上运行：均为 *M-600* 设备、均为 *M-500* 设备、均为 *M-200* 设备或均为 *Panorama* 虚拟设备。

日志冗余只有在每个日志收集器拥有相同数量的日志记录磁盘时才可用。要将磁盘添加到日志收集器，请参阅增加 M 系列设备上的存储空间。

STEP 1 | 从 Panorama 管理中移除日志收集器。

1. 选择 **Panorama** > **Collector Groups**（收集器组），然后编辑包含了您将要移动的日志收集器的收集器组。
2. 在 Collector Group Members（收集器组成员）部分中，选择并 **Delete**（删除）日志收集器。
3. 选择 **Device Log Forwarding**（设备日志转发），然后在 Log Forwarding Preferences（日志转发首选项）列表中，对分配到您将要移动的日志收集器的每一个防火墙集执行以下步骤：
   1. 在 Devices（设备）列中，单击分配到日志收集器的防火墙的链接。
   2. 在 Collectors（收集器）列中，选择并 **Delete**（删除）日志收集器。

      若要重新分配防火墙，应 *Add*（添加）将作为防火墙所转发日志目的地的新日志收集器。
   3. 单击 **OK**（确定）两次以保存更改。
4. 选择 **Panorama** > **Managed Collectors**（受管收集器），然后选择并 **Delete**（删除）将移动的日志收集器。

STEP 2 | 配置收集器组。

将日志收集器添加到其新收集器组，然后将防火墙分配到该日志收集器。

当您将更改推送到收集器组配置时，*Panorama* 将开始在各日志收集器之间重新分发日志。对于每 *1TB* 的日志，此过程可能需要数小时。在重新分发过程期间，会降低最大日志记录速率。在 *Panorama* > *Collector Groups*（收集器组）页面中，*Log Redistribution State*（日志重新分发状态）列将以百分比表示进程的完成状态。

STEP 3 | 配置 Panorama 的日志转发对于您配置的新收集器组。

STEP 4 | 选择 **Commit**（提交）> **Commit and Push**（提交并推送）以将更改提交到 Panorama 并将更改推送到设备组、模板和收集器组。

从收集器组删除防火墙

如果使用传统模式下的 Panorama 虚拟设备管理专用日志收集器，则可以选择将防火墙日志转发到 Panorama，而不是转发到日志收集器。对于这种情况，您必须从收集器组中删除防火墙；然后，防火墙会自动将其日志转发到 Panorama。

要暂时删除防火墙上的日志转发首选项列表，可以使用防火墙上的命令行界面来删除。但是，必须在 *Panorama* 上的收集器组配置中删除所分配的防火墙。否则，下次将更改推送到收集器组时，将会重新配置防火墙以便将日志发送到所分配的日志收集器。

STEP 1 | 选择 **Panorama** > **Collector Groups**（收集器组），然后编辑收集器组。

© 2019 Palo Alto Networks, Inc.

STEP 2 | 选择 **Device Log Forwarding**（设备日志转发），单击 Devices（设备）列表中的防火墙，**Modify**（修改）Devices（设备）列表，清除防火墙的复选框，然后单击 **OK**（确定）三次。

STEP 3 | 选择 **Commit**（提交）> **Commit and Push**（提交并推送），然后将更改 **Commit and Push**（提交并推送）到从防火墙删除的 Panorama 和收集器组。

© 2019 Palo Alto Networks, Inc.

配置 Panorama 的日志转发

每个防火墙默认在本地存储其日志文件，并且不能显示驻留在其他防火墙上的日志。因此，要实现全面了解所有防火墙监视的网络活动，必须将所有防火墙日志转发到 Panorama 并使用 Panorama 的可视化功能。如果组织中某些团队可以通过仅监视与其操作相关的日志来提高效率，则可以根据任何日志属性（例如：威胁类型或源用户）创建转发筛选器。例如，调查恶意软件攻击的安全运营分析师可能只对类型属性设置为 WildFire 病毒的威胁日志感兴趣。

以下步骤介绍如何使用 Panorama 模板和设备组配置多个防火墙转发日志。

如果 *Panorama* 管理运行软件版本早于 *PAN-OS 7.0* 的防火墙，则您应指定一个 *WildFire®* 服务器，使 *Panorama* 可以从该服务器收集这些防火墙提交的 *WildFire* 样本相关分析信息。*Panorama* 使用此信息来填写在 *PAN-OS 7.0* 中缺少引入字段值的 *WildFire* 提交日志。运行较早软件版本的防火墙将不会填充这些字段。若要指定服务器，应选择 *Panorama* > *Setup*（设置）> *WildFire*，编辑 *General Settings*（常规设置），然后输入 *WildFire Private Cloud*（*WildFire* 私有云）名称。默认服务器为 *wildfire-public-cloud*，它是主机设在美国的 *WildFire* 云。

您还可以将防火墙日志转发到外部服务（如 *syslog* 服务器）。有关详细信息，请参阅日志转发选项。

STEP 1 | 为将转发日志的防火墙配置添加设备组。

Panorama 需要一个设备组将日志转发配置文件推送到防火墙中。创建新的设备组或者将防火墙分配到一个已有设备组。

STEP 2 | 为将转发日志的防火墙配置添加模板。

Panorama 需要模板将日志设置推送到防火墙中。创建新的模板或者将防火墙分配到一个已有模板。

STEP 3 | 创建日志转发配置文件。

配置文件定义了流量、威胁、WildFire 提交、URL 筛选、数据筛选、隧道和身份验证日志的目标。

1. 选择 **Objects** > **Log Forwarding**（对象 > 日志转发），然后选择将转发日志的防火墙的 **Device Group**（设备组），**Add**（添加）一个配置文件。
2. 输入 **Name**（名称）以标识日志转发配置文件。
3. **Add**（添加）一个或多个匹配列表配置文件。

   配置文件指定日志查询筛选器、转发目的地和自动操作（如标记）。对于每个匹配列表配置文件：

   1. 输入 **Name**（名称）以标识配置文件。
   2. 选择 **Log Type**（日志类型）。
   3. 在 **Filter**（筛选器）下拉列表中，选择 **Filter Builder**（筛选器构建器）。指定以下内容，然后 **Add**（添加）每个查询：

      Connector（连接器）逻辑（和/或）

      日志 **Attribute**（属性）

      定义包含或排除逻辑的 **Operator**（运算符）

      用于查询匹配的属性 **Value**（值）
   4. 选择 **Panorama**。
4. 单击 **OK**（确定）保存日志转发配置文件。

STEP 4 | 将日志转发配置文件分配给安全规则和网络区域。

© 2019 Palo Alto Networks, Inc.

安全、身份验证和 DoS 保护规则支持日志转发。在本示例中，将配置文件分配至安全规则。

针对将触发日志转发的每种规则，执行以下步骤：

1. 选择规则库（例如 **Policies**（策略）> **Security**（安全）> **Pre Rules**（前导规则）），选择将转发日志的防火墙的 **Device Group**（设备组），然后编辑规则。
2. 选择 **Actions**（操作）选项卡，并选择您创建的 **Log Forwarding profile**（日志转发配置文件）。
3. 将 **Profile Type**（配置文件类型）设置为 **Profiles**（配置文件）或 **Group**（组），然后选择触发日志生成和转发所需的安全配置文件或 **Group Profile**（组配置文件）：
   - 威胁日志 — 流量必须匹配分配给规则的任何安全配置文件。
   - WildFire 日志 — 流量必须匹配分配给规则的 WildFire Analysis profile（WildFire 分析配置文件）。
4. 对于流量日志，选中 **Log At Session Start**（在会话开始时记录）和/或 **Log At Session End**（在会话结束时记录）。
5. 单击 **OK**（确定）保存规则。

STEP 5 | 配置系统日志、配置日志、User-ID™ 日志和 HIP 匹配日志的目标。

Panorama 基于它收到的防火墙日志而非防火墙提供的聚合关联日志生成关联日志。

1. 选择 **Device** > **Log Settings**（设备 > 日志设置），然后选择将转发日志的防火墙的 **Template**（模板）。
2. 对于防火墙将转发的每个日志类型，请参阅步骤添加一个或多个匹配列表配置文件。

STEP 6 | （仅限 PA-7000 系列防火墙）配置日志卡接口以执行日志转发。

当您将某个 PA-7000 系列网络处理卡 (NPC) 上的数据端口配置为日志卡接口时，防火墙将自动开始使用此接口将日志转发到您为 WildFire 分析配置和转发文件的日志记录目标。确保您配置的接口可以访问日志转发目标以及 WildFire 云，WildFire 设备或两者。

由于 *PA-7000* 系列防火墙现在可以将日志转发到 *Panorama*，因此 *Panorama* 不再将它作为日志收集器管理的 *PA-7000* 系列防火墙。如果您尚未将 *PA-7000* 系列防火墙配置为将日志转发到 *Panorama*，则受管 *PA-7000* 系列防火墙生成的所有日志只能从本地防火墙查看，而不能从 *Panorama* 查看。如果您还没有能够处理 *PA-7000* 系列防火墙的日志记录速率和数量的日志转发基础设施，则从 *PAN-OS 8.0.8* 开始，您可以在监控时启用 *Panorama* 直接查询 *PA-7000* 系列防火墙日志。要使用此功能，*Panorama* 和 *PA-7000* 系列防火墙必须运行 *PAN-OS 8.0.8* 或更高版本。通过从 *Panorama CLI* 输入以下命令，使 *Panorama* 能够直接查询 *PA-7000* 系列防火墙：

```
> debug reportd send-request-to-7k yes
```

运行此命令后，您将能够在 *Panorama Monitor*（监控）选项卡上查看受管 *PA-7000* 系列防火墙的日志。此外，与所有受管设备一样，您还可以通过选择 *Remote Device Data*（远程设备数据）作为 *Data Source*（数据源）生成包含 *PA-7000* 系列日志数据的报告。如果您稍后决定启用 *PA-7000* 系列防火墙以将日志转发到 *Panorama*，则必须先使用 ***debug reportd send-request-to-7k no*** 命令禁用此选项。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**，选择将转发日志的防火墙的 **Template**（模板），然后 **Add Interface**（添加模板）。
2. 选择 **Slot**（插槽）和 **Interface Name**（接口名称）。
3. 将 **Interface Type**（接口类型）设置为 **Log Card**（日志卡）。

© 2019 Palo Alto Networks, Inc.

4. 输入 **IP Address**（**IP** 地址）、 **Default Gateway**（默认网关）和（仅限 IPv4）**Netmask**（网络掩码）。
5. 选择 **Advanced**（高级），并指定 **Link Speed**（链接速度）、**Link Duplex**（链接双工）和 **Link State**（链接状态）。

   这些字段默认设置为 *auto*（自动），指示防火墙基于连接自动确定值。但是，针对任何连接推荐的最小 *Link Speed*（链接速度）为 *1000 (Mbps)*。
6. 单击 **OK**（确定）保存更改。

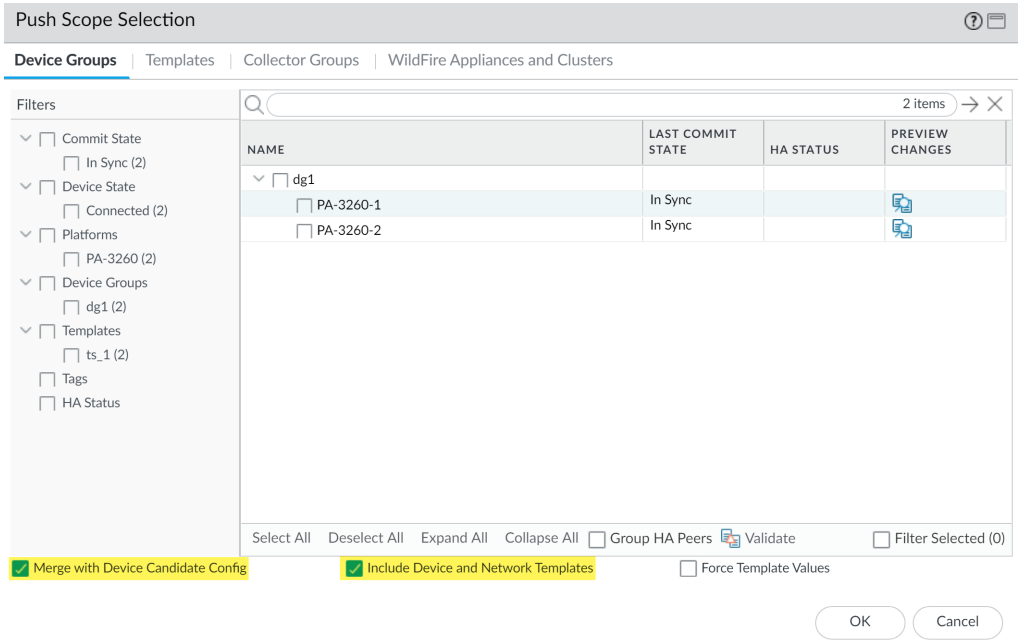
STEP 7 | 配置 Panorama 以接收日志。

如果您将在传统模式下将日志转发到 *Panorama* 虚拟设备，则可以跳过此步骤。

1. 对于将接收日志的每一个日志收集器，配置受管收集器。
2. 配置收集器组以将防火墙分配到特定的日志收集器以进行日志转发。

STEP 8 | Commit（提交）配置更改。

1. 选择 **Commit**（提交）> **Commit and Push**（提交并推送），然后 **Edit Selections**（编辑选择）。
2. 选中 **Merge with Device Candidate Config**（与设备待选配置合并）、**Include Device and Network Templates**（包含设备和网络模板），然后单击**OK**（确定）。



3. **Commit and Push**（提交并推送）您的更改到 Panorama 并将更改推送到设备组、模板和收集器组。
4. 验证 Panorama 日志转发，以确认配置成功。

若要更改防火墙用来将日志发送到 *Panorama* 的日志转发模式，您可以修改日志转发和缓冲默认设置。您也可以管理日志和报告的存储配额和过期期限。

© 2019 Palo Alto Networks, Inc.

配置到外部目标的 Syslog 转发

如果是具有高日志生成率的部署，则可以通过以太网接口转发 Syslog，以防止日志丢失并减少管理接口上的负载，从而优化管理操作。

仅使用 Panorama 模式或日志收集器模式的 Panorama™ 管理服务器才支持使用以太网接口进行 Syslog 转发。此外，无论 Panorama 处于 Panorama 模式还是日志收集器模式，您都只能在单一接口上启用 Syslog 转发。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 配置受管收集器。

STEP 3 | 配置收集器组。

在 M-Series 设备上，已预定义默认收集器组，并且已经包含本地日志收集器作为成员。然而，在 Panorama 虚拟设备上，您必须添加收集器组，并添加本地日志收集器作为成员。对于这两种配置，您都需要分配防火墙到日志收集器以进行日志转发。

STEP 4 | 配置 Syslog 服务器配置文件。

1. 选择 **Panorama** > **Server Profiles**（服务器配置文件）> **Syslog**，然后 **Add**（添加）一个新的 Syslog 服务器配置文件。
2. 为 Syslog 服务器配置文件输入一个 **Name**（名称）。
3. 对于每个 Syslog 服务器，**Add**（添加）Panorama 或专用日志收集器为连接到它所需的信息：
   - **Name**（名称）— Syslog 服务器的唯一名称。
   - **Syslog Server**（**Syslog** 服务器）- Syslog 服务器的 IP 地址或完全限定域名 (FQDN)。
   - **Transport**（传输）— 选择 **UDP**、**TCP** 或 **SSL** 作为与 Syslog 服务器通信的方法。
   - **Port**（端口）— 发送 Syslog 消息时使用的端口号（端口 514 的默认值为 UDP）；您必须在 Panorama 和专用日志收集器上使用相同端口号。
   - **Format**（格式）— 请选择要使用的 Syslog 消息格式：**BSD**（默认）或 **IETF**。通常来说，**BSD** 格式通过 UDP 发送，**IETF** 格式通过 TCP 或 SSL 发送。
   - **Facility**（工具）— 选择 Syslog 标准值（默认值为 **LOG_USER**），用于计算 Syslog 服务器实现中的优先级 (PRI) 字段。选择用于映射如何使用 PRI 字段管理 Syslog 的值。
4. （可选）要自定义 Panorama 或专用日志收集器发送的 Syslog 消息的格式，请选择 **Custom Log Format**（自定义日志格式）。有关如何为各个日志类型创建自定义格式的详情，请参阅通用事件格式配置指南。
5. 单击 **OK**（确定）保存 Syslog 服务器配置文件。

STEP 5 | 配置一个以太网接口用于转发 Syslog。

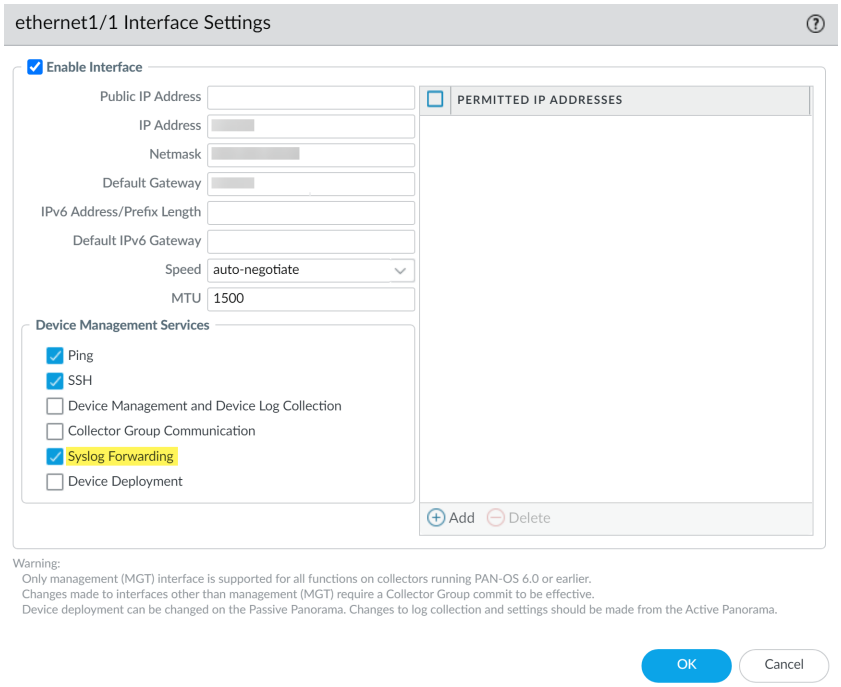
默认情况下，Syslog 转发在管理接口上启用，且一次仅在一个接口上受支持。

- 在 Panorama Web 界面的本地日志收集器上配置一个以太网接口。
  1. 选择 **Panorama** > **Setup**（设置）> **Interfaces**（接口），然后选择一个以太网接口。
  2. 启用接口。
  3. 酌情配置以太网接口。
  4. 在“设备管理服务”部分中，启用 **Syslog Forwarding**（**Syslog** 转发）。
  5. 选择 **Yes**（是）以确认您的 Syslog 转发更改。

     只能通过本地日志收集器的一个以太网接口进行 *Syslog* 转发。
  6. 单击 **OK**（确定）保存更改。

© 2019 Palo Alto Networks, Inc.

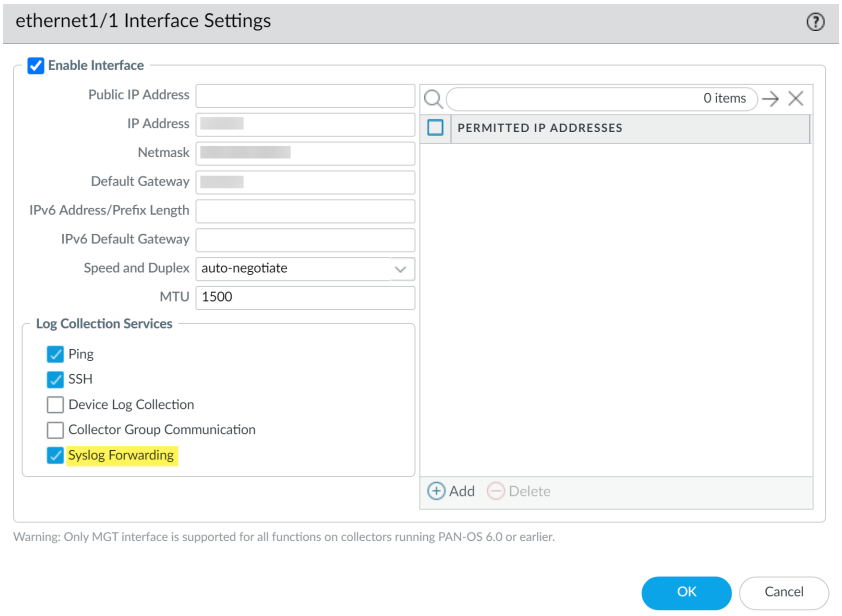
7. **Commit**（提交），然后 **Commit and Push**（提交并推送）您的配置更改。



- 在专用日志收集器上配置以太网接口。
  1. 选择 **Panorama** > **Managed Collectors**（受管收集器），然后选择一个专用日志收集器。
  2. 启用接口。
  3. 酌情配置以太网接口。
  4. 在“日志收集服务”部分中，启用 **Syslog Forwarding**（**Syslog** 转发）。
  5. 选择 **Yes**（是）以确认您的 Syslog 转发更改。

     只能通过专用日志收集器的一个以太网接口进行 *Syslog* 转发。
  6. 单击 **OK**（确定）保存更改。
  7. **Commit**（提交），然后 **Commit and Push**（提交并推送）您的配置更改。

© 2019 Palo Alto Networks, Inc.



- 在 Panorama CLI 的本地日志收集器或专用日志收集器上配置一个以太网接口。

  要成功配置通过 CLI 的以太网接口上进行 Syslog 转发，必须首先禁用通过管理接口进行 Syslog 转发，然后启用通过 CLI 的以太网接口进行 Syslog 转发；Panorama 不会自动禁用通过管理接口进行 Syslog 转发，如果您同时在管理接口和以太网接口上启用了 Syslog 转发，Syslog 转发将会继续通过管理接口进行。

  1. 登录到 Panorama 命令行界面
  2. 禁用通过管理接口进行 Syslog 转发：

     ```
     admin@Panorama> configure
     ```

     ```
     admin@Panorama> set log-collector <Log Collector Serial Number>
      deviceconfig system service disable-syslog-forwarding yes
     ```

  3. 启用通过以太网接口进行 Syslog 转发：

     ```
     admin@Panorama> configure
     ```

     ```
     admin@Panorama> set log-collector <Log Collector Serial Number>
      deviceconfig system eth<Interface Number>  service disable-syslog-
     forwarding no
     ```

     ```
     admin@Panorama> commit
     ```

  4. 提交您的配置更改：

     ```
     admin@Panorama> run commit-all log-collector-config log-collector-
     group <Collector Group name>
     ```

STEP 6 | 配置 Panorama 的日志转发。

STEP 7 | 配置从 Panorama 到 Syslog 服务器的 Syslog 转发。

© 2019 Palo Alto Networks, Inc.

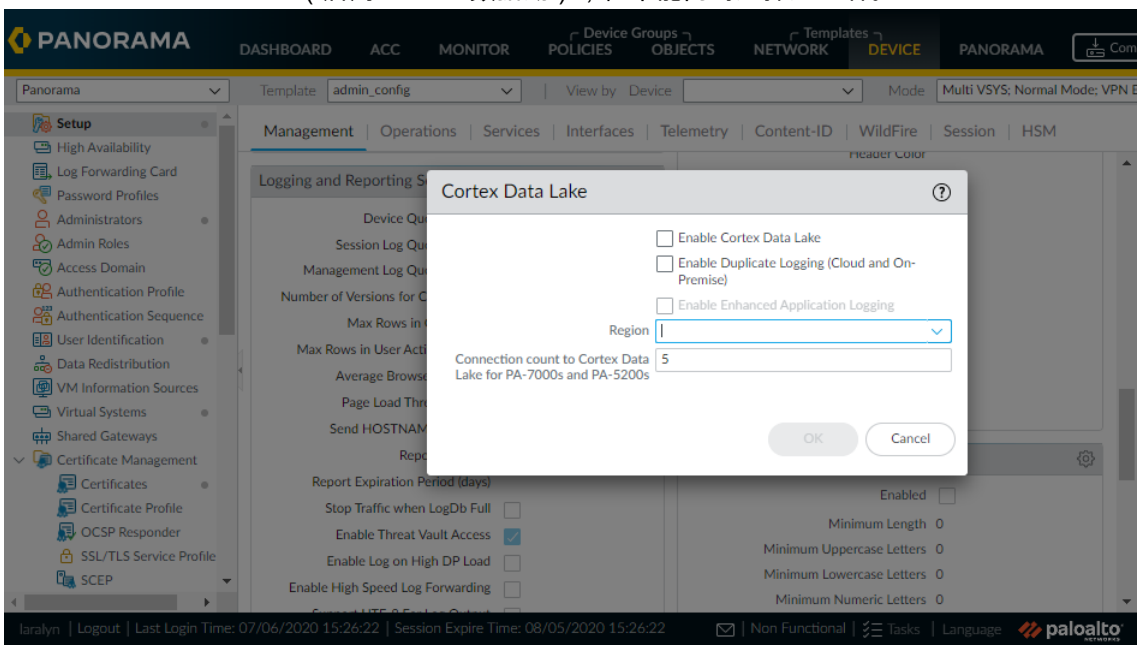
转发日志至 Cortex 数据湖

Cortex 数据湖是 Palo Alto Networks 基于云的日志记录基础架构。在配置受管防火墙以发送日志到 Cortex 数据湖（之前称为“日志记录服务”）之前，您需要为部署中的日志量购买许可证，并安装云服务插件。如果您已拥有本地日志收集器，则可以使用 Cortex 数据湖补充和增强现有设置。

STEP 1 | 安装 Panorama 插件。

STEP 2 | 配置防火墙以发送日志到 Cortex 数据湖。

对于运行 PAN-OS 8.1 或更高版本的防火墙，当您选择 **Enable Duplicate Logging (Cloud and On-Premise)**（启用重复日志记录（云和本地））时，您可以选择将日志发送至 Cortex 数据湖以及您的 Panorama 和本地日志收集设置。启用时，属于选中模板的防火墙将保存发送至这两个位置的日志副本。您可以选择 **Enable Duplicate Logging (Cloud and On-Premise)**（启用重复日志记录（云和本地））或 **Enable Cortex Data Lake**（启用 **Cortex** 数据湖），但不能同时选择这二者。



© 2019 Palo Alto Networks, Inc.

验证 Panorama 的日志转发

在配置日志转发至 Panorama 或 Cortex 数据湖后验证向 Panorama 的日志转发，以测试配置是否成功。

配置日志收集器的日志转发后，受管防火墙会打开所有已配置的日志收集器的 TCP 连接。这些连接每隔六十（60）秒超时一次，且不会指示防火墙已断开与日志收集器的连接。通过受支持以太网接口配置本地或专用日志收集器的日志转发后，尽管防火墙能够成功连接到日志收集器，但防火墙流量日志仍显示 `incomplete` 会话。如果通过管理端口配置日志转发，流量日志不会显示 `incomplete` 会话。除 PA-5200 和 PA-7000 系列防火墙外，其他防火墙的流量日志都会显示 `incomplete` 会话。

STEP 1 | 访问防火墙 CLI。

STEP 2 | 如果您已配置日志收集器，则应验证每一个防火墙都具有一个日志转发首选项列表。

```
> show log-collector preference-list
```

如果收集器组只具有一个日志收集器，则输出结果看上去将是这个样子：

```
Forward to all: No
Log collector Preference List
Serial Number: 003001000024
IP Address: 10.2.133.48
IPV6 Address: unknown
```

STEP 3 | 验证每一个防火墙都在发送日志。

```
> show logging-status
```

如果转发成功，输出结果将指明日志转发代理处于活动状态。

- 对于 Panorama 虚拟设备，代理为 `Panorama`。
- 对于 M 系列设备，代理为`LogCollector`。
- 对于 Cortex 数据湖，代理为 `Log CollectionService.`。而且

```
'Log Collection log forwarding agent' is active and connected
 to <IP_address>.
```

STEP 4 | 查看平均日志记录速率。显示的速率将是之前五分钟的平均每秒日志数。

- 如果是日志收集器接收日志，则应访问 Panorama Web 界面，选择 **Panorama** > **Managed Collectors**（Panorama > 受管收集器），然后在最右侧的那一列中单击 **Statistics**（统计信息）链接。
- 如果是处于传统模式下的 Panorama 虚拟设备接收日志，则应访问 Panorama CLI，然后运行以下命令：**`debug log-collector log-collection-stats show incoming-logs`**



此命令在 *M* 系列设备上同样有效。

© 2019 Palo Alto Networks, Inc.

修改日志转发和缓冲默认设置

您可以定义防火墙在将日志发送到 Panorama 时所用的日志转发模式，并且在高可用性配置中进行配置时，可以指定哪一个 Panorama 对端设备可以接收日志。要访问这些选项，选择 **Panorama** > **Setup**（设置）> **Management**（管理），编辑日志记录和报告设置，然后选择 **Log Export and Reporting**（日志导出和报告）。

- 定义防火墙的日志转发模式：无论是在缓冲日志转发模式下，还是在实时模式日志转发模式下，防火墙都可以将日志转发到 Panorama（适用于 M 系列设备和 Panorama 虚拟设备）。

日志记录选项	说明
（最佳实践）来自设备的缓冲日志转发 默认：已启用	允许每个受管防火墙缓冲日志并每隔 30 秒将日志发送到 Panorama（用户不可配置）。 当防火墙失去与 Panorama 的连接时，缓冲日志转发非常有用。防火墙将日志条目缓冲到其本地硬盘，并保留指针记录最后发送到 Panorama 的日志条目。在连接恢复后，防火墙将继续从其离开的位置转发日志。 用于缓冲的磁盘空间取决于防火墙型号的日志存储配额和等待处理的日志的总量。如果防火墙长时间断开连接且转发的最后日志顺序颠倒，则在重新建立连接后会将其本地硬盘中的所有日志转发到 Panorama。如果防火墙的本地硬盘的可用空间即将用完，将会删除最早的日志条目以便允许记录新的事件。
来自设备的实时模式日志转发 取消选中 **Buffered Log Forwarding from Device**（来自设备的缓冲日志转发）复选框之后，将会启用此选项。	在实时模式下，受管防火墙按照与在防火墙上记录日志事务相同的时间将每个日志事务发送到 Panorama。

- 在以高可用性 (HA) 配置部署且处于传统模式下的 Panorama 虚拟设备上定义日志转发首选项：
  - 当记录到虚拟磁盘时，仅允许记录到主要 Panorama 对端设备上的本地磁盘。默认情况下，高可用性配置中的 Panorama 对端设备将会接收日志。

    对于 *5200* 和 *7000* 系列防火墙，仅主动对等设备会接收日志。
  - 当记录到 NFS 时（仅限 ESXi 服务器），仅允许防火墙将新生成的日志发送到辅助 Panorama 对端设备，该对端设备可以在故障转移后晋升为主要对端设备。

日志记录选项	适用对象	说明
仅将主动主要设备日志记录到本地磁盘 默认：禁用	记录到虚拟磁盘并在高可用性配置中部署的传统模式下的 Panorama 虚拟设备。	可让您配置仅由主要 Panorama 对端设备将日志保存到本地磁盘。
仅获取主要设备转换期间的新日志 默认：禁用	安装到网络文件系统 (NFS) 数据存储，在 VMware ESXi 服务器上运行并在高可用性	通过 NFS 记录，当高可用性配置中配置了一对 Panorama 服务器时，只有主要 Panorama 对端设备才会安装 NFS 数据库。因此，防火墙只能将日志发送到主

© 2019 Palo Alto Networks, Inc.

日志记录选项	适用对象	说明
	配置中部署的传统模式下的 Panorama 虚拟设备。	要 Panorama 对端设备，该对端设备可以写入 NFS 数据存储。 当发生高可用性故障转移时，**Get Only New Logs on Convert to Primary**（仅获取主要设备转换期间的新日志）选项可让管理员配置受管防火墙以便只将新生成的日志发送到 Panorama。当活动的备用 Panorama 的优先级提升到主要并且可以开始记录到 NFS 时，将会触发此事件。启用此行为通常是为了阻止防火墙在很长时间之后恢复与 Panorama 的连接时发送大量的缓冲日志。

© 2019 Palo Alto Networks, Inc.

配置从 Panorama 到外部目标的日志转发

Panorama 让您能够将日志转发到多种外部服务器，包括 syslog、电子邮件、SNMP 陷阱和基于 HTTP 的服务。使用外部服务让您能够收到有关重要事件的警报，利用专用长期存储将监控信息存档在系统上，并与第三方安全监控工具集成。除了转发防火墙日志外，您还可以转发 Panorama 管理服务器和日志收集器生成的日志。转发日志的 Panorama 管理服务器或日志收集器将它们转换为适合目标（syslog 消息、电子邮件通知、SNMP 陷阱或 HTTP 有效负载）的格式。



如果 *Panorama* 管理服务器是处于传统模式的 *Panorama* 虚拟设备，则它转换并转发日志到外部服务，而不使用日志收集器。

您还可以将日志从防火墙直接转发到外部服务：请参阅日志转发选项。

在运行 *Panorama 5.1* 或更早版本的 *Panorama* 虚拟设备上，您可以使用来自 CLI 的安全复制 (SCP)命令以将整个日志数据库导出到 *SCP* 服务器并导入到另一个 *Panorama* 虚拟设备。运行 *Panorama 6.0* 或更高版本的 *Panorama* 虚拟设备以及运行任何版本的 *M* 系列设备均不支持这些选项，因为这些型号上的日志数据库过于庞大而使得将其导出或导入均不现实。

要将日志转发到外部服务，请先配置防火墙以将日志转发到 Panorama。然后，您必须配置定义 Panorama 和日志收集器如何连接到服务的服务器配置文件。最后，将服务器配置文件分配给 Panorama 和收集器组的日志设置。

STEP 1 | 配置防火墙以将日志转发到 Panorama。

配置 Panorama 的日志转发。

STEP 2 | 为将要接收日志信息的每种外部服务配置服务器配置文件。

1. 选择 **Panorama** > **Server Profiles**（Panorama > 服务器配置文件），然后选择将接收日志数据的服务器的类型：**SNMP Trap**（**SNMP** 陷阱）、**Syslog**、**Email**（电子邮件）或 **HTTP**。
2. 配置服务器配置文件：
   - 配置 SNMP 陷阱服务器配置文件。关于 SNMP 如何适用于 Panorama 和日志收集器的详细信息，请参阅 SNMP 支持。
   - 配置 Syslog 服务器配置文件。如果 syslog 服务器要求客户端身份验证，请使用 **Panorama** > **Certificate Management** > **Certificates**（Panorama > 证书管理 > 证书）页面来创建证书，以确保 SSL 上 syslog 通信的安全。
   - 配置电子邮件服务器配置文件。
   - 配置 HTTP 服务器配置文件。

STEP 3 | 为以下各项配置目标：

- 记录 Panorama 管理服务器和日志收集器生成的日志。
- Panorama 虚拟设备在传统模式下收集的防火墙日志。

1. 选择 **Panorama** > **Log Settings**（日志设置）。
2. 为每个日志类型 **Add**（添加）一个或多个匹配列表配置文件。

   配置文件指定日志查询筛选器、转发目的地和自动操作（如标记）。对于每个匹配列表配置文件：

   1. 输入 **Name**（名称）以标识配置文件。
   2. 选择 **Log Type**（日志类型）。
   3. 在 **Filter**（筛选器）下拉列表中，选择 **Filter Builder**（筛选器构建器）。指定以下内容，然后 **Add**（添加）每个查询：

      Connector（连接器）逻辑（和/或）

© 2019 Palo Alto Networks, Inc.

日志 **Attribute**（属性）

定义包含或排除逻辑的 **Operator**（运算符）

用于查询匹配的属性 **Value**（值）

4. **Add**（添加）您为每个外部服务配置的服务器配置文件。
5. 单击 **OK**（确定）保存配置文件。

STEP 4 | 配置日志收集器接收的防火墙日志的目标。



每个收集器组都可以将日志转发到不同的目标。如果日志收集器位于 *Panorama* 管理服务器的高可用性 *(HA)* 对的本地，您必须登录到每一个高可用性对端设备来为其收集器组配置日志转发。

1. 选择 **Panorama** > **Collector Groups**（收集器组），然后编辑接收防火墙日志的收集器组。
2. （可选，仅限 SNMP 陷阱转发）选择 **Monitoring**（监控）并配置 SNMP 设置。
3. 必要时，选择 **Collector Log Forwarding**（收集器日志转发）并 **Add**（添加）已配置的匹配列表配置文件。
4. 单击 **OK**（确定）保存对收集器组所作的更改。

STEP 5 | （仅限 Syslog 转发）如果 syslog 服务器要求客户端身份验证且防火墙将日志转发到专用日志收集器，则分配可以确保 SSL 上 syslog 通信安全的证书。

在每个专用日志收集器上完成以下步骤：

1. 选择 **Panorama** > **Managed Collectors**（Panorama > 受管收集器），然后编辑日志收集器。
2. 选择 **Certificate for Secure Syslog**（安全 **Syslog** 证书），然后单击 **OK**（确定）。

STEP 6 | （仅限 SNMP 陷阱转发）启用您的 SNMP 管理器以解读陷阱。

加载支持的 MIB 并在必要时编译它们。有关具体步骤，请参阅 SNMP 管理器的文档。

STEP 7 | 提交并验证配置更改。

1. 选择 **Commit**（提交）> **Commit and Push**（提交并推送）以将更改提交到 Panorama 并将更改推送到设备组、模板和收集器组。
2. 验证外部服务正在接收日志信息：
   - 电子邮件服务器 — 确认指定收件人收到电子邮件通知形式的日志。
   - **Syslog** 服务器 — 请参阅 syslog 服务器的文档，以确认它收到 syslog 消息形式的日志。
   - **SNMP** 管理器 — 请参阅 SNMP 陷阱服务器的文档，以确认它收到 SNMP 陷阱形式的日志。
   - **HTTP** 服务器 — 确认基于 HTTP 的服务器收到正确的有效负载格式的日志。

© 2019 Palo Alto Networks, Inc.

日志收集部署

以下主题介绍如何在最典型的部署中配置日志收集。在开始之前，根据您当前和未来的日志记录需求计划您的 Panorama 部署。

这些主题中的部署都描述了高可用性 *(HA)* 配置中的 *Panorama*。*Palo Alto Networks* 建议您采用高可用性，因为它可以使尚未保存为配置备份一部分的组件（在服务器发生故障的情况下）实现自动恢复。在高可用性部署中，*Panorama* 管理服务器仅支持主动/被动配置。

- 使用专用日志收集器部署 Panorama
- 使用本地日志收集器部署 Panorama M 系列设备
- 使用本地日志收集器部署 Panorama 虚拟设备
- 使用本地日志收集器在传统模式下部署 Panorama 虚拟设备

使用专用日志收集器部署 Panorama

下图显示了分布式日志收集部署中的 Panorama。在这些示例中，Panorama 管理服务器包括处于 Panorama 模式的两台 M 系列或 Panorama 虚拟设备，两者均部署在主动/被动高可用性 (HA) 配置中。防火墙将日志发送到专用日志收集器（处于日志收集器模式的 M 系列或 Panorama 虚拟设备）。如果防火墙生成日志的速率超过 10,000 条/秒，则建议使用此配置。

如果您将多个日志收集器分配到收集器组，请参阅具有多个日志收集器的收集器组的警告了解要求、风险和建议的缓解措施。

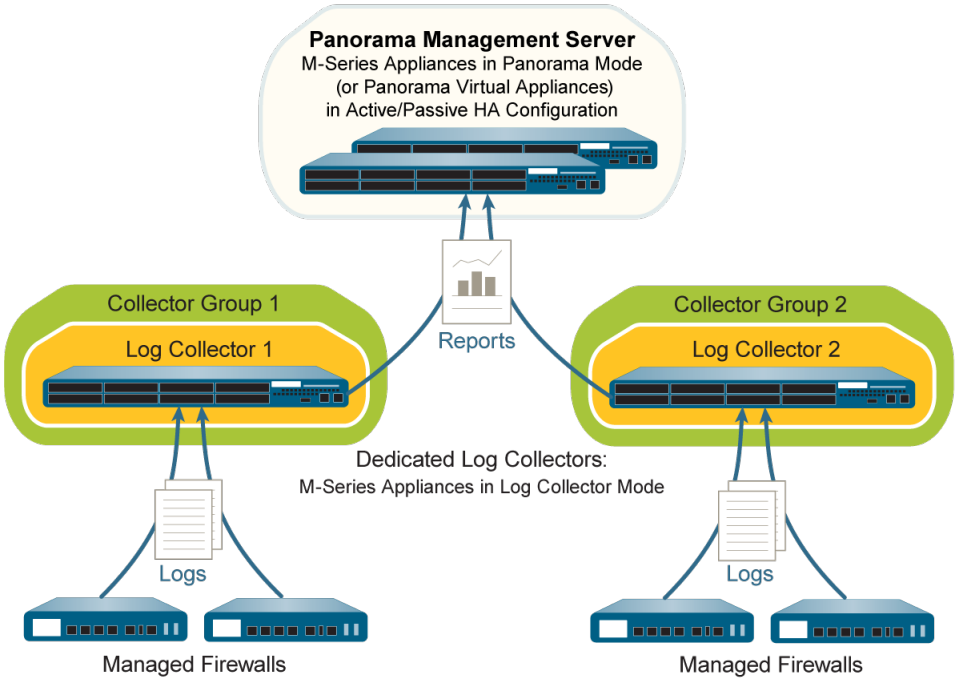


图 17: 每个收集器组一个专用日志收集器

© 2019 Palo Alto Networks, Inc.

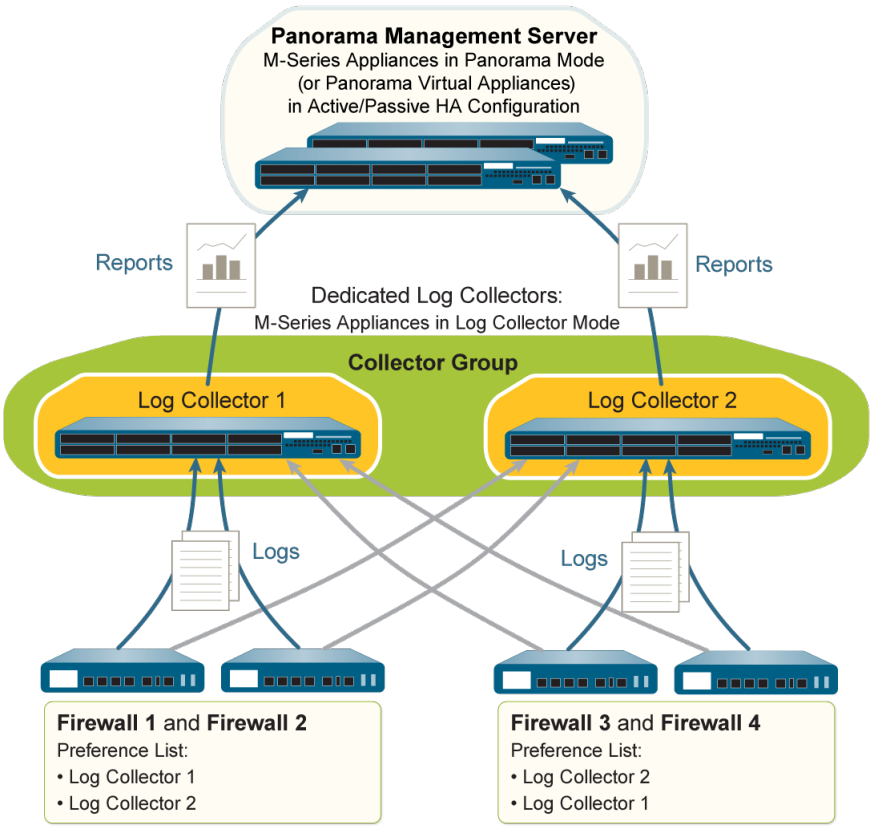


图 **18:** 每个收集器组多个专用日志收集器

执行以下步骤以使用专用日志收集器部署 Panorama。如果您已执行相关步骤（如初始设置），请跳过任何步骤。

STEP 1 | 对 Panorama 管理服务器（虚拟设备或 M 系列设备）和专用日志收集器执行初始设置。

对于每个 M 系列设备：

1. 将 M 系列设备安装到机架上。有关说明，请参阅《M 系列硬件参考指南》。
2. 执行 M 系列设备的初始配置。

   Palo Alto Networks 建议预留管理 *(MGT)* 接口用于 *Panorama* 的管理访问权限，并将单独的 M 系列设备接口专用于其他 *Panorama* 服务。

3. 配置每个阵列。需要执行此任务使 RAID 磁盘可用于日志记录。或者，您可以添加磁盘来增加 M 系列设备上的存储容量。
4. 注册 Panorama 和安装许可证。
5. 安装 Panorama 的内容和软件更新。

对于每个虚拟设备（如果有）：

1. 安装 Panorama 虚拟设备。
2. 执行 Panorama 虚拟设备的初始配置。
3. 注册 Panorama 和安装许可证。
4. 安装 Panorama 的内容和软件更新。

对于 Panorama 管理服务器（虚拟设备或 M 系列设备），您还必须设置 Panorama 高可用性。

STEP 2 | 在每个将成为专用日志收集器的每个 Panorama 管理设备上从 Panorama 模式切换到日志收集器模式。

© 2019 Palo Alto Networks, Inc.

切换 *M* 系列或 *Panorama* 虚拟设备的模式将删除任何现有日志数据，并删除除管理访问权限设置之外的所有配置。切换后，*M* 系列或 *Panorama* 虚拟设备仍可访问 *CLI*，但无法访问 *Web* 界面。

1. 按以下方式之一连接到 Panorama：
   - （仅限 M 系列设备）使用串行电缆将计算机与 M 系列设备上的控制台端口相连。然后，使用终端模拟软件 (9600-8-N-1) 进行连接。
   - 使用终端模拟软件（如 PuTTY）打开您在初始配置期间为 Panorama 管理服务器的 MGT 接口指定的 IP 地址的 SSH 会话。
2. 看到提示时登录到 CLI。使用初始配置过程中指定的默认 admin 帐户和密码。
3. 要切换到日志收集器模式，请输入以下命令：

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

4. 输入 **y** 确认模式更改。重新启动 Panorama 管理服务器。如果重启进程终止了终端模拟软件会话，请重新连接至 Panorama 以查看 Panorama 登录提示。

   如果您看到 ***CMS Login***（*CMS* 登录）提示，这意味着日志收集器没有完成重新启动。看到提示时按 *Enter* 键，而不输入用户名或密码。
5. 重新登录至此 CLI。
6. 验证切换到日志收集器模式是否成功：

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

   如果模式更改成功，输出显示：

```
system-mode: logger
```

STEP 3 | 启用每个日志收集器和 Panorama 管理服务器之间的连接。

必须执行此步骤才能在日志收集器上启用日志记录磁盘。

在各日志收集器的 CLI 输入以下命令。*<IPaddress1>* 是主动 Panorama 的 MGT 接口，*<IPaddress2>* 是被动 Panorama 的 MGT 接口。

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

STEP 4 | 记录每个日志收集器的序列号。

您需要此序列号在 Panorama 管理服务器上，将日志收集器添加为受管收集器。

1. 在每个日志收集器的命令行界面中，输入以下命令以显示它的序列号。

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

2. 记录序列号。

STEP 5 | 将每个日志收集器添加为受管收集器。

© 2019 Palo Alto Networks, Inc.

使用主要 Panorama 管理服务器对端设备的 Web 界面配置受管收集器：

1. 选择 **Panorama** > **Managed Collectors**（Panorama > 受管收集器），然后 **Add**（添加）受管收集器。
2. 在 **General**（常规）选项卡中，输入为日志收集器记录的序列号（**Collector S/N**（收集器序列号））。
3. 在 **Panorama Server IP**（**Panorama** 服务器 **IP**）字段和 **Panorama Server IP 2**（**Panorama** 服务器 **IP 2**）字段中，输入主动和被动 Panorama 高可用性对端设备的 IP 地址或 FQDN。以下字段为必填字段。
4. 选择 **Interfaces**（接口），单击 **Management**（管理），根据网络的 IP 协议为 MGT 接口配置以下一个或两个字段集。
   - IPv4 — **IP Address**（**IP** 地址）、**Netmask**（子网掩码）和 **Default Gateway**（默认网关）
   - IPv6 — **IPv6 Address/Prefix Length**（**IPv6** 地址/前缀长度）和 **Default IPv6 Gateway**（默认 **IPv6** 网关）
5. （可选）如果您将使用 SNMP 管理器监控日志收集器统计信息，请选择 **SNMP**。

   除了配置日志收集器之外，使用 SNMP 还需要执行其他步骤（请参阅使用 SNMP 监视 Panorama 和日志收集器统计信息）。
6. 单击 **OK**（确定）保存更改。
7. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

   必须执行此步骤才能在日志收集器上启用日志记录磁盘。
8. 核实 **Panorama** > **Managed Collectors**（Panorama > 受管收集器）页面列出了您已添加的日志收集器。Connected（已连接）列显示表明日志收集器已连接到 Panorama 的复选标记。您可能需要等待几分钟，等页面显示更新后的连接状态。

   此时，*Configuration Status*（配置状态）列显示 *Out of Sync*（不同步），*Run Time Status*（运行时间状态）列应显示 *disconnected*（已断开连接）。在配置收集器组后，状态将更改为同步中和已连接（步骤 9）。

STEP 6 | 在每个日志收集器上启用日志记录磁盘。

使用主要 Panorama 管理服务器对端设备的 Web 界面执行以下步骤：

1. 选择 **Panorama** > **Managed Collectors**（Panorama > 受管收集器），然后编辑日志收集器。
2. 选择 **Disks**（磁盘），**Add**（添加）每个磁盘对，然后单击 **OK**（确定）。
3. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

STEP 7 | （推荐）如果日志收集器使用 **Ethernet1**、**Ethernet2**、**Ethernet3**、**Ethernet4** 和 **Ethernet5** 接口进行 **Device Log Collection**（设备日志收集）（从防火墙接收日志）和 **Collector Group Communication**（收集器组通信），请配置这些接口。

默认情况下，日志收集器使用 MGT 接口进行日志收集和收集器组通信。将其他接口分配给这些功能可让您为管理流量预留 MGT 接口。在日志流量很大的环境中，请考虑在 M-500 设备上使用 10Gbps 接口（**Ethernet4** 和 **Ethernet5**）进行日志收集和收集器组通信。要跨接口负载平衡日志记录流量，可以在多个接口上启用 **Device Log Collection**（设备日志收集）。

使用主要 Panorama 管理服务器对端设备的 Web 界面为每个日志收集器执行这些步骤：

1. 选择 **Panorama** > **Managed Collectors**（受管收集器），编辑日志收集器，然后选择 **Interfaces**（接口）。
2. 为每个接口执行以下步骤：
   1. 单击接口名称进行编辑。
   2. 选择 **<interface-name>** 以启用接口。
   3. 根据您网络的 IP 协议，填写以下一个或两个字段集：

© 2019 Palo Alto Networks, Inc.

IPv4 — **IP Address**（**IP** 地址）、**Netmask**（子网掩码）和 **Default Gateway**（默认网关）

IPv6 — **IPv6 Address/Prefix Length**（**IPv6** 地址/前缀长度）和 **Default IPv6 Gateway**（默认 **IPv6** 网关）

4. 选择接口支持的设备管理服务：

   Device Log Collection（设备日志收集）— 您可以分配一个或多个接口。

   Collector Group Communication（收集器组通信）— 您只能分配一个接口。

5. 单击 **OK**（确定）保存对接口所作的更改。

3. 单击 **OK**（确定）保存对日志收集器所作的更改。
4. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并将更改 **Commit**（提交）到 Panorama 配置。

STEP 8 | 添加防火墙作为受管设备。

使用主要 Panorama 管理服务器对端设备的 Web 界面为每个将日志转发到日志收集器的防火墙执行此任务。

STEP 9 | 配置收集器组。

如果每个收集器组都将具有一个日志收集器，则在继续操作之前对每个收集器组重复本步骤。

如果您将把所有日志收集器都分配到一个收集器组，则只需要执行一次本步骤。

使用主要 Panorama 管理服务器对端设备的 Web 界面配置收集器组：

1. 选择 **Panorama** > **Collector Groups**（Panorama > 收集器组），然后 **Add**（添加）所需的收集器组。
2. 输入 **Name**（名称）以标识收集器组。
3. 将一个或多个日志收集器 **Add**（添加）到收集器组成员列表。

   在任何单个收集器组中，所有日志收集器均必须在相同的 *Panorama* 型号上运行：均为 *M-600* 设备、均为 *M-500* 设备、均为 *M-200* 设备或均为 *Panorama* 虚拟设备。

4. （最佳做法）如果将多个日志收集器添加到单个收集器组，请 **Enable log redundancy across collectors**（启用跨收集器记录冗余）。此选项要求每个日志收集器具有相同数量的日志记录磁盘。
5. （可选）如果您将使用 SNMP 来监控日志收集器的统计信息和陷阱，请选择 **Monitoring**（监控）并配置设置。
6. 选择 **Device Log Forwarding**（设备日志转发）并配置日志转发首选项列表。此列表定义哪些防火墙将日志转发到哪些日志收集器。根据此收集器组中的日志收集器数量分配防火墙：
   - 单个 — 将转发日志的防火墙分配给日志收集器，如每个收集器组一个专用日志收集器所述。
   - 多个 — 将每个防火墙同时分配给两个日志收集器以便提供冗余。配置首选项时，使用日志收集器 1 拥有防火墙一半的第一优先级，使日志收集器 2 拥有防火墙另一半的第一优先级，如每个收集器组多个专用日志收集器所述。
7. 单击 **OK**（确定）保存对收集器组所作的更改。
8. 选择 **Commit**（提交）> **Commit and Push**（提交并推送），然后将更改 **Commit and Push**（提交并推送）到 Panorama 和添加的收集器组。
9. 选择 **Panorama** > **Managed Collectors**（Panorama > 受管收集器），核实日志收集器配置是否已与 Panorama 同步。

   Configuration Status（配置状态）列应显示 In Sync（同步），Run Time Status（运行时间状态）列应显示 connected（已连接）。

STEP 10 | 配置从防火墙到 Panorama 的日志转发。

使用主要 Panorama 管理服务器对端设备的 Web 界面以：

1. 配置 Panorama 的日志转发。

© 2019 Palo Alto Networks, Inc.

2. 验证 Panorama 日志转发。
3. （可选）配置从 Panorama 到外部目标的日志转发。

使用本地日志收集器部署 Panorama M 系列设备

下图显示了集中日志收集部署中的 Panorama。在这些示例中，Panorama 管理服务器包含了 Panorama 模式下的两个 M 系列设备，两者均部署在主动/被动高可用性 (HA) 配置中。防火墙会将日志发送到每个 Panorama M 系列设备上的预定义（默认）本地日志收集器。如果防火墙生成日志的速率超过 10,000 条/秒，则建议使用此部署。

如果您将多个日志收集器分配到收集器组，请参阅具有多个日志收集器的收集器组的警告了解要求、风险和建议的缓解措施。

在实施此部署后，如果日志记录速率增加超过 *10,000* 条日志/秒，则 *Palo Alto Networks* 建议添加专用日志收集器（日志收集器模式下的 *M* 系列设备），如使用专用日志收集器部署 Panorama所述。这种扩展可能需要从本地日志收集器将防火墙重新分配到专用日志收集器。

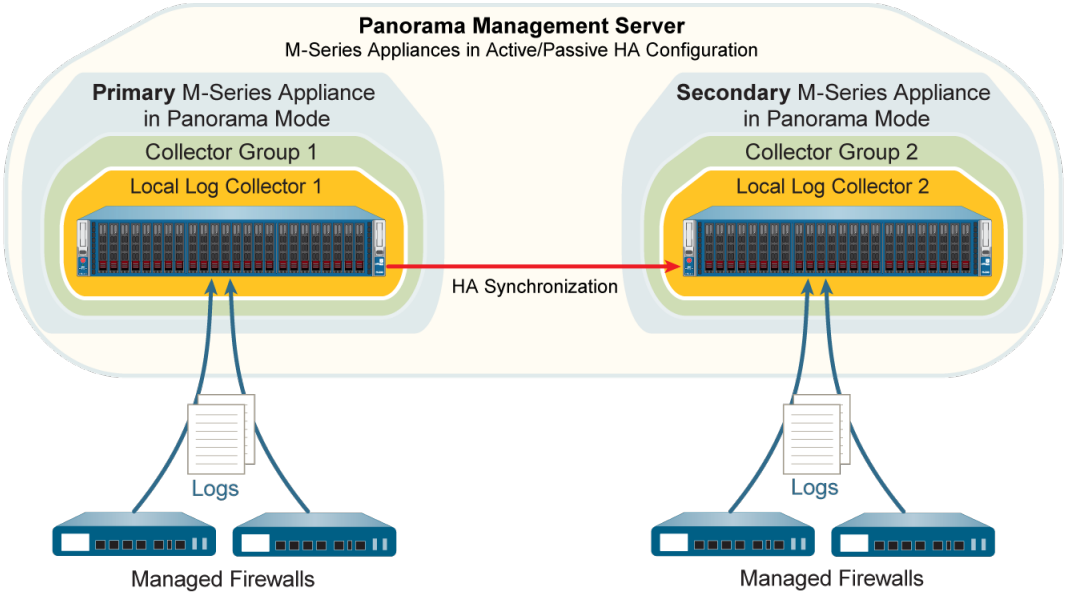


图 **19:** 每个收集器组一个本地日志收集器

© 2019 Palo Alto Networks, Inc.

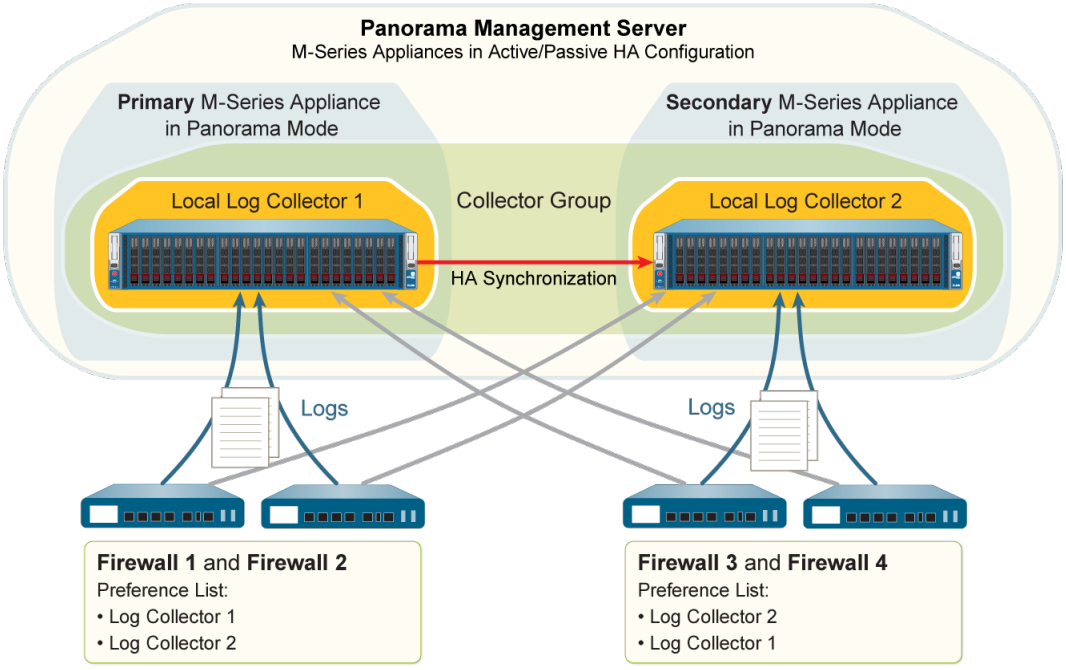


图 **20:** 每个收集器组多个本地日志收集器

执行以下步骤以使用本地日志收集器部署 Panorama。如果您已执行相关步骤（如初始设置），请跳过任何步骤。

STEP 1 | 对每个 M 系列设备执行初始设置。

1. 将 M 系列设备安装到机架上。有关说明，请参阅《M 系列硬件参考指南》。
2. 执行 M 系列设备的初始配置。

   Palo Alto Networks 建议预留管理 *(MGT)* 接口用于 *Panorama* 的管理访问权限，并将单独的 M 系列设备接口专用于其他 *Panorama* 服务。
3. 配置每个阵列。需要执行此任务使 RAID 磁盘可用于日志记录。或者，您可以添加磁盘来增加 M 系列设备上的存储容量。
4. 注册 Panorama 和安装许可证。
5. 安装 Panorama 的内容和软件更新。
6. 设置 Panorama 高可用性。

STEP 2 | 执行以下步骤，使 Panorama 为日志收集做好准备。

1. 按以下方式之一连接到主要 Panorama：
   - 使用串行电缆将计算机与主要 Panorama 上的控制台端口相连。然后，使用终端模拟软件 (9600-8-N-1) 进行连接。
   - 使用终端模拟软件（如 PuTTY），打开您在初始配置中为主要 Panorama 的 MGT 接口指定的 IP 地址的 SSH 会话。
2. 看到提示时登录到 CLI。使用初始配置过程中指定的默认 admin 帐户和密码。
3. 输入以下命令，其中 *<IPaddress2>* 代表辅助 Panorama 的 MGT 接口，使主要 Panorama 连接到辅助 Panorama：

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


© 2019 Palo Alto Networks, Inc.

4. 登录到辅助 Panorama 的 CLI。
5. 输入以下命令，其中 *<IPaddress1>* 代表主要 Panorama 的 MGT 接口，使辅助 Panorama 连接到主要 Panorama：

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

6. 在辅助 Panorama 的命令行界面中，输入以下命令以显示序列号，然后记录它：

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

您需要此序列号将辅助 Panorama 的日志收集器添加为主要 Panorama 的受管收集器。

STEP 3 | 编辑位于主要 Panorama 本地的日志收集器。

使用主要 Panorama 的 Web 界面执行以下步骤：

1. 选择 **Panorama** > **Managed Collectors**（受管收集器），然后选择默认（本地）日志收集器。
2. 选择 **Disks**（磁盘），**Add**（添加）每个日志记录磁盘对。
3. 单击 **OK**（确定）保存更改。

STEP 4 | 配置日志收集器（此收集器位于辅助 Panorama 本地）。

Panorama 将把此本地收集器视为远程设备，因为此收集器并不位于主要 *Panorama* 本地。因此，您必须手动地将它添加到主要 *Panorama* 上。

使用主要 Panorama 的 Web 界面配置受管收集器：

1. 选择 **Panorama** > **Managed Collectors**（Panorama > 受管收集器），然后 **Add**（添加）日志收集器。
2. 输入记录的辅助 Panorama 的日志收集器的序列号（**Collector S/N**（收集器序列号））。
3. 在 **Panorama Server IP**（**Panorama** 服务器 **IP**）字段和 **Panorama Server IP 2**（**Panorama** 服务器 **IP 2**）字段中，输入主要和辅助 Panorama 高可用性对端设备的 IP 地址或 FQDN。

   以下字段均为必填字段。
4. 选择 **Interfaces**（接口）并配置日志收集器将使用的每个接口。**Management**（管理）接口为必选项。为每个接口执行以下步骤：
   1. 单击接口名称。
   2. 根据您网络的 IP 协议，配置以下一个或两个字段集。

      IPv4 — **IP Address**（**IP** 地址）、**Netmask**（子网掩码）和 **Default Gateway**（默认网关）

      IPv6 — **IPv6 Address/Prefix Length**（**IPv6** 地址/前缀长度）和 **Default IPv6 Gateway**（默认 **IPv6** 网关）
   3. （仅限管理接口）如果您将使用 SNMP 管理器监控日志收集器统计信息，请选择 **SNMP**。

      除了配置日志收集器之外，使用 SNMP 还需要执行其他步骤（请参阅使用 SNMP 监视 Panorama 和日志收集器统计信息）。
   4. 单击 **OK**（确定）保存对接口所作的更改。
5. 单击 **OK**（确定）保存对日志收集器所作的更改。
6. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

   必须执行此步骤才能启用日志记录磁盘。
7. 通过单击其名称编辑日志收集器。
8. 选择 **Disks**（磁盘），**Add**（添加）每个 RAID 磁盘对，然后单击 **OK**（确定）。

© 2019 Palo Alto Networks, Inc.

9. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

STEP 5 | 添加防火墙作为受管设备。

使用主要 Panorama 的 Web 界面为每个将日志转发到日志收集器的防火墙执行此任务。

STEP 6 | 编辑在主要 Panorama 上预定义的默认收集器组。

使用主要 Panorama 的 Web 界面配置收集器组：

1. 选择 **Panorama** > **Collector Groups**（收集器组），然后选择 **default**（默认）收集器组。
2. 如果您将多个日志收集器添加到单个收集器组，请将辅助 Panorama 的本地日志收集器 **Add**（添加）到收集器组成员列表。默认情况下，由于主要 Panorama 的本地日志收集器已预先分配到默认收集器组，因此该列表将显示本地日志收集器。

   在任何单个收集器组中，所有日志收集器均必须在相同的 *Panorama* 型号上运行：均为 *M-600* 设备、均为 *M-500* 设备、均为 *M-200* 设备或均为 *Panorama* 虚拟设备。
3. （最佳做法）如果将多个日志收集器添加到单个收集器组，请 **Enable log redundancy across collectors**（启用跨收集器记录冗余）。此选项要求每个日志收集器具有相同数量的日志记录磁盘。
4. （可选）如果您将使用 SNMP 来监控日志收集器的统计信息和陷阱，请选择 **Monitoring**（监控）并配置设置。
5. 选择 **Device Log Forwarding**（设备日志转发）并配置日志转发首选项列表。此列表定义哪些防火墙将日志转发到哪些日志收集器。根据此收集器组中的日志收集器数量分配防火墙：
   - 单个 — 将转发日志的防火墙分配给主要 Panorama 的本地日志收集器，如每个收集器组一个本地日志收集器所述。
   - 多个 — 将每个防火墙同时分配给两个日志收集器以便提供冗余。配置首选项时，使用日志收集器 1 拥有防火墙一半的第一优先级，使日志收集器 2 拥有防火墙另一半的第一优先级，如每个收集器组多个本地日志收集器所述。
6. 单击 **OK**（确定）保存更改。

STEP 7 | 配置包含辅助 Panorama 的日志收集器的收集器组。

如果每个收集器组都只具有一个日志收集器，则必须执行此流程。

使用主要 Panorama 的 Web 界面配置收集器组：

1. 选择 **Panorama** > **Collector Groups**（Panorama > 收集器组），然后 **Add**（添加）所需的收集器组。
2. 输入 **Name**（名称）以标识收集器组。
3. 将辅助 Panorama 的本地日志收集器 **Add**（添加）到收集器组成员列表。
4. （可选）如果您将使用 SNMP 管理器来监控日志收集器的统计信息和陷阱，请选择 **Monitoring**（监控）并配置设置。
5. 选择 **Device Log Forwarding**（设备日志转发）并将条目 **Add**（添加）到日志转发首选项列表：
   1. **Modify**（修改）设备列表，选择将日志转发到辅助 Panorama 的本地日志收集器的防火墙（请参阅每个收集器组一个本地日志收集器），然后单击 **OK**（确定）。
   2. 将辅助 Panorama 的本地日志收集器 **Add**（添加）到收集器列表，然后单击 **OK**（确定）。
6. 单击 **OK**（确定）保存更改。

STEP 8 | 将更改提交并推送到 Panorama 配置和收集器组。

在主要 Panorama 的 Web 界面中，选择 **Commit**（提交）> **Commit and Push**（提交并推送），然后将更改 **Commit and Push**（提交并推送）到 Panorama 和添加的收集器组。

STEP 9 | 手动执行故障转换，使辅助 Panorama 变成主动。

使用主要 Panorama 的 Web 界面执行以下步骤：

© 2019 Palo Alto Networks, Inc.

1. 选择 **Panorama** > 高可用性。
2. 单击 Operational Commands（操作命令）部分中的 **Suspend local Panorama**（挂起本地 **Panorama**）。

STEP 10 | 在辅助 Panorama 上，将日志收集器的网络设置本地配置为主要 Panorama。

使用辅助 Panorama 的 Web 界面执行以下步骤：

1. 在 Panorama Web 界面中，选择 **Panorama** > **Managed Collectors**（受管收集器），并选择主要 Panorama 的本地日志收集器。
2. 在 **Panorama Server IP**（**Panorama** 服务器 **IP**）字段和 **Panorama Server IP 2**（**Panorama** 服务器 **IP 2**）字段中，输入主要和辅助 Panorama 高可用性对端设备的 IP 地址或 FQDN。

   以下字段均为必填字段。
3. 选择 **Interfaces**（接口），单击 **Management**（管理），然后使用主要 Panorama 的 MGT 接口值填写下列一个或两个字段集（根据您网络的 IP 协议）：
   - **IPv4** — **IP Address**（**IP** 地址）、**Netmask**（子网掩码）和 **Default Gateway**（默认网关）
   - **IPv6** — **IPv6 Address/Prefix Length**（**IPv6** 地址/前缀长度）和 **Default IPv6 Gateway**（默认 **IPv6** 网关）
4. 单击 **OK**（确定）保存更改。
5. 选择 **Commit**（提交）> **Commit and Push**（提交并推送），然后将更改 **Commit and Push**（提交并推送）到 Panorama 和添加的收集器组。

STEP 11 | 手动执行故障回复，使主要 Panorama 变成主动。

使用辅助 Panorama 的 Web 界面执行以下步骤：

1. 选择 **Panorama** > 高可用性。
2. 单击 Operational Commands（操作命令）部分中的 **Suspend local Panorama**（挂起本地 **Panorama**）。

STEP 12 | 配置从防火墙到 Panorama 的日志转发。

使用主要 Panorama 的 Web 界面以：

1. 配置 Panorama 的日志转发。
2. 验证 Panorama 日志转发。
3. （可选）配置从 Panorama 到外部目标的日志转发。



您可以将单独的外部服务器配置文件分配给每个 *Panorama* 高可用性对端设备。例如，您可能想要让每一个对端设备都向不同的 *syslog* 服务器转发日志。要让每一个 *Panorama* 高可用性对端设备向不同的外部设备转发日志，则登录到每个对端设备的 *Web* 界面，选择 *Panorama* > *Collector Groups*（*Panorama* > 收集器组），选择此收集器组，选择 *Collector Log Forwarding*（收集器日志转发），分配服务器配置文件，然后单击 *OK*（确定）。

使用本地日志收集器部署 Panorama 虚拟设备

您可以将防火墙配置为将日志发送到在 Panorama 模式下的 Panorama 虚拟设备上本地运行的日志收集器。在高可用性 (HA) 配置中，每个 Panorama HA 对端设备都可以拥本地日志收集器。您可以将 HA 对端设备上的本地日志收集器分配给相同的收集器组或单独的收集器组，如下图所示。在 VMware 虚拟架构中使用本地日志收集器部署 Panorama 虚拟设备时，请参阅设置 Panorama 虚拟设备的前提条件查看支持的每秒日志数。



如果您将多个日志收集器分配到收集器组，请参阅具有多个日志收集器的收集器组的警告了解要求、风险和建议的缓解措施。

© 2019 Palo Alto Networks, Inc.

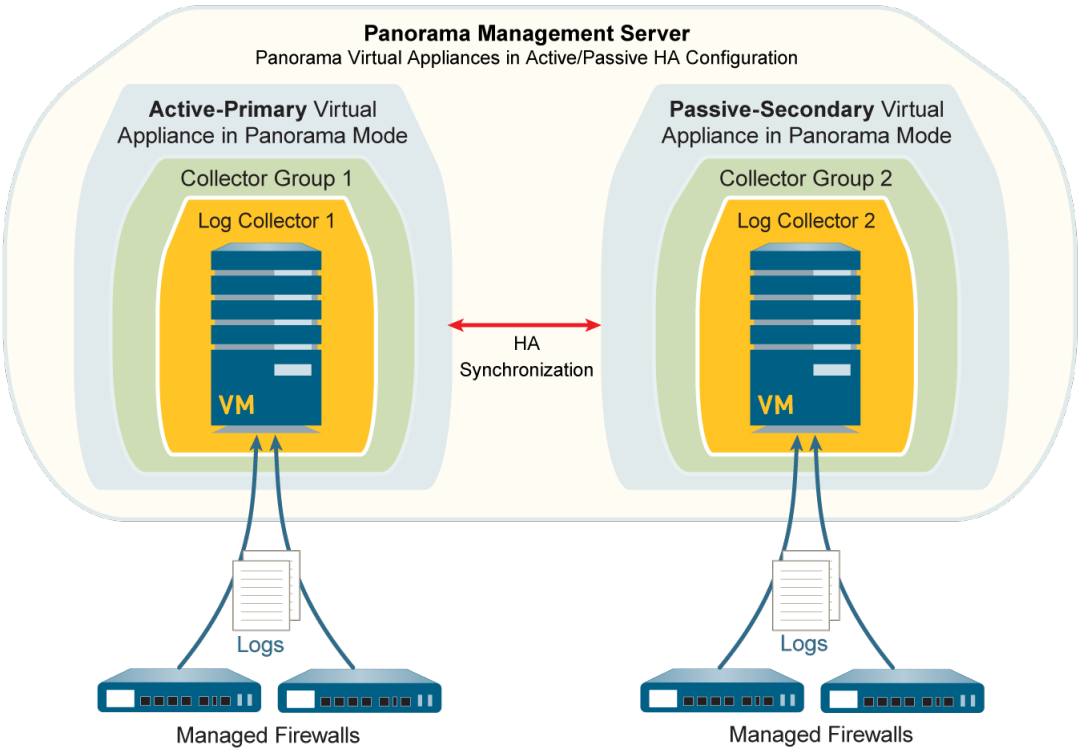


图 21: 每个收集器组一个日志收集器

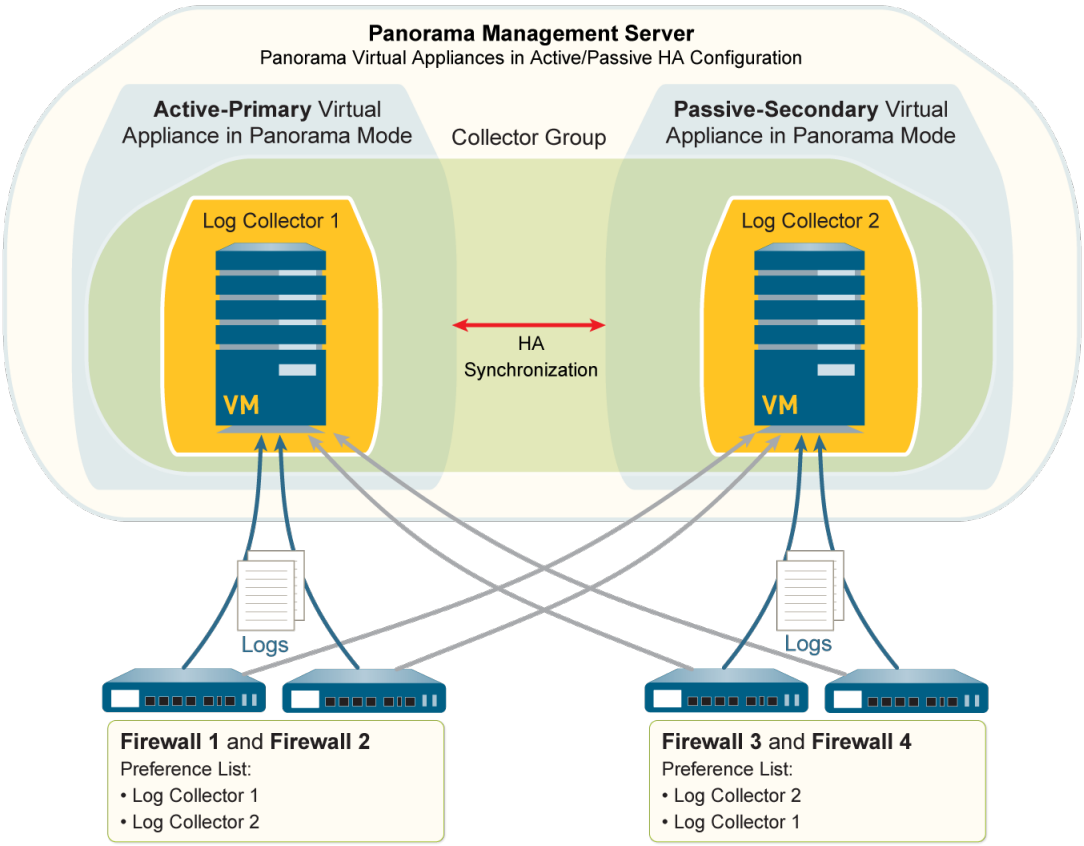


图 22: 每个收集器组多个日志收集器

© 2019 Palo Alto Networks, Inc.

执行以下步骤以使用本地日志收集器部署 Panorama。如果您已执行相关步骤（如初始设置），请跳过任何步骤。

STEP 1 | 对每个 Panorama 虚拟设备执行初始设置。

1. 安装 Panorama 虚拟设备。您必须配置以下资源以确保虚拟设备以 Panorama 模式启动：
   - 刚好具有 81GB 存储容量的系统磁盘。
   - 对 Panorama 将接收和存储的日志数量而言足够的 CPU 和内存。
   - 具有 2-24TB 存储容量的虚拟日志记录磁盘。

   Panorama 会自动将新磁盘分成 *2TB* 分区，每个分区将作为单独的虚拟磁盘。
2. 执行 Panorama 虚拟设备的初始配置。
3. 注册 Panorama 和安装许可证。
4. 安装 Panorama 的内容和软件更新。

STEP 2 | 在 HA 配置中设置 Panorama 虚拟设备。

1. 设置 Panorama 高可用性。
2. 测试 Panorama HA 故障转移。

STEP 3 | 添加位于主要 Panorama 本地的日志收集器。

在主要 Panorama 上：

1. 记录 Panorama 序列号。
   1. 访问 Panorama Web 界面。
   2. 选择 **Dashboard**（仪表盘），并记录 General Information（一般信息）部分中的 **Serial #**（序列号）。
2. 将日志收集器添加为受管收集器。
   1. 选择 **Panorama** > **Managed Collectors**（受管收集器），然后 **Add**（添加）新的日志收集器。
   2. 在 **General**（常规）设置中，输入为 Panorama 记录的序列号（**Collector S/N**（收集器序列号））。
   3. 单击 **OK**（确定）保存更改。
   4. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**）。

      必须执行此步骤才能添加虚拟日志记录磁盘。
3. 添加虚拟日志记录磁盘。
   1. 选择 **Panorama** > **Managed Collectors**（受管收集器），然后通过单击其名称编辑日志收集器。

      日志收集器名称具有与主要 Panorama 的主机名相同的值。
   2. 选择 **Disks**（磁盘）并 **Add**（添加）虚拟日志记录磁盘。
   3. 单击 **OK**（确定）保存更改。
   4. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**）。

STEP 4 | 添加位于辅助 Panorama 本地的日志收集器。

Panorama 将此日志收集器视为远程设备，因为它并不位于主要 *Panorama* 本地。

1. 记录辅助 Panorama 的序列号。
   1. 访问辅助 Panorama 的 Web 界面。

© 2019 Palo Alto Networks, Inc.

2. 选择 **Dashboard**（仪表盘），并记录 General Information（一般信息）部分中的 **Serial #**（序列号）。
2. 访问主要 Panorama 的 Web 界面。
3. 选择 **Panorama** > **Managed Collectors**（Panorama > 受管收集器），然后 **Add**（添加）日志收集器。
4. 在 **General**（常规）设置中，输入为辅助 Panorama 记录的序列号（**Collector S/N**（收集器序列号））。
5. 在 **Panorama Server IP**（**Panorama** 服务器 **IP**）字段和 **Panorama Server IP 2**（**Panorama** 服务器 **IP 2**）字段中，输入主要和辅助 Panorama 高可用性对端设备的 IP 地址或 FQDN。

   以下字段均为必填字段。
6. 单击 **OK**（确定）保存对日志收集器所作的更改。
7. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

   必须执行此步骤才能添加虚拟日志记录磁盘。
8. 通过单击其名称编辑日志收集器。

   日志收集器名称具有与辅助 Panorama 的主机名相同的值。
9. 选择 **Disks**（磁盘），**Add**（添加）虚拟日志记录磁盘，然后单击 **OK**（确定）。
10. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

STEP 5 | 添加防火墙作为受管设备。

使用主要 Panorama 为每个将日志转发到日志收集器的防火墙执行此任务。

STEP 6 | 配置收集器组。

如果您将两个日志收集器分配到同一收集器组，则执行此步骤一次。否则，请为每个日志收集器配置一个收集器组。

在主要 Panorama 上：

1. 选择 **Panorama** > **Collector Groups**（收集器组），然后 **Add**（添加）所需的收集器组。
2. **Add**（添加）一个或两个日志收集器作为收集器组成员。

   在任何单个收集器组中，所有日志收集器均必须在相同的 *Panorama* 型号上运行：均为 *M-600* 设备、均为 *M-500* 设备、均为 *M-200* 设备或均为 *Panorama* 虚拟设备。
3. （最佳做法）如果将多个日志收集器添加到单个收集器组，请 **Enable log redundancy across collectors**（启用跨收集器记录冗余）。此选项要求每个日志收集器具有相同数量的虚拟日志记录磁盘。

   启用冗余会使收集器组中的日志数量和日志处理流量增加一倍。如有需要，扩展 Panorama 虚拟设备上的日志存储容量。
4. 选择 **Device Log Forwarding**（设备日志转发）并配置日志转发首选项列表。此列表定义哪些防火墙将日志转发到哪些日志收集器。根据此收集器组中的日志收集器数量分配防火墙：
   - 单个 — 将转发日志的防火墙分配给主要 Panorama 的本地日志收集器，如每个收集器组一个本地日志收集器所述。
   - 多个 — 将每个防火墙同时分配给两个日志收集器以便提供冗余。配置首选项列表时，使用日志收集器 1 拥有防火墙一半的第一优先级，使日志收集器 2 拥有防火墙另一半的第一优先级，如每个收集器组多个日志收集器所述。
5. 单击 **OK**（确定）保存更改。
6. 选择 **Commit**（提交）> **Commit and Push**（提交并推送），然后将更改 **Commit and Push**（提交并推送）到 Panorama 和添加的收集器组。

STEP 7 | 在主要 Panorama 上触发故障转移，使辅助 Panorama 变成主动。

在主要 Panorama 上：

© 2019 Palo Alto Networks, Inc.

1. 选择 **Panorama** > 高可用性。
2. 单击 Operational Commands（操作命令）部分中的 **Suspend local Panorama**（挂起本地 **Panorama**）。

STEP 8 | 配置从辅助 Panorama 到主要 Panorama 的本地日志收集器的连接。

在辅助 Panorama 上：

1. 在 Panorama Web 界面中，选择 **Panorama** > **Managed Collectors**（受管收集器），并选择主要 Panorama 的本地日志收集器。
2. 在 **Panorama Server IP**（**Panorama** 服务器 **IP**）字段和 **Panorama Server IP 2**（**Panorama** 服务器 **IP 2**）字段中，输入主要和辅助 Panorama 高可用性对端设备的 IP 地址或 FQDN。

   以下字段均为必填字段。
3. 单击 **OK**（确定）保存更改。
4. 选择 **Commit**（提交）> **Commit and Push**（提交并推送），然后将更改 **Commit and Push**（提交并推送）到 Panorama 和收集器组。

STEP 9 | 在辅助 Panorama 上触发故障转移，使主要 Panorama 变成主动。

在辅助 Panorama 上：

1. 选择 **Panorama** > 高可用性。
2. 单击 Operational Commands（操作命令）部分中的 **Suspend local Panorama**（挂起本地 **Panorama**）。

STEP 10 | 配置从防火墙到 Panorama 的日志转发。

在主要 Panorama 上：

1. 从防火墙配置 Panorama 的日志转发
2. 验证 Panorama 日志转发。

使用本地日志收集器在传统模式下部署 Panorama 虚拟设备

下图显示了集中日志收集部署中的 Panorama。在本例中，Panorama 管理服务器包含处于传统模式下的两台 Panorama 虚拟设备，两者均部署在主动/被动高可用性 (HA) 配置中。此配置适合用于 Panorama 在其中每秒最多处理 10,000 条日志的 VMware 虚拟基础架构内的防火墙管理。防火墙将日志发送到 Panorama 管理服务器上的 NFS 数据存储（仅限 ESXi 服务器）或虚拟磁盘。默认情况下，主动和被动对端设备都会接收日志，但您可以修改日志转发和缓冲默认设置，从而仅让主动对端设备接收日志。对于 5200 和 7000 系列防火墙，仅主动对等设备会接收日志。默认情况下，处于传统模式下的 Panorama 虚拟设备使用大约 11GB 的其内部磁盘分区来存储日志，但必要时也可以扩展 Panorama 虚拟设备上的日志存储容量。



如果日志记录速率增加超过 *10,000* 条日志/秒，则建议使用专用日志收集器部署 Panorama。

© 2019 Palo Alto Networks, Inc.

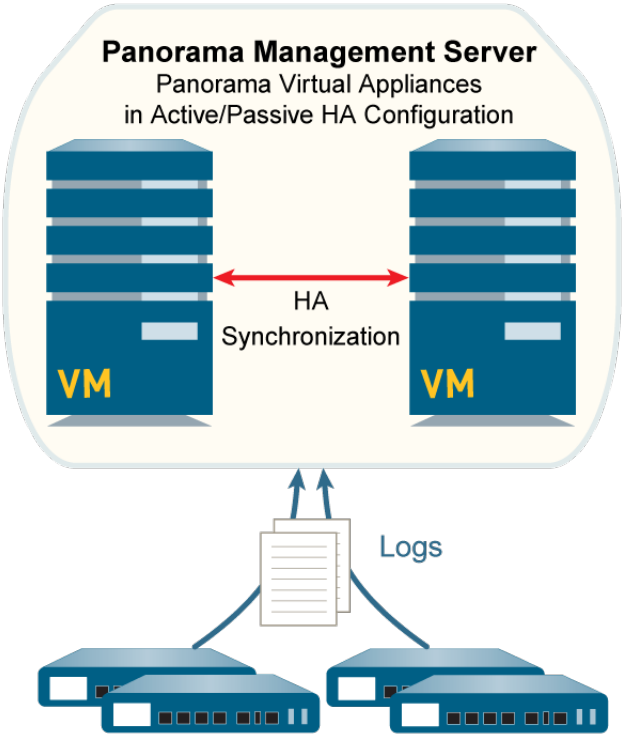


图 **23:** 传统模式下的 **Panorama** 虚拟设备与本地日志收集

执行以下步骤以使用本地日志收集部署 Panorama 虚拟设备。如果您已执行相关步骤（如初始设置），请跳过任何步骤。

STEP 1 | 对每个 Panorama 虚拟设备执行初始设置。

1. 安装 Panorama 虚拟设备。要确保虚拟设备在 Panorama 模式下启动，请不要在安装过程中添加虚拟日志记录磁盘。

   默认情况下，*Panorama* 在其系统磁盘上使用 *11GB* 分区进行日志存储。如果您需要更多的存储空间，可以在安装后添加最多 *8TB* 的专用虚拟日志记录磁盘。

2. 执行 Panorama 虚拟设备的初始配置。
3. 注册 Panorama 和安装许可证。
4. 安装 Panorama 的内容和软件更新。

STEP 2 | 在 HA 配置中设置 Panorama 虚拟设备。

1. 设置 Panorama 高可用性。
2. 测试 Panorama HA 故障转移。

STEP 3 | 执行以下步骤，使 Panorama 为日志收集做好准备。

1. 对于每个将转发日志到 Panorama 的防火墙，添加防火墙作为受管设备。
2. 配置 Panorama 的日志转发。

STEP 4 | 提交更改。

选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

管理 *Wildfire* 设备

您可以使用 Panorama M 系列或虚拟设备集中管理多达 200 个独立的 WildFire 设备和 WildFire 设备群集节点。与使用本地 CLI 单独管理 WildFire 设备和设备群集相比，使用 Panorama 可以集中管理和监控多个设备和设备群集。集中管理使您能够将常见配置、配置更新和软件升级推送到全部或部分受管 WildFire 设备，从而可以轻松确保 WildFire 设备和设备群集具有一致的配置。

使用 Panorama 管理 WildFire 设备集群时，Panorama 必须运行与受管 WildFire 设备相同或更高的版本。

> 添加独立 WildFire 设备以使用 Panorama 进行管理
> 在 Panorama 上配置基本 WildFire 设备设置
> 在 WildFire 设备和集群上使用自定义证书设置身份验证
> 从 Panorama 管理中删除 WildFire 设备
> 管理 WildFire 集群

添加独立 WildFire 设备以使用 Panorama 进行管理

您可以使用 Panorama M 系列或虚拟设备最多管理 200 个 WildFire 设备。200 个 WildFire 设备限制是独立设备和 WildFire 设备群集节点的总和（如果您也在 Panorama 上配置群集和添加节点）。

确保 Panorama 至少运行 8.0.1 版，并且添加到 Panorama 的任何 WildFire 设备至少也运行 8.0.1 版。

STEP 1 | 使用本地 CLI，验证您想要使用 Panorama 管理的每个 WildFire 设备是否运行 PAN-OS 8.0.1 版或更高版本。

```
admin@qa16> show system info | match version
sw-version: 8.0.1-c45
wf-content-version: 702-283
logdb-version: 8.0.15
```

STEP 2 | 在您希望用于管理 WildFire 设备的每个 Panorama 设备上，验证 Panorama 是否运行 8.0.1 版或更高版本：

Dashboard（仪表盘）> **General Information**（一般信息）> **Software Version**（软件版本）显示正在运行的软件版本。

STEP 3 | 如果您不确定 WildFire 设备是否属于 WildFire 设备群集或是否为本地 WildFire 设备 CLI 上的独立设备，请检查 **Node mode** 以确保状态为 **stand_alone**，并检查 **Application status** 以确保 **global-db-service** 和 **global-queue-service** 指示 **ReadyStandalone**。

```
admin@WF-500> show cluster membership
Service Summary:  wfpc signature
Cluster name:
Address:          10.10.10.100
Host name:        WF-500
Node name:        wfpc-012345678901-internal
Serial number:    012345678901
Node mode:     stand_alone
Server role:      True
HA priority:
Last changed:     Mon, 06 Mar 2017 16:34:25 -0800
Services:         wfcore signature wfpc infra
Monitor status:
                  Serf Health Status: passing
                      Agent alive and reachable
Application status:
                  global-db-service: ReadyStandalone
        wildfire-apps-service: Ready
        global-queue-service: ReadyStandalone
        wildfire-management-service: Done
        siggen-db: ReadyMaster
Diag report:
                  10.10.10.100: reported leader '10.10.10.100', age 0.
                  10.10.10.100: local node passed sanity check.
```


© 2019 Palo Alto Networks, Inc.

STEP 4 | 如果您希望使用 Panorama 管理的 WildFire 设备是新设备，请检查开始使用 WildFire 以确保您完成基本步骤，例如确认您的 WildFire 许可证处于活动状态，启用日志记录，并将防火墙连接到 WildFire 设备以及配置基本 WildFire 功能。

STEP 5 | 在 Panorama 服务器将管理的每个 WildFire 设备的本地 CLI 上，配置 Panorama 服务器的 IP 地址。

在将独立 WildFire 设备注册到 Panorama 设备之前，必须先在每个 WildFire 设备上配置 Panorama IP 地址或 FQDN。这就是每个 WildFire 设备知道 Panorama 设备管理它的方式。

1. 配置主要 Panorama 设备管理接口的 IP 地址或 FQDN：

```
admin@WF-500# set deviceconfig system panorama-server <ip-address | FQDN>
```

2. 如果您使用备份 Panorama 设备获得高可用性（推荐），请配置备份 Panorama 设备管理接口的 IP 地址或 FQDN：

```
admin@WF-500# set deviceconfig system panorama-server-2 <ip-address |
 FQDN>
```

STEP 6 | 在主要 Panorama 设备上注册 WildFire 设备。

1. 在 Panorama web 界面中，选择 **Panorama** > **Managed WildFire Appliances**（受管 **WildFire** 设备）并 **Add Appliance**（添加设备）。
2. 在单独的行中输入每个 WildFire 设备的序列号。如果您没有序列号列表，请在每个 WildFire 设备上运行：

```
admin@WF-500> show system info | match serial
serial: 012345678901
```

几个本地 CLI 命令显示 WildFire 设备序列号，包括 **show cluster membership**。

3. 单击 **OK**（确定）。

如果可用，则会显示有关 WildFire 设备上已提交的配置的信息，例如 IP 地址和软件版本。

STEP 7 | （可选）将 WildFire 设备配置导入 Panorama 设备。

1. 从受管 WildFire 设备列表中选择要导入配置的设备。
2. **Import Config**（导入配置）。
3. 选择 **Yes**（是）。

导入配置会更新显示的信息，并使导入的配置成为 Panorama 设备待选配置的一部分。

4. **Commit to Panorama**（提交到 **Panorama**）使导入的 WildFire 设备配置成为 Panorama 运行配置的一部分。

STEP 8 | 配置或确认 WildFire 设备接口的配置。

每个 WildFire 设备拥有四个接口：**Management**（管理）(Ethernet0)、**Analysis Network Environment**（分析网络环境）(Ethernet1)、**Ethernet2** 和 **Ethernet3**。

1. 选择 **Panorama** > **Managed WildFire Appliances**（受管 **WildFire** 设备），并选择 WildFire 设备。
2. 选择 **Interfaces**（接口）。
3. 选择用于进行配置或编辑的接口。您可以启用接口，并设置每个接口的速度和双工、IP 地址和网络掩码、默认网关、MTU、DNS 服务器、链接状态和 **Management Services**（管理服务）。您也可以 **Add**（添加）允许的 IP 地址，以便接口只接受来自指定地址的流量。

© 2019 Palo Alto Networks, Inc.

Analysis Network Environment（分析网络环境）、**Ethernet2** 和 **Ethernet3** 接口仅支持 **Ping** 作为 **Management Services**（管理服务）选项。

Management（管理）接口支持 **Ping**、**SSH** 和 **SNMP** 作为 **Management Services**（管理服务）选项。此外，**Management**（管理）接口支持代理服务器配置以防止无法直接连接到互联网。

4. 在配置或确认设置后，单击 **Ok**（确定）。

STEP 9 | 在 Panorama 设备上提交配置并将其推送到设备或多个设备。

1. **Commit and Push**（提交并推送）。
2. 如果 Panorama 设备上有不想推送的配置，**Edit Selections**（编辑选择）以选择您要推送配置的设备。推送的配置将覆盖 WildFire 设备上的运行配置。

STEP 10 | 验证配置。

1. 选择 **Panorama** > **Managed WildFire Appliances**（受管 **WildFire** 设备）。
2. 检查以下字段：
   - **Connected**（已连接）— 状态为 **Connected**（已连接）。
   - **Role**（角色）— 每个 WildFire 设备的角色 **Standalone**（独立）。
   - **Config Status**（配置状态）— 状态为 `In Sync`。
   - **Last Commit State**（最后提交状态）— `Commit succeeded`。

© 2019 Palo Alto Networks, Inc.

在 Panorama 上配置基本 WildFire 设备设置

配置基本设置（例如内容更新和 WildFire 云服务器、WildFire 云服务、日志记录、身份验证等），与在 Panorama 上配置常规群集设置的方式类似。无需选择群集并配置群集上的设置，选择 WildFire 设备并配置该设备的各个设置。选择并配置您添加到 Panorama 的每个 WildFire 设备。

配置 WildFire 设备介绍如何将 WildFire 设备集成到网络中并使用 CLI 执行基本设置，但这些概念与使用 Panorama 执行基本设置相同。



许多设置都已预先填入默认值，*WildFire* 设备上先前现有设置的信息或将 *WildFire* 设备添加到 *Panorama* 时配置的设置。

- 为 WildFire 设备配置身份验证

为 WildFire 设备配置身份验证

通过配置具有精细身份验证参数的本地管理用户，以及利用 RADIUS、TACAS+ 或 LDAP 进行授权和身份验证，为您的 WildFire 设备创建和配置增强的身份验证。

当您从 Panorama 配置和推送管理员时，将使用您在 Panorama 上配置的管理员覆盖 WildFire 设备上的现有管理员。

- 为 WildFire 设备配置管理员帐户
- 为 WildFire 设备配置 RADIUS 身份验证
- 为 WildFire 设备配置 TACACS+ 身份验证
- 为 WildFire 设备配置 LDAP 身份验证

为 *WildFire* 设备配置管理员帐户

为您的 WildFire 设备创建一个或多个具有精细身份验证参数的管理员，以便从 Panorama™ 管理服务器进行管理。此外，还可以从 Panorama 配置本地管理员，这可以在 WildFire 设备的 CLI 上直接进行配置。但是，向 WildFire 设备推送新配置更改会使用为 WildFire 设备配置的管理员覆盖现有本地管理员。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 添加独立 WildFire 设备以使用 Panorama 进行管理。

STEP 3 | （可选）配置身份验证配置文件以定义身份验证服务，该服务验证访问 WildFire 设备 CLI 的管理员的登录凭据。

STEP 4 | 根据需要配置一个或多个管理员帐户。

在 Panorama 上创建的管理员帐户之后会导入到 WildFire 设备并从 Panorama 进行管理。

STEP 5 | 为 WildFire 设备配置身份验证。

1. 选择 **Panorama** > **Managed WildFire Appliances**（受管 **WildFire** 设备），然后选择您之前添加的 WildFire 设备。
2. （可选）选择您在上一步中配置的 **Authentication Profile**（身份验证配置文件）。
3. 为 WildFire 设备配置身份验证 **Timeout Configuration**（超时配置）。
    1. 输入 **Failed Attempt**（失败尝试）次数，在此次数之后用户将被锁定在 WildFire 设备 CLI 之外。
    2. 输入 **Lockout Time**（锁定时间）（以分钟为单位），此时间即在用户达到配置的 **Failed Attempts**（失败尝试）次数后，WildFire 设备锁定用户帐户的时间。
    3. 输入 **Idle Timeout**（空闲超时）（以分钟为单位），在此时间之后用户会因为不活动而自动注销。

© 2019 Palo Alto Networks, Inc.

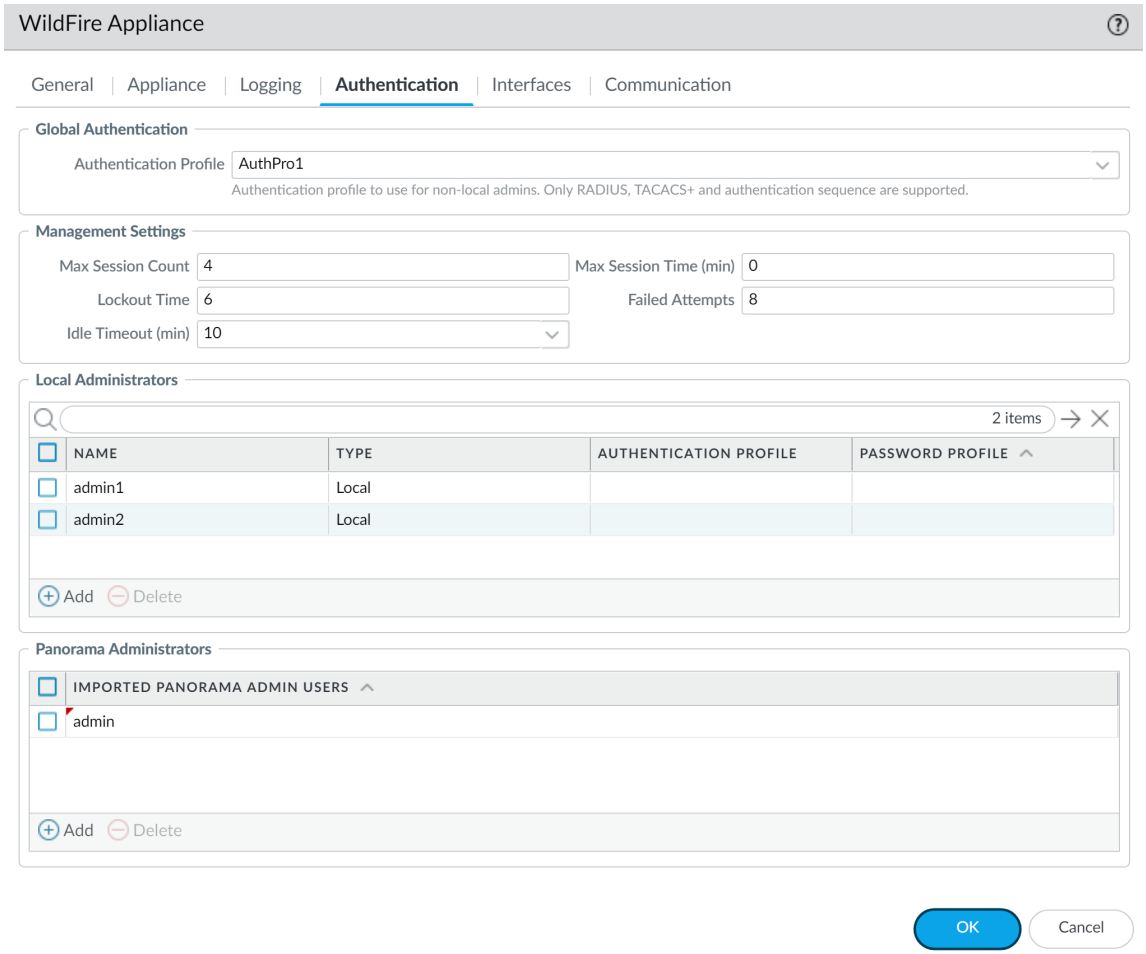
4. 输入 **Max Session Count**（最大会话计数）以设置多少用户帐户可以同时访问 WildFire 设备。
5. 输入管理员在自动注销之前可登录的 **Max Session Time**（最长会话时间）。

4. 添加 WildFire 设备管理员。

   管理员可以添加为本地管理员或作为导入的 Panorama 管理员 — 但不能同时为二者。不支持将同一管理员同时添加为本地管理员和作为导入的 Panorama 管理员，这会导致 Panorama 提交失败。例如，如果您将 **admin1** 同时添加为本地和 Panorama 管理员，向 Panorama 的提交将会失败。

   1. **Add**（添加）并配置专属于 WildFire 设备的新管理员。这些管理员特定于为其创建的 WildFire 设备，您可以从此表格管理这些管理员。
   2. **Add**（添加）在 Panorama 上配置的任何管理员。这些管理员在 Panorama 上创建，并导入至 WildFire 设备。

5. 单击 **OK**（确定）以保存 WildFire 设备身份验证配置。



STEP 6 | **Commit**（提交），然后 **Commit and Push**（提交并推送）您的配置更改。

STEP 7 | 使用本地管理员用户访问 WildFire 设备 CLI 以验证您能够成功访问 WildFire 设备。

为 *WildFire* 设备配置 *RADIUS* 身份验证

使用 RADIUS 服务器来验证对 WildFire 设备 CLI 的管理访问权限。您也可以在 RADIUS 服务器上定义供应商特定属性 (VSA) 来管理管理员授权。使用 VSA 使您能够通过目录服务来快速更改管理员的角色、访问域和用户组，这通常比在 Panorama™ 管理服务器上重新配置设置更为容易。

© 2019 Palo Alto Networks, Inc.

您可以将 Palo Alto Networks RADIUS 词典导入到 *RADIUS* 服务器，以定义实现 *Panorama* 和 *RADIUS* 服务器之间通信的身份验证属性。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 添加独立 WildFire 设备以使用 Panorama 进行管理。

STEP 3 | 配置 RADIUS 身份验证。

1. 添加 RADIUS 服务器配置文件。

   配置文件定义了 WildFire 设备连接到 RADIUS 服务器的方式。

   1. 选择 **Panorama** > **Server Profiles**（服务器配置文件）> **RADIUS**，并 **Add**（添加）配置文件。
   2. 输入 **Profile Name**（配置文件名称）以标识服务器配置文件。
   3. 输入身份验证请求超时后以秒为单位的 **Timeout**（超时）（默认为 3；范围为 1-20）。
   4. 选择 WildFire 设备用来对 RADIUS 服务器进行身份验证的 **Authentication Protocol**（身份验证协议）（默认为 **CHAP**）。

      如果 *RADIUS* 服务器支持该协议，请选择 *CHAP*；该协议比 *PAP* 更安全。

   5. **Add**（添加）每个 RADIUS 服务器，并输入以下内容：
      1. 标识服务器的 **Name**（名称）。
      2. **RADIUS Server**（**RADIUS** 服务器）IP 地址或 FQDN。
      3. **Secret**（密钥）/**Confirm Secret**（确认密钥）（加密用户名和密码的密钥）。
      4. 用于身份验证请求的服务器 **Port**（端口）（默认为 1812）。
   6. 单击 **OK**（确定）保存服务器配置文件。
2. 将 RADIUS 服务器配置文件分配到身份验证配置文件。

   身份验证配置文件定义了一组管理员通用的身份验证设置。

   1. 选择 **Panorama** > **Authentication Profile**（身份验证配置文件），并 **Add**（添加）配置文件。
   2. 输入 **Name**（名称）以标识身份验证配置文件。
   3. 将 **Type**（类型）设置为 **RADIUS**。
   4. 选择您配置的 **Server Profile**（服务器配置文件）。
   5. 选择 **Retrieve user group from RADIUS**（从 **RADIUS** 中检索用户组），以从 RADIUS 服务器上定义的 VSA 收集用户组信息。

      Panorama 与您在身份验证配置文件允许列表中指定的组在组信息方面进行匹配。
   6. 选择 **Advanced**（高级），并在允许列表中 **Add**（添加）允许使用此身份验证配置文件进行身份验证的管理员。
   7. 单击 **OK**（确定）保存身份验证配置文件。

STEP 4 | 为 WildFire 设备配置身份验证。

1. 选择 **Panorama** > **Managed WildFire Appliances**（受管 **WildFire** 设备），然后选择您之前添加的 WildFire 设备。
2. 选择您在上一步中配置的 **Authentication Profile**（身份验证配置文件）。

   如果没有分配全局身份验证配置文件，您必须为每个单独的本地管理员分配一个身份验证配置文件才能利用远程身份验证。
3. 为 WildFire 设备配置身份验证 **Timeout Configuration**（超时配置）。
   1. 输入 **Failed Attempt**（失败尝试）次数，在此次数之后用户将被锁定在 WildFire 设备 CLI 之外。

© 2019 Palo Alto Networks, Inc.

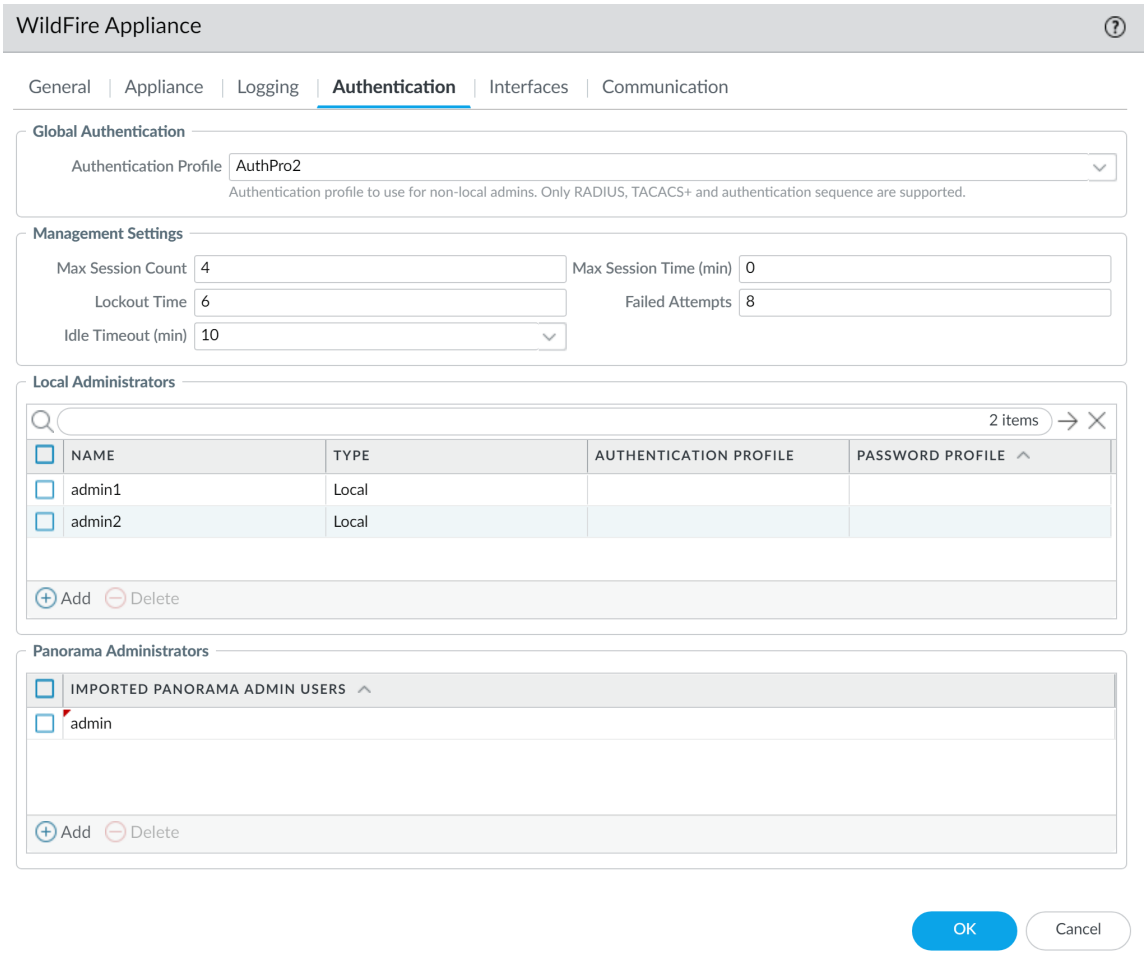
2. 输入 **Lockout Time**（锁定时间）（以分钟为单位），此时间即在用户达到配置的 **Failed Attempts**（失败尝试）次数后，WildFire 设备锁定用户帐户的时间。
3. 输入 **Idle Timeout**（空闲超时）（以分钟为单位），在此时间之后用户会因为不活动而自动注销。
4. 输入 **Max Session Count**（最大会话计数）以设置多少用户帐户可以同时访问 WildFire 设备。
5. 输入管理员在自动注销之前可登录的 **Max Session Time**（最长会话时间）。

4. 添加 WildFire 设备管理员。

   管理员可以添加为本地管理员或作为导入的 Panorama 管理员 — 但不能同时为二者。不支持将同一管理员同时添加为本地管理员和作为导入的 Panorama 管理员，这会导致 Panorama 提交失败。例如，如果您将 `admin1` 同时添加为本地和 Panorama 管理员，向 Panorama 的提交将会失败。

   1. **Add**（添加）并配置专属于 WildFire 设备的新管理员。这些管理员特定于为其创建的 WildFire 设备，您可以从此表格管理这些管理员。
   2. **Add**（添加）在 Panorama 上配置的任何管理员。这些管理员在 Panorama 上创建，并导入至 WildFire 设备。

5. 单击 **OK**（确定）以保存 WildFire 设备身份验证配置。



STEP 5 | **Commit**（提交），然后 **Commit and Push**（提交并推送）您的配置更改。

STEP 6 | 使用本地管理员用户访问 WildFire 设备 CLI 以验证您能够成功访问 WildFire 设备。

© 2019 Palo Alto Networks, Inc.

为 *WildFire* 设备配置 *TACACS+* 身份验证

您可以使用 TACACS+ 服务器来验证对 WildFire 设备 CLI 的管理访问权限。您也可以在 TACACS+ 服务器上定义供应商特定属性 (VSA) 来管理管理员授权。使用 SAML 使您能够通过目录服务来快速更改管理员的角色、访问域和用户组，这通常比在 Panorama 上重新配置设置更为容易。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 添加独立 WildFire 设备以使用 Panorama 进行管理。

STEP 3 | 配置 TACACS+ 身份验证。

1. 添加 TACACS+ 服务器配置文件。

   配置文件定义了 WildFire 设备连接到 TACACS+ 服务器的方式。

   1. 选择 **Panorama** > **Server Profiles**（服务器配置文件）> **TACACS+**，并 **Add**（添加）配置文件。
   2. 输入 **Profile Name**（配置文件名称）以标识服务器配置文件。
   3. 输入身份验证请求超时后以秒为单位的 **Timeout**（超时）（默认为 3；范围为 1-20）。
   4. 选择 Panorama 用来对 TACACS+ 服务器进行身份验证的 **Authentication Protocol**（身份验证协议）（默认为 **CHAP**）。
   5. 如果 TACACS+ 服务器支持该协议，请选择 **CHAP**；该协议比 **PAP** 更安全。
   6. **Add**（添加）每个 TACACS+ 服务器，并输入以下内容：

      1. 标识服务器的 **Name**（名称）。
      2. **TACACS+ Server**（**TACACS+** 服务器）IP 地址或 FQDN。
      3. **Secret**（密钥）/**Confirm Secret**（确认密钥）（加密用户名和密码的密钥）。
      4. 用于身份验证请求的服务器 **Port**（端口）（默认为 49）。
   7. 单击 **OK**（确定）保存服务器配置文件。
2. 将 TACACS+ 服务器配置文件分配到身份验证配置文件。

   身份验证配置文件定义了一组管理员通用的身份验证设置。

   1. 选择 **Panorama** > **Authentication Profile**（身份验证配置文件），并 **Add**（添加）配置文件。
   2. 输入 **Name**（名称）以标识配置文件。
   3. 将 **Type**（类型）设置为 **TACACS+**。
   4. 选择您配置的 **Server Profile**（服务器配置文件）。
   5. 选择 **Retrieve user group from TACACS+**（从 **TACACS+** 中检索用户组），以从 TACACS+ 服务器上定义的 VSA 收集用户组信息。

      Panorama 与您在身份验证配置文件允许列表中指定的组在组信息方面进行匹配。
   6. 选择 **Advanced**（高级），并在允许列表中 **Add**（添加）允许使用此身份验证配置文件进行身份验证的管理员。
   7. 单击 **OK**（确定）保存身份验证配置文件。

STEP 4 | 为 WildFire 设备配置身份验证。

1. 选择 **Panorama** > **Managed WildFire Appliances**（受管 **WildFire** 设备），然后选择您之前添加的 WildFire 设备。
2. 选择您在上一步中配置的 **Authentication Profile**（身份验证配置文件）。

   如果没有分配全局身份验证配置文件，您必须为每个单独的本地管理员分配一个身份验证配置文件才能利用远程身份验证。
3. 为 WildFire 设备配置身份验证 **Timeout Configuration**（超时配置）。

   1. 输入 **Failed Attempt**（失败尝试）次数，在此次数之后用户将被锁定在 WildFire 设备 CLI 之外。
   2. 输入 **Lockout Time**（锁定时间）（以分钟为单位），此时间即在用户达到配置的 **Failed Attempts**（失败尝试）次数后，WildFire 设备锁定用户帐户的时间。

© 2019 Palo Alto Networks, Inc.

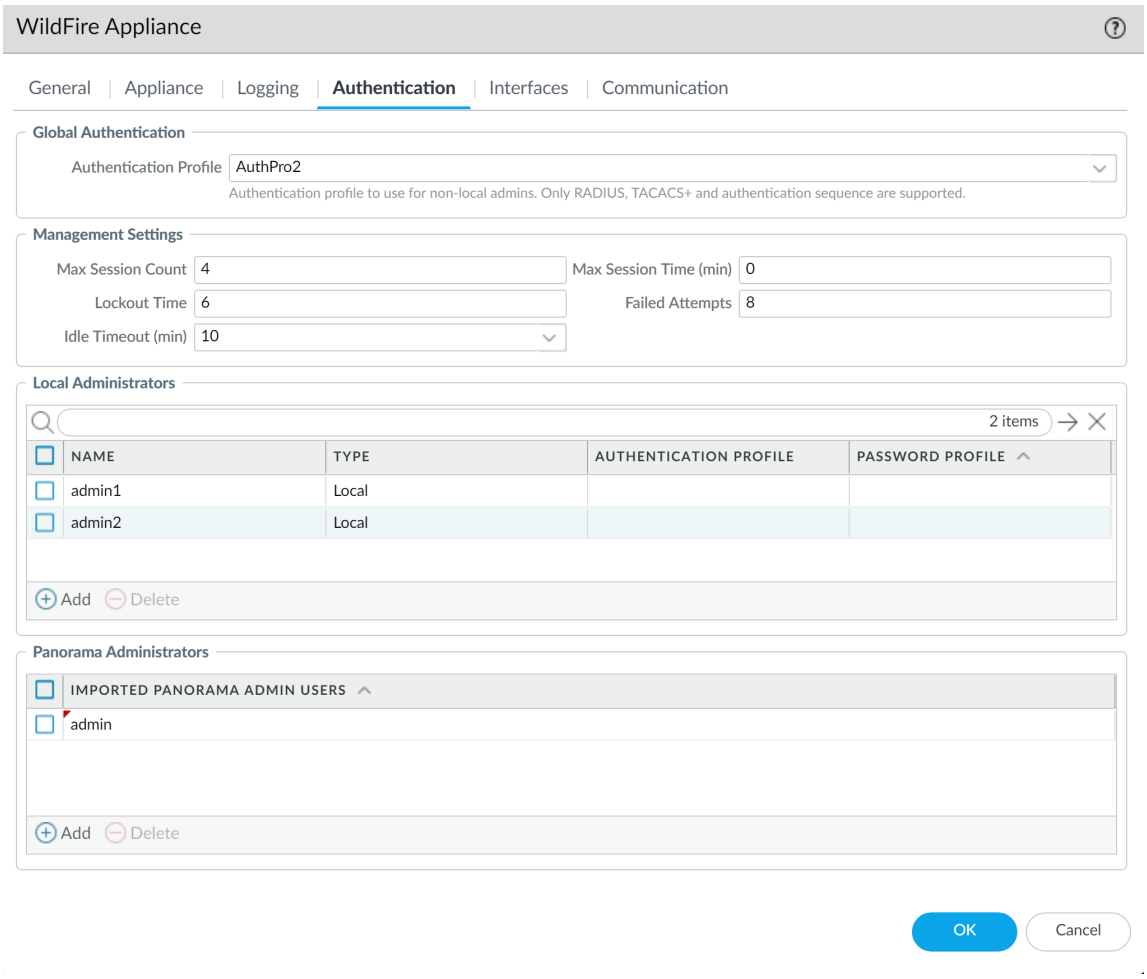
3. 输入 **Idle Timeout**（空闲超时）（以分钟为单位），在此时间之后用户会因为不活动而自动注销。
4. 输入 **Max Session Count**（最大会话计数）以设置多少用户帐户可以同时访问 WildFire 设备。
5. 输入管理员在自动注销之前可登录的 **Max Session Time**（最长会话时间）。

4. 添加 WildFire 设备管理员。

   管理员可以添加为本地管理员或作为导入的 Panorama 管理员 — 但不能同时为二者。不支持将同一管理员同时添加为本地管理员和作为导入的 Panorama 管理员，这会导致 Panorama 提交失败。例如，如果您将 **admin1** 同时添加为本地和 Panorama 管理员，向 Panorama 的提交将会失败。

   1. **Add**（添加）并配置专属于 WildFire 设备的新管理员。这些管理员特定于为其创建的 WildFire 设备，您可以从此表格管理这些管理员。
   2. **Add**（添加）在 Panorama 上配置的任何管理员。这些管理员在 Panorama 上创建，并导入至 WildFire 设备。

5. 单击 **OK**（确定）以保存 WildFire 设备身份验证配置。



STEP 5 | **Commit**（提交），然后 **Commit and Push**（提交并推送）您的配置更改。

STEP 6 | 使用本地管理员用户访问 WildFire 设备 CLI 以验证您能够成功访问 WildFire 设备。

为 *WildFire* 设备配置 *LDAP* 身份验证

您可以使用 LDAP 对访问 WildFire 设备 CLI 的最终用户进行身份验证。

STEP 1 | 登录到 Panorama Web 界面。

© 2019 Palo Alto Networks, Inc.

STEP 2 | 添加独立 WildFire 设备以使用 Panorama 进行管理。

STEP 3 | 添加 LDAP 服务器配置文件。

配置文件定义了 WildFire 设备连接到 LDAP 服务器的方式。

1. 选择 **Panorama** > **Server Profiles**（服务器配置文件）> **LDAP**，然后 **Add**（添加）服务器配置文件。
2. 输入 **Profile Name**（配置文件名称）以标识服务器配置文件。
3. **Add**（添加）LDAP 服务器（最多 4 个）。对于每个服务器，输入 **Name**（名称）（以标识服务器）、**LDAP Server**（**LDAP** 服务器）IP 地址或 FQDN 以及服务器 **Port**（端口）（默认为 389）。

   如果使用 *FQDN* 地址对象来标识服务器，并随后更改地址，则必须提交更改以使新服务器地址生效。
4. 选择服务器 **Type**（类型）。
5. 选择 **Base DN**（基本 **DN**）。

   要标识目录的基本 DN，请打开 **Active Directory Domains and Trusts**（活动目录域和信任）Microsoft 管理控制台控制单元，并使用顶级域的名称。
6. 输入 **Bind DN**（绑定 **DN**）和 **Password**（密码）以启用身份验证服务对防火墙进行身份验证。

   绑定 *DN* 账户必须有权读取 *LDAP* 目录。
7. 以秒为单位输入 **Bind Timeout**（绑定超时）和 **Search Timeout**（搜索超时）（默认均为 30）。
8. 输入 **Retry Interval**（重试时间间隔），以秒计（默认为 60）。
9. （可选）如果您希望端点使用 SSL 或 TLS 与目录服务器建立更安全的连接，启用 **Require SSL/TLS secured connection**（需要 **SSL/TLS** 安全连接）选项（默认启用）。端点使用的协议取决于服务器端口：
   - 389（默认）— TLS（具体来说，WildFire 设备使用 StartTLS 操作，这会将初始明文连接升级到 TLS。）
   - 636 — SSL
   - 任何其他端口 — WildFire 设备首先尝试使用 TLS。如果目录服务器不支持 TLS，则 WildFire 设备回退至 SSL。
10. （可选）如需额外的安全性，启用 **Verify Server Certificate for SSL sessions**（验证 **SSL** 会话的服务器证书）选项，使端点验证目录服务器为 SSL/TLS 连接出示的证书。要启用验证，还必须启用 **Require SSL/TLS secured connection**（需要 **SSL/TLS** 安全连接）选项。为了验证成功，证书必须符合以下条件之一：
    - 它位于 Panorama 证书列表中：**Panorama** > **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书）。必要时，将证书导入 Panorama。
    - 证书签发机构位于可信证书授权机构列表中：**Panorama** > **Certificate Management**（证书管理）> **Certificates**（证书）。
11. 单击 **OK**（确定）保存服务器配置文件。

STEP 4 | 为 WildFire 设备配置身份验证。

1. 选择 **Panorama** > **Managed WildFire Appliances**（受管 **WildFire** 设备），然后选择您之前添加的 WildFire 设备。
2. 为 WildFire 设备配置身份验证 **Timeout Configuration**（超时配置）。
   1. 输入 **Failed Attempt**（失败尝试）次数，在此次数之后用户将被锁定在 WildFire 设备 CLI 之外。
   2. 输入 **Lockout Time**（锁定时间）（以分钟为单位），此时间即在用户达到配置的 **Failed Attempts**（失败尝试）次数后，WildFire 设备锁定用户帐户的时间。
   3. 输入 **Idle Timeout**（空闲超时）（以分钟为单位），在此时间之后用户会因为不活动而自动注销。
   4. 输入 **Max Session Count**（最大会话计数）以设置多少用户帐户可以同时访问 WildFire 设备。
   5. 输入管理员在自动注销之前可登录的 **Max Session Time**（最长会话时间）。

© 2019 Palo Alto Networks, Inc.

3. 添加 WildFire 设备管理员。

   管理员可以添加为本地管理员或作为导入的 Panorama 管理员 — 但不能同时为二者。不支持将同一管理员同时添加为本地管理员和作为导入的 Panorama 管理员，这会导致 Panorama 提交失败。例如，如果您将 **admin1** 同时添加为本地和 Panorama 管理员，向 Panorama 的提交将会失败。

   - 配置本地管理员。

     配置专属于 WildFire 设备的新管理员。这些管理员特定于为其创建的 WildFire 设备，您可以从此表格管理这些管理员。

     1. **Add**（添加）一个或多个新本地管理员。
     2. 输入本地管理员的 **Name**（名称）。
     3. 配置一个您之前创建的 **Authentication Profile**（身份验证配置文件）。

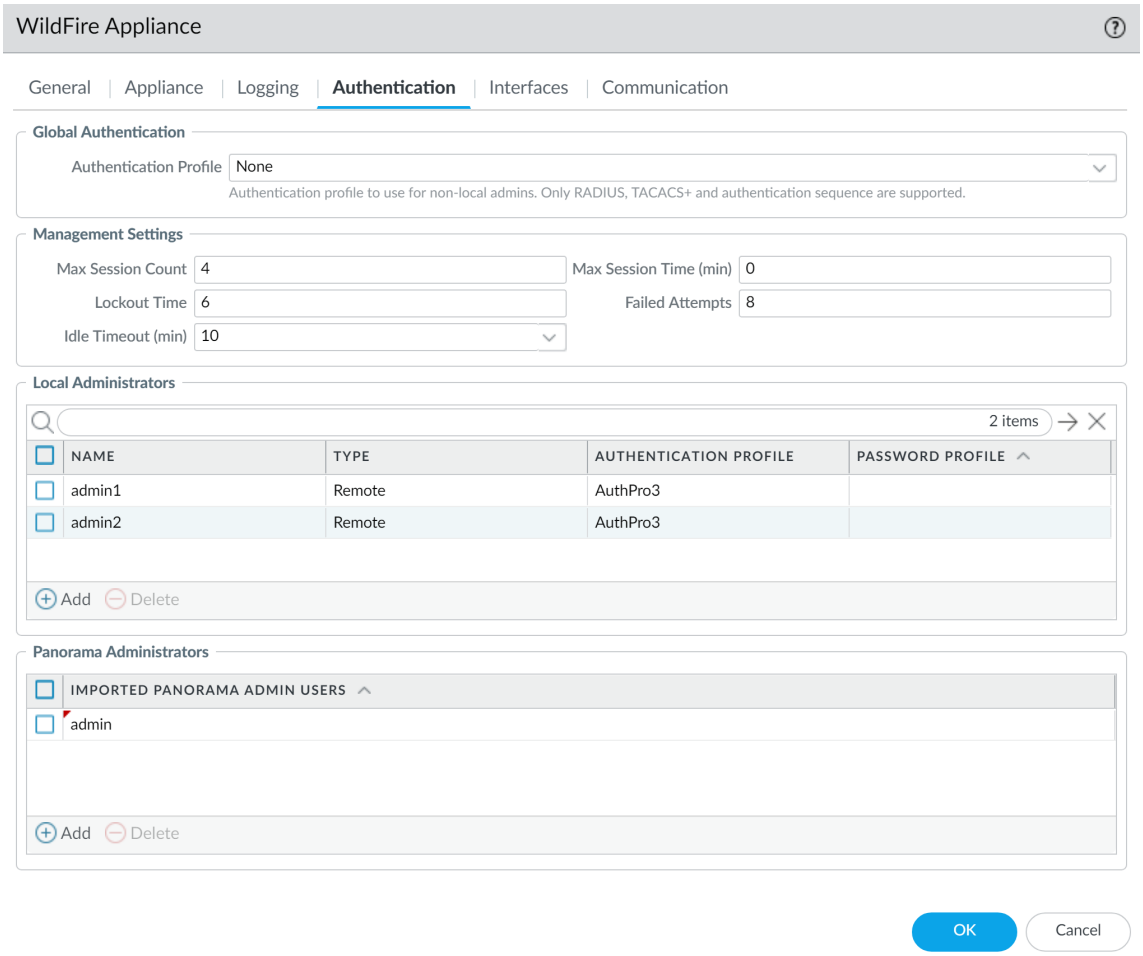
        仅单个本地管理员才支持 *LDAP* 身份验证配置文件。

     4. 启用（选中）**Use Public Key Authentication (SSH)**（使用公钥身份验证 **(SSH)**）以导入公钥文件进行身份验证。
     5. 选择一个 **Password Profile**（密码配置文件）以设置过期参数。
   - 导入现有 Panorama 管理员

     导入在 Panorama 上配置的现有管理员。这些管理员在 Panorama 上配置和管理，并导入至 WildFire 设备。

     1. **Add**（添加）现有 Panorama 管理员
4. 单击 **OK**（确定）以保存 WildFire 设备身份验证配置。

© 2019 Palo Alto Networks, Inc.



STEP 5 | **Commit**（提交），然后 **Commit and Push**（提交并推送）您的配置更改。

STEP 6 | 使用本地管理员用户访问 WildFire 设备 CLI 以验证您能够成功访问 WildFire 设备。

© 2019 Palo Alto Networks, Inc.

在 WildFire 设备和集群上使用自定义证书设置身份验证

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

更多有关使用自定义证书的信息，请参阅SSL/TLS 连接如何进行相互身份验证？

- 为 Panorama 管理的 WildFire 设备配置自定义证书
- 使用单个自定义证书为 WildFire 集群配置身份验证
- 在通过 Panorama 配置的 WildFire 设备上应用自定义证书

为 Panorama 管理的 WildFire 设备配置自定义证书

如果使用 Panorama™ 管理您的 WildFire® 设备或 WildFire 集群，则可以通过 Panorama Web 界面（而非 WildFire 设备 CLI）配置自定义证书身份验证。防火墙或 Panorama 会使用此连接将样本转发到 WildFire 进行分析。

此程序描述如何在单个 WildFire 设备上安装唯一证书。如果 WildFire 设备是集群的一部分，此设备和每个集群成员均拥有唯一客户端证书。要将单个证书部署到集群中的所有 WildFire 设备，请使用单个自定义证书为 WildFire 集群配置身份验证。

STEP 1 | 获取用于防火墙上 WildFire 设备的密钥对和证书颁发机构 (CA) 颁发的证书。

STEP 2 | 导入 CA 证书，以验证防火墙的标识和 WildFire 设备的密钥对。

1. 选择 **Panorama** > **Certificate Management**（证书管理）> **Certificate**（证书）> **Import**（导入）。
2. 在 Panorama 上导入 CA 证书和密钥对。

STEP 3 | 配置包含根 CA 和中间 CA 的证书配置文件。该证书配置文件定义 WildFire 设备和防火墙相互进行身份验证的方式。

1. 选择 **Panorama** > **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件）。
2. 配置证书配置文件。

   如果将中间 CA 配置为证书配置文件的一部分，则还必须包含根 CA。

STEP 4 | 配置用于 WildFire 设备的 SSL/TLS 配置文件。

PAN-OS 8.0 及更高版本仅支持 *TLS 1.2* 及更高版本，因此您 必须设置最大版本为*TLS 1.2* 或 *max*（更高版本）。

1. 选择 **Panorama** > **Certificate Management**（证书管理）> **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）。
2. 配置 SSL/TLS 服务配置文件以定义 WildFire 设备及其防火墙用于 SSL/TLS 服务的证书和协议。

STEP 5 | 在 WildFire 上配置安全服务器通信。

1. 选择**Panorama** > **Managed WildFire Clusters**（受管 **WildFire** 集群）或 **Panorama** > **Managed WildFire Appliances**（受管 **WildFire** 设备），然后选择集群或设备。
2. 选择 **Communication**（通信）。

© 2019 Palo Alto Networks, Inc.

3. 启用**Customize Secure Server Communication**（自定义安全服务器通信）功能。
4. 选择 **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）。该 SSL/TLS 服务配置文件适用于 WildFire 设备和防火墙或 Panorama 之间的所有 SSL 连接。
5. 选择专为 WildFire 设备和防火墙或 Panorama 之间通信配置的 **Certificate Profile**（证书配置文件）。
6. 验证 **Custom Certificate Only**（仅允许自定义证书）是否已禁用（取消选择）。此时，允许 WildFire 设备在迁移到自定义证书时继续通过预定义证书与防火墙进行通信。
7. （可选）配置授权列表。
   1. **Add**（添加）授权列表。
   2. 选择在证书配置文件中配置的 **Subject**（主题）或 **Subject Alt Name**（主题备用名称）作为标识符类型。
   3. 如果标识符为主题，则输入通用名，如果标识符为主题备用名称，则输入 IP 地址、主机名或电子邮件。
   4. 单击 **OK**（确定）。
   5. 启用 **Check Authorization List**（检查授权列表）以执行该列表。
8. 单击 **OK**（确定）。
9. **Commit**（提交）更改。

STEP 6 | 导入 CA 证书以验证 WildFire 设备证书。

1. 登录到防火墙 Web 界面。
2. 导入 CA 证书。

STEP 7 | 配置防火墙的本地或 SCEP 证书。

- 如果正在使用本地证书，则导入防火墙密钥对。
- 如果您使用 SCEP 作为防火墙证书，请配置 SCEP 配置文件。

STEP 8 | 配置防火墙或 Panorama 的证书配置文件。您可以单独在每个客户端防火墙或 Panorama 设备上配置此配置文件，也可以使用模板将配置从 Panorama 推送至受管防火墙。

1. 选择防火墙的**Device**（设备）> **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件）或 Panorama 的**Panorama** > **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件）。
2. 配置证书配置文件。

STEP 9 | 在每个防火墙或 Panorama 设备上部署自定义证书。

1. 登录到防火墙 Web 界面。
2. 选择防火墙 **Device**（设备）> **Setup**（设置）> **Management**（管理）的或 Panorama 的 **Panorama** > **Setup**（设置）> **Management**（管理），并 **Edit**（编辑）安全通信设置。
3. 选择 **Certificate Type**（证书类型）、**Certificate**（证书）和 **Certificate Profile**（证书配置文件）。
4. 从自定义通信设置中，选择 **WildFire Communication**（**WildFire** 通信）。
5. 单击 **OK**（确定）。
6. **Commit**（提交）更改。

STEP 10 | 在所有受管设备上部署自定义证书后，执行自定义证书身份验证。

1. 登录到 Panorama。
2. 选择**Panorama** > **Managed WildFire Clusters**（受管 **WildFire** 集群）或 **Panorama** > **Managed WildFire Appliances**（受管 **WildFire** 设备），然后选择集群或设备。
3. 选择 **Communication**（通信）。
4. 选择 **Custom Certificate Only**（仅允许自定义证书）。
5. 单击 **OK**（确定）。
6. **Commit**（提交）更改。

© 2019 Palo Alto Networks, Inc.

提交此更改后，WildFire 立即开始执行自定义证书。

使用单个自定义证书为 WildFire 集群配置身份验证

您可以将单个共享客户端证书分配给整个 WildFire 集群，而不是将唯一证书分配给集群中的每个 WildFire®，从而允许您将单个证书推送给集群中的所有 WildFire 设备，而非为每个集群成员配置单独的证书。因为单个 WildFire 设备共享客户端证书，因此，您必须为每个 WildFire 设备配置一个唯一的主机名（DNS 名称）。然后，您可以将所有主机名作为证书属性添加到共享证书中，或是使用与集群中所有 WildFire® 设备上所有自定义主机名匹配的单通配符字符串。

若要在与 Panorama™ 进行通信时配置供 WildFire 集群使用的单个自定义证书，请完成下列程序。

STEP 1 | 获取服务器密钥对和 CA 证书，以供 Panorama 使用。

STEP 2 | 配置包含根证书颁发机构 (CA) 和中间 CA 的证书配置文件。此证书配置文件定义 WildFire 集群（客户端）和 Panorama 设备（服务器）之间的身份验证。

1. 选择 **Panorama** > **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件）。
2. 配置证书配置文件。

   如果将中间 CA 配置为证书配置文件的一部分，则还必须包含根 CA。

STEP 3 | 配置 SSL/TLS 服务配置文件。

1. 选择 **Panorama** > **Certificate Management**（证书管理）> **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）。
2. 配置 SSL/TLS 服务配置文件以定义 WildFire 集群和 Panorama 设备用于 SSL/TLS 服务的证书和协议。

STEP 4 | 将集群中的每个节点与 Panorama 连接。

STEP 5 | 在集群内每个节点上配置唯一主机名（DNS 名称），或使用带有与集群内 WildFire 设备上所有自定义 DNS 名称集匹配的单个通配符的字符串。

如果使用单通配符字符串，请参阅 RFC-6125 第 6.4.3 节以了解通配符字符串值的要求和限制。配置自定义 DNS 名称时，必须了解这些要求和限制。

1. 登录到节点上的 WildFire CLI。
2. 使用以下命令将唯一自定义 DNS 名称分配给节点。

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

```
admin@WF-500# set deviceconfig setting wildfire custom-dns-name <dns-name>
```

3. **Commit**（提交）更改。
4. 为集群内各节点重复此步骤 。

STEP 6 | 在 Panorama，为集群内所有节点生成客户端证书。在证书属性下，为您已分配给集群节点的每个自定义 DNS 名称添加主机名条目，或是添加一个带有与所有节点主机名匹配的单通配符字符串的主机名条目，例如 *.example.com。只有当每个自定义 DNS 名称共享一个公共字符串时，才能执行此操作。

STEP 7 | 在 Panorama 上配置集群客户端证书的证书配置文件。

1. 选择 Panorama 的 **Panorama** > **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件）。

© 2019 Palo Alto Networks, Inc.

2. 配置证书配置文件。

STEP 8 | 在每个节点上部署自定义证书。此证书配置文件必须包含签有 Panorama 服务器证书的 CA 证书。

1. 选择 **Panorama** > **Managed WildFire Appliances**（受管 **WildFire** 设备），并单击集群名称。
2. 选择 **Communications**（通信）。
3. 在安全客户端通信中，选择**Certificate Type**（证书类型）、**Certificate**（证书）和 **Certificate Profile**（证书配置文件）。
4. 单击 **OK**（确定）。
5. **Commit**（提交）更改。

STEP 9 | 在 Panorama 上配置安全服务器通信。

1. 选择 **Panorama** > **Setup**（设置）> **Management**（管理），然后 **Edit**（编辑）以选择 **Customize Secure Server Communication**（自定义安全服务器通信）。
2. 启用**Customize Secure Server Communication**（自定义安全服务器通信）。
3. 选择 **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）。该 SSL/TLS 服务配置文件适用于 WildFire 和 Panorama 之间的所有 SSL 连接。
4. 选择 Panorama 的 **Certificate Profile**（证书配置文件）。
5. 启用 **Custom Certificates Only**（仅允许自定义证书）。
6. 单击 **OK**（确定）。
7. **Commit**（提交）更改。

在通过 Panorama 配置的 WildFire 设备上应用自定义证书

默认情况下，Panorama™ 在与 WildFire® 设备通信时使用预定义证书推送配置。或者，您可以使用自定义证书建立连接的相互身份验证，通过此连接， Panorama™ 将配置推送至受管 WildFire 设备或集群。完成以下程序，以在 Panorama 上配置服务器证书，在 WildFire 设备上配置客户端证书。

STEP 1 | 获取用于 Panorama 和 WildFire 设备的密钥对和证书颁发机构 (CA) 颁发的证书。

STEP 2 | 导入 CA 证书，以验证 WildFire 设备的标识和 Panorama 的密钥对。

1. 选择 **Panorama** > **Certificate Management**（证书管理）> **Certificate**（证书）> **Import**（导入）。
2. 在 Panorama 上导入 CA 证书和密钥对。

STEP 3 | 配置包含根 CA 和中间 CA 的证书配置文件。此证书配置文件定义 WildFire 设备（客户端）和 Panorama 虚拟设备或 M 系列设备（服务器）之间的身份验证。

1. 选择 **Panorama** > **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件）。
2. 配置证书配置文件。

   如果将中间 CA 配置为证书配置文件的一部分，则还必须包含根 CA。

STEP 4 | 配置 SSL/TLS 服务配置文件。

1. 选择 **Panorama** > **Certificate Management**（证书管理）> **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）。
2. 配置 SSL/TLS 服务配置文件以定义 WildFire 和 Panorama 设备用于 SSL/TLS 服务的证书和协议。

STEP 5 | 在 Panorama 设备上配置安全服务器通信。

1. 选择 **Panorama** > **Setup**（设置）> **Management**（管理），然后 **Edit**（编辑）以选择 **Customize Secure Server Communication**（自定义安全服务器通信）。
2. 启用**Customize Secure Server Communication**（自定义安全服务器通信）功能。
3. 选择 **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）。

© 2019 Palo Alto Networks, Inc.

4. 从 **Certificate Profile**（证书配置文件）下拉列表中选择证书配置文件。
5. 验证 **Custom Certificate Only**（仅允许自定义证书）是否已禁用（取消选择）。此时，允许 Panorama 在迁移到自定义证书时继续通过预定义证书与 WildFire 进行通信。
6. （可选）配置授权列表。
   1. **Add**（添加）授权列表。
   2. 选择在证书配置文件中配置的 **Subject**（主题）或 **Subject Alt Name**（主题备用名称）作为标识符类型。
   3. 如果标识符为 `Subject`（主题），则输入 **Common Name**（通用名），如果标识符为 `Subject Alt Name`（主题备用名称），则输入 **IP address**（IP 地址）、**hostname**（主机名）或 **email**（电子邮件）。
   4. 单击 **OK**（确定）。
   5. 启用 **Check Authorization List**（检查授权列表）选项，配置 Panorama，以执行授权列表。
7. 单击 **OK**（确定）。
8. **Commit**（提交）更改。

STEP 6 | 导入 CA 证书以验证 Panorama 上的证书。

1. 登录到 Panorama 用户界面。
2. 导入 CA 证书。

STEP 7 | 配置 WildFire 设备的本地或 SCEP 证书。

1. 如果正在使用本地证书，则导入 WF-500 设备密钥对。
2. 如果您使用 SCEP 作为 WildFire 设备证书，请配置 SCEP 配置文件。

STEP 8 | 配置 WildFire 设备的证书配置文件。

1. 选择 **Panorama** > **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件）。
2. 配置证书配置文件。

STEP 9 | 在每个受管 WildFire 设备上配置自定义证书。

1. 登录到 Panorama。
2. 选择 **Panorama** > **Managed WildFire Appliances**（受管 **WildFire** 设备），并单击集群或设备名称。
3. 选择 **Communications**（通信）。
4. 在安全客户端通信中，从相应的下拉列表中选择**Certificate Type**（证书类型）、**Certificate**（证书）和 **Certificate Profile**（证书配置文件）。
5. 单击 **OK**（确定）。
6. **Commit**（提交）更改。

STEP 10 | 在所有受管 WildFire 设备上部署自定义证书后，执行自定义证书身份验证。

1. 选择 **Panorama** > **Setup**（设置）> **Management**（管理），然后 **Edit**（编辑）安全通信设置。
2. **Allow Custom Certificate Only**（仅允许自定义证书）。
3. 单击 **OK**（确定）。
4. **Commit**（提交）更改。

提交这些更改后，断开等待时间将开始倒计时。等待时间结束时，若没有配置证书，则 Panorama 及其管理的 WildFire 设备无法进行连接。

© 2019 Palo Alto Networks, Inc.

从 Panorama 管理中删除 WildFire 设备

您可以从 Panorama 管理中删除 WildFire 独立设备。从 Panorama 管理中删除独立 WildFire 设备时，您不再享受集中管理的好处，并且必须使用本地 CLI 和脚本管理设备。

STEP 1 | 选择 **Panorama** > **Managed WildFire Appliances**（受管 **WildFire** 设备）。

STEP 2 | 通过选中每个设备旁边的复选框或单击设备的行，选择要从 Panorama 管理中删除的 WildFire 设备。

STEP 3 | 从 Panorama 管理中 **Remove**（删除）所选的 WildFire 设备。

© 2019 Palo Alto Networks, Inc.

管理 WildFire 集群

WildFire 设备集群是 WildFire 设备的互联分组，通过聚集资源增加样本分析和存储能力，支持较大的防火墙分组，并简化多台 WildFire 设备的配置和管理。对于增强安全性和保持传输内容的机密性，您还可以对集群中 WildFire 设备之间的通信进行加密。更多有关 WildFire 集群和部署流程的信息，请参阅 WildFire 设备集群。

可通过使用 Panorama 执行以下任务以管理您的 WildFire 集群。

- 在 Panorama 上集中配置集群
- 通过 Panorama 查看 WildFire 集群状态
- 通过互联网连接在 Panorama 上集中升级集群
- 不通过互联网连接在 Panorama 上集中升级集群
- 使用预定义证书在 Panorama 上集中配置设备到设备加密
- 使用自定义证书在 Panorama 上集中配置设备到设备加密

在 Panorama 上集中配置集群

在 Panorama M 系列或虚拟设备上配置 WildFire 设备集群之前，将两个 WildFire 设备配置为高可用性控制器节点对，其他额外的 WildFire 设备作为工作节点，增加分析、存储量，以及集群的弹性。

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

要创建 *WildFire* 设备集群，您必须升级所有 WildFire 设备至 *PAN-OS 8.0.1* 或以上版本，这些设备是您希望在集群内部署的设备。当使用 *Panorama* 管理 *WildFire* 设备集群时，*Panorama* 也必须运行 *PAN-OS 8.0.1* 或以上版本。在您想要添加至集群的各 *WildFire* 设备上，在 *WildFire* 设备 *CLI* 上运行 ***show system info | match version***，确保此设备正在运行 *PAN-OS 8.0.1* 或以上版本。在您使用的各 *Panorama* 设备上管理集群（或独立设备），*Dashboard*（仪表盘）> *General Information*（常规信息）> *Software Version*（软件版本）显示运行的软件版本。

当您的 WildFire 设备可用时，执行相应的任务：

- 在 Panorama 上配置集群和添加节点
- 在 Panorama 上配置常规集群设置
- 为 WildFire 集群配置身份验证
- 从 Panorama 管理移除集群

不支持通过 *Panorama* 从集群移除节点。取而代之的是，通过本地 *WildFire CLI* 从集群本地移除节点。

在 *Panorama* 上配置集群和添加节点

从 Panorama 配置 WildFire 设备集群之前，您必须升级 Panorama 至 8.0.1 或以上并升级所有 WildFire 设备至 8.0.1 或以上，这些设备是您计划添加至集群的设备。所有 WildFire 设备必须运行 PAN-OS 的相同版本。

您可以使用 Panorama M 系列或虚拟设备最多管理 200 个 WildFire 设备。200 台 WildFire 设备限制是指独立设备和 WildFire 设备集群节点的总数（如果您也添加独立 WildFire 设备以通过 Panorama 进行管理）。除非另有注明，配置发生在 Panorama 上。

各 *WildFire* 设备集群节点必须在相同子网内有一个静态 *IP* 地址和低延迟连接。

© 2019 Palo Alto Networks, Inc.

STEP 1 | 通过本地 CLI，配置将要用于管理 WildFire 设备集群的 Panorama 服务器 IP 地址。

在您注册集群或独立 WildFire 设备至 Panorama 设备之前，您必须先在各 WildFire 设备上，通过本地 WildFire CLI 配置 Panorama IP 地址或 FQDN。这就是每个 WildFire 设备知道 Panorama 设备管理它的方式。

1. 在各 WildFire 设备上，配置主 Panorama 设备管理接口的 IP 地址或 FQDN：

```
admin@WF-500# set deviceconfig system panorama-server <ip-address | FQDN>
```

2. 在各 WildFire 设备上，如果您为实现高可用性（建议）使用备份 Panorama 设备，配置备份 Panorama 设备管理接口的 IP 地址或 FQDN：

```
admin@WF-500# set deviceconfig system panorama-server-2 <ip-address |
 FQDN>
```

3. 提交各 WildFire 设备上的配置：

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

STEP 2 | 在主 Panorama 设备上，注册 WildFire 设备。

新注册设备处于独立模式，除非它们由于本地集群配置的原因已经属于集群。

1. 选择 **Panorama** > **Managed WildFire Appliances**（受管理的 **WildFire** 设备）并 **Add Appliance**（添加设备）。
2. 在单独的行中输入每个 WildFire 设备的序列号。如果您没有 WildFire 设备序列号列表，使用本地 CLI，在各 WildFire 设备上运行 **show system info** 以获得序列号。
3. 单击 **OK**（确定）。

   如果可用，则会显示有关 WildFire 设备上已提交的配置的信息，例如 IP 地址和软件版本。已经属于一个集群的 WildFire 设备（例如，由于本地集群配置）显示其集群信息和连接状态。

STEP 3 | （可选）将 WildFire 设备配置导入 Panorama 设备。

导入配置可节省时间，因为您可以重复使用或编辑 Panorama 上的配置，然后将其推送至一个或多个 WildFire 设备集群或独立 WildFire 设备。如果没有您想要导入的配置，跳过此步骤。当您从 Panorama 推送配置时，推送的配置覆盖本地配置。

1. 选择 **Panorama** > **Managed WildFire Appliances**（受管理的 **WildFire** 设备），然后从受管理的 WildFire 设备列表选择带有您想要导入配置的设备。
2. **Import Config**（导入配置）。
3. 选择 **Yes**（是）。

   导入配置会更新显示的信息，并使导入的配置成为 Panorama 设备待选配置的一部分。
4. **Commit to Panorama**（提交到 **Panorama**）使导入的 WildFire 设备配置成为 Panorama 运行配置的一部分。

STEP 4 | 创建新的 WildFire 设备集群。

1. 选择 **Managed WildFire Clusters**（受管理的 **WildFire** 集群）。

   Appliance（设备）> **No Cluster Assigned**（无指派的集群）显示独立 WildFire 设备（节点）并显示有多少可用的节点未指派至集群。
2. **Create Cluster**（创建集群）。
3. 输入由字母和数字组成的集群 **Name**（名称），最长可包含 63 个字符。**Name**（名称）可以包含小写字母和数字，以及连词符和点（不得是第一个或最后一个字符）。不允许使用空格或其他字符。
4. 单击 **OK**（确定）。

© 2019 Palo Alto Networks, Inc.

新集群名称显示但无指派的 WildFire 节点。

STEP 5 | 添加 WildFire 设备至新集群。

添加至集群的第一台 WildFire 设备自动成为控制器节点，添加至集群的第二台 WildFire 设备自动成为控制器备份节点。所有后续添加的 WildFire 设备成为工作节点。工作节点使用控制器节点设置，因此集群配置保持一致。

1. 选择新集群。
2. 选择 **Clustering**（集群）。
3. **Browse**（浏览）不属于集群的 WildFire 设备列表。
4. 添加 (⊕) 您想要包含到集群中的各 WildFire 设备。您最多可以向集群添加二十个节点。您添加至集群的各 WildFire 设备与其自动指派的角色一同显示。
5. 单击 **OK**（确定）。

STEP 6 | 配置 **Management**（管理）、**Analysis Environment Network**（分析环境网络）、HA 和集群管理接口。

如果未配置，则配置各集群成员（控制器和工作节点）上的 **Management**（管理）、**Analysis Environment Network**（分析环境网络）和集群管理接口。集群管理接口是管理和在集群内通讯的专用接口，与管理接口不同。

在控制器节点和控制器备份节点上单独配置 HA 接口。HA 接口链接主和备份控制器节点，并使其保持同步和就绪，以对故障转移做出响应。



集群节点需要四个 *WildFire* 设备接口的各个 *IP* 地址。您无法在工作节点上配置 *HA* 服务。

1. 选择新集群。
2. 选择 **Clustering**（集群）。
3. 如果未在集群节点上配置管理接口，选择 **Interface Name**（接口名称）> **Management**（管理）并输入 IP 地址、网络掩码、服务和接口的其他信息。
4. 如果未在集群节点上配置分析环境网络的接口，选择 **Interface Name**（接口名称）> **Analysis Environment Network**（分析环境网络）并输入 IP 地址、网络掩码、服务和接口的其他信息。
5. 在控制器节点和控制器备份节点上，选择 HA 控制链接使用的接口。您必须在两个控制器节点上为 HA 服务配置相同的接口。例如，在控制器节点和控制器备份节点上，选择 **Ethernet3**。
6. 对于各控制器节点，选择 **Clustering Services**（集群服务）> **HA**。（**HA** 选项不适用于工作节点。）如果您还想要 ping 接口的能力，选择 **Management Services**（管理服务）> **Ping**。
7. 单击 **OK**（确定）。
8. （建议）选择接口作为控制器节点和控制器备份节点之间的备份 HA 控制链接。您必须在两个节点上使用相同的接口，以实现 HA 备份服务。例如，在两个节点上，选择 **Management**（管理）。

   为两个节点选择 **Clustering Services**（集群服务）> **HA Backup**（**HA** 备份）。您也可以选择 **Ping**、**SSH** 和 **SNMP**，如果您想要在接口上实现 **Management Services**（管理服务）。

   Analysis Environment Network（分析环境网络）接口无法作为 *HA* 或 *HA* 备份接口或集群管理接口。
9. 选择在集群内进行管理和通讯的专属接口。您必须在两个节点上使用相同的接口，例如，**Ethernet2**。
10. 为两个节点选择 **Clustering Services**（集群服务）> **Cluster Management**（集群管理）。如果您还想要 ping 接口的能力，选择 **Management Services**（管理服务）> **Ping**。

    集群上的工作节点自动继承控制器节点设置，用于专属的管理和通讯接口。

© 2019 Palo Alto Networks, Inc.

STEP 7 | 在 Panorama 设备上提交配置并推送至集群。

1. **Commit and Push**（提交并推送）。
2. 如果 Panorama 设备上有不想推送的配置，**Edit Selections**（编辑选择）以选择您要推送配置的设备。推送的配置覆盖集群节点上正在运行的配置，因此所有集群节点运行相同的配置。

STEP 8 | 验证配置。

1. 选择 **Panorama** > **Managed WildFire Clusters**（受管理的 **WildFire** 集群）。
2. 检查以下字段：
   - **Appliance**（设备）— 添加到集群的 WildFire 节点显示在集群名称下，而不是显示为独立设备。
   - **Cluster Name**（集群名称）— 为各节点显示的集群名称。
   - **Role**（角色）— 为各节点显示的对应角色（**Controller**（控制器）、**Controller Backup**（控制器备份）或 **Worker**（工作设备））。
   - **Config Status**（配置状态）— 状态为 `In Sync`。
   - **Last Commit State**（最后提交状态）— `Commit succeeded`。

STEP 9 | 通过主控制器节点上的本地 CLI（非 Panorama Web 界面），检查确保配置已同步。

如果未同步，手动同步控制器节点上的高可用性配置，并提交配置。

尽管您可以在 Panorama 上执行大部分其他配置，同步控制器节点高可用性配置必须在主控制器节点的 CLI 上完成。

1. 在主控制器节点上，检查确保配置已同步：

```
admin@WF-500(active-controller)> show high-availability all
```

输出结束时，查找配置同步输出：

```
Configuration Synchronization:
    Enabled: yes
    Running Configuration: synchronized
```

如果运行的配置已同步，您无需手动同步配置。但是，如果配置未同步，您需要手动同步配置。

2. 如果配置未同步，在主控制器节点上，同步高可用性配置至远程对端控制器节点：

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

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

3. 提交配置：

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

在 *Panorama* 上配置常规集群设置

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

- 连接至 WildFire 公共云和提交样本至公共云：
- 配置数据保留政策。
- 配置日志。

© 2019 Palo Alto Networks, Inc.

- 设置分析环境（最符合您环境的 VM 映像）和自定义分析环境，以适用于防火墙提交至 WildFire 的样本类型。
- 为 DNS 服务器、NTP 服务器等设置 IP 地址。

STEP 1 | 为 WildFire 设备集群节点配置设置。

许多设置通过默认设置、控制器节点上之前存在的设置，或您刚配置的设置自动填充。

1. 选择集群。
2. 选择 **Appliance**（设备）。
3. 输入新信息，保留来自集群控制器节点的预填充信息，或编辑预填充信息，包括：
   - **Domain**（域）名。
   - **Primary DNS Server**（主 **DNS** 服务器）和 **Secondary DNS Server**（辅助 **DNS** 服务器）的 IP 地址。
   - **Primary NTP Server**（主 **NTP** 服务器）和 **Secondary NTP Server**（辅助 **NTP** 服务器）的 **NTP Server Address**（**NTP** 服务器地址）和 **Authentication Type**（验证类型）。**Authentication Type**（验证类型）选项为 **None**（无）、**Symmetric Key**（对称式密钥）和 **AutoKey**（自动密钥）。

STEP 2 | 配置常规集群设置。

许多设置通过默认设置、控制器节点上之前存在的设置，或您刚配置的设置自动填充。

1. 选择新集群 > **General**（常规）。
2. （可选）为控制器节点 **Enable DNS**（启用 **DNS**）以通过 DNS 协议播发服务状态。集群控制器在管理 (MGT) 接口端提供 DNS 服务。
3. **Register Firewall To**（注册防火墙以）使用集群控制器播发的服务。Palo Alto Networks 建议添加两个控制器作为授权服务器，并提供高可用性的优点。使用格式：

   ```
   wfpc.service.<cluster-name>.<domain>
   ```

   例如，*paloaltonetworks.com* 域中集群名为 *mycluster* 的集群域名如下：

   ```
   wfpc.service.mycluster.paloaltonetworks.com
   ```

4. 输入集群的 **Content Update Server**（内容更新服务器）。使用默认 `updates.paloaltonetworks.com` FQDN 连接最近的服务器。**Check Server Identity**（检查服务器标识）可通过将证书中的通用名 (CN) 与服务器的 IP 地址或 FQDN 进行相匹配，以确认更新服务器的标识（默认检查）。
5. （(可选）输入公共 **WildFire Cloud Server**（**WildFire** 云服务器）位置或使用默认 `wildfire.paloaltonetworks.com`，以便集群（或 Panorama 管理的独立设备）可以将信息发送到最近的 WildFire 云服务器。如果您将此字段留空且不连接 WildFire 云服务器，集群无法直接从 WildFire 公共云接收签名更新，且无法发送样本进行分析或贡献数据到公共云。
6. 如果您连接集群至公共 WildFire 云，选择您想要启用的云服务：
   - **Send Analysis Data**（发送分析数据）— 发送关于本地恶意软件分析的 XML 报告。如果您发送实际样本，集群不会发送报告。
   - **Send Malicious Samples**（发送恶意样本）— 发送恶意软件样本。
   - **Send Diagnostics**（发送诊断）— 发送诊断数据。
   - **Verdict Lookup**（判定查询）— 在执行本地分析，降低本地 WildFire 设备集群上的负载之前，自动查询 WildFire 公共云判定情况。
7. 根据集群分析的样本类型，选择 **Sample Analysis Image**（样本分析映像）以使用。

© 2019 Palo Alto Networks, Inc.

8. 配置集群的时间量以保留 **Benign/Grayware**（良性/灰色软件）样本数据（1-90 天的范围，默认为 14 天）和 **Malicious**（恶意）样本数据（至少 1 天，无最大值（无限），默认为无限）。恶意样本数据包括网络钓鱼判定。
9. （可选）选择 **Preferred Analysis Environment**（首选分析环境）以将多个资源分配给 **Executables**（可执行文件）或 **Documents**（文档），具体取决于环境而定。**Default**（默认）分配是在 **Executables**（可执行文件）和 **Documents**（文档）之间进行平衡。可用资源量取决于集群内 WildFire 节点数量。

STEP 3 | 检查确保主和备份 Panorama 服务器已配置。

如果您未配置备份 Panorama 服务器并希望进行配置，您可以添加备份 Panorama 服务器。

1. 选择集群。
2. 选择 **Appliance**（设备）。
3. 如果您正在使用集中集群管理的高可用性配置，检查（或输入）主 **Panorama Server**（**Panorama** 服务器）以及备份 **Panorama Server 2**（**Panorama** 服务器 **2**）的的 IP 地址或 FQDN。

STEP 4 | （可选）配置系统和集群的配置日志设置，包括日志转发。

1. 选择集群。
2. 选择 **Logging**（日志记录）。
3. 选择 **System**（系统）或 **Configuration**（配置）以分别配置系统或配置日志。其配置过程类似。
4. **Add**（添加）(⊕) 并 **Name**（命名）日志转发实例，选择 **Filter**（筛选器），然后配置 **Forward Method**（转发方法）（**SNMP**、**Email**、**Syslog** 或 **HTTP**）。

STEP 5 | 配置管理员验证。

1. 选择集群。
2. 选择 **Authentication**（验证）。
3. 选择 **Authentication Profile**（验证配置文件），**None**（无）或**radius**。RADIUS 是唯一支持的外部验证方法。
4. 设置管理员用户的 **Local Authentication**（本地验证）模式为 **Password**（密码）或 **Password Hash**（密码哈希），然后输入 **Password**（密码）。

STEP 6 | 在 Panorama 设备上提交配置并推送至集群。

1. **Commit and Push**（提交并推送）。
2. 如果 Panorama 设备上有不想推送的配置，**Edit Selections**（编辑选择）以选择您要推送配置的设备。推送的配置覆盖集群节点上正在运行的配置，因此所有集群节点运行相同的配置。

为 *WildFire* 集群配置身份验证

通过配置具有精细身份验证参数的本地管理用户，以及利用 RADIUS、TACAS+ 或 LDAP 进行授权和身份验证，为 WildFire 集群中的所有 WildFire 设备创建和配置增强的身份验证。

当您从 Panorama 配置和推送管理员时，将使用您在 Panorama 上配置的管理员覆盖 WildFire 集群中的所有 WildFire 设备的现有管理员。

- 为 WildFire 集群配置管理员帐户
- 为 WildFire 集群配置 RADIUS 身份验证
- 为 WildFire 集群配置 TACACS+ 身份验证
- 为 WildFire 集群配置 LDAP 身份验证

为 **WildFire** 集群配置管理员帐户

为 WildFire 集群中的所有 WildFire 设备创建一个或多个具有精细身份验证参数的管理员，以便从 Panorama™ 管理服务器进行管理。此外，还可以从 Panorama 配置本地管理员，这可以在 WildFire 设备的

© 2019 Palo Alto Networks, Inc.

CLI 上直接进行配置。但是，向 WildFire 设备推送新配置更改会使用为 WildFire 设备配置的管理员覆盖现有本地管理员。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 在 Panorama 上集中配置集群。

STEP 3 | （可选）配置身份验证配置文件以定义身份验证服务，该服务验证访问 WildFire 设备 CLI 的管理员的登录凭据。

STEP 4 | 根据需要配置一个或多个管理员帐户。

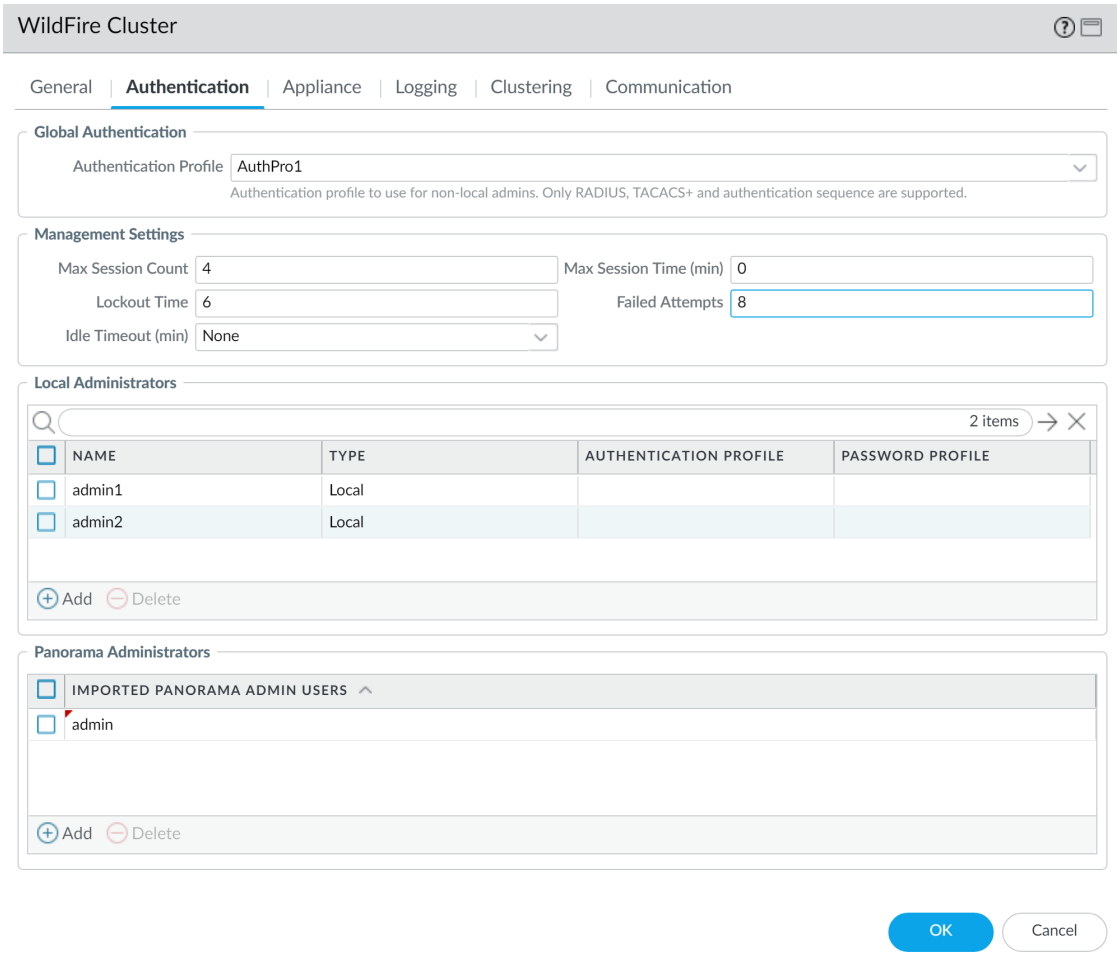
在 Panorama 上创建的管理员帐户之后会导入到 WildFire 集群中的 WildFire 设备并从 Panorama 进行管理。

STEP 5 | 为 WildFire 集群中的 WildFire 设备配置身份验证。

1. 选择 **Panorama** > **Managed WildFire Clusters**（受管 **WildFire** 集群），然后选择您之前配置的 WildFire 集群。
2. （可选）选择您在上一步中配置的 **Authentication Profile**（身份验证配置文件）。
3. 为 WildFire 设备配置身份验证 **Timeout Configuration**（超时配置）。
   1. 输入 **Failed Attempt**（失败尝试）次数，在此次数之后用户将被锁定在 WildFire 设备 CLI 之外。
   2. 输入 **Lockout Time**（锁定时间）（以分钟为单位），此时间即在用户达到配置的 **Failed Attempts**（失败尝试）次数后，WildFire 设备锁定用户帐户的时间。
   3. 输入 **Idle Timeout**（空闲超时）（以分钟为单位），在此时间之后用户会因为不活动而自动注销。
   4. 输入 **Max Session Count**（最大会话计数）以设置多少用户帐户可以同时访问 WildFire 设备。
   5. 输入管理员在自动注销之前可登录的 **Max Session Time**（最长会话时间）。
4. 添加 WildFire 设备管理员。

   管理员可以添加为本地管理员或作为导入的 Panorama 管理员 — 但不能同时为二者。不支持将同一管理员同时添加为本地管理员和作为导入的 Panorama 管理员，这会导致 Panorama 提交失败。例如，如果您将 `admin1` 同时添加为本地和 Panorama 管理员，向 Panorama 的提交将会失败。
   1. **Add**（添加）并配置专属于 WildFire 集群中 WildFire 设备的新管理员。这些管理员特定于为其创建的 WildFire 集群中的 WildFire 设备，您可以从此表格管理这些管理员。
   2. **Add**（添加）在 Panorama 上配置的任何管理员。这些管理员在 Panorama 上创建，并导入至 WildFire 集群中的 WildFire 设备。
5. 单击 **OK**（确定）以保存 WildFire 集群身份验证配置。

© 2019 Palo Alto Networks, Inc.



STEP 6 | **Commit**（提交），然后 **Commit and Push**（提交并推送）您的配置更改。

STEP 7 | 使用本地管理员用户访问 WildFire 设备 CLI 以验证您能够成功访问 WildFire 设备。

为 WildFire 集群配置 RADIUS 身份验证

使用 RADIUS 服务器来验证对 WildFire 集群中所有 WildFire 设备的 CLI 的管理访问权限。您也可以在 RADIUS 服务器上定义供应商特定属性 (VSA) 来管理管理员授权。使用 VSA 使您能够通过目录服务来快速更改管理员的角色、访问域和用户组，这通常比在 Panorama™ 管理服务器上重新配置设置更为容易。

您可以将 Palo Alto Networks RADIUS 词典导入到 *RADIUS* 服务器，以定义实现 *Panorama* 和 *RADIUS* 服务器之间通信的身份验证属性。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 在 Panorama 上集中配置集群。

STEP 3 | 配置 RADIUS 身份验证。

1. 添加 RADIUS 服务器配置文件。

   配置文件定义了 WildFire 集群中的 WildFire 设备连接到 RADIUS 服务器的方式。

   1. 选择 **Panorama** > **Server Profiles**（服务器配置文件）> **RADIUS**，并 **Add**（添加）配置文件。

© 2019 Palo Alto Networks, Inc.

2. 输入 **Profile Name**（配置文件名称）以标识服务器配置文件。
3. 输入身份验证请求超时后以秒为单位的 **Timeout**（超时）（默认为 3；范围为 1-20）。
4. 选择 WildFire 设备用来对 RADIUS 服务器进行身份验证的 **Authentication Protocol**（身份验证协议）（默认为 **CHAP**）。

   如果 *RADIUS* 服务器支持该协议，请选择 *CHAP*；该协议比 *PAP* 更安全。
5. **Add**（添加）每个 RADIUS 服务器，并输入以下内容：
   1. 标识服务器的 **Name**（名称）。
   2. **RADIUS Server**（**RADIUS** 服务器）IP 地址或 FQDN。
   3. **Secret**（密钥）/**Confirm Secret**（确认密钥）（加密用户名和密码的密钥）。
   4. 用于身份验证请求的服务器 **Port**（端口）（默认为 1812）。
6. 单击 **OK**（确定）保存服务器配置文件。

2. 将 RADIUS 服务器配置文件分配到身份验证配置文件。

   身份验证配置文件定义了一组管理员通用的身份验证设置。
   1. 选择 **Panorama** > **Authentication Profile**（身份验证配置文件），并 **Add**（添加）配置文件。
   2. 输入 **Name**（名称）以标识身份验证配置文件。
   3. 将 **Type**（类型）设置为 **RADIUS**。
   4. 选择您配置的 **Server Profile**（服务器配置文件）。
   5. 选择 **Retrieve user group from RADIUS**（从 **RADIUS** 中检索用户组），以从 RADIUS 服务器上定义的 VSA 收集用户组信息。

      Panorama 与您在身份验证配置文件允许列表中指定的组在组信息方面进行匹配。
   6. 选择 **Advanced**（高级），并在允许列表中 **Add**（添加）允许使用此身份验证配置文件进行身份验证的管理员。
   7. 单击 **OK**（确定）保存身份验证配置文件。

STEP 4 | 为 WildFire 集群配置身份验证。

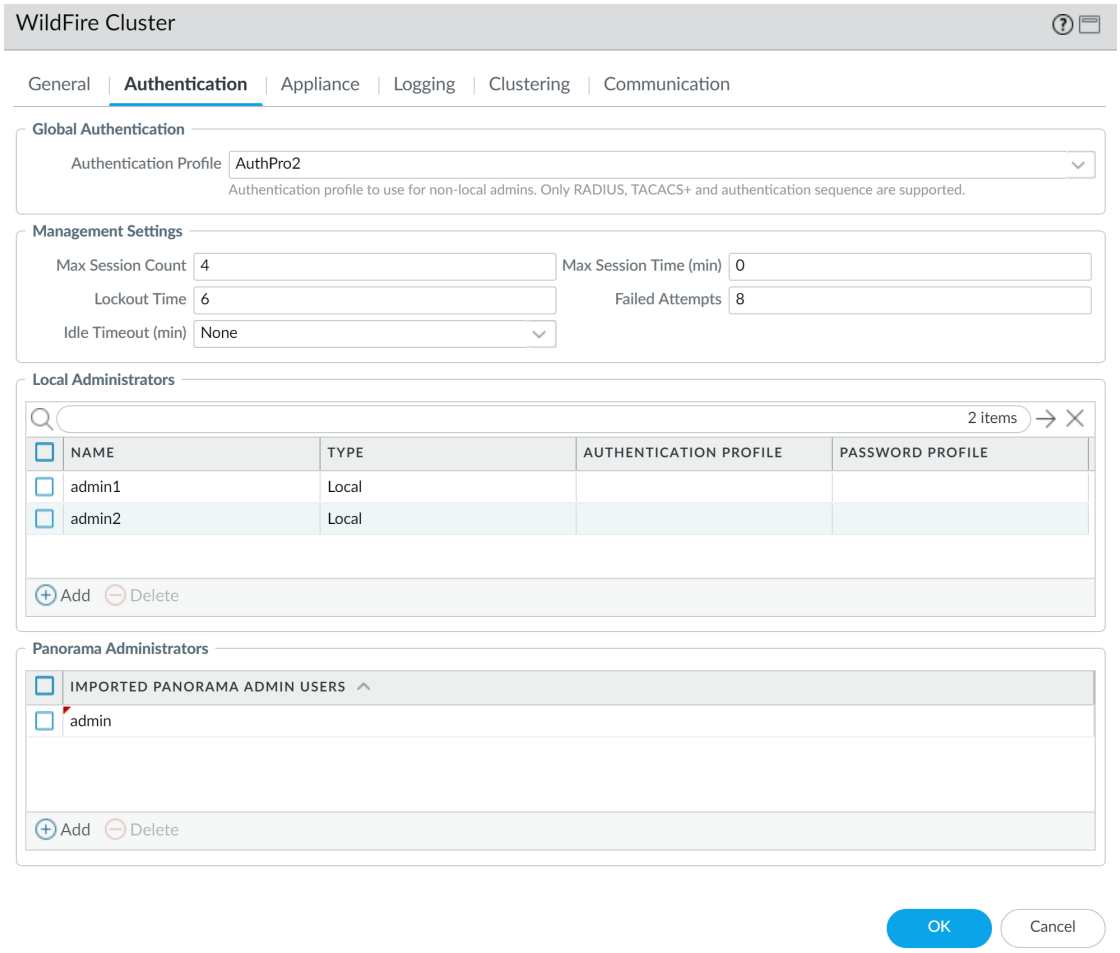
1. 选择 **Panorama** > **Managed WildFire Clusters**（受管 **WildFire** 集群），然后选择您之前添加的 WildFire 集群。
2. 选择您在上一步中配置的 **Authentication Profile**（身份验证配置文件）。

   如果没有分配全局身份验证配置文件，您必须为每个单独的本地管理员分配一个身份验证配置文件才能利用远程身份验证。
3. 为 WildFire 设备配置身份验证 **Timeout Configuration**（超时配置）。
   1. 输入 **Failed Attempt**（失败尝试）次数，在此次数之后用户将被锁定在 WildFire 设备 CLI 之外。
   2. 输入 **Lockout Time**（锁定时间）（以分钟为单位），此时间即在用户达到配置的 **Failed Attempts**（失败尝试）次数后，WildFire 设备锁定用户帐户的时间。
   3. 输入 **Idle Timeout**（空闲超时）（以分钟为单位），在此时间之后用户会因为不活动而自动注销。
   4. 输入 **Max Session Count**（最大会话计数）以设置多少用户帐户可以同时访问 WildFire 设备。
   5. 输入管理员在自动注销之前可登录的 **Max Session Time**（最长会话时间）。
4. 添加 WildFire 设备管理员。

   管理员可以添加为本地管理员或作为导入的 Panorama 管理员 — 但不能同时为二者。不支持将同一管理员同时添加为本地管理员和作为导入的 Panorama 管理员，这会导致 Panorama 提交失败。例如，如果您将 `admin1` 同时添加为本地和 Panorama 管理员，向 Panorama 的提交将会失败。
   1. **Add**（添加）并配置专属于 WildFire 集群中 WildFire 设备的新管理员。这些管理员特定于为其创建的 WildFire 集群中的 WildFire 设备，您可以从此表格管理这些管理员。
   2. **Add**（添加）在 Panorama 上配置的任何管理员。这些管理员在 Panorama 上创建，并导入至 WildFire 集群中的 WildFire 设备。

© 2019 Palo Alto Networks, Inc.

5. 单击 **OK**（确定）以保存 WildFire 集群身份验证配置。



STEP 5 | **Commit**（提交），然后 **Commit and Push**（提交并推送）您的配置更改。

STEP 6 | 使用本地管理员用户访问 WildFire 设备 CLI 以验证您能够成功访问 WildFire 设备。

为 WildFire 集群配置 TACACS+ 身份验证

您可以使用 TACACS+ 服务器来验证对 WildFire 集群中所有 WildFire 设备的 CLI 的管理访问权限。您也可以在 TACACS+ 服务器上定义供应商特定属性 (VSA) 来管理管理员授权。使用 SAML 使您能够通过目录服务来快速更改管理员的角色、访问域和用户组，这通常比在 Panorama 上重新配置设置更为容易。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 在 Panorama 上集中配置集群。

STEP 3 | 配置 TACACS+ 身份验证。

1. 添加 TACACS+ 服务器配置文件。

   配置文件定义了 WildFire 设备连接到 TACACS+ 服务器的方式。

   1. 选择 **Panorama** > **Server Profiles**（服务器配置文件）> **TACACS+**，并 **Add**（添加）配置文件。
   2. 输入 **Profile Name**（配置文件名称）以标识服务器配置文件。
   3. 输入身份验证请求超时后以秒为单位的 **Timeout**（超时）（默认为 3；范围为 1-20）。

© 2019 Palo Alto Networks, Inc.

4. 选择 Panorama 用来对 TACACS+ 服务器进行身份验证的 **Authentication Protocol**（身份验证协议）（默认为 **CHAP**）。
5. 如果 TACACS+ 服务器支持该协议，请选择 **CHAP**；该协议比 **PAP** 更安全。
6. **Add**（添加）每个 TACACS+ 服务器，并输入以下内容：
    1. 标识服务器的 **Name**（名称）。
    2. **TACACS+ Server**（**TACACS+** 服务器）IP 地址或 FQDN。
    3. **Secret**（密钥）/**Confirm Secret**（确认密钥）（加密用户名和密码的密钥）。
    4. 用于身份验证请求的服务器 **Port**（端口）（默认为 49）。
7. 单击 **OK**（确定）保存服务器配置文件。

2. 将 TACACS+ 服务器配置文件分配到身份验证配置文件。

   身份验证配置文件定义了一组管理员通用的身份验证设置。

    1. 选择 **Panorama** > **Authentication Profile**（身份验证配置文件），并 **Add**（添加）配置文件。
    2. 输入 **Name**（名称）以标识配置文件。
    3. 将 **Type**（类型）设置为 **TACACS+**。
    4. 选择您配置的 **Server Profile**（服务器配置文件）。
    5. 选择 **Retrieve user group from TACACS+**（从 **TACACS+** 中检索用户组），以从 TACACS+ 服务器上定义的 VSA 收集用户组信息。

       Panorama 与您在身份验证配置文件允许列表中指定的组在组信息方面进行匹配。
    6. 选择 **Advanced**（高级），并在允许列表中 **Add**（添加）允许使用此身份验证配置文件进行身份验证的管理员。
    7. 单击 **OK**（确定）保存身份验证配置文件。

STEP 4 | 为 WildFire 集群配置身份验证。

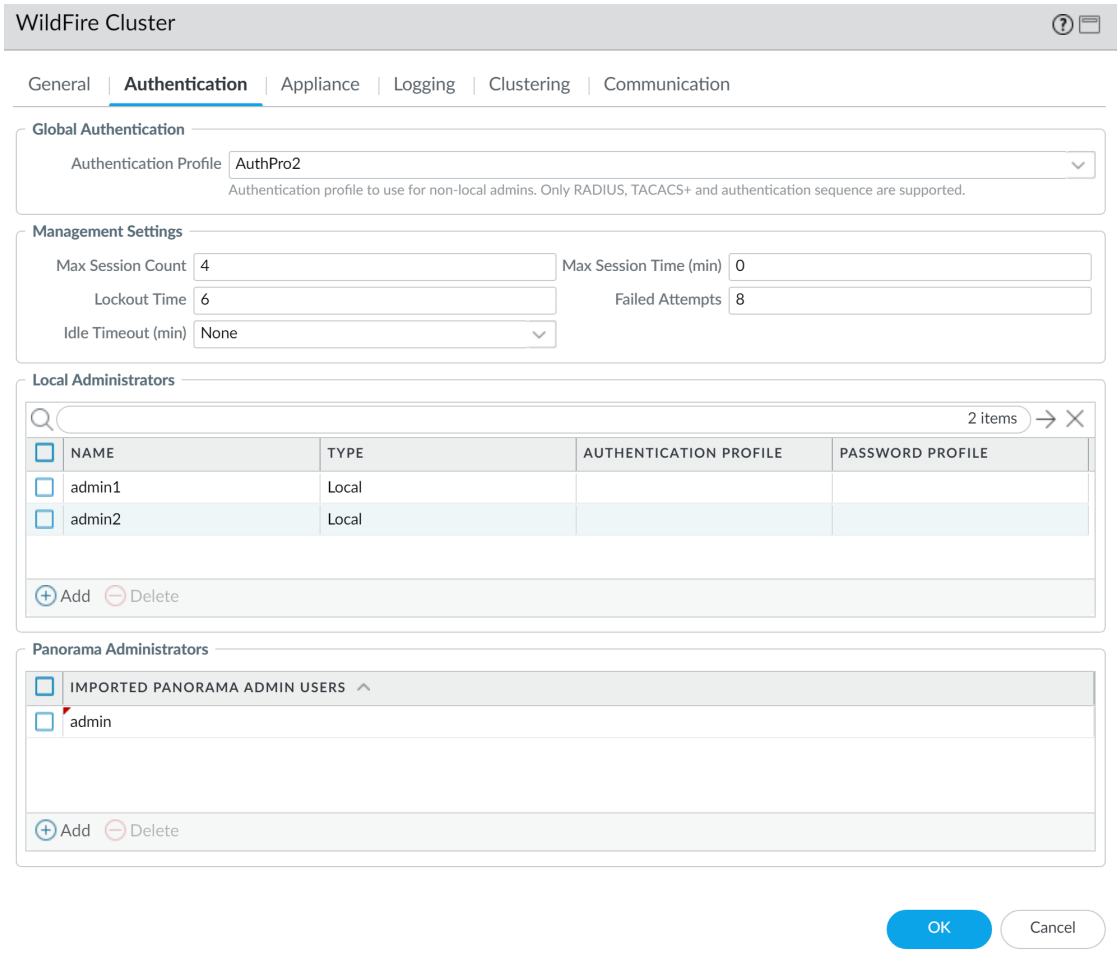
1. 选择 **Panorama** > **Managed WildFire Clusters**（受管 **WildFire** 集群），然后选择您之前添加的 WildFire 集群。
2. 选择您在上一步中配置的 **Authentication Profile**（身份验证配置文件）。

   如果没有分配全局身份验证配置文件，您必须为每个单独的本地管理员分配一个身份验证配置文件才能利用远程身份验证。
3. 为 WildFire 设备配置身份验证 **Timeout Configuration**（超时配置）。
    1. 输入 **Failed Attempt**（失败尝试）次数，在此次数之后用户将被锁定在 WildFire 设备 CLI 之外。
    2. 输入 **Lockout Time**（锁定时间）（以分钟为单位），此时间即在用户达到配置的 **Failed Attempts**（失败尝试）次数后，WildFire 设备锁定用户帐户的时间。
    3. 输入 **Idle Timeout**（空闲超时）（以分钟为单位），在此时间之后用户会因为不活动而自动注销。
    4. 输入 **Max Session Count**（最大会话计数）以设置多少用户帐户可以同时访问 WildFire 设备。
    5. 输入管理员在自动注销之前可登录的 **Max Session Time**（最长会话时间）。
4. 添加 WildFire 设备管理员。

   管理员可以添加为本地管理员或作为导入的 Panorama 管理员 — 但不能同时为二者。不支持将同一管理员同时添加为本地管理员和作为导入的 Panorama 管理员，这会导致 Panorama 提交失败。例如，如果您将 `admin1` 同时添加为本地和 Panorama 管理员，向 Panorama 的提交将会失败。

    1. **Add**（添加）并配置专属于 WildFire 集群中 WildFire 设备的新管理员。这些管理员特定于为其创建的 WildFire 集群中的 WildFire 设备，您可以从此表格管理这些管理员。
    2. **Add**（添加）在 Panorama 上配置的任何管理员。这些管理员在 Panorama 上创建，并导入至 WildFire 集群中的 WildFire 设备。
5. 单击 **OK**（确定）以保存 WildFire 集群身份验证配置。

© 2019 Palo Alto Networks, Inc.



STEP 5 | **Commit**（提交），然后 **Commit and Push**（提交并推送）您的配置更改。

STEP 6 | 使用本地管理员用户访问 WildFire 设备 CLI 以验证您能够成功访问 WildFire 设备。

为 **WildFire** 集群配置 **LDAP** 身份验证

您可以使用 LDAP 对访问 WildFire 集群中 WildFire 设备 CLI 的最终用户进行身份验证。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 在 Panorama 上集中配置集群。

STEP 3 | 添加 LDAP 服务器配置文件。

配置文件定义了 WildFire 设备连接到 LDAP 服务器的方式。

1. 选择 **Panorama** > **Server Profiles**（服务器配置文件）> **LDAP**，然后 **Add**（添加）服务器配置文件。
2. 输入 **Profile Name**（配置文件名称）以标识服务器配置文件。
3. **Add**（添加）LDAP 服务器（最多 4 个）。对于每个服务器，输入 **Name**（名称）（以标识服务器）、**LDAP Server**（**LDAP** 服务器）IP 地址或 FQDN 以及服务器 **Port**（端口）（默认为 389）。

   如果使用 *FQDN* 地址对象来标识服务器，并随后更改地址，则必须提交更改以使新服务器地址生效。
4. 选择服务器 **Type**（类型）。

© 2019 Palo Alto Networks, Inc.

5. 选择 **Base DN**（基本 **DN**）。

   要标识目录的基本 DN，请打开 **Active Directory Domains and Trusts**（活动目录域和信任）Microsoft 管理控制台控制单元，并使用顶级域的名称。
6. 输入 **Bind DN**（绑定 **DN**）和 **Password**（密码）以启用身份验证服务对防火墙进行身份验证。

   绑定 *DN* 账户必须有权读取 *LDAP* 目录。
7. 以秒为单位输入 **Bind Timeout**（绑定超时）和 **Search Timeout**（搜索超时）（默认均为 30）。
8. 输入 **Retry Interval**（重试时间间隔），以秒计（默认为 60）。
9. （可选）如果您希望端点使用 SSL 或 TLS 与目录服务器建立更安全的连接，启用 **Require SSL/TLS secured connection**（需要 **SSL/TLS** 安全连接）选项（默认启用）。端点使用的协议取决于服务器端口：
   - 389（默认）— TLS（具体来说，WildFire 设备使用 StartTLS 操作，这会将初始明文连接升级到 TLS。）
   - 636 — SSL
   - 任何其他端口 — WildFire 设备首先尝试使用 TLS。如果目录服务器不支持 TLS，则 WildFire 设备回退至 SSL。
10. （可选）如需额外的安全性，启用 **Verify Server Certificate for SSL sessions**（验证 **SSL** 会话的服务器证书）选项，使端点验证目录服务器为 SSL/TLS 连接出示的证书。要启用验证，还必须启用 **Require SSL/TLS secured connection**（需要 **SSL/TLS** 安全连接）选项。为了验证成功，证书必须符合以下条件之一：
    - 它位于 Panorama 证书列表中：**Panorama** > **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书）。必要时，将证书导入 Panorama。
    - 证书签发机构位于可信证书授权机构列表中：**Panorama** > **Certificate Management**（证书管理）> **Certificates**（证书）。
11. 单击 **OK**（确定）保存服务器配置文件。

STEP 4 | 为 WildFire 集群配置身份验证。

1. 选择 **Panorama** > **Managed WildFire Clusters**（受管 **WildFire** 集群），然后选择您之前添加的 WildFire 集群。
2. 为 WildFire 设备配置身份验证 **Timeout Configuration**（超时配置）。
   1. 输入 **Failed Attempt**（失败尝试）次数，在此次数之后用户将被锁定在 WildFire 设备 CLI 之外。
   2. 输入 **Lockout Time**（锁定时间）（以分钟为单位），此时间即在用户达到配置的 **Failed Attempts**（失败尝试）次数后，WildFire 设备锁定用户帐户的时间。
   3. 输入 **Idle Timeout**（空闲超时）（以分钟为单位），在此时间之后用户会因为不活动而自动注销。
   4. 输入 **Max Session Count**（最大会话计数）以设置多少用户帐户可以同时访问 WildFire 设备。
   5. 输入管理员在自动注销之前可登录的 **Max Session Time**（最长会话时间）。
3. 添加 WildFire 设备管理员。

   管理员可以添加为本地管理员或作为导入的 Panorama 管理员 — 但不能同时为二者。不支持将同一管理员同时添加为本地管理员和作为导入的 Panorama 管理员，这会导致 Panorama 提交失败。例如，如果您将 `admin1` 同时添加为本地和 Panorama 管理员，向 Panorama 的提交将会失败。
   - 配置本地管理员。

     配置专属于 WildFire 集群中 WildFire 设备的新管理员。这些管理员特定于为其创建的 WildFire 集群中的 WildFire 设备，您可以从此表格管理这些管理员。
     1. **Add**（添加）一个或多个新本地管理员。
     2. 输入本地管理员的 **Name**（名称）。
     3. 配置一个您之前创建的 **Authentication Profile**（身份验证配置文件）。

© 2019 Palo Alto Networks, Inc.

仅单个本地管理员才支持 *LDAP* 身份验证配置文件。

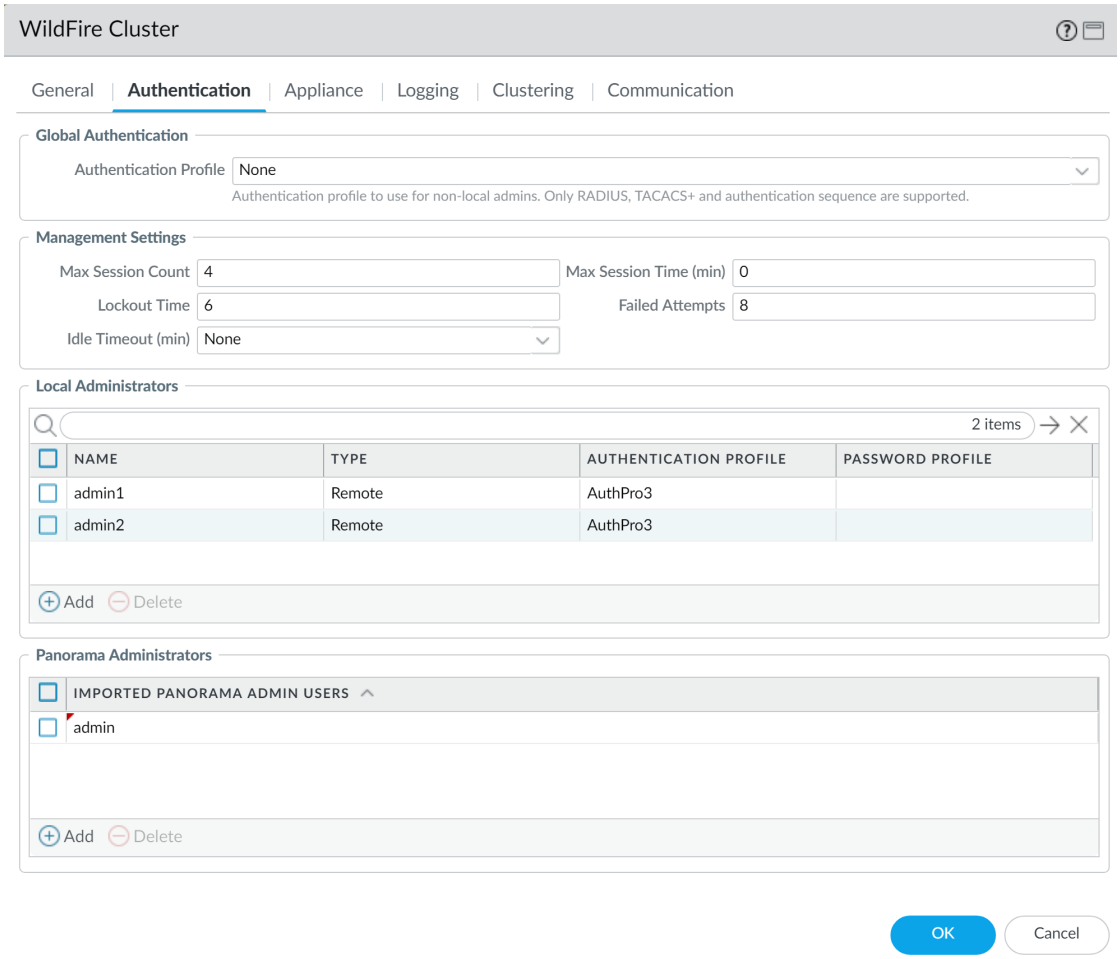
4. 启用（选中）**Use Public Key Authentication (SSH)**（使用公钥身份验证 **(SSH)**）以导入公钥文件进行身份验证。
5. 选择一个 **Password Profile**（密码配置文件）以设置过期参数。

- 导入现有 Panorama 管理员

  导入在 Panorama 上配置的现有管理员。这些管理员在 Panorama 上配置和管理，并导入至 WildFire 集群中的所有 WildFire 设备。

1. **Add**（添加）现有 Panorama 管理员

4. 单击 **OK**（确定）以保存 WildFire 集群身份验证配置。



STEP 5 | **Commit**（提交），然后 **Commit and Push**（提交并推送）您的配置更改。

STEP 6 | 使用本地管理员用户访问 WildFire 设备 CLI 以验证您能够成功访问 WildFire 设备。

从 *Panorama* 管理移除集群

要从 Panorama 管理移除集群，**Panorama** > **Managed WildFire Clusters**（受管理的 **WildFire** 集群）并选择您想要移除的集群行（请勿点击集群名称）**Remove From Panorama**（从 **Panorama** 移除）。

如果您从 Panorama 管理中移除 WildFire 设备集群，Panorama 网络界面将该集群内的 WildFire 设备转为只读模式。尽管被移除集群内的 WildFire 设备显示于 Panorama 网络界面，当在只读模式时，您无法推送配置

© 2019 Palo Alto Networks, Inc.

至 WildFire 设备或通过 Panorama 进行管理。从 Panorama 管理中被移除后，WildFire 设备集群成员使用本地集群配置，且您可以通过本地 CLI 管理集群。

从 Panorama 管理移除集群后，要在集群内通过 Panorama 管理 WildFire 设备，将集群重新导入 Panorama（**Panorama** > **Managed WildFire Clusters**（受管理的 **WildFire** 集群）> **Import Cluster Config**（导入集群配置））。

STEP 1 | 选择集群控制器节点。集群名称自动填充 **Cluster**（集群）。

STEP 2 | 单击 **OK**（确定）。集群备份控制器节点和工作节点自动填充。

STEP 3 | 单击 **OK**（确定）以导入集群。

STEP 4 | **Commit**（提交）更改。

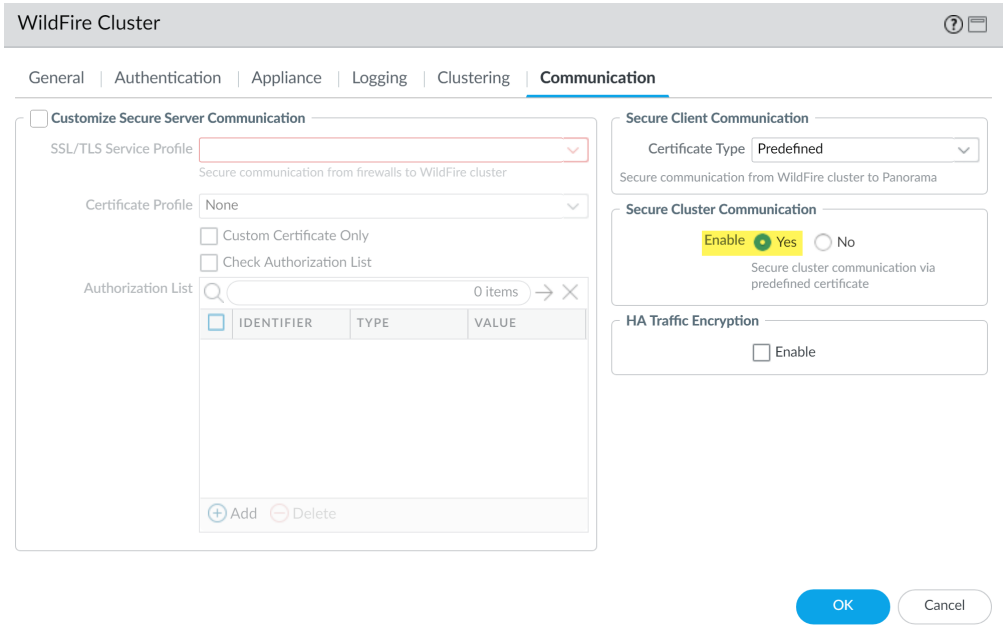
使用预定义证书在 *Panorama* 上集中配置设备到设备加密

STEP 1 | 将每个受管 Wildfire 设备升级到 PAN-OS 8.1.x。所有受管设备必须运行 PAN-OS 8.1 版或更高版本才能启用设备到设备加密。

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

STEP 3 | 在 Panorama 上选择 **Panorama> Managed WildFire Clusters**（受管 **Wildfire** 集群）> *WF_cluster_name*> **Communication**（通信）。

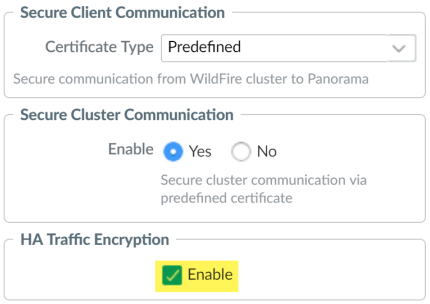
STEP 4 | **Enable**（启用）安全集群通信。



STEP 5 | （推荐）启用 HA 流量加密。该设置（可选）可对 HA 对之间的 HA 流量进行加密，也是 Palo Alto Networks 推荐的最佳做法。

在 *FIPS/CC* 模式下运行时，不得禁用 *HA* 流量加密。

© 2019 Palo Alto Networks, Inc.



STEP 6 | 单击 **OK**（确定）以保存**WildFire Cluster**（**WildFire** 集群）设置。

STEP 7 | **Commit**（提交）更改。

使用自定义证书在 *Panorama* 上集中配置设备到设备加密

STEP 1 | 将每个受管 Wildfire 设备升级到 PAN-OS 8.1.x。所有受管设备必须运行 PAN-OS 8.1 版或更高版本才能启用设备到设备加密。

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

STEP 3 | 查看您现有的 WildFire 安全通信配置。请记住，如果您先前已使用自定义证书完成 WildFire 设备和防火墙配置为进行安全通信，则还可以使用该自定义证书来实现 WildFire 设备之间的安全通信.

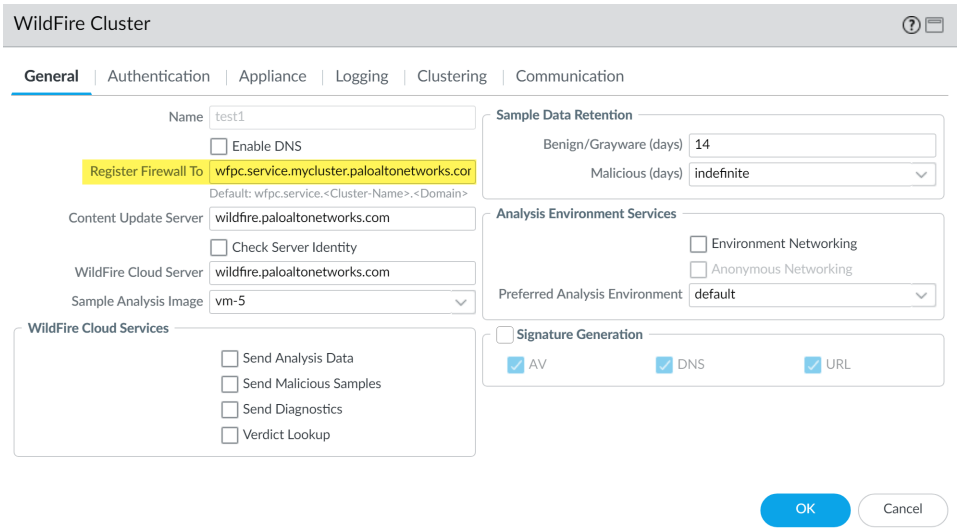
1. 选择 **Panorama >Managed WildFire Clusters**（受管理的 **Wildfire** 集群）> *WF_cluster_name*> **Communication**（通信）。
2. 如果已启用 **Customize Secure Server Communication**（自定义安全服务器通信），且您要使用此证书，则确定正在使用的自定义证书详细信息。否则，请继续步骤 5 ，以开始安装新的自定义证书的流程。
3. 确定将在步骤 4 中用于定义防火墙注册地址的自定义证书 FQDN（DNS 名称）。

必须注意自定义证书的名称和关联 *FQDN*。配置时会多次引用。

STEP 4 | 在 Panorama 上配置防火墙注册地址。

1. 在 Panorama 上选择 **Panorama >Managed WildFire Clusters**（受管理的 **Wildfire** 集群）> *WF_cluster_name*> **General**（常规）。
2. 在 注册防火墙至字段中，指定用于自定义证书中找到的身份验证 DNS 名称（通常是主题名称或主题备用名称）。例如，默认域名为 **`wfpc.service.mycluster.paloaltonetworks.com`**。

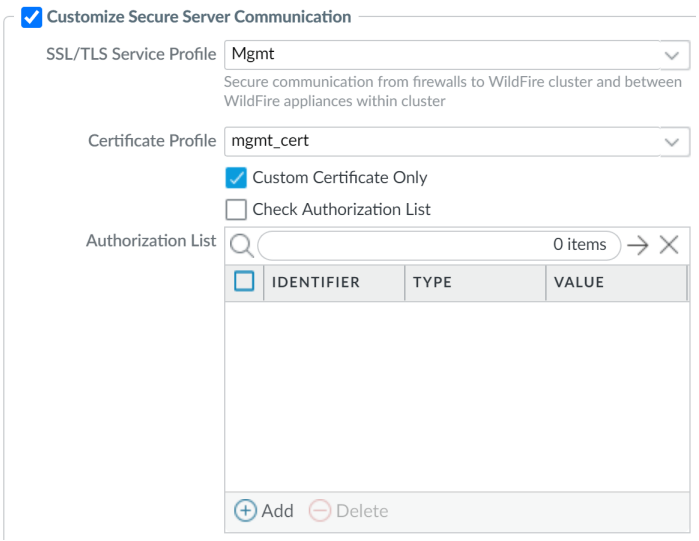
© 2019 Palo Alto Networks, Inc.



STEP 5 | 在 Panorama 上配置 安全服务器通信设置。如果您已成功配置防火墙和 WildFire 集群之间的安全通信，且正在使用现有的自定义证书，请继续下面的步骤 4。

1. 在 Panorama 上选择 **Panorama> Managed WildFire Clusters**（受管理的 **Wildfire** 集群）> *WF_cluster_name*> **Communication**（通信）。
2. 单击 **Customize Secure Server Communication**（自定义安全服务器通信）。
3. 配置并部署用于 WildFire 设备和关联防火墙的自定义证书。SSL/TLS 服务配置文件定义 WildFire 设备用于与 WildFire 设备对等体和防火墙进行通信的自定义证书。此外，还必须在与 WildFire 设备集群关联的防火墙上配置自定义证书设置。稍后将在步骤 9 进行配置。
   1. 打开 SSL/TLS 服务配置文件下拉列表，并单击 SSL/TLS 服务配置文件。通过您要使用的自定义证书配置 SSL/TLS 服务配置文件。SSL/TLS 服务配置文件配置完成后，单击确定，然后选择新创建的 SSL/TLS 服务配置文件。
   2. 打开证书配置文件下拉列表，并单击证书配置文件。配置证书配置文件，以标识用于在防火墙和 WildFire 设备之间，以及 WildFire 对等设备之间建立安全连接的自定义证书。证书配置文件配置完成后，单击确定，然后选择新创建的配置文件。
4. 选中 **Custom Certificate Only**（仅允许自定义证书）复选框。此时，您可以使用配置的自定义证书，而不是默认的预配置证书。
5. （可选）配置授权列表。授权列表检查自定义证书的主题名称或主题备用名称；如果使用自定义证书的 主题 或 主题备用名名称不与授权列表上的标识符匹配，则拒绝身份验证。
   1. **Add**（添加）授权列表。
   2. 选择在自定义证书配置文件中配置的 **Subject**（主题）或 **Subject Alt Name**（主题备用名称）作为标识符类型。
   3. 如果标识符为 Subject（主题），则输入通用名，如果标识符为 Subject Alt Name（主题备用名称），则输入 IP 地址、主机名或电子邮件。
   4. 单击 **OK**（确定）。
   5. 选择 **Check Authorization List**（检查授权列表）以执行授权列表。
6. 单击 **OK**（确定）。

© 2019 Palo Alto Networks, Inc.



STEP 6 | **Enable**（启用）安全集群通信。

STEP 7 | （推荐）启用 HA 流量加密。该设置（可选）可对 HA 对之间的 HA 流量进行加密，也是 Palo Alto Networks 推荐的最佳做法。

在 *FIPS/CC* 模式下运行时，不得禁用 *HA* 流量加密。

STEP 8 | 单击 **OK**（确定）以保存**WildFire Cluster**（**WildFire** 集群）设置。

STEP 9 | 在 Panorama 上配置防火墙 安全通行设置，将 WildFire 设备集群与防火墙自定义证书相关联。这便为防火墙和 WildFire 设备集群之间创建一条安全通信通道。如果您已成功配置防火墙和 WildFire 设备集群之间的安全通信，且正在使用现有的自定义证书，请继续下一步。

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

STEP 10 | **Commit**（提交）更改。

通过 Panorama 查看 WildFire 集群状态

要确认配置的 WildFire 设备集群正常运行，您可以通过 Panorama 设备查看当前状态。

Palo Alto Networks 建议使用 *WildFire* 设备 *CLI* 验证您的 *WildFire* 集群状态。无法从 *Panorama* 看到的其他状态详情在命令输出中显示。

STEP 1 | 在主 Panorama 设备上，选择**Panorama > Managed WildFire Clusters**（管理的 **WildFire** 集群）。

STEP 2 | 在 **Cluster Status**（集群状态）列中，验证：

© 2019 Palo Alto Networks, Inc.

1. Wfpc 和签名服务正在运行。
2. 无其他操作。异常操作及其状态条件包括：
   - 取消授权 [已请求/正在进行/已拒绝/成功/失败]
   - 暂停 [已请求/正在进行/已拒绝/成功/失败]
   - 重启 [已请求/正在进行/已拒绝/成功/失败]
   - 集群 [离线/裂脑/未就绪]
   - 服务 [已暂停/无]
   - 高可用性 [对等机离线 / cfg-not-sync / cfg-sync-off]

STEP 3 | 在 **Config Status**（配置状态）列中，验证：

1. 设备配置为与 Panorama 设备上存储的配置 **In Sync**（同步）。
2. 无其他状态。异常状态条件包括：
   - **Out of Sync**（不同步）[设备配置与在 Panorama 上保存的配置不同步。可以将鼠标悬停在放大镜上方以显示同步失败的原因。]

STEP 4 | 在 **Connected**（已连接）列中，验证配置的 WildFire 设备显示 **Connected**（已连接）状态。

通过互联网连接在 Panorama 上集中升级集群

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 只能管理运行相同软件版本或更新软件版本的 *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。

© 2019 Palo Alto Networks, Inc.

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 6.1 升级至 PAN-OS 7.1，您必须首先下载并安装版本 7.0。

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. 选择安装模式：
    - （8.0.2 和以上）**Select Reboot device after install**（选择安装后重启设备）。
    - （8.0.1 和以上）选择 **Upload only**（仅上传）。
5. 单击 **OK**（确定）以开始安装。
6. （可选）在 Panorama 上监控安装进度。
7. （仅 8.0.1）在升级包上传完成后，在各节点上安装升级：
    1. ```
       admin@WF-500 (passive-controller)> request system software install
        version 8.0.2
       ```
    2. 确认是否已完成升级。运行以下命令，然后查找作业类型 **Install** 和状态 **FIN**：

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

       Enqueued Dequeued ID Type Status Result Completed
       ------------------------------------------------
       14:53:15 14:53:15 5 Install FIN    OK   14:53:19
       ```
    3. 重启设备：

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

       升级程序可能需要 *10* 分钟至一个小时以上，具体取决于 *WildFire* 设备上存储的样本数。
    4. 为集群内的各 WildFire 工作节点重复操作。

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
```


© 2019 Palo Alto Networks, Inc.
```

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 8.0.1：

```
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
```

不通过互联网连接在 Panorama 上集中升级集群

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 只能管理运行相同软件版本或更新软件版本的 *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：

© 2019 Palo Alto Networks, Inc.

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 6.1 升级至 PAN-OS 7.1，您必须首先下载并安装版本 7.0。

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. 选择安装模式：
   - （8.0.2 和以上）**Select Reboot device after install**（选择安装后重启设备）。
   - （8.0.1 和以上）选择 **Upload only**（仅上传）。
5. 单击 **OK**（确定）以开始安装。
6. （可选）在 Panorama 上监控安装进度。
7. （仅 8.0.1）在升级包上传完成后，在各节点上安装升级：
   1. ```
      admin@WF-500 (passive-controller)> request system software install
       version 8.0.2
      ```
   2. 确认是否已完成升级。运行以下命令，然后查找作业类型 **Install** 和状态 **FIN**：

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

      Enqueued Dequeued ID Type Status Result Completed
      ------------------------------------------------------
      14:53:15 14:53:15 5 Install FIN    OK   14:53:19
      ```
   3. 重启设备：

© 2019 Palo Alto Networks, Inc.
      ```

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



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

4. 为集群内的各 WildFire 工作节点重复步骤 7。

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 8.0.1：

```
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
```

管理许可证和更新

您可以使用 Panorama™ 管理服务器集中管理防火墙和专用日志收集器上的许可证、软件更新和内容更新。当您部署许可证或更新时，Panorama 将检查 Palo Alto Networks® 许可服务器或更新服务器，验证请求有效性，然后允许检索和安装许可证或更新。该功能消除了在每个防火墙或专用日志收集器上重复执行相当任务的需要，因此使部署更为便利。它特别适合用于管理无法直接访问互联网的防火墙或管理没有 Web 界面的专用日志收集器。

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更新版本兼容性的重要详细信息。

您必须在每个防火墙上直接激活支持订阅；不能使用 Panorama 部署支持订阅。

若要在 Panorama 管理服务器上激活或安装更新，请参阅注册 Panorama 和安装许可证和安装 Panorama 的内容和软件更新。

> 在防火墙上使用 Panorama 管理许可证
> 使用 Panorama 将更新部署到防火墙、日志收集器和 WildFire 设备

在防火墙上使用 Panorama 管理许可证

以下步骤介绍了如何使用身份验证（身份验证）代码获取新许可证并将许可证密钥推送到受管防火墙。此外，这些步骤还介绍了如何手动更新（刷新）无法直接访问互联网的防火墙的状态。对于可直接访问互联网的防火墙，Panorama™ 将使用许可服务器自动执行每日签到、检索许可证更新和续期，并将其推送到防火墙。签到采用硬编码，时间设定在凌晨 1 点和 2 点；您不可更改此时间安排。



您不能使用 *Panorama* 激活防火墙的支持许可证。您必须单独访问防火墙才能激活其支持许可证。

要激活 *Panorama* 的许可证，请参阅注册 Panorama 和安装许可证。

- 激活新买的许可证。
  1. 选择 **Panorama** > **Device Deployment**（设备部署）> **Licenses**（许可证）和 **Activate**（激活）。
  2. 输入 Palo Alto Networks® 为每个有新许可证的防火墙提供的 **Auth Code**（身份验证代码）。
  3. **Activate**（激活）许可证。
  4. （仅限 WildFire® 订阅）在每个有 WildFire 新订阅的防火墙上执行提交，完成激活：
     - **Commit**（提交）任何暂挂的更改。您必须访问每个防火墙 Web 界面来完成此操作。
     - 如果没有配置更改暂挂，请进行小的更改并 **Commit**（提交）。例如，更新规则说明并提交更改。如果防火墙属于同一设备组，您可以从 Panorama 推送规则更改，在所有这些防火墙上启动提交，而不是单独访问每个防火墙。

     检查 WildFire 分析配置文件规则是否包括 *WildFire* 订阅支持的高级文件类型。

- 更新防火墙的许可证状态。
  1. 选择 **Panorama** > **Device** > **Deployment**（设备部署）。

     页面上的每个条目都可表明许可证是有效或无效，并显示有效许可证的到期日期。
  2. 如果您之前已在防火墙上直接激活支持订阅的身份验证代码，请单击 **Refresh**（刷新）并从列表中选择防火墙。Panorama 检索许可证、将其部署到防火墙并在 Panorama Web 界面上更新许可状态。
  3. （仅限企业数据丢失防护 (DLP) 许可证）将更新的许可证推送到利用企业 DLP 的受管防火墙。
     1. 单击 **Commit**（提交）和 **Commit to Panorama**（提交至 **Panorama**）。
     2. 选择 **Commit**（提交）> **Push to Devices**（推送到设备）和 **Edit Selections**（编辑选择）。
     3. 选择 **Templates**（模板），然后选择与利用企业 DLP 的受管防火墙关联的模板堆栈。

        单击 **OK**（确定）继续。
     4. **Push**（推送）模板配置以成功更新企业 DLP 许可证。

© 2019 Palo Alto Networks, Inc.

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。

- 支持的更新
- 使用 Panorama 计划内容更新
- 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
- 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
- 从 Panorama 恢复内容更新

支持的更新

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 BrightCloud URL 筛选 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

© 2019 Palo Alto Networks, Inc.

设备类型	软件更新	内容更新
		BrightCloud URL 筛选 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。

Panorama 一次只能下载一个更新以获取相同类型的更新，因此如果您安排在相同时间间隔内下载相同类型的多个更新，则只有第一个下载会成功。要确保相同类型的多个更新成功，请在不同时段下载更新。

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。

© 2019 Palo Alto Networks, Inc.

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。

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。

PAN-OS® 9.0 已引入了用于本地和专用日志收集器的新日志数据格式。在向 PAN-OS 10.0 升级路径中，现有日志数据会在升级到 PAN-OS 9.0 时自动迁移到新格式。在重新格式化期间，**ACC** 或 **Monitor**（监控）选项卡中不会显示日志数据。此外，在重新格式化未完成之前，新的日志数据不会转发到日志收集器。重新格式化时，会将新日志写入到防火墙系统磁盘，且在此程序成功完成后，新日志会转发到相应的日志收集器。

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 *Panorama* 软件版本，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（或更高版本）的软件版本，但必须具有相同或更早版本的内容版本：

- 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更新受管防火墙（使用 Panorama），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 | 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. **Check Now**（立即检查）（**Panorama** > **Device Deployment**（设备部署）> **Dynamic Updates**（动态更新））最新更新。如果有更新可用，“操作”列会显示 **Download**（下载）链接。
2. 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）。
3. 在任何其他更新之前安装内容更新（应用程序或应用程序和威胁更新）：

   单击 **Install**（安装），选择日志收集器，然后单击 **OK**（确定）。

© 2019 Palo Alto Networks, Inc.

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。

4. 对于任何其他更新（Antivirus、WildFire 或 URL 筛选），根据需要一次性以任何顺序重复上述子步骤 2 和 3。

STEP 3 | 确定到 PAN-OS 10.0 的升级路径。

在从当前运行的 PAN-OS 版本升级到 PAN-OS 10.0 的路径中，您无法跳过任何功能发行版本的安装。查看发行说明中的已知问题和对默认行为的更改，以及新功能指南中的升级/降级考虑因素，了解通过其作为升级路径的一部分的每个版本。

（从 7.1 或更早版本升级时需要）PAN-OS 8.0 引入了新的日志存储格式。升级到 PAN-OS 8.0 后，在继续升级之前，必须将 Panorama 日志迁移到新日志格式。日志迁移是一次性任务；如果您已迁移日志收集器上的日志以升级到 PAN-OS 8.0，则无需再次迁移它们。

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 4 | 对于您打算更新到 PAN-OS 10.0 的所有日志收集器，请继续使用在步骤 3 中确定的升级路径将日志收集器升级到目标 Panorama 版本。

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. 对于升级路径中的每个版本，**Download**（下载）您正在升级的发行版本的型号特定文件。例如，要将 M-Series 设备升级到 Panorama 10.-.0，请下载 `Panorama_m-10.0.0` 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. 单击升级路径中第一个（或下一个）版本的 **Install**（安装），然后选择相应的日志收集器。
4. 根据您在升级路径内安装的版本（步骤 3），选择以下一项：
   - **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）。
5. 单击 **OK**（确定）开始安装（或上传）。
6. 重复上述子步骤3至 5，直到日志收集器运行所需的版本。

STEP 5 | 成功升级到 PAN-OS 10.0 后，请检查日志格式迁移状态。

1. 登录到 Panorama 命令行界面日志收集器。
2. 运行以下命令以检查日志格式迁移的状态：

```
admin> debug logdb show-es-upgrade-time
```

示例 — 日志格式迁移仍在运行时的响应：

```
Response from logger 23456212: 50.98% of indices upgraded complete.
 Approximately less than a minute remaining until migration is complete.
 Once the log migration is complete, please run the 'show log-collector-
es-cluster health' command to check the ElasticSearch cluster status to
 verify logging and reporting functionality is restored.
```

日志格式迁移完成后的响应：

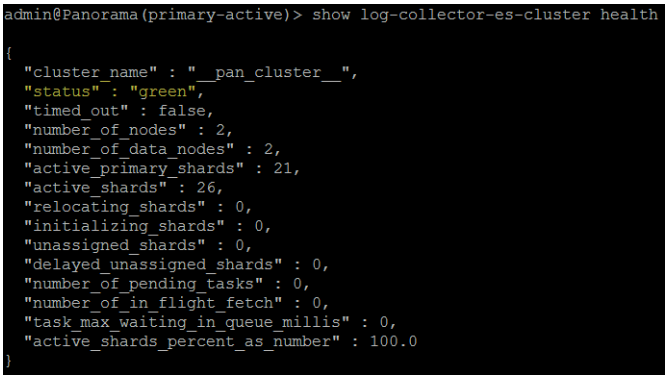
© 2019 Palo Alto Networks, Inc.

```
Response from logger 23456212: 100% of indices complete, please
 run the 'show log-collector-es-culster health' command to check
 the ElasticSearch cluster status to verify logging and reporting
 functionality is restored.
```

3. 日志格式迁移结束后继续进行下一步之前，运行以下命令以检查 ElasticSearch 群集的状态：

```
admin> show log-collector-es-cluster health
```

当 ElasticSearch 群集的健康 `status` 显示为 `green`时，可继续进行下一步：



STEP 6 | 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-version: 10.0.0
app-version: 8270-6076
app-release-date: 2020/05/08 18:21:51
```

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。

PAN-OS® 9.0 已引入了用于本地和专用日志收集器的新日志数据格式。在向 PAN-OS 10.0 升级路径中，现有日志数据会在升级到 PAN-OS 9.0 时自动迁移到新格式。在重新格式化期间，**ACC** 或 **Monitor**（监控）选项卡中不会显示日志数据。此外，在重新格式化未完成之前，新的日志数据不会转发到日志收集器。重新格式化时，会将新日志写入到防火墙系统磁盘，且在此程序成功完成后，新日志会转发到相应的日志收集器。

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 *Panorama* 软件版本，并且 *Panorama*、日志收集器和所有受管防火墙运行相同的内容版本。有关软件和内容兼

© 2019 Palo Alto Networks, Inc.

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（或更高版本）的软件版本，但必须具有相同或更早版本的内容版本：

- 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，或者至少运行比您将安装或在 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更新受管防火墙（使用 Panorama），然后更新日志收集器（请参阅安装 Panorama 的内容和软件更新）。

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 | 确定您需要在日志收集器上安装的内容更新。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。

在安装软件更新之前，必须安装内容更新。

1. 运行 **`show system info`** CLI 命令查看当前更新版本。
2. 对于每个内容更新，确定是否需要更新并记下您需要在步骤 4 中下载的内容更新。

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。

3. （根据需要）在更新日志收集器的内容版本之前，首先将受管防火墙升级到相同或更高版本的内容发行版本。

STEP 3 | 确定到 PAN-OS 9.2 的升级路径。

在从当前运行的 PAN-OS 版本升级到 PAN-OS 10.0 的路径中，您无法跳过任何功能发行版本的安装。查看发行说明中的已知问题和对默认行为的更改，以及新功能指南中的升级/降级考虑因素，了解通过其作为升级路径的一部分的每个版本。

（从 7.1 或更早版本升级时需要）PAN-OS 8.0 引入了新的日志存储格式。升级到 PAN-OS 8.0 后，在继续升级之前，必须将 Panorama 日志迁移到新日志格式。日志迁移是一次性任务；如果您已迁移日志收集器上的日志以升级到 PAN-OS 8.0，则无需再次迁移它们。

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 4 | 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 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. 下载内容更新：
   1. 在 Resources（资源）部分中单击 **Dynamic Updates**（动态更新）。
   2. **Download**（下载）所需内容更新，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。

© 2019 Palo Alto Networks, Inc.

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-Series 设备升级到 Panorama 10.0.0，请下载 `Panorama_m-10.0.0` 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 | 在日志收集器上安装内容更新。



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. 在 Panorama 中，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）至主机上的相应内容更新文件，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更新的 **File Name**（文件名）。
4. 选择日志收集器。
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 6 | 安装软件更新。

1. 选择 **Panorama** > **Device Deployment** > **Software**（Panorama > 设备部署 > 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. 选择要安装更新的日志收集器。
5. 根据您在升级路径内安装的软件版本（步骤 3），选择以下一项：
   - **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）以开始安装。

STEP 7 | 成功升级到 PAN-OS 10.0 后，请检查日志格式迁移状态。

1. 登录到 Panorama 命令行界面日志收集器。
2. 运行以下命令以检查日志格式迁移的状态：

```
admin> debug logdb show-es-upgrade-time
```

示例 — 日志格式迁移仍在运行时的响应：

© 2019 Palo Alto Networks, Inc.

```
Response from logger 23456212: 50.98% of indices upgraded complete.
 Approximately less than a minute remaining until migration is complete.
 Once the log migration is complete, please run the 'show log-collector-
es-cluster health' command to check the ElasticSearch cluster status to
 verify logging and reporting functionality is restored.
```

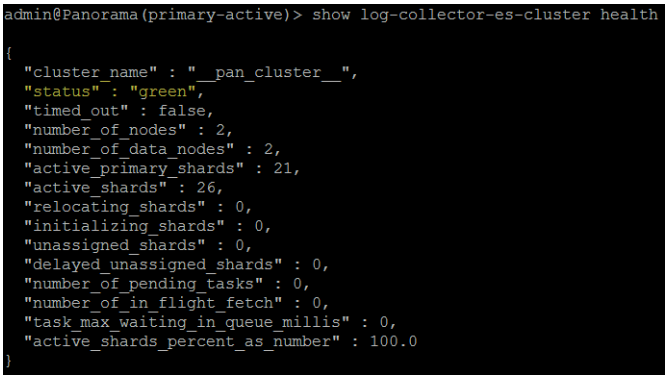
日志格式迁移完成后的响应：

```
Response from logger 23456212: 100% of indices complete, please
 run the 'show log-collector-es-culster health' command to check
 the ElasticSearch cluster status to verify logging and reporting
 functionality is restored.
```

3. 日志格式迁移结束后继续进行下一步之前，运行以下命令以检查 ElasticSearch 群集的状态：

```
admin> show log-collector-es-cluster health
```

当 ElasticSearch 群集的健康 `status` 显示为 `green`时，可继续进行下一步：



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-version: 10.0.0
app-version: 8270-6076
app-release-date: 2020/05/08 18:21:51
```

当 Panorama 连接上互联网时升级防火墙

查看 PAN-OS 10.0 发行说明，然后遵循以下流程升级通过 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。

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。

更新 Panorama 的防火墙前，必须：

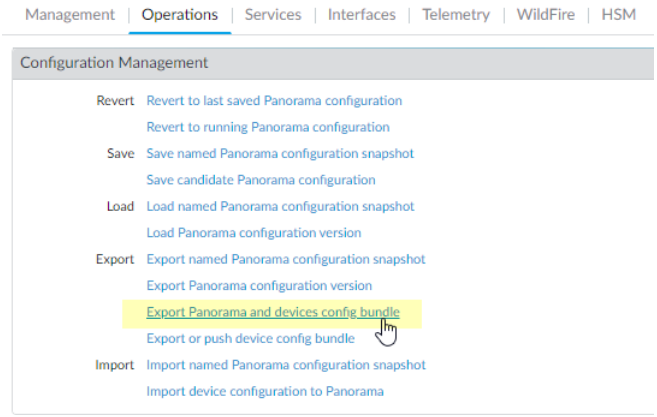
- 确保 Panorama 运行的 PAN-OS 版本与更新到的版本相同或，高于更新到的版本。在将受管防火墙升级到 PAN-OS 10.0 之前，您必须安装关于 Panorama 的内容和软件更新，并使用 Panorama 将升级部署到防火墙、日志收集器和 WildFire 设备以便将 Panorama 和日志收集器升级到 PAN-OS 10.0。
- 确保防火墙已连接至可靠的电源。升级时断电可能导致防火墙无法使用。

© 2019 Palo Alto Networks, Inc.

STEP 1 | 将当前配置文件的备份保存在计划要升级的每个受管防火墙上。

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. 从 Panorama Web 界面选择 **Panorama** > **Setup**（设置）> **Operations**（操作），然后单击 **Export Panorama and devices config bundle**（导出 **Panorama** 和设备配置包）以生成和导出 Panorama 和每个受管防火墙的最新配置备份。

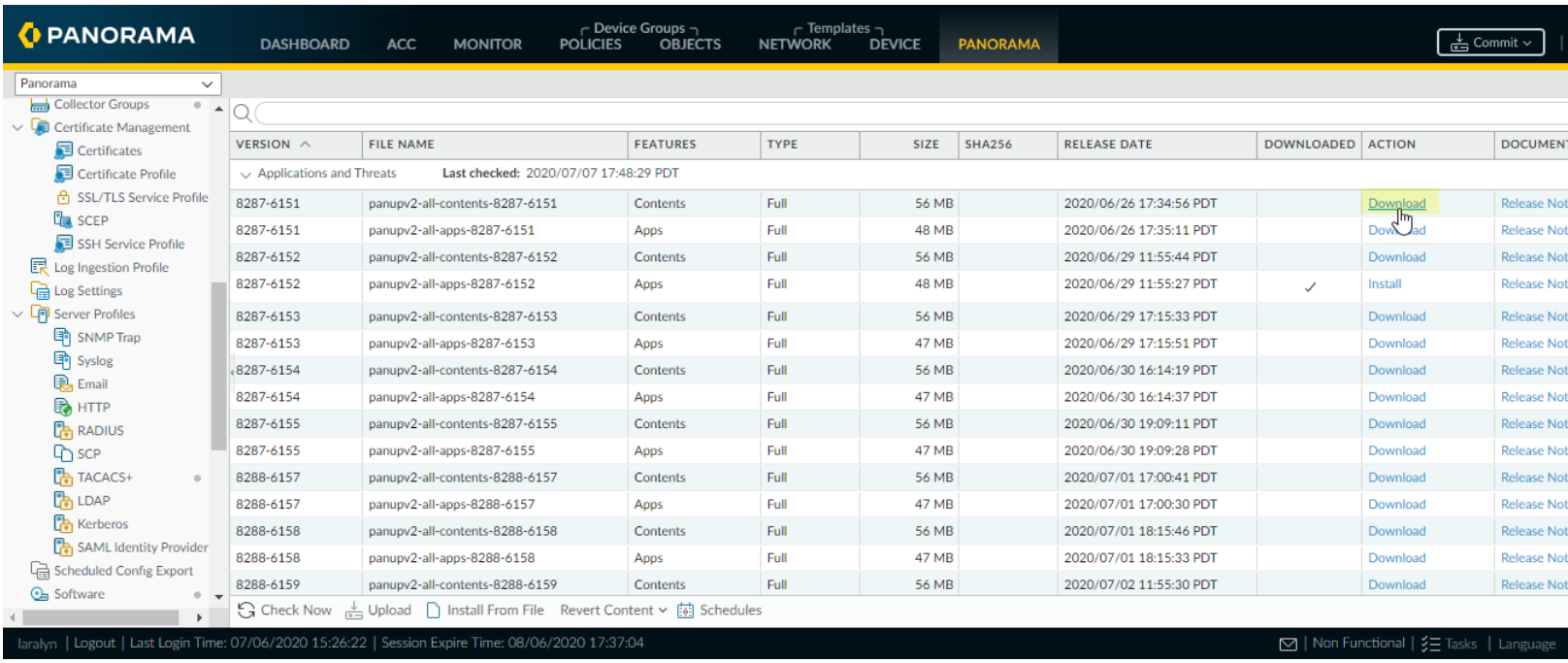


2. 将导出的文件保存到防火墙外部的位置。如果升级出现问题，您可以使用此备份还原配置。

STEP 2 | 更新计划更新的防火墙上的内容发行版本。

要了解 PAN-OS 10.0 所需的最低内容发行版本，请参阅发行说明。在将内容更新到 Panorama 到受管防火墙时，必须遵循应用程序和威胁更新的最佳实践。

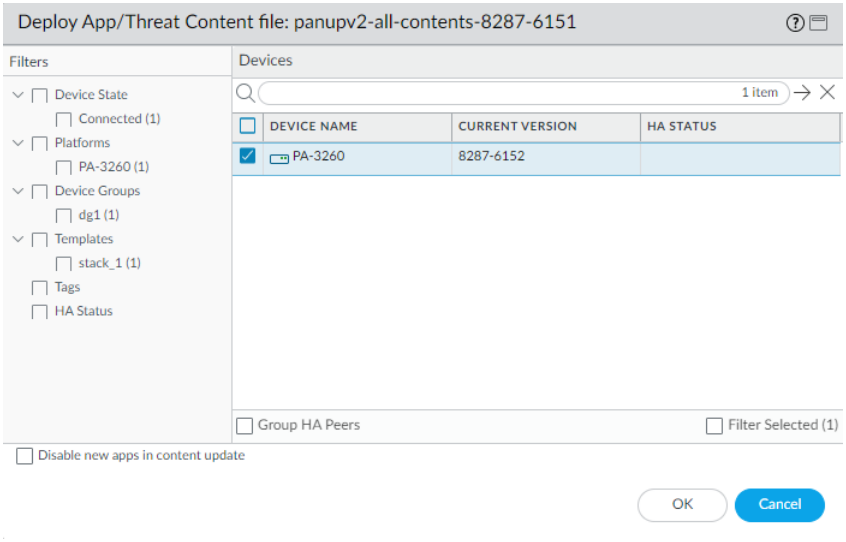
1. 选择 **Panorama** > **Device Deployment**（设备部署）> **Dynamic Updates**（动态更新），然后 **Check Now**（立即检查）最近更新。如果有更新可用，“操作”列会显示 **Download**（下载）链接。



2. 如果尚未安装，请 **Download**（下载）最新内容发行版本。

© 2019 Palo Alto Networks, Inc.

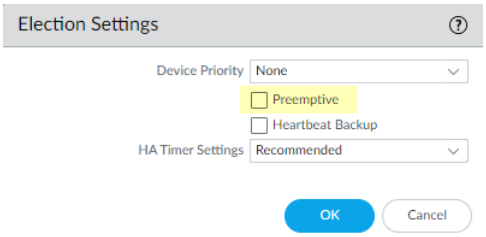
3. 单击 **Install**（安装）并选择要在其中安装更新的防火墙，然后单击 **OK**（确定）。如果更新 HA 防火墙，则必须更新两个对端设备的内容。



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* 命令增加最大值。

STEP 3 | （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 4 | 确定到 PAN-OS 10.0 的升级路径。

在从当前运行的 PAN-OS 版本升级到 PAN-OS 10.0.0 的路径中，您无法跳过任何功能发行版本的安装。查看发行说明中的已知问题和对默认行为的更改，以及新功能指南中的升级/降级考虑因素，了解通过其作为升级路径的一部分的每个版本。

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 5 | 下载目标 PAN-OS 10.0 版本映像。

1. 选择 **Panorama** > **Device Deployment**（设备部署）> **Software**（软件），然后 **Check Now**（立即检查）最新发行版本。
2. **Download**（下载）您正在升级的发行版本的防火墙特定文件。您必须下载您打算升级的每个防火墙型号（或防火墙系列）的单个安装文件。

© 2019 Palo Alto Networks, Inc.

例如，要将 PA-220 和 PA-5250 防火墙升级到 PAN-OS 10.0.0，请下载 `PanOS_220-10.0.0`、`PanOS_3000-10.0.0` 和 `PanOS_5200-10.0.0` 映像。成功下载映像后，操作列将更改为 **Install**（安装）此映像。

STEP 6 | 在防火墙上安装 PAN-OS 10.0 软件更新。

在升级分支防火墙之前，您必须将中心防火墙从 *PAN-OS 10.0.0* 升级到 *PAN-OS 10.0.1* 或更高发行版本。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`（禁用）。

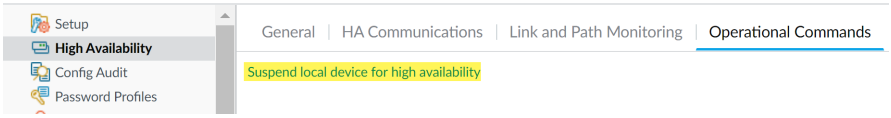
1. 单击与想要更新的防火墙型号匹配的操作列中的 **Install**（安装）。例如，如果想升级 PA-220 防火墙，请单击与 PanOS_220-10.0.0 相对应的行中的 **Install**（安装）。
2. 在部署软件文件对话框，选择想要升级的所有防火墙。要减少停机时间，请仅在每个 HA 对中选择一个对端设备。对于主动/被动对，选择主动对端设备；对于主动/主动对，选择主动-辅助对端设备。
3. （仅限 HA 防火墙更新）请勿选择**Group HA Peers**（组高可用性对端设备）。
4. 选择**Reboot device after install**（在安装之后重新启动设备）。
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）。
7. 防火墙完成重启后，请选择 **Panorama** > **Managed Devices**（受管设备），然后验证用于已升级的防火墙的软件版本是否是 10.0.0。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 7 | （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. （仅限主动/被动更新）挂起您正在升级的每个主动/被动对中的主动设备。
   1. 切换上下文至主动防火墙。
   2. 在 **Dashboard**（仪表盘）的高可用性小部件中，验证 **Local**（本地）防火墙状态是否是 **Active**（主动），**Peer**（对端设备）是否是 **Passive**（被动））。



   3. 选择 **Device**（设备）> **High Availability**（高可用性）> **Operational Commands**（操作命令）> **Suspend local device**（挂起本地设备）。



   4. 返回至 **Dashboard**（仪表盘）上的高可用性小部件，然后检验 **Local**（本地）是否已更改为 **Passive**（被动），**Peer**（对端设备）是否已更改为 **Active**（主动）。



2. 返回至 Panorama 上下文，然后选择 **Panorama** > **Device Deployment**（设备部署）> **Software**（软件）。
3. 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）。
4. 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 防火墙的对端设备。
5. 请勿选择 **Group HA Peers**（组高可用性对端设备）。
6. 选择**Reboot device after install**（在安装之后重新启动设备）。
7. 要开始更新，请单击 **OK**（确定）。

© 2019 Palo Alto Networks, Inc.

8. 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）。
9. （仅限主动/被动升级）在刚升级的对端设备的 CLI 中，运行以下命令使防火墙再次运行：

   ```
   request high-availability state functional
   ```

STEP 8 | 验证每个受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**（受管设备）。
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端设备的 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 9 | （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，然后 **Commit**（提交）更改。

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。

STEP 1 | 在升级受管防火墙之前，请确保您在 Panorama 管理服务器和日志收集器上运行适当的 Panorama™ 软件版本。

Palo AltoNetworks® 强烈建议 *Panorama* 和日志收集器运行相同的 *Panorama* 软件版本，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 必须与防火墙运行相同（或更高版本）的软件版本，但必须具有相同或更早版本的内容版本：

- 软件发布版本 — 如果 Panorama 管理服务器或日志收集器尚未运行与您打算更新防火墙的版本相同或更高版本的软件版本，则在更新任何防火墙之前必须在 Panorama 和日志收集器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）。
- 内容发布版本 — 对于内容发布版本，您应该确保所有防火墙都运行最新的内容发布版本，或者至少运行比在 Panorama 和日志收集器上运行的版本更新的版本；否则，在更新 Panorama 管理服务器的内容发布版本之前更新受管防火墙，然后当 Panorama 未连接互联网时升级日志收集器（请参阅安装 Panorama 的内容和软件更新）。

检查软件和内容版本：

© 2019 Palo Alto Networks, Inc.

- **Panorama** 管理服务器 — 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 — 登录到每个日志收集器的 CLI，并运行 **`show system info`** 命令。

STEP 2 | 将当前配置文件的备份保存在计划要升级的每个受管防火墙上。



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 3 | 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，确定是否需要更新并记下您需要在步骤 5 中下载的内容更新。



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 4 | 确定您打算更新到 Panorama 10.0 的防火墙的软件升级路径。请参阅新功能指南了解更新到 PAN-OS 10.0 的升级路径。

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



我们强烈建议您查看发行说明中的已知问题和对默认行为的更改，以及新功能指南中的升级/降级考虑因素，了解通过其作为升级路径的一部分的每个版本。

STEP 5 | 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 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）。

© 2019 Palo Alto Networks, Inc.

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-220 和 PA-5260 防火墙升级到 PAN-OS 8.0.8，请下载 `PanOS_220-8.0.8`、`PanOS_3000-8.0.8` 和 `PanOS_5200-8.0.8` 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 6 | 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 7 | （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 8 | 上传 PAN-OS 软件更新。

1. 选择 **Panorama** > **Device Deployment** > **Software**（Panorama > 设备部署 > 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）。

STEP 9 | 安装 Upload PAN-OS 软件更新。

© 2019 Palo Alto Networks, Inc.

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）。

在升级分支防火墙之前，您必须将中心防火墙从 *PAN-OS 10.0.0* 升级到 *PAN-OS 10.0.1* 或更高发行版本。在中心防火墙之前升级分支防火墙会产生错误的监视数据（*Panorama* > *SD-WAN* > *Monitoring*（监视））， 且 *SD-WAN* 链接会错误地显示为 `down`（禁用）。

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 Action（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. 在 fw2 完成重新启动后，在 fw1（**Dashboard**（仪表盘）> 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**（仪表盘）> High Availability（高可用性）小），并核实本地防火墙状态为 `active`，对端设备为 `suspended`。
     6. 访问 Panorama，选择相应版本的 Action（操作）列中的 **Panorama** > **Device Deployment**（设备部署）> **Software**（软件），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**（操作命令）），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**（仪表盘）> High Availability（高可用性）小）上，核实本地防火墙状态为 `passive`，对端设备 (fw2) 为 `active`。
2. 完成上述 PAN-OS 版本更新步骤后，重复步骤 8 和步骤 9，以根据需要在升级路径中上传下一个 PAN-OS 版本，直到所有防火墙都运行目标 PAN-10.0 版本。

© 2019 Palo Alto Networks, Inc.

STEP 10 | 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 11 | 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。

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 | 添加 ZTP 防火墙到 Panorama。

STEP 2 | 登录到 Panorama Web 界面 作为管理员用户。

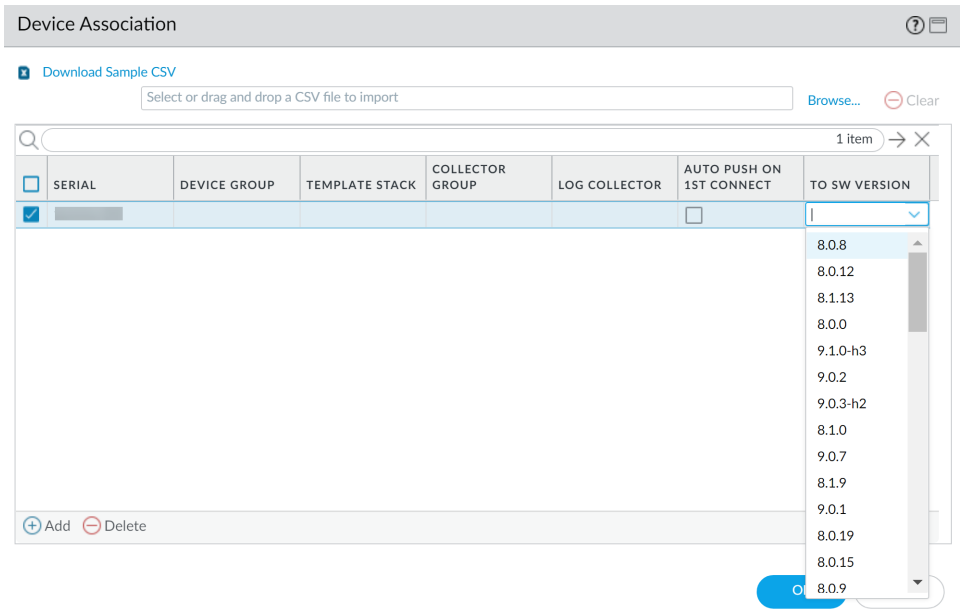
STEP 3 | 选择 **Panorama** > **Device Deployment**（设备部署）> **Updates**（更新），然后 **Check Now**（立即检查）最新 PAN-OS 版本。

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

STEP 7 | 单击 **OK**（确定）保存您的配置更改。



STEP 8 | 选择 **Commit**（提交），然后 **Commit and Push**（提交并推送）您的配置更改。

© 2019 Palo Alto Networks, Inc.

STEP 9 | 验证 ZTP 防火墙是否升级。

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

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。在将内容更新部署到受管设备时，必须使用应用程序和威胁更新的最佳实践。

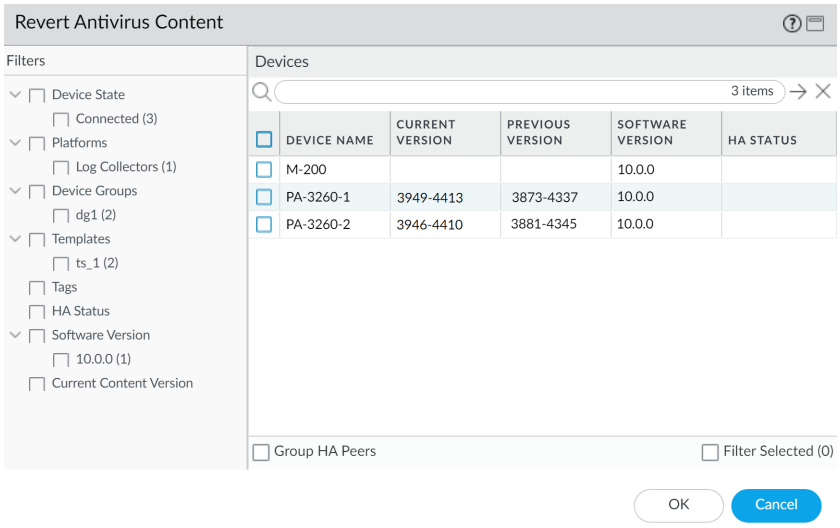
STEP 1 | 登录到 Panorama Web 界面。

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。



© 2019 Palo Alto Networks, Inc.

监控网络活动

Panorama™ 管理服务器提供网络通信的综合图形视图。使用 Panorama 上的可见性工具，包括应用程序命令中心 (ACC)、日志和报告生成功能。利用这些工具可以集中分析、调查和报告全部网络活动，识别有潜在安全影响的区域，并将它们转化为安全应用程序启用策略。

本部分包含以下主题：

> 使用 Panorama 的可视化功能
> 在 Panorama 上提取 Traps ESM 日志
> 用例：使用 Panorama 监控应用程序
> 用例：使用 Panorama 来响应事件

使用 Panorama 的可视化功能

除了中心部署和防火墙配置功能，Panorama 还允许您监控和报告遍历网络的所有通信。尽管 Panorama 和防火墙上的报告功能非常近似，但 Panorama 提供的优势在于，它是跨越所有受管防火墙的聚合信息的一个单独窗格视图。此聚合视图提供有关整个网络的用户活动、通信模式和潜在威胁方面的趋势的实用信息。

使用 Panorama 上的应用程序命令中心 (ACC)、应用层面、日志查看器及标准和可自定义的报告选项，您可快速了解有关遍历网络通信的详细信息。如果能够查看此信息，则可让您评估当前策略在哪些方面充分，以及在哪些方面不充分。可使用此数据增强您的网络安全策略。例如，您可以增强安全规则来提高网络中所有用户的合规性及责任心，或管理网络容量并最大限度地降低资产风险，同时满足网络中用户丰富的应用程序需求。

以下主题提供 Panorama 上报告功能的高级视图（包括若干使用案例），以说明您如何在自己的网络基础结构中使用这些功能。有关可用报告和图表及其说明的完整列表，请参阅在线帮助。

- 使用 ACC 和 AppScope 监控网络
- 分析日志数据
- 生成、计划和用电子邮件发送报告
- 为已计划报告配置密钥限制

使用 ACC 和 AppScope 监控网络

ACC 和 AppScope 都允许您监控和报告从遍历网络的通信记录的数据。

Panorama 上的 ACC 显示网络通信的摘要。Panorama 可从网络上的所有受管防火墙动态查询数据，并在 ACC 中显示这些数据。此显示允许您根据应用程序、用户和内容活动（URL 类别、威胁、可有效阻止数据或文件的安全策略）来监控 Palo Alto Networks 下一代防火墙整个网络的通信。

AppScope 帮助快速识别网络上意外或不常见的行为。它包括一批图表和报告，如摘要报告、更改监控、威胁监控、威胁地图、网络监控、通信地图等，从而允许您根据威胁或应用程序，或根据通信流的源或目的地分析通信流。您也可以按会话或字节计数排序。

设备组和模板管理员仅能在其访问域内查看设备组的网络和 *ACC* 数据。

使用 ACC 和 AppScope 回答问题，例如：

ACC	监控 > AppScope
• 网络上使用最多的应用程序是什么，有多少高风险应用程序？网络上使用高风险应用程序最多的用户是谁？ • 过去一小时查看最多的 URL 类别是什么？	• 应用程序使用趋势如何—使用率最高的前五个应用程序是什么，使用率下降的前五个程序是什么？ • 与上一周或上个月对比，当前一周用户活动发生了怎样的变化？
• 占用带宽最多的应用程序是什么？消耗最高带宽的用户/主机是哪些？ • 阻止了哪些内容或文件，是否有特定用户触发此文件阻止/数据筛选规则？ • 两个特定 IP 地址之间交换的或特定用户生成的通信量是多少？目的地服务器或客户端的地理位置在哪里？	• 哪些用户和应用程序占用了大多数网络带宽？此消耗在过去 30 天有何变化？ • 网络上的威胁是什么，这些传入和传出通信威胁的地理位置分布如何？

© 2019 Palo Alto Networks, Inc.

然后，您可利用信息来维护或实施对网络通信模式的更改。请参阅用例：使用 Panorama 监控应用程序了解 Panorama 上的可见性工具如何影响您为自己的网络制定可接受的使用策略。

下面是可帮助您导航 ACC 的一些提示：

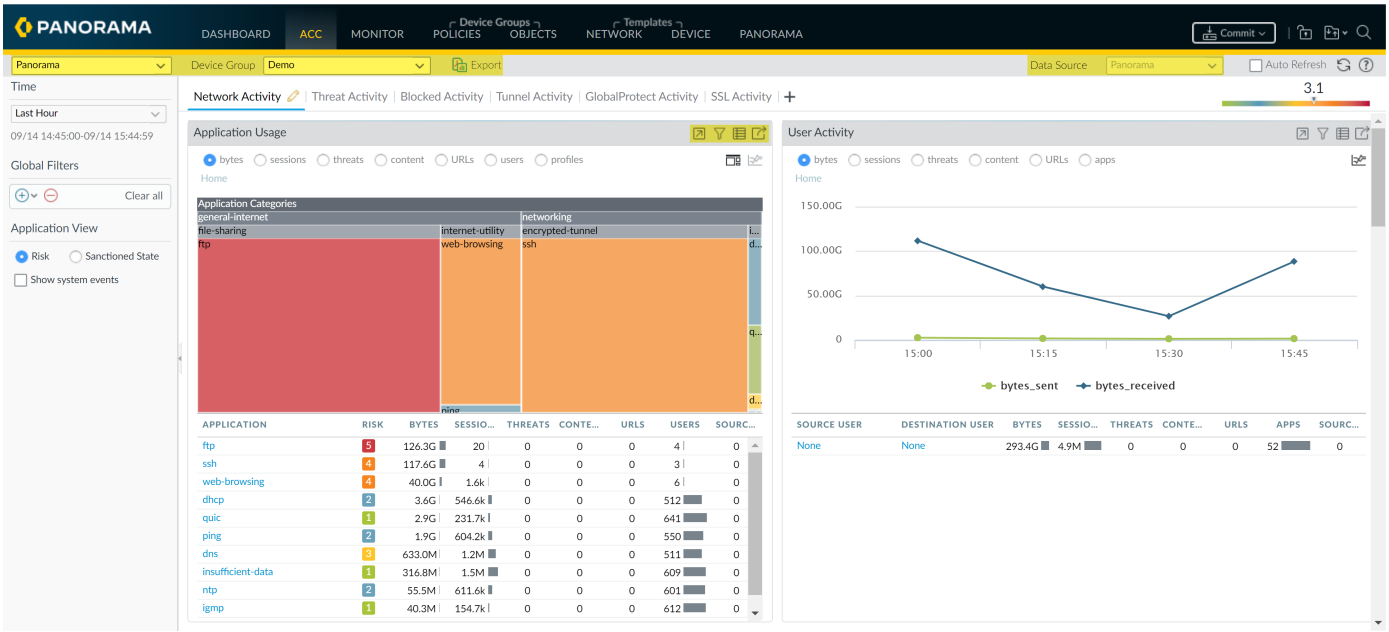


图 24: ACC 导航提示

- 从 **Panorama** 视图切换到设备视图 — 使用 **Context**（上下文）下拉列表即可访问任何受管防火墙的 Web 界面。有关详细信息，请参阅上下文切换 — 防火墙或 Panorama。
- 更改设备组和数据源 — 用于在 ACC 中图表上显示统计信息的默认 **Data Source**（数据源）为 **Panorama** 本地数据，而默认 **Device Group**（设备组）设置则为 **All**（所有）。使用 Panorama 上的本地数据为图表提供快速加载时间。但是，如果所有受管防火墙都为 PAN-OS 7.0 或以上版本，那么您可以将数据源更改为 **Remote Device Data**（远程设备数据）。如果受管防火墙为 PAN-OS 7.0 版本和更早版本的混合搭配，那么您只能查看 Panorama 数据。经配置使用远程设备数据时，Panorama 将轮询所有受管防火墙并提供数据的聚合视图。屏幕信息指示被轮询的防火墙总数，以及响应信息查询的防火墙数量。
- 选择选项卡和小部件进行查看 — ACC 包含了三个选项卡和一系列小部件，它们能够让您找到您关注的信息。除了应用程序使用状况小部件和主机信息小部件之外，其余的所有小部件都只有在相应的功能已在防火墙上获得许可且您已启用日志记录时才会显示数据。
- 调整时间框架和细化数据 — ACC 中的报告时段范围为从前 15 分钟到前一小时、一天、一周、一个月或任何自定义时间。默认情况下，每个小部件显示前 10 个项目，并将其余的所有项目聚合为 **others**（其他）。您可以使用不同的属性（例如，会话、字节、威胁、内容和 URL）在每个小部件中对数据进行排序。您也可以将本地筛选器设置为筛选小部件中表格和图标内的显示，然后将该小部件筛选器提升为全局筛选器，从而在 ACC 中的所有小部件之间转动视图。

分析日志数据

Panorama 上的 **Monitor**（监控）选项卡提供对日志数据的访问；这些日志是受管防火墙处理并转发到 Panorama 的会话存档列表。

日志数据可大致分组为两种类型：有关网络上通信流详细信息的类型（例如应用程序、威胁、主机信息配置文件、URL 类别、内容/文件类型）和记录系统事件、配置更改和 User-ID™ 映射信息的类型。

根据受管防火墙上的日志转发配置，**Monitor**（监控）> **Logs**（日志）选项卡可包括通信流、威胁、URL 筛选、数据筛选、主机信息配置文件 (HIP) 匹配和 WildFire™ 提交的日志。您可以检查日志以验证指定会话或事物方面的丰富信息。此类信息的部分示例包括启动会话的用户，防火墙在会话中执行的操作（允许或拒

© 2019 Palo Alto Networks, Inc.

绝），以及源端口、目标端口，区域和地址。系统日志和配置日志可指示在超出配置的阈值时防火墙触发的配置更改或警报。

如果 *Panorama* 将管理运行软件版本早于 *PAN-OS 7.0* 的防火墙，则您应指定一个 *WildFire* 服务器，使 *Panorama* 可以从该服务器收集这些防火墙提交的 *WildFire* 样本相关分析信息。*Panorama* 使用此信息来填写在 *PAN-OS 7.0* 中缺少引入字段值的 *WildFire* 提交日志。运行较早软件版本的防火墙将不会填充这些字段。若要指定服务器，应选择 *Panorama* > *Setup*（设置）> *WildFire*，编辑 *General Settings*（常规设置），然后输入 *WildFire Private Cloud*（*WildFire* 私有云）名称。默认服务器为 *wildfire-public-cloud*，它是主机设在美国的 *WildFire* 云。

生成、计划和用电子邮件发送报告

您可以配置报告以立即运行或安排它们按特定时间间隔运行。您可以保存并导出报告或将其发送给特定收件人。如果您要和没有 Panorama 访问权限的管理员共享报告，则通过发送电子邮件共享报告特别有用。Panorama 支持与 Palo Alto Networks 防火墙相同的报告类型。

从 Panorama 10.0.2 和云服务插件版本 1.8.0 开始，您可以生成有关 Cortex 数据湖数据的计划报告。

在 *PAN-OS 10.0.3* 和更高版本中，此功能默认启用。

为此，您必须先从 Panorama CLI 启用此功能，启用方式为输入

```
admin@Panorama> request plugins cloud_services logging-service sched-report-enable
```

常规提交不会启用此更改。相反，您必须切换至配置模式：

```
admin@Panorama> configure
```

并输入

```
admin@Panorama# commit force
```

然后，按照以下步骤生成计划报告。

建议您在 *Panorama* 和要生成报告的防火墙上安装相符的软件版本。例如，如果 *Panorama* 管理服务器运行的是 *Panorama 10.0*，则请在其受管防火墙上安装 *PAN-OS 10.0* 之后再生成报告。这样当您创建包括在 *Panorama* 版本上受支持，但在防火墙上更早的 *PAN-OS* 版本中不受支持的字段的报告时，就可以避免出现问题。

STEP 1 | 配置 Panorama 预定义报告。

1. 选择 **Panorama** > **Setup**（设置）> **Management**（管理），然后编辑 **Logging and Reporting**（日志记录和报告）。
2. （可选）选择 **Log Export and Reporting**（日志导出和报告），然后启用（选中）**Use Data for Pre-Defined Reports**（将数据用于预定义报告）以将每小时报告聚合卸载到日志收集器。

   建议为 *VM-50*、*VM-50 Lite* 和 *PA-200* 防火墙启用此设置。
3. 选择 **Pre-Defined Reports**（预定义报告），然后启用（选中）预定义报告以从 Panorama 进行推送。

© 2019 Palo Alto Networks, Inc.

4. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）配置更改。
5. （仅限 VM-50、VM-50 Lite 和 PA-200 防火墙）访问防火墙 CLI以启用预定义报告。

   此命令必须在每个 VM-50、VM-50 Lite 和 PA-200 防火墙上运行。

```
admin> debug run-panorama-predefined-report yes
```

STEP 2 | 配置 Panorama 以接收和存储从防火墙接收的用户和用户组信息。

根据用户名和组生成报告，而不仅仅是 IP 地址。

1. 如果您希望 Panorama 在报告中包含用户组信息，请将受管防火墙升级到 PAN-OS 8.1 或更高版本。Panorama 无法同步来自运行早期版本的防火墙的组信息。
2. 选择 **Panorama** > **Setup**（设置）> **Management**（管理），编辑 Panorama 设置，然后 **Enable reporting and filtering on groups**（对组启用报告和筛选功能）。
3. 如果您还没有，请添加设备组。对于每个设备组：
   - 选择 **Master Device**（主设备），它是向 Panorama 提供用户和用户组信息的防火墙。
   - 使 Panorama 能够 **Store users and groups from Master Device**（存储主设备所发送的用户和用户组）。

STEP 3 | 生成报告。

生成报告的步骤取决于报告类型。

- 自定义报告：
  1. 选择 **Monitor**（监控）> **Manage Custom Reports**（管理自定义报告），然后 **Add**（添加）报告。
  2. 输入 **Name**（名称）以标识报告。
  3. 选择用于报告的 **Database**（数据库）。

     您可以将报告基于 **Summary Databases**（摘要数据库）或 **Detailed Logs**（详细日志）数据库。

     要将报告基于存储在 Panorama 管理服务器和日志收集器上的日志，请选择 **Panorama Data**（**Panorama** 数据）（为实现更快的性能推荐）。

     要将报告基于存储在受管防火墙上的日志，请选择 **Remote Device Data**（远程设备数据）。此选项适用于防火墙可能拥有日志尚未转发到 Panorama 的情况。但是，由于 Panorama 必须直接查询防火墙，因此此选项执行较慢。
  4. 选择 **Scheduled**（调度）。
  5. 通过选择 **Time Frame**（时间范围）、**Sort By**（排序）顺序、**Group By**（分组方式）首选项和报告将显示的列（日志属性）定义日志筛选条件。

     必须选择 *Sort By*（排序方式）顺序，以生成准确的报告。如果未选择 *Sort By*（排序方式）顺序，则生成的自定义报告会使用选中数据库中的最新日志匹配进行填充。
  6. （可选）根据日志属性，使用 **Query Builder**（查询生成器）进一步改进日志筛选条件。
  7. 要测试报告设置，请选择 **Run Now**（立即运行）。必要时，可修改设置以更改报告显示的信息。
  8. 单击 **OK**（确定）保存定制报告。
- **PDF Summary Report**（**PDF** 摘要报告）：
  1. 选择 **Monitor**（监控）> **PDF Reports**（**PDF** 报告）> **Manage PDF Summary**（管理 **PDF** 摘要），然后添加报告。
  2. 输入 **Name**（名称）以标识报告。
  3. 使用每个报告组的下拉列表，然后选择一个或多个元素以设计 PDF 摘要报告。最多可以选择 18 个元素。

© 2019 Palo Alto Networks, Inc.

4. 单击 **OK**（确定）以保存设置。

STEP 4 | 配置 **Report Group**（报告组）。

它可包括预定义报告、PDF 摘要报告和自定义报告。Panorama 将包括的所有报告编译成一个单独的 PDF。

1. 选择 **Monitor**（监控）> **PDF Reports**（**PDF** 报告）> **Report Groups**（报告组），然后 **Add**（添加）报告组。
2. 输入 **Name**（名称）以标识报告组。
3. （可选）选择 **Title Page**（标题页面）并为 PDF 输出添加 **Title**（标题）。
4. 在预定义报告，自定义报告和 PDF 摘要报告列表中选择报告。
5. 将所选报告 **Add**（添加）到报告组。
6. 单击 **OK**（确定）以保存设置。

STEP 5 | 配置电子邮件服务器配置文件。

配置文件定义防火墙如何连接到服务器和发送电子邮件。

1. 选择 **Panorama** > **Server Profiles**（服务器配置文件）> **Email**（电子邮件），然后 **Add**（添加）服务器配置文件。
2. 输入 **Name**（名称）以标识配置文件。
3. **Add**（添加）最多四个 SMTP 服务器并 **Add**（添加）每个服务器的以下信息：
   - **Name**（名称）— 标识 SMTP 服务器的名称（1 至 31 个字符）。此字段只是一个标签，不必是现有服务器的主机名。
   - **Email Display Name**（电子邮件显示名称）— 显示在电子邮件的 From（发件人）字段中的名称。
   - **From**（发件人）— 发送通知电子邮件的源电子邮件地址。
   - **To**（收件人）— 将通知电子邮件发送到的电子邮件地址。
   - **Additional Recipient**（其他收件人）— 要向另一个帐户发送通知，请在此处输入其他地址。
   - **Email Gateway**（电子邮件网关）— 用于发送电子邮件的 SMTP 网关的 IP 地址或主机名。
4. 单击 **OK**（确定）保存配置文件。

STEP 6 | 为电子邮件投递调度报告。

1. 选择 **Monitor**（监控）> **PDF Reports**（**PDF** 报告）> **Email Scheduler**（电子邮件调试程序），然后 **Add**（添加）电子邮件调度程序配置文件。
2. 输入 **Name**（名称）以标识配置文件。
3. 选择 **Report Group**（报告组）、您刚刚创建的电子邮件服务器配置文件（**Email Profile**（电子邮件配置文件））和报告的 **Recurrence**（重复周期）（默认为 **Disable**（禁用））。
4. **Send test email**（发送测试邮件）验证电子邮件设置是否准确。
5. 单击 **OK**（确定）保存更改。
6. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

为已计划报告配置密钥限制

Panorama™ 管理服务器和 PA-7000 系列防火墙报告利用来自一个或多个日志收集器的密钥（您可以对其进行聚合的唯一值）来构建和生成报告。为提高已计划报告的准确性，您现在可以配置最大和最小密钥限制。通过增加支持的密钥数，已计划报告现在可以包含更多数据，可对这些数据进行聚合、排序和分组。

默认最小密钥限制基于为已计划报告配置的 **Sort By**（排序依据）和 **Group By**（分组依据）值，计算方法如下：

```
<Sort By value> x 100 x <Group By value>
```


© 2019 Palo Alto Networks, Inc.

例如，如果 **Sort By**（排序依据）配置为 **Top 25**（前 25），**Group By**（分组依据）配置为 **5 Groups**（5 个组），则默认最小密钥限制为 12,500 个密钥。当 **Group By**（分组依据）值设置为 **None**（无）时，将不纳入计算。默认最小密钥限制受限于且不能超过最大密钥限制。

您只能为 *M-Series* 设备和 *Panorama* 虚拟设备配置密钥限制。*PA-7000* 系列密钥限制不可配置。

以下 Panorama 型号增加了受支持的最大和最小密钥：

Panorama 型号	最小密钥限制	最大密钥限制
PA-7000 系列	1,000 - 默认值，不可配置	25,000 - 默认值，不可配置
M-200	15,000	50,000
M-500	15,000	50,000
M-600	15,000	50,000
传统模式下的 Panorama 虚拟设备	5,000	25,000
Panorama 虚拟设备（所有受支持的型号）	15,000	50,000

STEP 1 | 登录到 Panorama 命令行界面。

STEP 2 | 使用以下命令配置最大密钥限制：

您可以将最大密钥限制设置在 0 到 50 之间，其中 50 等于 50,000 个密钥。在此示例中，我们将 Panorama 虚拟设备的最大密钥限制设置为 30,000 个密钥。

```
admin@Panorama> request max-report-keys set limit <Key Limit>
```

```
admin@Panorama> request max-report-keys set limit 30

cfg.report.max-keys-limit: 30
```

STEP 3 | 使用以下命令配置最小密钥限制：

您可以将最小密钥限制设置在 0 到 15 之间，其中 15 等于 15,000 个密钥。在此示例中，我们将 Panorama 虚拟设备的最小密钥限制设置为 15,000 个密钥。

```
admin@Panorama> request min-report-keys set limit <Key Limit>
```

```
admin@Panorama> request min-report-keys set limit 15

cfg.report.min-keys-limit: 15
```

STEP 4 | （可选）将最小密钥限制设置为默认设置。

```
admin@Panorama> request min-report-keys set limit 0
```


© 2019 Palo Alto Networks, Inc.

STEP 5 | 使用以下命令将新的最大和最小密钥限制提交到 Panorama：

```
admin@Panorama> commit-all
```


© 2019 Palo Alto Networks, Inc.

在 Panorama 上提取 Traps ESM 日志

可见性是防止和减少攻击影响的关键第一步。为帮助您应对这一挑战，Panorama 提供了防火墙日志（网络上的事件）和 Traps™ ESM 服务器日志（端点上的安全事件）的集成视图，以便您可以跟踪任何可疑或恶意活动。

要了解网络和端点上观察到的事件的意识和上下文，请在 Panorama 上转发 Traps 代理向 ESM 服务器报告的安全事件。Panorama 可以充当通过 TCP、UDP 或 SSL 使用 Syslog 从 Traps ESM 组件获取这些日志的 Syslog 接收器。然后，Panorama 可以将端点上发生的离散安全事件与网络上发生的事件相关联，并生成匹配证据。这些证据为您提供更多关于事件年表和事件流的上下文，以调查问题并解决网络中的安全漏洞。

STEP 1 | 在 Panorama 上定义日志提取配置文件并将其附加到收集器组。

传统模式下的 *Panorama* 虚拟设备无法提取 *Traps* 日志。

1. 选择 **Panorama** > **Log Ingestion Profile**（日志提取配置文件），然后单击 **Add**（添加）。
2. 输入配置文件的 **Name**（名称）。
3. 单击 **Add**（添加），并输入 ESM 服务器的详细信息。最多可将四台 ESM 服务器添加到配置文件。
   1. 输入 **Source Name**（源名称）。
   2. 指定 Panorama 将在其中侦听 Syslog 消息的 **Port**（端口）。范围为 23000 至 23999。
   3. 选择 **Transport**（传输）层协议 — TCP、UDP 或 SSL。
   4. 选择 **External Log type**（外部日志类型）的 Traps_ESM 和您的 Traps ESM **Version**（版本）。例如，对于 Traps ESM 4.0 或 4.1，请选择 **3.4.1+**。

      更新 Traps 日志格式时，可通过 Panorama 的内容更新提供更新的日志定义。
4. 选择 **Panorama** > **Collector Groups**（收集器组）> **Log Ingestion**（日志提取）并 **Add**（添加）日志提取配置文件，以便收集器组可以从配置文件中列出的 ESM 服务器中接收日志。

   如果启用 SSL 以在 Panorama 和 ESM 服务器之间进行 syslog 通信，则必须将证书附加到属于收集器组的受管理收集器（**Panorama** > **Managed Collectors**（受管收集器）> **General**（常规），然后选择要用于 **Inbound Certificate for Secure Syslog**（安全 **Syslog** 的入站证书）的证书）。
5. 将更改 **Commit**（提交）到 Panorama 和收集器组。

STEP 2 | 将 Panorama 配置为 ESM 服务器上的 Syslog 接收器。

Traps ESM 4.0 和更高版本支持将日志转发至外部 syslog 接收器和 Panorama。因为早期的 Traps ESM 版本不支持将日志转发到多个 syslog 接收器，因此必须在 **Syslog** 设置中将 Panorama 配置为 syslog 接收器（对于 ESM 3.4，请参阅启用将日志转发到外部日志记录平台 ）。

对于 Traps ESM 4.0 以及更高版本：

1. 在 ESM 控制台中，选择 **Settings**（设置）> **ESM** > **Panorama**，然后 **Enable log forwarding to Panorama**（启用将日志转发到 **Panorama**）。
2. 输入 Panorama 主机名或 IP 地址作为 **Panorama Server**（**Panorama** 服务器）和 Panorama 正在其中侦听的 **Panorama Server Port**（**Panorama** 服务器端口）。对于可选的 **Panorama Failover Server**（**Panorama** 故障转移服务器）重复此步骤。
3. 选择传输层 **Communication Protocol**（通信协议）：TCP、TCP with SSL（TCP（带 SSL））或 UDP。如果您选择 TCP（带 SSL），则 ESM 服务器需要启用服务器证书以客户端身份验证。

   在 Panorama 中，必须导出安全 Syslog 的入站证书的根 CA 证书，并将证书导入已安装 ESM 服务器的主机的受信任根证书存储区。

STEP 3 | 查看 ESM 日志和关联事件。

© 2019 Palo Alto Networks, Inc.

1. 选择 **Monitor**（监控）> **External Logs**（外部日志）> **Traps ESM** 以查看提取到 Panorama 的日志。
2. 选择 **Monitor**（监控）> **Automated Correlation Engine**（自动关联引擎）> **Correlated Events**（关联事件），然后对 **Wildfire and Traps ESM Correlated C2**（**Wildfire** 和 **Traps ESM** 关联 **C2**）关联对象名称进行筛选以查找关联事件。当网络上的主机展示的命令和控制活动与 WildFire 虚拟环境中针对恶意文件观察到的行为相匹配时，Panorama 生成关联事件。此关联事件会提醒您 Trap 代理和防火墙从网络上的一个或多个受感染主机观察到可疑活动。

© 2019 Palo Alto Networks, Inc.

用例：使用 Panorama 监控应用程序

此示例为您介绍评估当前策略效率并确定何处需要作出调整的流程，从而为您的网络加强可接受的使用策略。

登录 Panorama 时，**Dashboard**（仪表盘）上的 **Top Applications**（顶级应用程序）小部件会提供过去一小时使用最多的应用程序预览。要显示此小部件，选择工具栏中的 **Widgets (**小部件 **)** > **Application (**应用程序**)** > **Top Applications (**顶级应用程序**)**。可浏览排名居前的应用程序列表并将鼠标放在希望检查详情的每个应用程序阻止条目上，也可选择 **ACC** 选项卡查看与排序列表相同的信息。下图是 **Dashboard**（仪表盘）上的 **Top Applications**（顶级应用程序）小部件的视图。

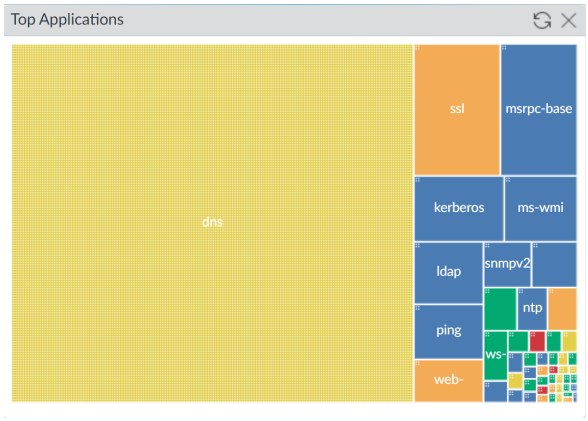


图 **26:** 顶级应用程序小部件

此画面的数据源是应用程序统计信息数据库；它不使用通信日志，并且无论您是否启用安全规则记录都会生成。此视图是您网络的通信情况，显示网络上允许的一切内容，并且通过您定义的任何策略规则解除阻止流动。

在 **ACC** 选项卡中，您可以选择 **Data Source**（数据源）并将其切换到 **Panorama** 本地，也可以查询受管防火墙（**Remote Device Data**（远程设备数据））获得数据；Panorama 会自动聚合并显示信息。对于更快流动，请考虑使用 Panorama 作为数据源（启用将日志转发到 Panorama），因为您选择查看数据的时间段和您网络生成的通信量不同，从受管防火墙加载数据的时间也存在差异。如果您的受管防火墙为 PAN-OS 7.0 版本和更早版本的混合搭配，那么您无法获得 **Remote Device Data**（远程设备数据）。

图 26: 顶级应用程序小部件 中的 **Dashboard**（仪表板）示例将 DNS 显示为流行的应用程序。如果单击 DNS 应用程序块，Panorama 打开将 DNS 应用为全局筛选器的 **ACC** > **Network Activity (**网络活动**)**选项卡，显示与该应用程序、之前访问该应用程序的用户以及该应用程序的风险等级和特征详情有关的信息。

© 2019 Palo Alto Networks, Inc.

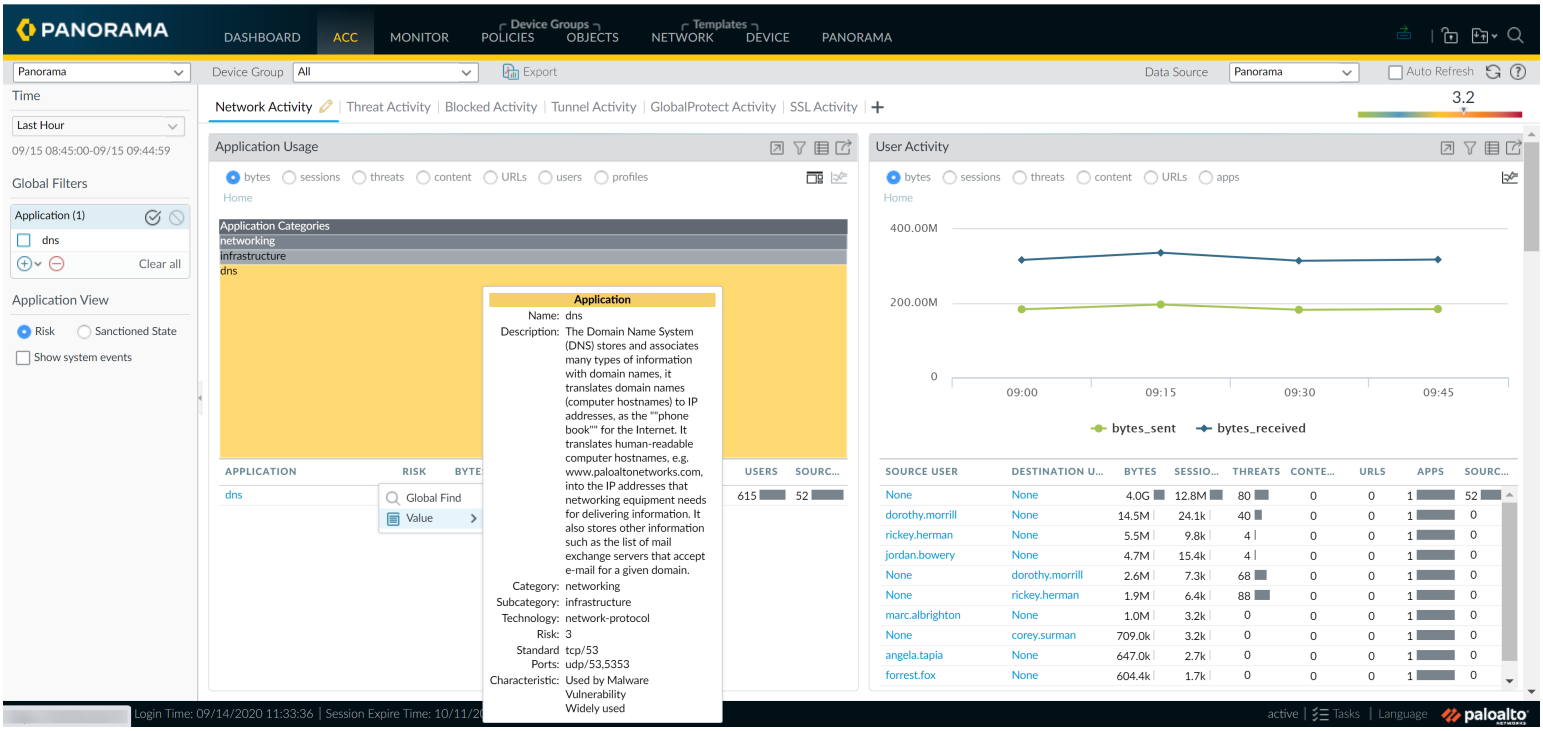


图 **27:** 网络活动选项卡

在 **User Activity**（用户活动）小部件中，可以看到使用 DNS 的用户数量和生成的通信量。如果您启用了 User-ID，您可以查看正在产生此通信的用户的名称，并向下深入地检查与每一个用户相关的所有会话、内容或威胁。

在 **Threat Activity**（威胁活动）选项卡中，查看 **Compromised Hosts**（受影响主机）小部件以了解匹配的关联对象都有哪些，然后查看与用户和应用程序相关的匹配证据。您也可以在 **Threat Activity**（威胁活动）小部件中查看威胁名称、类别和 ID。

在 DNS 被设置为全局筛选器的情况下，使用 **Destination IP Activity**（目标 IP 活动）和 **Destination Regions**（目标区域）小部件可验证哪里是通信目的地。您也可以查看入口区、出口区以及让此连接得以接通的安全规则。

有关详细信息，请向下展开 筛选视图的通信日志，并检查已使用端口、已发送数据包、已发送字节和已接收字节的每一个日志条目。根据需要调整列，以查看更多或更少信息。

Monitor（监控）> **App-Scope**（应用层面）**Traffic Map**（通信地图）选项卡显示通信流的地理地图，并提供传入通信与传出通信的对比视图。也可使用 **Monitor** > **App-Scope** > **Change Monitor**（监控 > 应用层面 > 更改监控）选项卡，查看通信模式中的更改。例如，将这一小时使用的排名居前的应用程序与上周或上月进行对比，以确定是否存在规律或趋势。

通过当前发现的所有信息，您可评估对您的策略配置进行的更改。下面是供您考虑的一些建议：

- 做到严格管理，并在 Panorama 上创建预处理规则以阻止或允许所有 DNS 通信。然后使用 Panorama 设备组创建并将此策略规则推送到一个或多个防火墙。
- 实施带宽使用限制并创建取消非业务通信优先级的 QoS 配置文件和策略规则。使用 Panorama 设备组和模板配置 QoS，然后将规则推送到一个或多个防火墙。
- 计划一个自定义报告组，汇总特定用户和网络上使用的排名居前的应用程序活动，在执行操作前，请再观察该模式一到两周。

除了检查特定应用程序外，也可检查排名居前的应用程序列表中的任何未知应用程序。这些是与定义的 App-ID™ 签名不匹配的应用程序，并显示为“unknown-udp”和“unknown-tcp”。要深入研究这些应用程序，请单击名称以向下展开未分类通信的详细信息。

© 2019 Palo Alto Networks, Inc.

使用相同流程调查启动未知通信的排名居前的主机源 IP 地址，以及建立会话的目的地主机 IP 地址。对于未知通信，检测到未知应用程序时，通信日志在默认情况下执行数据包捕获 (pcap)。左列中的绿色箭头代表应用程序数据的数据包捕获片段。单击绿色箭头可在浏览器中显示 pcap。

借助服务器 IP 地址（目标 IP）、目的地端口和数据包捕获的组合，您更容易识别应用程序并作出如何对网络采取措施的决策。例如，可创建标识此通信的自定义应用程序，而非将其标记为未知 TCP 或 UDP 通信。请参阅文章“识别未知应用程序”来查看识别未知应用程序的详细信息，以及参阅“自定义应用程序签名”来了解制作自定义签名以识别应用程序的信息。

© 2019 Palo Alto Networks, Inc.

用例：使用 Panorama 来响应事件

网络威胁可能源自不同的媒介，包括由于驱动下载而导致的恶意软件和间谍软件感染、网络钓鱼攻击、未打补丁的服务器以及随机或针对性拒绝服务 (DoS) 攻击，这些只是其中部分攻击方法。对网络攻击或感染做出反应的能力需要警告管理员攻击的流程和系统，并提供所需的辩论证据以跟踪用于启动攻击的来源和方法。

Panorama 提供的优势是从您网络的受管防火墙收集的模式和日志的集中与合并视图。您可以仅仅使用来自自动化关联引擎的信息，或将其与安全信息事件管理器 (SIEM) 生成的报告和日志配合使用，以调查攻击如何触发，以及如何预防将来的攻击和网络损坏而造成的损失。

此用例探索的问题包括：

- 如何获得事件通知？
- 如何确认该事件不是误判？
- 直接行动方案是什么？
- 如何使用可用资源重组触发事件之前或之后的事件顺序？
- 您需要考虑哪些更改以保证网络安全？

此用例跟踪特定事件，并为您介绍 Panorama 上的可见性工具如何帮助您响应该报告。

- 事件通知
- 查看 ACC 中的小部件
- 检查威胁日志
- 检查 WildFire 日志
- 检查数据筛选日志
- 更新安全规则

事件通知

根据您在 Palo Alto Networks 防火墙中的配置方式和深入分析可采用的第三方工具，有几种方法可向您提示事件。您可能收到记录到 Panorama 或您的 syslog 服务器的日志条目触发的电子邮件通知，也可通过您的 SIEM 解决方案上生成的专用报告通知您，第三方付费服务或代理也可能通知您。对于本例，我们假设您是从 Panorama 收到了一封电子邮件通知。该电子邮件通知您与间谍软件签名匹配的 Zero Access gent.Gen Command And Control Traffi（零访问 gent.Gen 命令和控制通信）警报触发的事件。电子邮件中还会列出会话的源和目的地 IP 地址、威胁 ID 和记录事件时的时间戳。

查看 ACC 中的小部件

在 **ACC** > **Threat Activity**（威胁活动）选项卡中，为任何关键或高严重性威胁勾选 **Compromised Hosts**（受影响主机）小部件和 **Threat Activity**（威胁活动）小部件。在 **Compromised Hosts**（受影响的主机）小部件中，浏览 Matching Objects（匹配对象），单击 Match Count（匹配计数）值查看关联事件的匹配证据。

检查威胁日志

要开始调查警报，请使用威胁 ID 搜索 Panorama 上的威胁日志（**Monitor** > **Logs** > **Threat**（监控 > 日志 > 威胁））。您可从威胁日志找到受害者的 IP 地址、导出数据包捕获（PCAP，点击日志条目中的下载图标 ）并使用一个诸如 WireShark 的网络分析工具检查数据包详情。对于 HTTP，请寻找不正确的协议、可疑主机、URL 字符串、用户代理、IP 地址和端口或伪造的 HTTP REFERER 来验证事件。在搜索类似数据模式和创建自定义签名，或修改安全策略以更好应对将来的威胁时，来自这些 pcaps 的数据也同样有用。

作为此手动检查的结果，如果您确信签名，请考虑将签名从提示操作转换为阻止操作以获得更主动方法。在某些情况下，您可选择将攻击者 IP 添加到 IP 阻止列表，以防止来自该 IP 地址的更多通信进入内部网络。

© 2019 Palo Alto Networks, Inc.

如果看到基于 *DNS* 的间谍软件签名，您本地 *DNS* 服务器的 *IP* 地址可能显示为 *Victim IP*（受害者 *IP*）地址。这通常是由于防火墙位于本地 *DNS* 服务器北侧，因此 *DNS* 查询将本地 *DNS* 服务器显示为源 *IP*，而并非显示启动请求的客户端的 *IP* 地址。

如果看到此问题，则启用安全规则防间谍软件配置文件中的 *DNS Sinkholing* 操作，以便标识网络中受感染的主机。*DNS Sinkholing* 可让您控制恶意域的出站连接，并将 *DNS* 查询重定向到未使用的内部 *IP* 地址；此 *Sinkhole* 不会做出响应。当受影响的主机开始连接到恶意域（而非连接到互联网）时，防火墙将请求重定向到您定义的 *IP* 地址，此主机受到 *Sinkhole* 攻击。现在，通过检查连接到 *Sinkhole* 的所有主机的流量日志，您可以找到所有受影响的主机，并采取补救措施防止攻击扩散。

要继续事件调查，请使用攻击者和受害者 IP 地址信息以查找详细信息，例如：

- 攻击者的地理位置在哪里？该 IP 地址是一个单独 IP 地址还是 NATed IP 地址？
- 导致该事件的原因是用户被诱使访问某个站点、下载而遭受攻击，还是通过电子邮件附件直接将威胁发送给用户的？
- 恶意软件是否正在传播？网络上是否有其他受影响的主机/终端？
- 它是一个零天漏洞吗？

每个日志条目的日志详情都显示该事件的相关日志。此信息会指导您找到通信、威胁、URL 筛选或其他日志，以便进行并将其关联到造成该事件的事件。例如，筛选通信日志（**Monitor** > **Logs** > **Traffic**（监控 > 日志 > 通信））使用 IP 地址作为源和目的地 IP，以获得受害者 IP 地址和其建立连接的所有外部和内部主机/客户端的完整视图。

检查 WildFire 日志

除了威胁日志外，请使用受害者 IP 地址筛选 WildFire 提交日志。WildFire 提交日志包含上传到 WildFire 服务进行分析的文件信息。因为间谍软件通常会悄悄地将自身嵌入在其他对象之中，检查 WildFire 提交日志会告诉您受害者最近是否下载了可疑文件。WildFire 辩证报告显示从其获得文件或 .exe 的 URL 的信息，以及内容的行为。它通知您文件是否存在恶意、是否修改注册表项、读/写文件、创建新文件、打开网络通信通道、导致应用程序崩溃、产生进程、下载文件或表现出其他恶意行为。使用此信息可确定是否阻止导致感染的应用程序（Web 浏览、SMTP、FTP），制定更严格的 URL 筛选规则，限制某些应用程序/操作（例如，将文件下载到特定用户组）。

从 *Panorama* 访问 *WildFire* 日志需要以下条件：*WildFire* 订阅，附加到安全规则的一个文件传送阻止配置文件，和转发到 *Panorama* 的威胁日志。

如果 *Panorama* 将管理运行软件版本早于 *PAN-OS 7.0* 的防火墙，则您应指定一个 *WildFire* 服务器，使 *Panorama* 可以从该服务器收集这些防火墙提交的 *WildFire* 样本相关分析信息。*Panorama* 使用此信息来填写在 *PAN-OS 7.0* 中缺少引入字段值的 *WildFire* 提交日志。运行较早软件版本的防火墙将不会填充这些字段。若要指定服务器，应选择 *Panorama* > *Setup*（设置）> *WildFire*，编辑 *General Settings*（常规设置），然后输入 *WildFire Private Cloud*（*WildFire* 私有云）名称。默认服务器为 *wildfire-public-cloud*，它是主机设在美国的 *WildFire* 云。

如果 WildFire 确定一个文件存在恶意，则会在 24-48 小时内创建一个新的防病毒签名并提供给您。如果您有 WildFire 订阅，该签名将作为下一个 WildFire 签名更新的组成部分，在 30-60 分钟内提供给您。一旦 Palo Alto Networks 下一代防火墙收到恶意软件的签名，且如果您的配置是阻止恶意软件，则会阻止该文件，同时被阻止文件的信息会显示在威胁日志中。此流程紧密集成以防止您受到此威胁，阻断恶意软件在您网络上扩散。

检查数据筛选日志

数据筛选日志（**Monitor** > **Logs** > **Data Filtering**（监控 > 日志 > 数据筛选））是调查恶意网络活动的另一个重要来源。您可定期检查获得警告的所有文件的日志，也可使用日志跟踪文件以及在受害者 IP 地址或用户

© 2019 Palo Alto Networks, Inc.

之间往返的数据，并验证通信的方向和流动：服务器到客户端或客户端到服务器。要在事件之前和之后重新创建事件，请将受害者 IP 地址的日志筛选为目的地，并检查网络活动的日志。

因为 Panorama 聚合来自所有受管防火墙的信息，因此它能很好地显示网络中全部活动的概况。您可用于调查网络上通信的部分其他可视工具包括 **Threat Map**（威胁地图）、**Traffic Map**（通信地图）和 **Threat Monitor**（威胁监视器）。威胁地图和通信地图（**Monitor** > **AppScope** > **Threat Map**（监控 > 应用层面 > 威胁地图）或 **Traffic Map**（通信地图））允许您查看传入和传出通信的地理区域。这对查看代表外来潜在攻击的反常活动非常有用，例如 DDoS 攻击。例如，如果您没有与东欧地区发生许多业务事务，而地图显示指向该地区的通信量存在异常，请单击地图的相应区域启动并查看 ACC 信息，包括排名居前的应用程序、会话计数的通信详情、发送和接收的字节数、排名居前的源和目的地、用户或 IP 地址以及检测到的威胁严重程度（如有）。威胁监控（**Monitor** > **AppScope** > **Threat Monitor**（监控 > 应用层面 > 威胁监视器））显示网络的前十大威胁，或排名居前的攻击列表或网络排名居前的受害者。

更新安全规则

通过现在发现的所有信息，您可汇总网络上的威胁影响（即攻击程度、来源、受影响的主机、风险系数）以及评估可遵循哪些更改（如有）。下面是供您考虑的一些建议：

- 通过增强 DoS 保护配置文件以配置早期随机丢弃，或为 TCP 洪水攻击丢弃 SYN Cookie，从而抵御 DDoS 攻击。考虑限制 ICMP 和 UDP 通信。根据您在日志中发现的趋势和模式评估可用选项，并使用 Panorama 模板执行更改。

  创建一个动态阻止列表（**Objects** > **Dynamic Block Lists**（对象 > 动态阻止列表）），阻止您从几个情报来源发现的特定 IP 地址：您自己威胁日志的分析，来自特定 IP 地址的 DDoS 攻击，或第三方 IP 阻止列表。

  列表必须是位于 Web 服务器上的一个文本文件。使用 Panorama 上的设备组，将对象推送到受管防火墙，从而使防火墙可以访问 Web 服务器并以定义的频率导入列表。创建动态阻止列表对象后，定义在源和目的地字段中使用地址对象的安全规则，以阻止在定义的 IP 地址、范围或子网之间往返的通信。此方法允许您在解决问题之前阻止入侵者，并执行更大程度的策略更改来保证网络安全。
- 确定是否创建共享策略规则或设备组规则来阻止导致感染的特定应用程序（Web 浏览、SMTP、FTP）、制定更严格的 URL 筛选规则、限制某些应用程序/操作（例如，将文件下载到特定用户组）。
- 在 Panorama 上，您也可切换到防火墙上下文，并且为识别网络上可能感染 botnet 的主机的 Botnet 报告配置防火墙。

Panorama 高可用性

为了在系统或网络出现故障时提供冗余，您可以在高可用性 (HA) 配置中部署两台 Panorama™ 管理服务器。Panorama 支持高可用性配置，其中一个对端设备为主动-主要对端设备，另一个对端设备为被动-辅助对端设备。如果主要对端设备发生故障，则它会自动故障转移且辅助对端设备变为主动对端设备。

> Panorama 高可用性前提条件
> Panorama 高可用性的优先级和故障转移
> 故障转移触发
> Panorama 高可用性的日志记录注意事项
> Panorama 高可用性对端设备之间的同步
> 管理 Panorama 高可用性对

Panorama 高可用性前提条件

要配置 Panorama 高可用性，您需要符合下列要求的两台相同的 Panorama 服务器：

- 相同外形规格 — 对端设备必须具有相同型号和模式：均为 Panorama 模式、“仅管理”模式或“传统”模式（仅限 ESXi 和 vCloud Air）下的 M-600 设备、M-500 设备、M-200 设备或 AWS、Azure、GCP 和 ESXi 上的 Panorama 虚拟设备。日志收集器模式下的 Panorama 设备不支持高可用性。
- **Panorama** 操作系统版本相同 — 必须运行相同版本的 Panorama，以同步配置信息和维持无缝故障转移所需的平等性。
- 许可证集合相同 — 必须拥有相同的防火墙管理功能许可证。
- （仅限 Panorama 虚拟设备）唯一的序列号 — 必须拥有唯一的序列号；如果两个 Panorama 实例的序列号相同，那么这两个实例将会处于挂起模式，直到您解决问题。

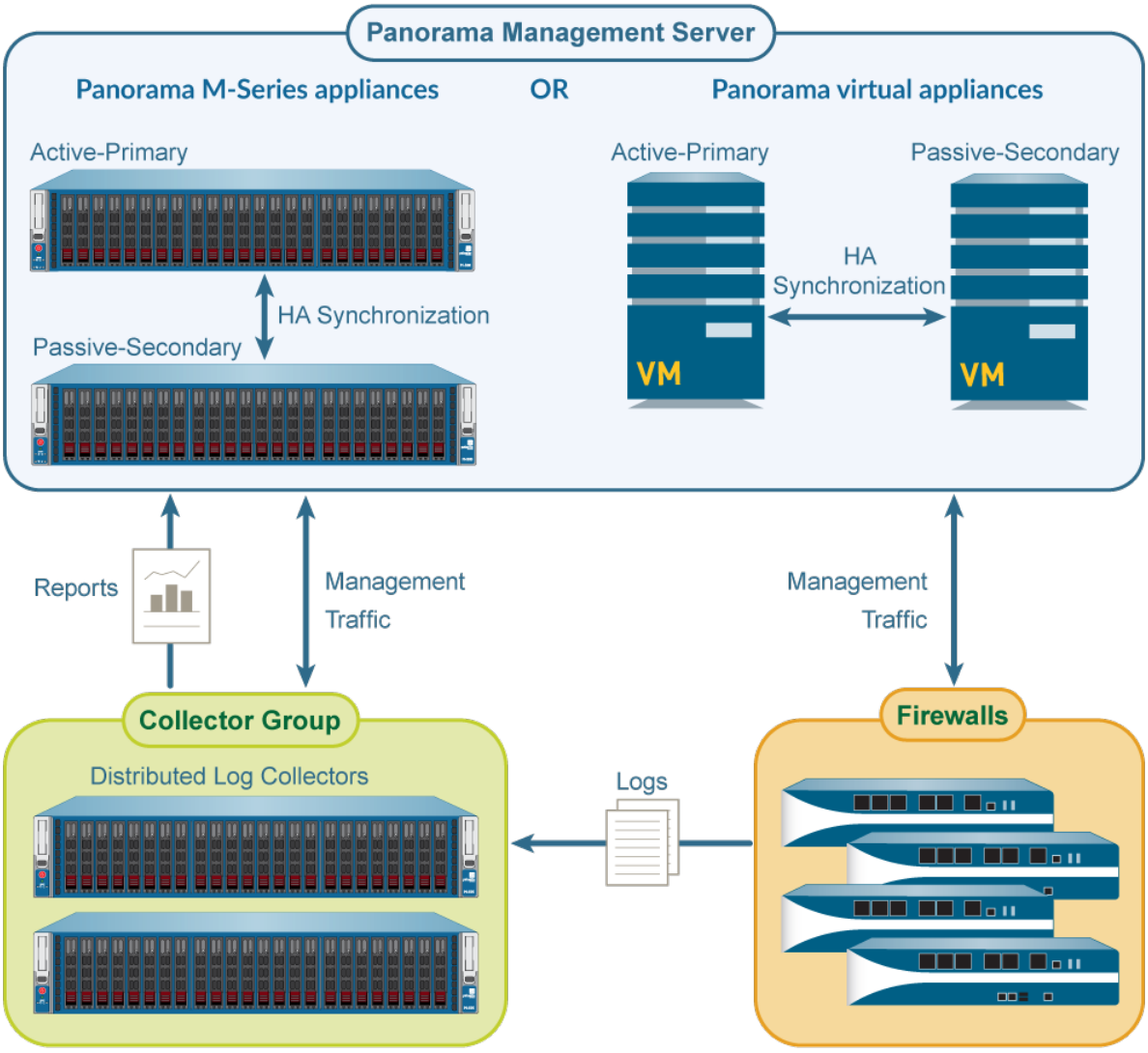


图 **28: Panorama HA** 组织

高可用性配置中的 Panorama 服务器为对端设备，您可以使用其中任何一个（主动或被动）来集中地管理防火墙、日志收集器、WildFire 设备和设备集群，但在少数情况下例外（请参阅 Panorama 高可用性对端设备之间的同步）。高可用性对端设备使用管理 (MGT) 接口同步推送到受管防火墙、日志收集器、WildFire 设备和设备群集的配置元素以维护状态信息。通常情况下，Panorama 高可用性对端设备在地理位置上位于不

© 2019 Palo Alto Networks, Inc.

同的地址，因此您需要确保可以通过网络路由分配给每个对端设备的 MGT 接口 IP 地址。高可用性连接使用启用加密的 TCP 端口 28。如果不启用加密，则使用端口 28769 和 28260 进行高可用性连接并同步高可用性对端设备之间的配置。建议对端设备之间的延迟小于 500ms。要确定延迟，可以在正常通信期间使用 Ping。

© 2019 Palo Alto Networks, Inc.

Panorama 高可用性的优先级和故障转移

将会为高可用性对中的每个 Panorama 对端设备分配一个优先级值。主要或辅助对端设备的优先级值可确定将有资格成为管理和日志管理的主点的对端设备。将对端设备设置为主要对端设备将呈现主动状态，而辅助对端设备将变成被动状态。主动对端设备处理所有配置更改并将其推送到受管防火墙；被动对端设备无法进行任何配置更改或将配置推送到受管防火墙。但是，任何一台对端设备都可以用来运行报告或执行日志查询。

被动对端设备已同步，并且准备过渡到主动状态（如果在主动 Panorama 上出现路径、链接、系统或网络故障）。

当发生故障转移时，只有 Panorama 对端设备的状态（主动或被动）会发生变化；优先级（主要和辅助）不会发生变化。例如，当主要对端设备出现故障时，其状态将会从主动-主要更改成被动-主要。

处于主动辅助状态的对端设备可以执行所有功能，但有两种例外情况：

- 无法管理防火墙或日志收集器部署功能，例如许可证更新或软件升级。
- 无法记录到网络文件共享，直到手动将其优先级更改为主要。只有传统模式下的 Panorama 虚拟设备支持 NFS。

下表根据 Panorama 的状态和优先级设置列出了其功能：

Capability	active-primary	passive-primary passive-secondary	active-secondary
Switch device context	■	■	■
Perform distributed reporting	■	■	■
Manage shared policy	■	■	■
Log to local disk	■	■ (Optional on the Panorama virtual appliance only)	■ (Optional on the Panorama virtual appliance only)
Log to an NFS partition (Panorama virtual appliance only)	■	■	■
Deploy software and licenses	■	■	■
Export Panorama configuration	■	■	■

图 29: Panorama HA 功能

有关详细信息，请参阅Panorama 高可用性前提条件或设置 Panorama 高可用性。

© 2019 Palo Alto Networks, Inc.

故障转移触发

当在主动 Panorama 上发生故障和被动 Panorama 接管管理防火墙任务时，该事件称为故障转移。当主动 Panorama 上监视的指标失败时，将触发故障转移。这种故障将使主要 Panorama 的状态从主动主要转换为被动主要，而辅助 Panorama 的状态则将变成主动辅助。

触发故障转移的条件有：

- Panorama 对端设备无法互相通信，且主动对端设备无法对运行状况和状态轮询做出响应；使用的指标为高可用性检测信号轮询和呼叫消息。

  如果 Panorama 对端设备无法互相通信，主动对端设备将会在触发故障转移前监控是否仍然能够将对端设备已连接。在两台 Panorama 对端设备同时处于主动状态的情况下，此检查有助于避免发生故障转移和导致脑裂情景。
- 无法到达在主动对端设备上指定的一个或多个目标（IP 地址）；使用的指标为高可用性路径监控。

除上面列出的故障转移以外，当管理员将 Panorama 对端设备置于挂起状态或发生抢先时，同样也会发生故障转移。抢先是主要 Panorama 从故障（或用户发起的挂起）恢复后恢复主动角色的首选方法。默认情况下，已启用抢先，以及当主要 Panorama 从故障恢复且变为可用时，辅助 Panorama 将放弃控制并恢复为被动状态。当发生抢先行为时，该事件会记录在系统日志中。

如果将该事件记录到网络文件共享数据存储设备，则不会禁用抢先，因为它允许主要对端设备（即安装到网络文件共享的设备）恢复主动角色并写入网络文件共享数据存储设备。对于所有其他部署，仅当您希望确保特定 Panorama 为首选主动对端设备时才需要发生抢先行为。

高可用性检测信号轮询和呼叫消息

高可用性对端设备使用呼叫消息和检测信号来验证对端设备是否能够做出响应和正常运行。呼叫消息按照所配置的问候间隔从一个对端设备发送到另一个对端设备，用于验证另一个对端设备的状态。检测信号是对高可用性对端设备进行的 ICMP ping 操作，对端设备响应 ping 操作以确定该对端设备已连接并且可响应。默认情况下，发送检测信号的间隔是 1,000 毫秒，发送呼叫消息的间隔是 8,000 毫秒。

高可用性路径监控

路径监控为一个 IP 地址或一组 IP 地址（路径组）检查网络连接和链接状态。主动对端设备使用 ICMP ping 来验证是否可以访问一个或多个目标 IP 地址。例如，您可以监控互连网络设备（如路由器或交换机）、与服务器本身的连接性或者流量流中某些其他重要设备的可用性。确保要监控的节点/设备不可能无响应，尤其是其在负载情况下，因为这可能会导致路径监控失败并触发故障转移。

默认的 ping 操作间隔为 5,000 毫秒。当连续三次 ping 操作（默认值）失败时，将认为无法访问该 IP 地址，并且当监控的任何或全部 IP 地址都变得无法访问后将触发对端设备故障。默认情况下，如果其中任何一个 IP 地址变得无法访问，则高可用性状态将过渡到非功能性。

© 2019 Palo Alto Networks, Inc.

Panorama 高可用性的日志记录注意事项

在高可用性配置中设置 Panorama 可为日志收集提供冗余。由于受管防火墙已经通过 SSL 连接到两个 Panorama 对端设备，因此当状态发生变化时，每个 Panorama 会向受管防火墙发送一则消息。系统将 Panorama 高可用性状态通知防火墙，并且可以相应地转发日志。

默认情况下，当受管防火墙不能连接到 *Panorama* 时，它们会缓存日志；当恢复连接时，它们会从上次中断的位置恢复发送日志。

基于硬件的 Panorama 和 Panorama 虚拟设备的日志记录选项不同：

- 在传统模式下 Panorama 虚拟设备的日志记录故障转移
- 在 Panorama 模式下 M 系列设备或 Panorama 虚拟设备的日志记录故障转移

在传统模式下 Panorama 虚拟设备的日志记录故障转移

传统模式下的 Panorama 虚拟设备提供以下日志故障转移选项：

日志存储类型	说明
虚拟磁盘	默认情况下，受管防火墙将日志作为独立的流发送到每个 Panorama 高可用性对端设备。默认情况下，如果对端设备变成不可用，则受管防火墙会缓冲日志并当对端设备与其重新建立连接时从离开的位置恢复发送日志（受磁盘存储容量和断开连接的持续时间限制）。 最大日志存储容量取决于虚拟平台（VMware ESXi 或 vCloud Air）；有关详细信息，请参阅Panorama 型号。 您可以选择是否只将日志转发到主动对端设备（请参阅修改日志转发和缓冲默认设置）。但是，*Panorama* 不支持在高可用性对之间累积日志。因此，如果您将日志记录到虚拟磁盘用于监控和报告，则必须查询从受管防火墙收集日志的 *Panorama* 对端设备。
网络文件系统 (NFS)	您只能将 NFS 存储安载到在 VMware ESXi 服务器上运行的 Panorama 虚拟设备。只能将主动-主要 Panorama 安装到基于 NFS 的日志分区且可以接收日志。在发生故障转移后，主要设备进入被动-主要状态。在这种情况下，直到发生抢先，主动-辅助 Panorama 才可管理防火墙，但它不能接收日志且无法写入 NFS。要允许主动-辅助对端设备记录到 NFS，您必须手动将其切换到主要对端设备，从而使得可以将其安装到 NFS 分区。有关说明，请参阅 在 Panorama 故障转移后切换优先级以恢复 NFS 日志记录。

在 Panorama 模式下 M 系列设备或 Panorama 虚拟设备的日志记录故障转移

如果您将防火墙日志转发到 Panorama 模式下的 M-600 设备、 M-500 设备、M-200 设备或 Panorama 虚拟设备的 HA 对中的本地日志收集器，则可以在配置收集器组时指定由哪些防火墙将日志发送到哪些日志收集器。您可以为每个 Panorama 对端设备的日志收集器配置单独的收集器组，或配置单个收集器组以包含两个对端设备的日志收集器。在同时包含本地日志收集器的收集器组中，日志转发首选项列表确定从防火墙接收日志的日志收集器。对于 PA-7000 系列和 PA-5200 系列防火墙，您可以选择将日志发送到收集器组中的所

© 2019 Palo Alto Networks, Inc.

有日志收集器，在这种情况下 Panorama 使用循环调度负载均衡来选择在任何指定时间接收日志的日志收集器。

在包含两个日志收集器的收集器组中，还可以启用冗余，以便每个日志都有两个副本，并且每个副本将驻留在不同的日志收集器中。如果任何一个日志收集器变成不可用，此冗余可确保不会丢失任何日志：可以查看转发到收集器组的所有日志并运行所有日志信息的报告。日志冗余只有在收集器组中的每个日志收集器拥有相同数量的磁盘时才可用。



任何特定收集器组的所有日志收集器均必须为相同的型号：均为 *M-200* 设备、均为 *M-500* 设备、均为 *M-600* 设备或均为 *Panorama* 模式下的 *Panorama* 虚拟设备。

由于启用冗余会创建更多日志，因此该配置需要更多存储容量。启用冗余会将收集器组中的日志处理通信增加一倍，从而将其最大日志记录速率降低一半，因为每个日志收集器均必须分发其收到的每个日志的副本。（当收集器组用完容量空间后，将会删除较早的日志。）

© 2019 Palo Alto Networks, Inc.

Panorama 高可用性对端设备之间的同步

Panorama 高可用性对端设备在您每次在主动 Panorama 对端设备上提交更改时同步运行配置。当您每次在主动对端设备上保存配置或在发生故障转移前，同步两个对端设备之间的待选配置。

在 Panorama 高可用性对等设备之间同步的设置在设备对之间是通用的，例如共享对象和策略规则、设备组对象和规则、模板配置、证书和 SSL/TLS 服务配置文件、以及管理访问配置。

当您启用自动提交恢复时，只有在 Panorama 推送后防火墙成功测试自身与 Panorama 之间的连接后，才会进行 HA 同步。

不同步的设置是每台对端设备的独有设置，如以下设置：

- Panorama 高可用性配置 — 优先级设置、对端设备 IP 地址、路径监控组和 IP 地址
- Panorama 配置 — 管理接口 IP 地址、FQDN 设置、登录提示、NTP 服务器、时区、地理位置、DNS 服务器、允许访问 Panorama 的 IP 地址、SNMP 系统设置和动态内容更新调度
- 计划配置导出
- 用于日志记录的网络文件共享分区配置和所有磁盘配额分配。这仅适用于在 VMware ESXi 服务器上运行的传统模式下的 Panorama 虚拟设备。
- Panorama 本地存储 (SSD) 上不同类型的日志和数据库的磁盘配额分配



如果您在 *Panorama* 上使用主密钥对私钥和证书进行加密，必须在两个高可用性对端设备上同时使用同一主密钥。如果主密钥不同，*Panorama* 将无法同步高可用性对端设备。

有关详细信息，请参阅Panorama 高可用性前提条件或设置 Panorama 高可用性。

© 2019 Palo Alto Networks, Inc.

管理 Panorama 高可用性对

- 设置 Panorama 高可用性
- 在 HA 对端设备之间使用自定义证书设置身份验证
- 测试 Panorama 高可用性故障转移
- 在 Panorama 故障转移后切换优先级以恢复 NFS 日志记录
- 将主要 Panorama 还原至主动状态



要安装软件或内容更新，请参阅 在高可用性配置中安装 Panorama 更新。

设置 Panorama 高可用性

在执行以下步骤之前，请参阅Panorama 高可用性前提条件：

STEP 1 | 设置高可用性对端设备上 MGT 端口之间的连接。

Panorama 对端设备使用端口进行互相通信。确保您分配给高可用性对中 Panorama 服务器的 MGT 端口的 IP 地址可路由，并且对端设备可以通过您的网络互相通信。要设置 MGT 端口，请参阅 执行 Panorama 虚拟设备的初始配置 或 执行 M 系列设备的初始配置。

挑选对中的 **Panorama** 对端设备并完成剩余任务。

STEP 2 | 启用高可用性并（可选）为高可用性连接启用加密。

1. 选择 **Panorama** > **High Availability**（Panorama > 高可用性），然后编辑 **Setup**（设置）部分。
2. 选择 **Enable HA**（启用 **HA**）。
3. 在 **Peer HA IP Address**（对端设备高可用性 **IP** 地址）字段中，输入分配给对端设备 Panorama 的 IP 地址。
4. 在 **Peer HA Serial**（**HA** 对序列号）字段，输入对端 Panorama 的序列号。

   输入 Panorama HA 对序列号，以减少对 Panorama IP 进行暴力攻击的攻击面。
5. 在 **Monitor Hold Time**（监控保持时间）字段中，输入在对控制链路故障起作用之前系统将要等待的时间长度（毫秒）（范围为 1000-60000，默认为 3000）。
6. 如果不想加密，可以取消选中 **Encryption Enabled**（启用加密）复选框，然后单击 **OK**（确定）：不需要执行更多步骤。如果想要加密，可以选中 **Encryption Enabled**（启用加密）复选框，然后单击 **OK**（确定）并执行以下任务：
   1. 选择 **Panorama** > **Certificate Management** > **Certificates**（Panorama > 证书管理 > 证书）。
   2. 选择 **Export HA key**（导出 **HA** 密钥）。将高可用性密钥保存到对端设备 Panorama 可以访问的网络位置。
   3. 在对端设备 Panorama 上，导航到 **Panorama** > **Certificate Management** > **Certificates**（Panorama > 证书管理 > 证书），然后选择 **Import HA key**（导入高可用性密钥），浏览到保存密钥的位置并将其导入。

STEP 3 | 设置高可用性优先级。

1. 在 **Panorama** > **High Availability**（Panorama > 高可用性）中，编辑 **Election Settings**（选择设置）部分。
2. 将 **Device Priority**（设备优先级）定义为 **Primary**（主要）或 **Secondary**（辅助）。确保将一台对端设备设置为主要，并将另一台对端设备设置为辅助。



如果两台对端设备都拥有相同的优先级设置，则将具有较高序列号的对端设备置于挂起状态。

© 2019 Palo Alto Networks, Inc.

3. 定义 **Preemptive**（抢先）行为。默认情况下，抢先已启用。必须在两台对端设备中同时启用或禁用抢先选择。

   如果您正在使用网络文件共享进行日志记录且已禁用抢先，要恢复至网络文件共享，请参阅在 Panorama 故障转移后切换优先级以恢复 NFS 日志记录。

STEP 4 | 要配置路径监控，请定义一个或多个路径组。

路径组列出了 Panorama 必须 ping 以验证网络连接的目标 IP 地址（节点）。

对于包括您想要监控的节点的每个路径组，请执行以下步骤。

1. 选择 **Panorama** > **High Availability**（Panorama > 高可用性），然后在“Path Group（路径组）”部分中单击 **Add**（添加）。
2. 输入路径组的 **Name**（名称）。
3. 选择此组的 **Failure Condition**（故障条件）：
   - **any**（任何）触发路径监控故障（如果其中任何一个 IP 地址变得不可访问）。
   - **all**（所有）触发路径监控故障（只有当没有任何 IP 地址可访问时）。
4. **Add**（添加）您想要监控的每一个目标 IP 地址。
5. 单击 **OK**（确定）。Path Group（路径组）部分将会显示新组。

STEP 5 | （可选）在 Panorama 上选择路径监控的失败条件。

1. 选择 **Panorama** > **High Availability**（Panorama > 高可用性），然后编辑“Path Monitoring（路径监控）”部分。
2. 选择 **Failure Condition**（故障条件）：
   - **all**（所有），用于触发故障转移（只有当所有监控的路径组都出现故障时）。
   - **any**（任何），用于触发故障转移（当任何监控的路径组都出现故障时）。
3. 单击 **OK**（确定）。

STEP 6 | Commit（提交）配置更改。

选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

STEP 7 | 配置其他 Panorama 对端设备。

在高可用性对的其他对端设备上重复步骤 2 至步骤 6。

STEP 8 | 同步 Panorama 对端设备。

1. 访问主动 Panorama 上的 **Dashboard**（仪表盘），然后选择 **Widgets**（小部件）> **System**（系统）> **High Availability**（高可用性）以显示高可用性小部件。
2. **Sync to peer**（同步到对端设备），单击 **Yes**（是），然后等待 **Running Config**（运行配置）显示 **Synchronized**（已同步）。
3. 访问被动 Panorama 上的 **Dashboard**（仪表盘），然后选择 **Widgets**（小部件）> **System**（系统）> **High Availability**（高可用性）以显示高可用性小部件。
4. 确认 **Running Config**（运行配置）显示 **Synchronized**（已同步）。

在 HA 对端设备之间使用自定义证书设置身份验证

您可以使用自定义证书设置身份验证保护 Panorama HA 对端设备之间的 HA 连接。

STEP 1 | 在 Panorama 上生成证书签发结构 (CA) 证书。

1. 选择 **Panorama** > **Certificate Management** > **Certificates**（Panorama > 证书管理 > 证书）。
2. 创建自签名根 CA 证书或从企业 CA 导入证书。

© 2019 Palo Alto Networks, Inc.

STEP 2 | 配置包含根 CA 和中间 CA 的证书配置文件。

1. 选择 **Panorama** > **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件）。
2. 配置证书配置文件。

STEP 3 | 配置 SSL/TLS 服务配置文件。

1. 选择 **Panorama** > **Certificate Management**（证书管理）> **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）。
2. 配置 SSL/TLS 配置文件定义 Panorama 及其受管设备用于 SSL/TLS 服务的证书和协议。

STEP 4 | 在 Panorama 上配置安全服务器通信。

1. 选择 **Panorama** > **Setup**（设置）> **Management**（管理），然后 **Edit**（编辑）Panorama 设置。
2. 验证 **Custom Certificate Only**（仅允许自定义证书）复选框未选中。这允许您在迁移到自定义证书的同时继续管理所有设备。

   如果选中 *Custom Certificate Only*（仅允许自定义证书）复选框，则 *Panorama* 不会进行身份验证，并且无法使用预定义证书管理设备。
3. 从 **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）下拉列表中选择 SSL/TLS 服务配置文件。此 SSL/TLS 服务配置文件适用于 Panorama、防火墙、日志收集器和 Panorama HA 对端设备之间的所有 SSL 连接。
4. 从 **Certificate Profile**（证书配置文件）下拉列表中选择证书配置文件。
5. （可选）配置授权列表。
   1. 单击 Authorization List（授权列表）下的 **Add**（添加）。
   2. 选择 **Subject**（主题）或 **Subject Alt Name**（主题备用名称）作为标识符类型。
   3. 输入通用名
6. 在 **Disconnect Wait Time (min)**（断开连接等待时间（分钟））中，输入 Panorama 在与其受管设备断开并重新建立连接之前所需的分钟数。该字段默认为空，范围为 0 至 44,640 分钟。

   在您提交新配置之前，断开连接等待时间不会开始倒计时。

1. 单击 **OK**（确定）。
2. **Commit**（提交）更改。

STEP 5 | 将客户端 Panorama 升级到 8.1。

升级 Panorama。

STEP 6 | 配置安全客户端通信。

1. 选择 **Panorama** > **High Availability**（高可用性），然后 **Edit**（编辑）高可用性设置。
2. 选择 **Certificate**（证书）和 **Certificate Profile**（证书配置文件）。
3. 单击 **OK**（确定）。
4. **Commit**（提交）更改。

测试 Panorama 高可用性故障转移

要测试您的高可用性配置是否工作正常，请触发手动故障转移并验证对端设备是否能够成功转换状态。

STEP 1 | 登录到主动 Panorama 对端设备。

您可以在 Web 界面的右上角验证 Panorama 服务器的状态。

STEP 2 | 挂起主动 Panorama 对端设备。

© 2019 Palo Alto Networks, Inc.

选择 **Panorama** > **High Availability**（高可用性），然后单击 Operational Commands（操作命令）部分中的 **Suspend local Panorama**（挂起本地 **Panorama**）链接。

STEP 3 | 验证是否已将被动 Panorama 对端设备接管为主动 Panorama 对端设备。

在 Panorama **Dashboard**（仪表盘）的 **High Availability**（高可用性）小部件上，验证 **Local**（本地）被动服务器的状态是否为 **active**（主动）和 **Peer**（对端设备）的状态是否为 **suspended**（挂起）。

STEP 4 | 将挂起的对端设备还原为运行状态。等待几分钟时间，然后验证是否已发生抢先（如果已启用抢先）。

在之前挂起的 Panorama 上：

1. 选择 **Panorama** > **High Availability**（Panorama > 高可用性），然后在“Operational Commands（操作命令）”部分中单击 **Make local Panorama functional**（运行本地 Panorama）。
2. 在 **Dashboard**（仪表盘）上的 **High Availability**（高可用性）小部件中，确认该（本地）Panorama 服务器已接管为主动对端设备，并且其他对端设备现在处于被动状态。

在 Panorama 故障转移后切换优先级以恢复 NFS 日志记录

在 ESXi 服务器上运行处于传统模式的 Panorama 虚拟设备可以使用 NFS 数据存储进行日志记录。在高可用性配置中，只能将主要 Panorama 对端设备安装到基于 NFS 的日志分区且可以写入 NFS。当发生故障转移和被动 Panorama 变成主动 Panorama 时，其状态变成主动-辅助。尽管辅助 Panorama 对端设备可以主动管理防火墙，但它无法接收日志或将日志写入网络文件共享，因为它不拥有网络文件共享分区。如果防火墙无法将日志转发到主要 Panorama 对端设备，各个防火墙将日志写入它们的本地磁盘。防火墙将保持最后一组转发到 Panorama 的日志条目的指针，这样当被动-主要 Panorama 再次变成可用时，它们可以恢复向其转发日志。

使用本节中的说明在主动-辅助 Panorama 对端设备上手动切换优先级，使得它可以开始记录到 NFS 分区。在如下所示的典型情况下，您可能需要触发此更改：

- 抢先已禁用。默认情况下，在 Panorama 上已启用抢先，并且当主要对端设备再次变为可用时恢复为主动。如果禁用抢先，则您需要在辅助对端设备上将优先级切换至主要，以便可以将其安装到 NFS 分区、接收来自受管防火墙的日志并写入 NFS 分区。
- 主动 Panorama 发生故障，且在短期内无法从故障中恢复。如果不切换优先级，则当达到防火墙的最大日志存储容量时，将会覆盖最早的日志，使其能够继续记录到其本地磁盘。这种情况可能会导致日志丢失。

STEP 1 | 登录到当前的被动-主要 Panorama，选择 **Panorama** > **Setup** > **Operations**（Panorama > 设置 > 操作），然后在“Device Operations（设备操作）”部分中单击 **Shutdown Panorama**（关闭 Panorama）。

STEP 2 | 登录到主动-辅助 Panorama，选择 **Panorama** > **High Availability**（高可用性），编辑 Election Settings（选择设置），然后将 **Priority**（优先级）设置为 **Primary**（主要）。

STEP 3 | 单击 **OK**（确定）保存更改。

STEP 4 | 选择 **Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

当系统显示提示时，请不要重新启动。

STEP 5 | 登录到 Panorama 命令行界面，并输入以下命令将 NFS 分区的所有权更改为此对端设备：**`request high-availability convert-to-primary`**

© 2019 Palo Alto Networks, Inc.

STEP 6 | 选择 **Panorama** > **Setup** > **Operations**（Panorama > 设置 > 操作），然后在“Device Operations（设备操作）”部分中单击 **Reboot Panorama**（重新启动 Panorama）。

STEP 7 | 启动在步骤 1 中关闭的 Panorama 对端设备。现在，该对端设备将处于被动辅助状态。

将主要 Panorama 还原至主动状态

默认情况下，Panorama 的抢先功能允许在主要 Panorama 变为可用时将运行状态恢复为主动对端设备。但是，如果已禁用抢先，强制主要 Panorama 从故障、非运行或已挂起状态恢复后变为主动的唯一方法是通过挂起辅助 Panorama 对端设备。

在主动-辅助 Panorama 进入挂起状态之前，它会将候选配置传输到被动 Panorama，从而保存所有未提交的配置更改并在其他对端设备上可以访问。

STEP 1 | 挂起 Panorama。

1. 登录到您想要置于挂起状态的 Panorama 对端设备。
2. 选择 **Panorama** > **High Availability**（Panorama > 高可用性），然后单击“Operational Commands（操作命令）”部分中的 **Suspend local Panorama**（挂起本地 Panorama）链接。

STEP 2 | 验证状态是否指示 Panorama 已按用户请求挂起。

在 **Dashboard**（仪表盘）的 **High Availability**（高可用性）小部件上，验证 **Local**（本地）状态是否为 **suspended**（挂起）。

在您挂起对端设备时可能会触发故障转移，并且其他 Panorama 接管为主动对端设备。

STEP 3 | 将挂起的 Panorama 还原至可用状态。

1. 在 **Panorama** > **High Availability**（Panorama > 高可用性）选项卡的“Operational Commands（操作命令）”部分中，单击 **Make local Panorama functional**（运行本地 Panorama）链接。
2. 在 **Dashboard**（仪表盘）的 **High Availability**（高可用性）小部件上，确认 Panorama 已过渡到主动状态或被动状态。

© 2019 Palo Alto Networks, Inc.

管理 *Panorama*

本节介绍如何管理和维护 Panorama™ 管理服务器。本节包含以下主题：

- 预览、验证或提交配置更改
- 启用自动提交恢复
- 管理 Panorama 和防火墙配置备份
- 比较 Panorama 配置的更改
- 管理配置更改限制锁
- 将自定义徽标添加到 Panorama
- 使用 Panorama 任务管理器
- 管理日志和报告的存储配额和过期期限
- 监视 Panorama
- 重新启动或关闭 Panorama
- 配置 Panorama 密码配置文件和复杂性

有关完成初始设置（包括定义网络访问设置、许可、升级 Panorama 软件版本和设置 Panorama 管理访问权限）的说明，请参阅设置 Panorama。

预览、验证或提交配置更改

您可以执行 Panorama 提交、验证和预览操作对 Panorama 配置进行暂挂更改，然后将这些更改推送到 Panorama 管理的设备，包括防火墙、日志收集器、WildFire 设备和设备群集。您可以按管理员或位置筛选暂挂更改，然后仅提交、推送、验证或预览这些更改。位置可以是特定设备组、模板、收集器组、日志收集器、共享设置或 Panorama 管理服务器。

由于 Panorama 会推送其运行配置，因此只有先将它们提交给 Panorama 才能将更改推送到设备。如果尚未准备在设备上激活更改，可以选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**）将更改提交到 Panorama 配置而不将其推送到设备。稍后，当准备在设备上激活更改时，可以选择 **Commit**（提交）> **Push to Devices**（推送到设备）。如果准备同时在 Panorama 和设备上激活更改，可以选择 **Commit**（提交）> **Commit and Push**（提交并推送），如以下过程所述。

STEP 1 | 配置要提交、验证或预览的配置更改范围。

1. 单击 Web 界面顶部的 **Commit**（提交）。
2. 选择以下任一选项：
   - **Commit All Changes**（提交所有更改）（默认）-— 将提交应用于具有管理权限的所有更改。选择此选项时，不能手动筛选提交范围。而是分配给您用于登录的帐户的管理员角色确定提交范围。
   - **Commit Changes Made By**（提交所做的更改）-— 使您能够通过管理员或位置筛选提交范围。分配给您用于登录的帐户的管理角色确定可以筛选的更改。

   要提交其他管理员的更改，您用于登录的帐户必须分配给“超级用户”角色或管理角色配置文件，并启用 *Commit For Other Admins*（为其他管理员提交）权限。
3. （可选）要根据管理员筛选提交范围，请选择 **Commit Changes Made By**（提交所做的更改），单击相邻链接，选择管理员，然后单击 **OK**（确定）。
4. （可选）要根据位置筛选，请选择 **Commit Changes Made By**（提交所做的更改），并清除要从 Commit Scope（提交范围）中排除的任何更改。

   如果您启用及禁用的配置更改间的相关性导致验证错误，请在启用所有更改的情况下进行提交。例如，在将更改提交到特定设备组后，必须在此设备组中加入添加、删除或重新定位相同规则库规则的所有管理员的更改。

STEP 2 | 预览提交将激活的更改。

在删除后预览变更，并重新添加相同设备到策略规则时，*Panorama* 会显示在运行中配置内删除以及在待选配置内添加的相同设备。此外，运行中配置内设备目标列表上的设备顺序可能与待选配置中的不同，并在预览更改时显示为更改，即便并未对配置做出任何更改。

预览在您忘记自己的更改或您不确定自己是否想要激活这些更改等情况下很有用处。

Panorama 让您将 Commit Scope（提交范围）中选择的配置与正在运行的配置进行比较。预览窗口并排显示配置，并使用颜色编码表示添加（绿色）、修改（黄色）或删除（红色）的更改。

Preview Changes（预览更改）并选择 **Lines of Context**（上下文行数），这是比较配置文件中的行数，以显示高亮差异之前和之后的信息。这些行有助于使预览输出与 Web 界面设置相互关联。完成更改审核后，关闭预览窗口。

由于预览结果会在新窗口中显示，所以您的浏览器必须设置为允许弹出窗口。如果预览窗口未打开，请参阅浏览器文档，了解允许弹出窗口的相关步骤。

STEP 3 | 预览您用于提交更改的各个设置。

© 2019 Palo Alto Networks, Inc.

如果您想了解有关更改的详细信息（例如设置类型和实施更改的人员），预览会很有用。

1. 单击 **Change Summary**（更改摘要）。
2. （可选）列名称**Group By**（分组方式）（例如，设置 **Type**（类型））。
3. 完成更改审核后，**Close**（关闭）“更改摘要”对话框。

STEP 4 | 提交前验证更改以确保成功提交。

1. **Validate Changes**（验证更改）。

   验证结果显示的所有错误及警告均与实际提交所显示的一致。
2. 解决验证结果找到的任何错误。

STEP 5 | （可选）修改 Push Scope（推送范围）。

默认情况下，Push Scope（推送范围）包含需要执行 Panorama 提交的更改的所有位置。



如果您选择 *Commit*（提交）> *Push to Devices*（推送到设备），则推送范围包括与 *Panorama* 运行配置不同步的设备相关联的所有位置。

1. **Remove Selections**（删除选择）以删除“推送范围”内列出的防火墙。
2. **Edit Selections**（编辑选择）并选择：
   - **Device Groups**（设备组）— 选择设备组或单个防火墙或虚拟系统。
   - **Templates**（模板）— 选择模板、模板堆栈或单个防火墙。
   - **Collector Groups**（收集器组）— 选择收集器组。
3. 单击 **OK**（确定）保存对推送范围所作的更改。

STEP 6 | 验证您将推送到设备组或模板的更改。

1. **Validate Device Group Push**（验证设备组推送）或 **Validate Template Push**（验证模板推送）。

   验证结果显示的所有错误及警告均与实际推送操作所显示的一致。
2. 解决验证结果找到的任何错误。

STEP 7 | 将更改提交到 Panorama 并将更改推送到设备。

Commit and Push（提交并推送）配置更改。



使用 Panorama 任务管理器可查看挂起（或者，可以取消这些）、进行中、已完成或失败提交的详细信息。

© 2019 Palo Alto Networks, Inc.

启用自动提交恢复

如要确保从 Panorama™ 管理服务器推送到受管防火墙或在防火墙本地提交的配置更改不会引起配置破坏，请启用 **Automated Commit Recovery**（自动提交恢复）使受管防火墙可以测试每次提交的配置更改并确认更改没有中断 Panorama 与受管防火墙之间的连接。您可以配置在受管防火墙自动将其配置恢复到上一次运行配置之前每个受管防火墙执行的测试次数和测试时间间隔。当您启用自动提交恢复时，受管防火墙配置将恢复，而非 Panorama 配置。此外，受管防火墙每隔 60 分钟测试一次与 Panorama 的连接，以确保在不相关网络配置更改中断防火墙与 Panorama 之间的连接或者过去提交的配置影响了连接时能够持续通信。对于高可用性 (HA) 配置，在从 Panorama 推送后只可在连接测试之后在 HA 对端之间进行同步。

默认情况下启用自动提交恢复。但是，如果您禁用了自动提交恢复，然后又想在现有生产环境中重新启用该功能，则首先要验证没有策略规则会破坏Panorama 与受管防火墙之间的连接。例如，在管理流量遍历数据平面时，可能有策略规则限制从防火墙到 Panorama 的流量。

当防火墙配置成功恢复到最后运行配置时，防火墙会生成配置日志。此外，当管理员禁用此功能时、当配置推送后因连接测试失败而导致配置恢复事件开始时，以及当每隔 60 分钟执行的 Panorama 连接测试失败并导致防火墙配置恢复时，防火墙会生成配置日志。

独立于任何其他配置更改启用 *Automated Commit Recovery*（自动提交恢复）。如果同时启用了任何其他会导致 *Panorama* 与受管防火墙之间连接中断的配置更改，那么防火墙配置不能自动恢复。

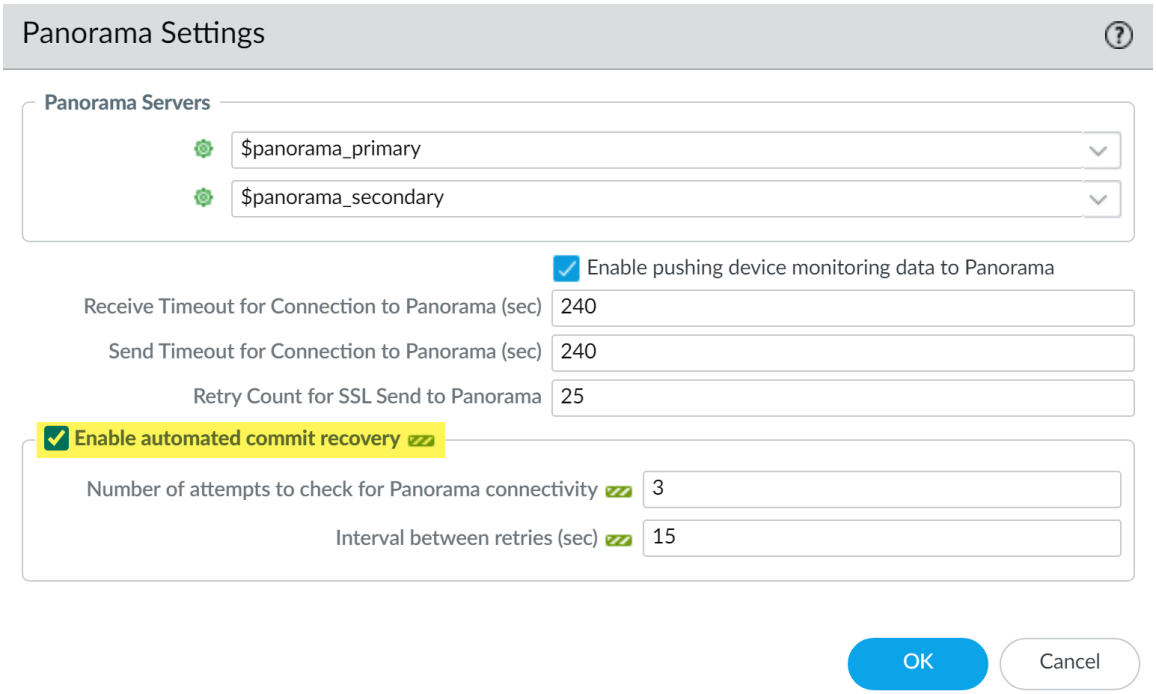
STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后从 **Template**（模板）上下文下拉列表中选择需要的模板或模板堆栈。

STEP 3 | 启用自动提交恢复。

1. 编辑 (⚙) Panorama 设置。
2. 启用自动提交恢复。
3. 配置 **Number of attempts to check for Panorama connectivity**（检查 **Panorama** 连接的尝试次数）（默认为 1 次尝试）。
4. 配置 **Interval between retries**（重试时间间隔）（默认为 10 秒）。
5. 单击 **OK**（确定）保存更改。

© 2019 Palo Alto Networks, Inc.



STEP 4 | **Commit**（提交）> **Commit and Push**（提交并推送），**Commit and Push**（提交并推送）更改。

STEP 5 | 验证受管防火墙上已启用自动提交恢复功能。

1. 启动防火墙 Web 界面。
2. 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），并在 Panorama 设置中验证已启用 **Enable automated commit recovery**（启用自动提交恢复）。

© 2019 Palo Alto Networks, Inc.

管理 Panorama 和防火墙配置备份

Panorama 上的运行中配置由您已提交的所有设置组成，因此处于激活状态。待选配置是运行中配置连同自上次提交之后您所作任何未激活更改的副本。保存运行中或待选配置的备份版本可以让您能够稍后恢复这些版本。例如，如果一个提交验证显示当前待选配置错误太多，不容易修复，您可以恢复之前的待选配置。您也可以还原到当前的运行配置，而无需先保存备份。



请参阅 Panorama 提交、验证和预览操作 了解有关将配置更改提交到 *Panorama* 并将更改推送到受管设备的更多信息。

在运行 PAN-OS 5.0 或更高版本的本地防火墙上提交后，将其运行配置的备份发送到 Panorama。在本地防火墙上执行任何的提交都会触发备份，包括管理员在防火墙本地执行的提交或 PAN-OS 启动时的自动提交（例如 FQDN 刷新）。默认情况下，Panorama 最多可以为每个防火墙存储 100 个备份（尽管可以配置）。要在外部主机上存储 Panorama 和防火墙配置备份，您可在 Panorama 上调度导出或在需要时导出。您还可以将配置从防火墙导入 Panorama 设备组和模板，以从防火墙过渡到 Panorama Management。

（仅限 VMware ESXi 和 vCloud Air ）部署在 VMware ESXi 和 vCloud Air 上的 Panorama 虚拟设备不支持 VMware 快照功能。拍摄 Panorama 虚拟设备的快照会影响性能，导致间歇性和不一致的数据包丢失，且 Panorama 可能会变得无响应。此外，您可能失去对 Panorama CLI 和 Web 界面的访问，且切换至 Panorama 模式不受支持。请将您命名的配置快照 save and export（保存并导出）到任何网络位置。

- 调度导出配置文件
- 保存并导出 Panorama 和防火墙配置
- 还原 Panorama 配置更改
- 配置 Panorama 上的配置备份最大数量
- 在受管防火墙上加载配置备份

调度导出配置文件

Panorama 可保存其运行配置以及所有受管防火墙运行配置的备份。这些备份采用 XML 格式，其文件名则是根据（Panorama 或防火墙的）序列号命名。使用以下说明即可调度备份向远程主机的每日导出。Panorama 会将备份导出为单个 gzip 文件。您必须具备超级用户权限才能调度导出。



如果 *Panorama* 具有高可用性 *(HA)* 配置，则您必须在每个对端设备上执行以下说明以确保在故障转移后计划导出能够继续。*Panorama* 不会在高可用性对端设备之间同步计划配置。

要按需导出备份，请参阅保存并导出 Panorama 和防火墙配置。

STEP 1 | 选择 **Panorama** > **Scheduled Config Export**（Panorama > 调度配置导出），然后单击 **Add**（添加）。

STEP 2 | 输入调度文件导出的 **Name**（名称）和 **Description**（说明），然后 **Enable**（启用）该导出。

STEP 3 | 使用 24 小时时钟格式，输入一个每日 **Scheduled Export Start Time**（调度导出开始时间），或者从下拉列表中选取一个时间。



如果您要对两个或多个服务器配置调度导出，请错开调度导出开始时间。在同一开始时间调度多个导出会导致导出配置之间存在分歧。

STEP 4 | 将导出 **Protocol**（协议）设置为 Secure Copy（安全复制）(**SCP**) 或 File Transfer Protocol（文件传输协议）(**FTP**)。

© 2019 Palo Alto Networks, Inc.

STEP 5 | 输入访问服务器的详细信息，包括：**Hostname**（主机名）或 IP 地址、**Port**（端口）、上传文件的 **Path**（路径）、**Username**（用户名）和 **Password**（密码）。

Path（路径）支持以下字符：**.**（句点）、**+**、**{** and **}**、**/**、**-**、**_**、**0-9**、**a-z** 和 **A-Z**。文件 **Path**（路径）中不支持空格。

如果您导出至 *FTP* 服务器时使用 *IPv6* 地址作为 *Hostname*（主机名），则输入的地址必须以方括号 *([])* 括起。例如：***[2001:0db8:0000:0000:0000:8a2e:0370:7334]***。

如果要导出到 *BSD* 服务器，则需要将 *SSHD* 密码提示修改为 ***<username>@<hostname> <password>:*** 。

STEP 6 | （仅 SCP）单击 **Test SCP server connection**（测试 **SCP** 服务器连接）。要实现数据的安全传输，必须验证并接受 SCP 服务器的主机密钥。在您接受主机密钥之前，Panorama 将不会建立连接。如果 Panorama 具有高可用性配置，则您应在每个高可用性对端设备上执行此步骤，从而使得每个高可用性对端设备都可以接受 SCP 服务器的主机密钥。如果 Panorama 可以成功连接到 SCP 服务器，则它会创建并上传名为 ssh-export-test.txt 的测试文件。

STEP 7 | 单击 **OK**（确定）保存更改。

STEP 8 | 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

保存并导出 Panorama 和防火墙配置

将待选配置的备份保存到 Panorama 上的永久存储中，以备稍后还原该备份（请参阅还原 Panorama 配置更改）。此外，Panorama 允许保存并导出您指定的设备组、模板和模板堆栈配置。这对于保留在系统事件或管理员操作导致 Panorama 重启时将会丢失的更改十分有用。重新启动后，Panorama 自动还原至当前运行的配置版本，其中 Panorama 将该版本存储于名为 `running-config.xml` 的文件中。如果要还原到比当前运行的配置更早的 Panorama 配置，则保存备份也很有用。Panorama 不会自动将待选配置保存为永久存储。您必须手动将待选配置保存为默认快照文件 (`.snapshot.xml`) 或自定义命名快照文件。Panorama 本地存储快照文件，但您可以将其导出到外部主机。

您不必保存配置备份以还原自上次提交或重新启动以来所做的更改；只需选择 *Config*（配置）> *Revert Changes*（恢复更改）即可完成（请参阅还原 Panorama 配置更改）。

Palo Alto Networks 建议您将任何重要配置备份到外部主机。

STEP 1 | 保存对候选配置的更改。

- 要替换带所有管理员所做的所有更改的默认快照文件 (`.snapshot.xml`)，请执行以下步骤之一：
  - 选择 **Panorama** > **Setup**（设置）> **Operations**（操作）并 **Save candidate Panorama configuration**（保存待选 **Panorama** 配置）。
  - 使用已分配给超级用户角色或管理员角色配置文件的管理帐户登录 Panorama，并启用 **Save For Other Admins**（为其他管理员保存）权限。然后在 Web 界面顶部选择 **Config**（配置）> **Save Changes**（保存更改），选择 **Save All Changes**（保存所有更改），并 **Save**（保存）。
- 要覆盖带管理员所做的所有更改的默认快照 (`.snapshot.xml`)，以指定设备组、模板、或模板堆栈配置：
  1. 选择 **Panorama** > **Setup**（设置）> **Operations**（操作），**Save candidate Panorama configuration**（保存待选 **Panorama** 配置）和 **Select Device Group & Templates**（选择设备组和模板）。
  2. 选择要恢复的特定设备组、模板或模板堆栈
  3. 单击 **Yes**（是）以确认操作。

© 2019 Palo Alto Networks, Inc.

4. （可选）选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改以使用快照覆盖运行中的配置。

- 要创建包含所有管理员所做的所有更改的快照但不替换默认快照文件：

  1. 选择 **Panorama** > **Setup** > **Operations**（Panorama > 设置 > 操作），再选择 **Save named Panorama configuration snapshot**（保存命名的 Panorama 配置快照）。
  2. 指定新的或现有配置文件的 **Name**（名称）。
  3. 单击 **OK**（确定）和 **Close**（关闭）。

- 仅保存待选配置的特定更改，而不替换默认快照文件的任何部分：

  1. 使用具有角色权限的管理帐户登录到 Panorama，以保存所需更改。
  2. 在 Web 界面顶部选择 **Config**（配置）> **Save Changes**（保存更改）。
  3. 选择 **Save Changes Made By**（所作更改保存依据）。
  4. 要按管理员筛选保存范围，请单击 **<*administrator-name*>**，选择管理员，然后单击 **OK**（确定）。
  5. 要按位置筛选保存范围，请清除要排除的任何位置。位置可以是特定设备组、模板、收集器组、日志收集器、共享设置或 Panorama 管理服务器。
  6. 单击 **Save**（保存），指定新配置文件或现有配置文件的 **Name**（名称），然后单击 **OK**（确定）。

- 要保存特定的设备组、模板、或模板堆栈配置：

  1. 选择 **Panorama** > **Setup**（设置）> **Operations**（操作），**Save named Panorama configuration snapshot**（保存已命名 **Panorama** 配置快照）和 **Select Device Group & Templates**（选择设备组和模板）。
  2. 选择要保存的特定设备组、模板、或模板堆栈。
  3. 单击 **Yes**（是）以确认操作。

STEP 2 | 将待选或运行中配置导出到 Panorama 外部主机或防火墙上。

您可以安排每日导出到 SCP 或 FTP 服务器（请参阅 调度导出配置文件）或按需导出配置。要按需导出，请选择 **Panorama** > **Setup**（设置）> **Operations**（操作），然后选择以下选项之一：

- **Export named Panorama configuration snapshot**（导出命名的 **Panorama** 配置快照）— 导出当前运行的配置、待选配置快照，或之前导入的配置（待选配置或正在运行的配置）。Panorama 将配置导出为带有您指定 **Name**（名称）的 XML 文件。**Select Device Groups & Templates**（选择设备组和模板）以指定要导出的设备组、模板或模板堆栈配置。
- **Export Panorama configuration version**（导出 **Panorama** 配置版本）— 选择运行中配置的 **Version**（版本），导出为 XML 文件。**Select Device Groups & Templates**（选择设备组和模板）以指定要作为 XML 文件导出的设备组、模板或模板堆栈配置。
- **Export Panorama and devices config bundle**（导出 **Panorama** 和设备配置捆绑包）— 生成和导出 Panoram 和每个受管防火墙的运行配置备份的最新版本。要实现每天创建配置包并将其导出到安全复制 (SCP) 或 FTP 服务器的流程自动化，请参阅调度导出配置文件 。
- **Export or push device config bundle**（导出或推送设备配置包）— 当您把防火墙配置导入到 Panorama 中之后，Panorama 会创建一个名为 <firewall_name>_import.tgz 的防火墙配置包，而所有的本地策略和对象都将从该配置包中删除。随后，您可以选择 **Export or push device config bundle**（导出或推送设备配置包）来执行以下操作之一：

  - **Push & Commit**（推送并提交）配置捆绑包到防火墙会从防火墙中删除任何本地配置，使您能够从 Panorama 管理防火墙。
  - 将配置导出到防火墙，而不加载。当您准备好加载配置时，应登录到防火墙 CLI，然后运行配置模式命令 **`load device-state`**。此命令按照与推送和提交选项相同的方式清理防火墙。

从防火墙过渡到 Panorama Management的完整过程需要执行额外步骤。

© 2019 Palo Alto Networks, Inc.

还原 Panorama 配置更改

还原更改时，是将当前待选配置中的设置替换为另一个配置中的设置。当您想要撤销多个设置的更改以作为单个操作，而不是手动重新配置每个设置时，还原更改十分有用。

您可以还原自上次提交以来对 Panorama 配置所做的暂挂更改。您可以还原 Panorama 上所有暂挂的更改，或选择特定的设备组、模板、或模板堆栈。Panorama 提供按管理员或位置筛选暂挂更改的选项。位置可以是特定设备组、模板、收集器组、日志收集器、共享设置或 Panorama 管理服务器。如果您已为比当前运行中配置更早的待选配置保存快照文件（请参阅保存并导出 Panorama 和防火墙配置），还可以还原到该待选配置快照。还原到快照可以还原在最后一次提交之前存在的候选配置。无论您何时提交更改，Panorama 都会自动保存运行中配置的新版本，您可以还原任何这些版本。

恢复 Panorama 管理服务器配置需要完整提交，并且必须由超级用户执行。在执行恢复和加载 Panorama 配置等特定 Panorama 操作时需要完整提交，而自定义管理员角色配置文件不支持完整提交。

- 还原到当前运行的 Panorama 配置（文件名为 **`running-config.xml`**）。

  此操作将撤销自上次提交之后，对待选配置所作的更改。

  - 要还原所有管理员所做的所有更改，请执行以下步骤之一：
    - 选择 **Panorama** > **Setup**（设置）> **Operations**（操作），**Revert to running Panorama configuration**（还原到正在运行的 **Panorama** 配置），然后单击 **Yes**（是）确认操作。
    - 使用已分配给超级用户角色或管理员角色配置文件的管理帐户登录 Panorama，并启用 **Commit For Other Admins**（为其他管理员提交）权限。然后选择**Config**（配置）> **Revert Changes**（还原更改），选择 **Revert All Changes**（还原所有更改），并 **Revert**（还原）。
  - 要仅还原待选配置的特定更改：
    1. 使用具有角色权限的管理帐户登录到 Panorama，以还原所需更改。

       控制提交操作的权限也可控制还原操作。
    2. 选择 **Config**（配置）> **Revert Changes**（还原更改）.
    3. 选择 **Revert Changes Made By**（所作更改还原依据）。
    4. 要按管理员筛选还原范围，请单击 *<administrator-name>*，选择管理员，然后单击 **OK**（确定）。
    5. 要按位置筛选还原范围，请清除要排除的任何位置。
    6. **Revert**（还原）更改。
  - 要还原对运行中配置做出的特定设备组、模板、或模板堆栈更改：
    1. 选择 **Panorama** > **Setup**（设置）> **Operations**（操作），**Revert to running Panorama configuration**（还原到正在运行的 **Panorama** 配置）和 **Select Device Group & Templates**（选择设备组和模板）。
    2. 选择要恢复的特定设备组、模板或模板堆栈
    3. 单击 **Yes**（是）以确认操作。
    4. （可选）选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改以覆盖运行中的配置。

- 还原到 Panorama 待选配置的默认快照（**`.snapshots.xml`**）。
  - 要还原所有管理员做出的所有更改：
    1. 选择 **Panorama** > **Setup**（设置）> **Operations**（操作），**Revert to last saved Panorama configuration**（恢复到上次保存的 **Panorama** 配置）。
    2. 单击 **Yes**（是）以确认操作。
    3. （可选）选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改以使用快照覆盖运行中的配置。
  - 要还原对运行中配置做出的特定设备组、模板、或模板堆栈更改：

© 2019 Palo Alto Networks, Inc.

1. 选择 **Panorama** > **Setup**（设置）> **Operations**（操作），**Revert to running Panorama configuration**（还原到正在运行的 **Panorama** 配置）和 **Select Device Group & Templates**（选择设备组和模板）。
2. 选择要恢复的特定设备组、模板或模板堆栈
3. 单击 **Yes**（是）以确认操作。
4. （可选）要将运行中配置替换为，选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并使用快照 **Commit**（提交）您的更改。

- 还原到存储在 Panorama 上运行配置的先前版本。
  - 要还原管理员做出的所有更改：
    1. 选择 **Panorama** > **Setup**（设置）> **Operations**（操作）、**Load Panorama configuration version**（加载 **Panorama** 配置版本）和 **Select Device Group & Templates**（选择设备组和模板）。
    2. 选择一个配置 **Version**（版本），单击 **OK**（确定）。
    3. （可选）要将运行中配置替换为刚还原的版本，选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）您的更改。
  - 要还原对运行中配置做出的特定设备组、模板、或模板堆栈更改：
    1. 选择 **Panorama** > **Setup**（设置）> **Operations**（操作）、**Load Panorama configuration version**（加载 **Panorama** 配置版本），并选择配置版本**Name**（名称）。
    2. **Select Device Groups & Templates**（选择设备组和模板）并选择要还原的特定设备组、模板或模板堆栈。
    3. 单击 **Yes**（是）以确认操作。
    4. （可选）要将运行中配置替换为快照，选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）您的更改。

- 还原到以下之一：
  - 您之前导入的 Panorama 运行中配置的自定义命名版本。
  - 自定义命名的 Panorama 待选配置快照（而非默认快照）。

  1. 选择 **Panorama** > **Setup**（设置）> **Operations**（操作）和 **Load named Panorama configuration snapshot**（加载已命名的 **Panorama** 配置快照），并选择刚导入的配置 **Name**（名称）。
  2. （可选）**Load Shared Objects**（加载共享对象）或 **Load Shared Policies**（加载共享策略）以加载所有共享对象或策略。您可以加载所有共享对象和策略，以及加载在下一步中指定的设备组和模板中配置的所有对象和策略。
  3. （可选）**Select Device Groups & Templates**（选择设备组和模板），并选择要加载的特定设备组、模板或模板堆栈配置。如果想要还原整个 Panorama 配置，请跳过此步骤。
  4. 单击 **Yes**（是）以确认操作。
  5. （可选）要将运行中配置替换为快照，选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）您的更改。

- 还原您之前导出到外部主机的 Panorama 运行中或待选配置。
  1. 选择 **Panorama** > **Setup** > **Operations**（Panorama > 设置 > 操作），**Import named Panorama configuration snapshot**（导入已命名的 Panorama 配置快照），**Browse**（浏览）外部主机上的配置文件，然后单击 **OK**（确定）。
  2. **Load named Panorama configuration snapshot**（加载已命名的 **Panorama** 配置快照），选择您刚才所导入配置文件的 **Name**（名称）。
  3. （可选）**Load Shared Objects**（加载共享对象）或 **Load Shared Policies**（加载共享策略）以加载所有共享对象或策略。您可以加载所有共享对象和策略，以及加载在下一步中指定的设备组和模板中配置的所有对象和策略。

© 2019 Palo Alto Networks, Inc.

4. （可选）**Select Device Groups & Templates**（选择设备组和模板），并选择要加载的特定设备组、模板或模板堆栈配置。如果想要还原整个 Panorama 配置，请跳过此步骤。
5. 单击 **Yes**（是）以确认操作。
6. （可选）要将运行中配置替换为刚导入的快照，选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）您的更改。

配置 Panorama 上的配置备份最大数量

STEP 1 | 选择 **Panorama** > **Setup** > **Management**（Panorama > 设置 > 管理），然后编辑“Logging and Reporting Settings（日志记录和报告设置）”。

STEP 2 | 选择 **Log Export and Reporting**（日志导出和报告）并输入 **Number of Versions for Config Backups**（配置备份的版本数）（默认为 100；范围为 1 至 1,048,576）。

STEP 3 | 单击 **OK**（确定）保存更改。

STEP 4 | 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

在受管防火墙上加载配置备份

使用 Panorama 可在受管防火墙上加载配置备份。您可以选择恢复到在防火墙上先前保存或提交的配置。Panorama 将选定版本推送到受管防火墙，从而覆盖防火墙上的当前待选配置。

STEP 1 | 选择 **Panorama** > **Managed Devices**（受管设备）> **Summary**（摘要）。

STEP 2 | 选择 Backups（备份）列中的 **Manage**（管理）。

STEP 3 | 从 Saved Configurations（保存的配置）或 Committed Configurations（提交的配置）中选择。

- 单击版本号可查看该版本的内容。
- **Load**（加载）配置版本。

STEP 4 | 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

© 2019 Palo Alto Networks, Inc.

比较 Panorama 配置的更改

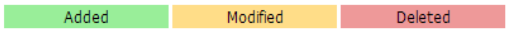
要比较 Panorama 上的配置更改，您可以选择任何两组配置文件：待选配置、运行配置或以前已保存或 Panorama 上提交的任何其他配置版本。并排比较可让您：

- 在将更改提交至 Panorama 之前预览配置更改。例如，您可以预览待选配置和运行配置之间的更改。作为最佳做法，请在左侧窗格上选择较旧的版本并在右边窗格上选择较新的版本，以便比较和识别出修改。
- 执行配置审核以检查和比较两组配置文件之间的更改。

设备组和模板管理员仅能在其访问域内比较设备组和模板的配置。

- 比较 Panorama 配置的更改。
  1. 选择 **Panorama** > **Config Audit**（Panorama > 配置审核）。
  2. 在每个下拉列表中，请选择配置以进行比较。
  3. 选择要作为 **Context**（上下文）包含的行数，然后单击**Go**（转至）。

     Panorama 使用彩色突出显示您添加（绿色）、修改（黄色）或删除（红色）的项目。



- 配置 Panorama 存储的版本数以进行配置审核。
  1. 选择 **Panorama** > **Setup** > **Management**（Panorama > 设置 > 管理），然后编辑“Logging and Reporting Settings（日志记录和报告设置）”。
  2. 输入 **Number of Versions for Config Audit**（配置审核的版本号）（范围为 1–1,048,576；默认为 100）。
  3. 单击 **OK**（确定）保存更改。
  4. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

- 在提交之前查看和比较 Panorama 配置文件。
  1. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**）和 **Preview Changes**（预览更改）。
  2. 选择要查看的 **Lines of Context**（上下文行数），然后单击 **OK**（确定）。

© 2019 Palo Alto Networks, Inc.

管理配置更改限制锁

锁定待选或运行中配置可以防止其他管理员更改配置，除非您手动取消锁定或 Panorama 自动取消（提交后）。锁定确保管理员不会在并行登录会话中对同一设置或互相依赖的设置进行有冲突的更改。

如果您要更改的设置与其他管理员在并行会话中要更改的设置无关，那么就不需要锁定配置来防止提交冲突。*Panorama* 让提交操作排队，按管理员发起提交的顺序执行。有关详细信息，请参阅Panorama 提交、验证和预览操作。

如果分配给模板或设备组的防火墙有管理员在此防火墙本地设置的提交或配置锁定，则此模板或设备组配置推送会失败。

- 查看关于当前锁定的详情。

  例如，您可以查看其他管理员是否设置了锁定，阅读他们为了解释锁定原因而输入的备注。

  单击 Web 界面顶部的锁定挂锁图标 ()。相邻的数字表示当前锁定数量。

- 锁定配置。

  不能修改防火墙或 Panorama 配置的只读管理员不能设置锁定。

  1. 单击 Web 界面顶部的挂锁图标。

     此图标因设置现有锁定 () 或未设置 () 现有锁定而异。
  2. **Take a Lock**（执行锁定），选择锁定 **Type**（类型）：
     - **Config**（配置）— 阻止其他管理员对待选配置进行更改。

       不能提交更改的自定义角色管理员可进行设置 *Config*（配置）锁定，并将更改保存到待选配置。但是，因为此类管理员不能提交更改，*Panorama* 不会在提交后自动解除锁定；管理员必须在进行所需的更改后手动删除 *Config*（配置）锁定。

     - **Commit**（提交）— 阻止其他管理员对正在运行的配置进行更改。
  3. 选择 **Location**（位置），用于确定锁定范围：
     - **Shared**（共享）— 将更改限制为整个 Panorama 配置，包括所有设备组和模板。
     - **Template**（模板）— 限制更改选定模板所包括的防火墙。（您无法锁定模板堆栈，而只能锁定堆栈中的单个模板。）
     - **Device group**（设备组）— 限制更改选定的设备组而非其后代设备组。
  4. （可选）作为最佳做法，请输入 **Comment**（注释）以描述执行锁定的原因。
  5. 单击 **OK**（确定）和 **Close**（关闭）。

- 解锁配置。

  只有超级用户或锁定配置的管理员可手动解锁。但是，设置锁定的管理员完成提交操作后，Panorama 可自动删除此锁定。

  1. 单击 Web 界面顶部的锁定挂锁图标 ()。
  2. 在列表中选择锁定条目。
  3. 单击 **Remove Lock**（删除锁定）、**OK**（确定）和 **Close**（关闭）。

- 更改待选配置时，配置 Panorama 自动锁定运行中配置。此设置适用于所有 Panorama 管理员。

© 2019 Palo Alto Networks, Inc.

1. 选择 **Panorama** > **Setup** > **Management**（Panorama > 设置 > 管理），然后编辑“General Settings（常规设置）”。
2. 选择 **Automatically Acquire Commit Lock**（自动获取提交锁定），然后单击 **OK**（确定）。
3. 选择 **Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

© 2019 Palo Alto Networks, Inc.

将自定义徽标添加到 Panorama

您可以上传图像文件，以自定义 Panorama 上的以下区域：

- 登录屏幕上的背景图像
- Web 界面左上角的标头；您还可以隐藏 Panorama 的默认背景
- PDF 报告中的标题页和页脚图像

支持的图像类型包括 .jpg、.gif 和 .png。PDF 报告中使用的图像文件不包含 Alpha 通道。图像的大小必须小于 128 千字节（131,072 字节）；建议的规格会显示在屏幕上。如果规格大于建议的大小，则会自动裁剪图像。

STEP 1 | 选择 **Panorama** > **Setup** > **Operations**（Panorama > 设置 > 操作）。

STEP 2 | 在 Miscellaneous（其他）部分中，单击 **Custom Logos**（自定义徽标）。

STEP 3 | 单击上传徽标图标，然后选择以下任何选项的图像：登录屏幕，主用户界面的左角、PDF 报告标题页面和 PDF 报告页脚。

STEP 4 | 单击 **Open**（打开）添加图像。要预览图像，单击预览徽标图标。

STEP 5 | （可选）要清除 Panorama Web 界面上的绿色背景标头，请选中 **Remove Panorama background header**（移除 **Panorama** 背景标头）复选框。

STEP 6 | 单击 **Close**（关闭）保存更改。

STEP 7 | 选择 **Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

© 2019 Palo Alto Networks, Inc.

使用 Panorama 任务管理器

单击 Web 界面底部的 **Tasks**（任务）(Tasks) 打开任务管理器，其中显示自上次 Panorama 或防火墙重新启动后，管理员发起（例如手动提交）的所有操作或者 Panorama 或受管防火墙发起（例如生成调度的报告）的所有操作。您可使用任务管理器排除失败操作的故障、调查与已完成提交有关的警告或取消挂起提交。



设备组和模板管理员仅能在其访问域内查看任务的任务。

STEP 1 | 单击 **Tasks**（任务）。

STEP 2 | **Show**（显示）**Running**（正在运行）任务或 **All**（全部）任务（默认，可以按类型（**Reports**（报告）；**Log Requests**（日志请求）；或提交、下载和安装 **Jobs**（作业））筛选，然后选择要查看任务的 **Panorama**（默认）或防火墙。

STEP 3 | 执行以下任何操作：

- 显示或隐藏任务详细信息 — 默认情况下，任务管理器显示每个任务的类型、状态、开始时间和消息。要查看某个任务的结束时间和作业 ID，您必须手动显示这些列。要显示或隐藏列，打开任何列标头的下拉菜单，选择 **Columns**（列），根据需要选择或清除列。
- 调查警告或故障 — 阅读 Messages（消息）列的条目了解任务详细信息。如果此列显示 `Too many messages`（消息过多），单击 Type（类型）列中的此条目了解更多信息。
- 显示提交说明 — 如果管理员输入了提交说明，单击 Messages（消息）列中的 **Commit Description**（提交说明）显示说明。
- 检查提交在队列中的位置 — Messages（消息）列指示了正在进行中的提交的队列位置。
- 取消挂起提交 — **Clear Commit Queue**（清除提交队列）可取消所有暂挂提交（仅限预定义管理角色）。要取消单个提交，在 Action（操作）列中单击 **x**（提交保留在队列中，直到 Panorama 将此提交移除队列）。您不能取消正在进行的提交。

© 2019 Palo Alto Networks, Inc.

管理日志和报告的存储配额和过期期限

- 日志和报告存储
- 日志和报告过期期限
- 配置日志和报告的存储配额和过期期限
- 配置 Panorama 报告的运行时间

日志和报告存储

您可以为每种类型的日志编辑默认的存储配额。日志配额达到上限后，Panorama 会开始使用新日志条目覆盖最早的日志条目。不可以配置报告的存储容量。日志存储位置和报告存储容量因 Panorama 型号而异：

- **Panorama** 模式下的 **Panorama** 虚拟设备 — 报告存储空间为 200MB。设备使用其虚拟系统磁盘来存储 Panorama 和日志收集器生成的系统和配置日志。虚拟系统磁盘还存储 Panorama 从所有受管防火墙以 15 分钟的时间间隔自动接收的应用程序统计信息 (App Stats) 日志。Panorama 将所有其他日志类型存储到其虚拟日志记录磁盘（1 到 12）。
- 仅管理模式下的 **Panorama** 虚拟设备 — 报告存储空间为 500MB。设备使用其虚拟系统磁盘来存储 Panorama 和日志收集器生成的系统和配置日志。虚拟系统磁盘还存储 Panorama 从所有受管防火墙以 15 分钟的时间间隔自动接收的应用程序统计信息 (App Stats) 日志。因为仅管理模式下的 Panorama 无法存储任何其他日子类型，因此您必须配置受管收集器以从受管防火墙转发日志。
- 传统模式下的 **Panorama** 虚拟设备 — Panorama 8.0 或更早版本的报告存储空间为 200 MB，Panorama 8.0.1 和更高版本的报告存储空间为 500MB。Panorama 会将所有日志写入其分配的存储空间，而该存储空间可能为以下任何一项：
  - 虚拟系统磁盘 — 默认情况下，在安装 Panorama 时创建的虚拟系统磁盘上将分配大约 11GB 的日志存储空间。如果添加虚拟日志记录磁盘或 NFS 分区，Panorama 仍会使用系统磁盘来存储 Panorama 和日志收集器生成的系统和配置日志，并存储从防火墙收集的应用程序统计信息日志。
  - 专用虚拟日志记录磁盘 — 存储除驻留在系统磁盘上的所有日志类型。
  - **NFS** 分区 — 此选项仅适用于在 VMware ESXi 服务器上运行的 Panorama。NFS 分区存储除驻留在系统磁盘上的所有日志类型。
- **M-600**、**M-500** 或 **M-200** 设备 — 对于 Panorama 6.1 或更高版本，用于报告的存储空间大小为 500 MB；而对于较早版本，存储空间大小则为 200MB。M 系列设备使用其内部 SSD 来存储 Panorama 和日志收集器生成的配置日志和系统日志，并存储从防火墙收集的应用程序统计信息日志。Panorama 会把所有其他类型的日志保存到其 RAID 启用式磁盘上。RAID 磁盘要么位于 Panorama 模式下的 M 系列设备本机内，要么位于专用日志收集器内（M 系列设备处于日志收集器模式下）。当您配置收集器组时，可以在 RAID 磁盘上编辑日志存储配额。



有关日志存储选项和容量的详细信息，请参阅 Panorama 型号。您可通过添加虚拟日志记录磁盘或 *NFS* 存储的方式扩展 Panorama 虚拟设备上的日志存储容量。您可以通过添加 *RAID* 驱动器或从 *1TB* 驱动器升级到 *2TB* 驱动器增加 M 系列设备上的存储容量。

日志和报告过期期限

您可以根据 Panorama 管理服务器和日志收集器从防火墙收集日志的时间以及 Panorama 和日志收集器在本地生成日志和报告的时间来配置自动删除。在需要或有必要定期删除监控信息的情况下，这样做将有助于部署。例如，出于法律原因，您的组织必须在一定时间之后删除用户信息。您可以为以下各项单独配置过期期限：

- 报告 — Panorama 删除过期的报告，同时生成新的报告（请参阅配置 Panorama 报告的运行时间）。
- 每种类型的日志 — Panorama 会在收到日志时评估它们，并删除超过配置过期期限的日志。

© 2019 Palo Alto Networks, Inc.

- *Panorama* 会在整个高可用性 *(HA)* 对之间同步过期期限。因为只有主动高可用性对端设备会生成日志，所以除非故障转移发生并开始生成日志，否则被动对端设备不会有任何需要删除的日志或报告。

  即使您没有设置过期期限，当日志配额达到上限后，*Panorama* 也会开始使用新日志条目覆盖最早的日志条目。

配置日志和报告的存储配额和过期期限

STEP 1 | 为以下各项配置存储配额和过期期限：

- Panorama 虚拟设备在传统模式下从防火墙接收到的所有类型的日志。
- Panorama 从防火墙接收的应用统计信息日志。
- Panorama 和日志收集器在本地生成的系统和配置日志。

Panorama 管理服务器将在本地存储这些日志。

如果您削减存储配额而使得当前日志超出配额，那么在您提交更改之后，*Panorama* 会删除一部分最早的日志来适应配额。

1. 选择 **Panorama** > **Setup** > **Management**（Panorama > 设置 > 管理），然后编辑“Logging and Reporting Settings（日志记录和报告设置）”。
2. 在 **Log Storage**（日志存储）设置中，输入每种类型日志的存储 **Quota**（配额）**(%)**。

   当您更改百分比值时，页面会刷新以根据 Panorama 上分配的总存储容量显示相应的绝对值（配额 GB/MB 列）。
3. 输入每种日志类型的 **Max Days**（最大天数）（到期期限），范围为 1 至 2,000。

   默认情况下，该字段留空，这意味着日志永远不会过期。

   如果您要将配额和到期期限重置为出厂默认值，请 *Restore Defaults*（恢复默认值）。

STEP 2 | 配置 Panorama 生成的报告的到期期限。

1. 选择 **Log Export and Reporting**（日志导出和报告），并输入 **Report Expiration Period**（报告到期期限），以天为单位（范围为 1 至 2,000）。

   默认情况下，该字段留空，这意味着报告永远不会过期。
2. 单击 **OK**（确定）保存更改。

STEP 3 | 配置 M-600、M-500、M-200 或 Panorama 虚拟设备在 Panorama 模式下从防火墙接收的所有类型日志（应用统计信息日志除外）的存储配额和到期期限。

本地或专用日志收集器将存储这些日志。

您是在收集器组这一层面配置这些存储配额，而不是为单个日志收集器配置存储配额。

1. 选择 **Panorama** > **Collector Groups**（收集器组），然后编辑收集器组。
2. 在 **General**（常规）设置中，单击 **Log Storage**（日志存储）值。

   除非您已将日志收集器分配到收集器组，否则此字段不会显示值。如果此字段在您分配日志收集器之后显示为 *0MB*，请核实您在配置受管收集器时已启用磁盘对并核实您已提交更改（*Panorama* > *Managed Collectors*（受管收集器）> *Disks*（磁盘））。
3. 输入每种日志类型的存储 **Quota**（配额）**(%)**。

© 2019 Palo Alto Networks, Inc.

当更改百分比值时，页面会刷新以根据分配给收集器组的总存储容量显示相应的绝对值（配额 GB/MB 列）。

4. 输入每种日志类型的 **Max Days**（最大天数）（到期期限），范围为 1 至 2,000。

   默认情况下，该字段留空，这意味着日志永远不会过期。

   如果您要将配额和到期期限重置为出厂默认值，请 *Restore Defaults*（恢复默认值）。

5. 单击 **OK**（确定）保存更改。

STEP 4 | 将更改提交到 Panorama，并将更改推送到收集器组。

1. 选择 **Commit**（提交）> **Commit and Push**（提交并推送）和推送范围中的 **Edit Selections**（编辑选择）。
2. 选择 **Collector Groups**（收集器组），选择您所修改的收集器组，然后单击 **OK**（确定）。
3. **Commit and Push**（提交并推送）更改。

STEP 5 | 核实 Panorama 已应用存储配额更改。

1. 选择 **Panorama** > **Setup** > **Management**（Panorama > 设置 > 管理），然后在“Logging and Reporting Settings（日志记录和报告设置）”中核实 **Log Storage**（日志存储）值与 Panorama 管理服务器所存储的日志保持一致。
2. 选择 **Panorama** > **Collector Groups**（Panorama > 收集器组），选择您已修改的收集器组，然后核实 **General**（常规）选项卡中的 **Log Storage**（日志存储）值与日志收集器所存储的日志保持一致。

   您也可以通过登录到日志收集器 *CLI* 并输入操作命令 ***show log-diskquota-pct*** 来核实收集器组存储配额。

配置 Panorama 报告的运行时间

Panorama 会在您指定的时间每天生成报告。在生成新报告后，Panorama 将删除任何过期的报告。

STEP 1 | 选择 **Panorama** > **Setup** > **Management**（Panorama > 设置 > 管理），然后编辑“Logging and Reporting Settings（日志记录和报告设置）”。

STEP 2 | 选择 **Log Export and Reporting**（日志导出和报告），并将 **Report Runtime**（报告运行时间）设置为 24 小时制时间表中的一个小时（默认为 02:00；范围为 00:00 [午夜] 至 23:00）。

STEP 3 | 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

© 2019 Palo Alto Networks, Inc.

监视 Panorama

若要监控 Panorama 及其受管收集器，您可以定期查看它们的系统和配置日志（按类型筛选日志），配置 SNMP 管理器以定期收集（获取）Panorama 统计信息，或将 SNMP 陷阱或电子邮件警报配置为在监视指标发生状态变化或达到 Panorama 上的阈值时向您发出通知。电子邮件警报和 SNMP 陷阱有助于即时向您通报需要注意的重要系统事件。若要配置电子邮件警报或 SNMP 陷阱，请参阅 配置从 Panorama 到外部目标的日志转发。

- Panorama 系统和配置日志
- 使用 SNMP 监视 Panorama 和日志收集器统计信息

Panorama 系统和配置日志

您可以将 Panorama 配置为在发生系统事件或配置更改时发送通知。默认情况下，Panorama 会在配置日志中记录每个配置更改。在系统日志中，每个事件均有一个表明其紧迫性和影响的严重性级别。当您配置从 Panorama 到外部目标的日志转发时，可以转发所有系统和配置日志，或根据诸如接收时间或严重性级别（仅限系统日志）等属性筛选日志。下表概括了系统日志的严重性级别：

严重性级别	说明
关键	表示需要立即引起注意的故障，如硬件故障，包括高可用性 (HA) 故障转移和链接故障。
高	将会危害系统操作的严重问题，包括日志收集器断开连接或提交故障。
中	中等级别的通知，如抗病毒程序数据包升级或收集器组配置推送。
低	不太严重的通知，例如用户密码更改。
参考	通知事件，如登入/登出、任何配置更改、身份验证成功和失败通知、提交成功以及其他严重性级别未包含的其他所有事件。

Panorama 在本地存储系统和配置日志；确切的位置和存储容量因 Panorama 型号而异（请参阅日志和报告存储）。达到容量限制后，Panorama 会删除最早的日志以为新日志创建空间。如果您需要将日志存储比本地存储允许时间更长的时间，则可以配置从 Panorama 到外部目标的日志转发。

有关使用 *Panorama* 监视防火墙日志的信息，请参阅 监控网络活动。

使用 SNMP 监视 Panorama 和日志收集器统计信息

您可以将 SNMP 管理器配置为请求从 Panorama 管理服务器获取信息，并将 Panorama 配置为对此作出响应。例如，SNMP 管理器可以请求高可用性 (HA) 模式、Panorama 状态和 Panorama 版本。如果 Panorama 管理服务器具有本地日志收集器，则 Panorama 还可以提供日志统计信息：每秒平均日志、存储时间、保留期、日志磁盘使用情况、从单个防火墙到 Panorama 和外部服务器的日志转发状态以及防火墙到日志收集器的连接。Panorama 不会在高可用性对端设备之间同步 SNMP 配置；您必须在每一台对端设备上启用 SNMP 请求和响应。

您还可以配置专用日志收集器以对与 Panorama 管理服务器相同的日志统计信息请求作出响应。在评估您是否需要扩大日志存储容量时，此类信息非常有用。

© 2019 Palo Alto Networks, Inc.

您无法将 *SNMP* 管理器配置为（利用“设置”消息）控制 *Panorama* 或日志收集器；*SNMP* 管理器只能（利用“获取”消息）收集统计信息。

有关 *Panorama* 如何实施 *SNMP* 的详细信息，请参阅 SNMP 支持。

STEP 1 | 将 SNMP 管理器配置为从 Panorama 和日志收集器获取统计信息。

以下步骤概述了您将要在 SNMP 管理器上执行的任务。有关具体步骤，请参阅 SNMP 管理器的文档。

1. 若要启用 SNMP 管理器来解读统计信息，应加载配套 MIB，并在必要时编译它们。
2. 对于 SNMP 管理器将监视的每一台 Panorama 设备，应定义连接设置（IP 地址和端口）和身份验证设置（SNMPv2c 团体字符串或 SNMPv3 用户名和密码）。所有 Panorama 设备都使用端口 161。

   对于多个 Panorama 管理服务器和日志收集器，SNMP 管理器可以使用相同或不同的连接和身份验证设置。这些设置必须与您在 Panorama 上配置 SNMP 时定义的设置相匹配（请参阅将 Panorama 管理服务器配置为对来自 SNMP 管理器的统计信息请求作出响应。和将专用日志收集器（如有）配置为对 SNMP 请求作出响应。）。例如，如果使用 SNMPv2c，则您在配置 Panorama 时定义的团体字符串必须与您为 SNMP 管理器中为该 Panorama 定义的团体字符串相匹配。
3. 确定您将监视的统计信息的对象标识符 (OID)。例如，在监视日志记录速率时，MIB 浏览器会显示此统计信息与 PAN-PRODUCT-MIB.my 中的 OID 1.3.6.1.4.1.25461.2.3.30.1.1 相对应。有关详细信息，请参阅使用 SNMP 管理器浏览 MIB 和对象。
4. 配置 SNMP 管理器以监控所需的 OID

STEP 2 | 启用 Panorama 管理服务器管理 (MGT) 接口上的 SNMP 流量。

1. 选择 **Panorama** > **Setup** > **Management**（Panorama > 设置 > 管理），然后编辑“Management Interface Settings（管理界面设置）”。
2. 在 Services（服务）部分中，选中 **SNMP** 复选框，然后单击 **OK**（确定）。

STEP 3 | 启用日志收集器模式下任何 M 系列设备管理 (MGT) 接口上的 SNMP 流量：

1. 选择 **Panorama** > **Managed Collectors**（Panorama > 受管收集器），然后选择日志收集器。
2. 选择 **Management**（管理）选项卡，选择 **SNMP** 复选框，然后单击 **OK**（确定）。

STEP 4 | 将 Panorama 管理服务器配置为对来自 SNMP 管理器的统计信息请求作出响应。

1. 选择 **Panorama** > **Setup** > **Operations**（Panorama > 设置 > 操作），然后在“Miscellaneous（其他）”部分中单击 **SNMP Setup**（SNMP 设置）。
2. 选择 SNMP **Version**（版本），并按照以下方式配置身份验证值。有关版本详细信息，请参阅 SNMP 支持。

   - **V2c** — 输入 **SNMP Community String**（**SNMP** 团体字符串），该字符串不仅可以识别 SNMP 管理器和受监视设备（本例中为 Panorama）的团体，而且还可以用作密码对团体成员彼此进行身份验证。

     切勿使用默认的团体字符串 ***public***；该字符串广为人知，因此并不安全。

   - **V3** — 创建至少一个 SNMP 视图组和一个用户。当 SNMP 管理器获取统计信息时，用户帐户和视图将提供身份验证、隐私和访问控制。

     视图 — 每个视图都是一个配对的 OID 和位掩码：OID 指定 MIB，而掩码（采用十六进制格式）则指定可以在该 MIB 内部（包括匹配）或外部（排除匹配）访问的对象。单击第一个列表中的 **Add**（添加），并输入视图组的 **Name**（名称）。对于组中的每个视图，单击 **Add**（添加）并配置视图 **Name**（名称）、**OID**、匹配 **Option**（选项）（**include**（包括）或 **exclude**（排除））以及 **Mask**（掩码）。

     用户 — 在第二个列表中单击 **Add**（添加），并在 Users（用户）列中输入用户名，然后从下拉列表中选择 **View**（视图）组，输入用于向 SNMP 管理器进行身份验证的身份验证密码（**Auth**

© 2019 Palo Alto Networks, Inc.

Password（身份验证密码）），并输入用于向 SNMP 服务器加密 SNMP 消息的隐私密码（**Priv Password**（隐私密码））。

3. 单击 **OK**（确定）以保存设置。

STEP 5 | 将专用日志收集器（如有）配置为对 SNMP 请求作出响应。

对于每一个收集器组：

1. 选择 **Panorama** > **Collector Groups**（Panorama > 收集器组），然后选择收集器组。
2. 选择 **Monitoring**（监控）选项卡，配置相同的设置，如步骤 将 Panorama 管理服务器配置为对来自 SNMP 管理器的统计信息请求作出响应所示，然后单击 **OK**（确定）。

STEP 6 | 将更改提交到 Panorama，并将更改推送到收集器组。

1. 选择 **Commit**（提交） > **Commit and Push**（提交并推送）和推送范围中的 **Edit Selections**（编辑选择）。
2. 选择 **Collector Groups**（收集器组），选择您所编辑的收集器组，然后单击 **OK**（确定）。
3. **Commit and Push**（提交并推送）更改。

STEP 7 | 监视 SNMP 管理器中的 Panorama 和日志收集器统计信息。

请参阅 SNMP 管理器的文档。

© 2019 Palo Alto Networks, Inc.

重新启动或关闭 Panorama

重新启动选项可平稳重启 Panorama。关闭会使系统停止并断电。要重启 Panorama，请在重启后手动断开并重新连接系统上的电源线。

STEP 1 | 选择 **Panorama** > **Setup** > **Operations**（Panorama > 设置 > 操作）。

STEP 2 | 在 Device Operations（设备操作）部分中，选择 **Reboot Panorama**（重新启动 **Panorama**）或 **Shutdown Panorama**（关闭 **Panorama**）。

© 2019 Palo Alto Networks, Inc.

配置 Panorama 密码配置文件和复杂性

要保护本地管理员帐户，您可以定义当管理员更改或创建新密码时强制执行的密码复杂性要求。与可以应用于个人帐户的密码配置文件不同，密码复杂性规则属于整个防火墙范围且适用于所有密码。

要强制执行密码定期更新，请创建可定义密码有效期的密码配置文件。

STEP 1 | 配置密码最低复杂性设置。

1. 选择 **Panorama** > **Setup** > **Management**（Panorama > 设置 > 管理），然后编辑“Minimum Password Complexity（最小密码复杂性）”部分。
2. 选择 **Enabled**（启用）。
3. 定义 **Password Format Requirements**（密码格式要求）。您可以强制执行密码必须包含大写字母、小写字母、数字和特殊字符的要求。
4. 要阻止在密码中使用帐户用户名（或相反的名称版本），请选择 **Block Username Inclusion (including reversed)**（阻止包括用户名（反之亦然））。
5. 定义密码 **Functionality Requirements**（功能要求）。

   如果您已经配置了管理员的密码配置文件，则密码配置文件中定义的值将代替您在此部分中定义的值。

STEP 2 | 创建密码配置文件。

根据需要创建多个密码配置文件并将其应用于管理员帐户，以实现安全性。

1. 选择 **Panorama** > **Password Profiles**（Panorama > 密码配置文件），然后单击 **Add**（添加）。
2. 输入密码配置文件的 **Name**（名称）并定义以下内容：
   1. **Required Password Change Period**（需要密码更改期限）— 密码必须更改的频率，即天数。
   2. **Expiration Warning Period**（到期警告期限）— 到期之前管理员将收到密码提醒的天数。
   3. **Post Expiration Grace Period**（发布到期宽限期）— 密码到期后，管理员仍可以登录系统的天数。
   4. **Post Expiration Admin Login Count**（发布到期后管理员登录次数）— 密码到期后，管理员可以登录系统的次数。

Panorama 插件

Panorama 可扩展插件架构支持第三方集成插件，例如 VMware NSX 以及 GlobalProtect 云服务等其他 Palo Alto Networks 产品。借助这种模块化架构，您无需等待新的 PAN-OS 版本即可利用新功能。

您还可以从 Panorama 配置 VM 系列插件。VM 系列插件是一个可与公共云环境（例如，Google Cloud Platform (GCP)、Azure、AWS）和专有云管理程序（例如，KVM、ESXi 等）集成的单一插件。通过 VM 系列防火墙，您可以从部署在公共云中的 VM 系列防火墙发布指标。您可以使用 Panorama 为公共云配置 VM 系列插件设置，并推送配置到受管防火墙。

> 关于 Panorama 插件
> VM 系列插件和 Panorama 插件

关于 Panorama 插件

Panorama 支持可以启用如下集成和配置功能的可扩展插件架构：

- **AWS** — 您可以通过 AWS 插件监控 AWS 上的 EC2 工作负载。您可以通过此插件启用 Panorama（PAN-OS 8.1.3 及更高版本）与您的 AWS VPC 之间的通信，这样，Panorama 就可以收集一组预定义属性（或元数据元素）作为 EC2 实例标记，并将信息注册到 Palo Alto Networks 防火墙。当您在动态地址组内引用这些标记，并将其与安全策略规则内的标记进行匹配时，可以在 VPC 内部署的所有资产中统一执行该策略。
- **Azure** — 您可以通过 Azure 插件监控 Azure 公共云上的虚拟机。您可以通过此插件启用 Panorama（PAN-OS 8.1.6 及更高版本）与您的 Azure 订阅之间的通信，这样，Panorama 可以收集一组预定义属性（或元数据元素）作为 Azure 虚拟机标记，并将信息注册到 Palo Alto Networks 防火墙。在动态地址组引用这些标记并在安全策略规则进行匹配时，您可以在订阅中 VNet 内部署的所有资产上一致实施策略。
- **Cisco ACI** — 您可以通过 Cisco ACI 插件监控 Cisco ACI 结构中的端点。您可以通过此插件启用 Panorama（8.1.6 及更高版本）与您的 Cisco APIC 之间的通信，以便 Panorama 可以收集端点信息作为端点组标记，并将信息注册到 Palo Alto Networks 防火墙。当您在动态地址组内引用这些标记，并将其与安全策略规则内的标记进行匹配时，可以对 Cisco ACI 结构内部署的所有资产统一执行该策略。
- **Cisco TrustSec** — 您可以通过 Cisco TrustSec 插件在您的 Cisco TrustSec 环境中启用端点监控。您可以通过此插件启用 Panorama 与您的 Cisco pxGrid 服务器之间的通信，以便 Panorama 可以收集端点信息作为端点标记，并将信息注册到 Palo Alto Networks 防火墙。当您在动态地址组内引用这些标记，并将其与安全策略规则内的标记进行匹配时，可以对 Cisco TrustSec 环境中部署的所有资产统一实施策略。
- **Cloud Services** — 您可以通过 Cloud Services 插件使用 Cortex 数据湖和 Prisma Access。Cortex 数据湖解决操作日志记录质询问题，而 Prisma Access 云服务则可将您的安全基础架构扩展至远程网络位置和移动办公人员。
- 企业数据丢失防护 **(DLP)** — 企业数据丢失防护 (DLP) 是一组工具和进程，允许您保护敏感信息免遭未经授权访问、滥用、提取和共享。企业 DLP 通过云服务启用，帮助您检查内容并在正确的上下文中分析数据，以便您可以准确地识别敏感数据并进行保护以防止发生事故。企业 DLP 在运行 PAN-OS 10.0.2 及更高版本的 Panorama 和受管防火墙上受支持。
- **GCP** — 使您能够在 Google Kubernetes Engine (GKE) 群集中保护 Kubernetes 服务。配置用于 Google Cloud Platform (GCP) 的 Panorama 插件，以连接到您的 GKE 群集，并了解暴露于互联网的服务。
- **Interconnect**— 您可以通过 Interconnect 插件管理大规模防火墙部署。可以使用 Interconnect 插件为横向扩展架构设置两层 Panorama 部署（在 Panorama PAN-OS 8.1.3 及更高版本上）。通过 Interconnect 插件，您可以部署一个最多有 64 个 Panorama 节点或 32 个 Panorama HA 对的 Panorama 控制器，以集中管理大量防火墙。
- **Nutanix** — 您可以通过面向 Nutanix 的 Panorama 插件在您的 Nutanix 环境中启用 VM 监控。它允许您跟踪 Nutanix Prism Central 内的虚拟机库存，这样您就可以持续实施自动适应 Nutanix 环境变化的安全策略。当配置、取消配置或移动虚拟机时，该解决方案允许您收集 IP 地址和相关联的属性组（或元数据元素）作为标记。您可以使用这些标记来定义动态地址组并在安全策略中使用。面向 Nutanix 的 Panorama 插件要求 Panorama 9.0.4 或更高版本。
- **SD-WAN** — 软件定义广域网 (SD-WAN) 插件使您能够使用多种互联网和私有服务来创建一种既有助于降低成本、又有助于最大化提升应用程序质量和可用性的智能、动态 WAN。在将您的 WAN 连接到互联网时，您无需使用带路由器、防火墙、WAN 路径控制器和 WAN 优化器等组件的昂贵且耗时的 MPLS，只要通过 Palo Alto Network 防火墙上的 SD-WAN 就可以使用更少设备获得更优惠的互联网服务。
- **VMware NSX** — 您可以通过 VMware NSX 插件使用 VMware NSX 管理器启用 VMware NSX 上 VM 系列防火墙之间的集成。通过此集成，您可以将 VM 系列防火墙作为服务部署在 ESXi 服务器上。
- **VMware vCenter** — 您可以通过面向 VMware vCenter 的 Panorama 插件监控 vCenter 环境中的虚拟机。该插件检索 vCenter 环境中虚拟机的 IP 地址并将它们转换为标记，您可以使用这些标记来构建使用动态地址组的策略。

© 2019 Palo Alto Networks, Inc.

- 零接触配置 — 零接触配置 (ZTP) 旨在简化和自动化将新防火墙登入到 Panorama 的流程。ZTP 允许网络管理员直接将受管防火墙发送到其分支并自动将防火墙添加到 Panorama，因此简化了防火墙初始部署流程，从而让企业在部署新防火墙时可以节省时间和资源。PAN-OS 9.1.3 和更高版本支持 ZTP。
- **IPS** 签名转换器 — 用于 Panorama 的 IPS 签名转换器插件提供了一种自动化解决方案，用于将来自第三方入侵防护系统（Snort 和 Suricata）的规则转换为自定义的 Palo Alto Networks 威胁签名。然后，可以在属于所指定设备组的防火墙上注册这些签名，并使用它们在漏洞保护和防间谍软件安全配置文件中强制执行策略。

可以在单个 Panorama 实例中安装多个插件，并从多个源检索 IP 地址更新。这可让您创建和执行一致的安全策略，以跨多个云环境保护应用程序和工作负载。检索到的 IP 地址通过动态地址组在安全策略中使用；当在您的环境中添加或删除工作负载时，Panorama 会注册更改并将更新推送到防火墙。当在 Panorama 上部署多个插件时，必须仔细规划您的设备组层次结构，以确保更新能正确传递到您的防火墙。

有关不同插件版本和兼容性信息的详情，请参阅 Palo Alto Networks 兼容性矩阵。

安装 Panorama 插件

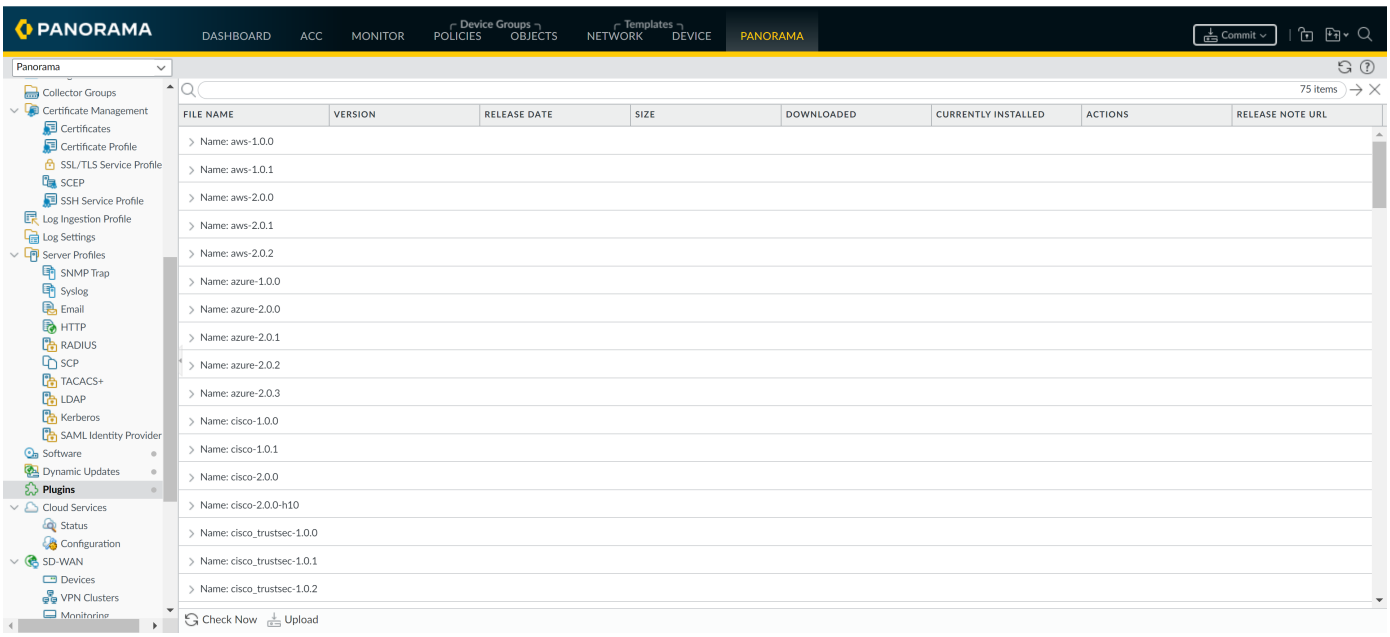
您可以在 Panorama 上安装一个或多个可用插件，以便集成 GlobalProtect 云服务和 Cortex 数据湖、VMware NSX，或是监控 AWS 或 Azure 公共云上的虚拟机。

对于云服务插件，必须激活客户支持门户上的有效身份验证代码，然后选择您想要向其发送日志的区域（美国或欧洲）。

如果当前已安装有一个插件版本，且 *Install*（安装）有该插件的新版本，*Panorama* 将替换当前已安装的版本。

STEP 1 | 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。

   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 | 安装插件。

© 2019 Palo Alto Networks, Inc.

选择插件的版本并在“操作”列中点击 **Install**（安装）以安装插件。安装完成后，Panorama 会提醒您。更多信息，请参阅安装 VMware NSX 插件 或云服务插件。



在 *Panorama HA* 对中首次安装插件时，请在主动对等设备之前将该插件安装在被动对等设备上。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设备上安装插件后，被动对等设备将恢复到运行状态。

© 2019 Palo Alto Networks, Inc.

VM 系列插件和 Panorama 插件

VM 系列插件和各种 Panorama 插件之间的区别是什么？

VM 系列插件适用于 VM 系列防火墙，并且是一个可与公共云环境（例如，Google Cloud Platform (GCP)、Azure 和 AWS）和专用云虚拟机监控程序（例如，KVM、ESXi 等）集成的单一插件。部署防火墙时，内置插件会自动检测部署防火墙的虚拟环境，并加载能够让您管理与该云环境交互的插件组件。例如，在 GCP 上部署 VM 系列防火墙时，VM 系列防火墙会加载支持与 GCP 集成的插件组件。然后，您可以使用 VM 系列插件在 GCP 上配置 VM 系列防火墙，以将指标发布到 Google Stackdriver 监控。同样，通过 Azure 上 VM 系列防火墙上的 VM 插件，您可以配置防火墙以将指标发布到 Azure Application Insights，或设置防火墙作为 HA 对所需的详细信息。VM 系列插件已预先安装在 VM 系列防火墙上，您可以升级或降级该插件，但无法删除。在 Panorama 上，可以使用 VM 系列插件，但尚未预先安装。如果您选择使用 Panorama 管理防火墙上的集成，请在 Panorama 上安装 VM 系列防火墙，以与防火墙上的 VM 系列插件建立通信。

Panorama 插件同时适用于基于硬件的防火墙和 VM 系列防火墙。由于 Panorama 插件是可选的，因此您可以在 Panorama 上添加、删除、重新安装或升级它们。Panorama 插件不是内置的，您必须安装该插件才能与管理所需环境进行通信。例如，您可以使用 Panorama 上的云服务插件启用 Panorama/防火墙和 Cortex Data Lake 之间的设置。Panorama 上的 GCP 插件支持 Panorama 和 GCP 部署之间的通信，从而可以保护进入或退出 Google Kubernetes 引擎 (GKE) 集群中部署的服务的流量。

在 Panorama 上安装 VM 系列插件

要查看并配置部署在 VM 系列防火墙上的云集成，必须在 Panorama 和 VM 系列防火墙上安装 VM 系列插件。插件会自动安装在防火墙上，但在可以将配置推送到设备组之前，必须在 Panorama 上手动安装插件。

VM 系列防火墙支持所有云，因此，您的 *VM* 系列防火墙可能不适合升级。升级插件前，请查阅版本说明。仅在出现云相关更改时才能更新插件。

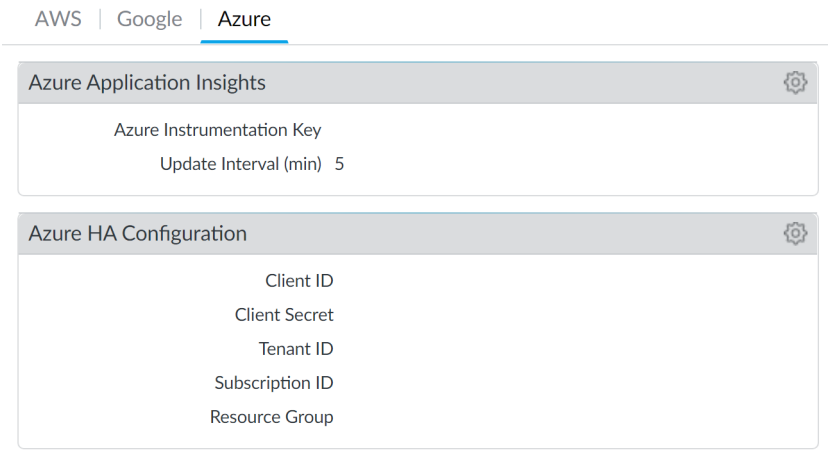
STEP 1 | 下载 VM 系列插件。

1. 选择 **Panorama** > **Plugins**（插件），并使用**Check Now**（立即检查）查找新的插件数据包。VM 系列插件名称为 `vm_series`。
2. 请参阅插件版本说明，以确定哪个版本提供的升级对您有用。
3. 选择插件的版本，并在“操作”列中选择 **Download**（下载）。

STEP 2 | 安装 VM 系列插件。

1. 单击“操作”列中的 **Install**（安装）。安装完成后，Panorama 会提醒您。
2. 要查看插件，请选择 **Device**（设备）> **VM-Series**（**VM** 系列）。
   - 如果防火墙安装在专有云上，且管理程序或服务没有集成，则会看到名为 VM 系列的选项卡和默认消息 `VM Series plugin infrastructure support is installed to allow the firewall's functionality to be enhanced in response to new features launched by hypervisor, or to meet new security needs`。
   - 如果防火墙部署在专有云上，Panorama 会显示所有受支持云的相应选项卡。

© 2019 Palo Alto Networks, Inc.



STEP 3 | （可选）保存您的配置，并将其推送到受管防火墙。

STEP 4 | （可选）在 VM 系列防火墙上，选择 **Device**（设备）> **VM-Series**（**VM** 系列）。如果已为平台配置集成，则会在部署防火墙的云中看到单个选项卡。如果尚未配置集成，则会看到 VM 系列插件基础架构的相关默认消息。

故障排除

以下主题解决了 Panorama™ 管理服务器和专用日志收集器的问题：

- Panorama 系统问题故障排除
- 日志存储和连接问题故障排除
- 替换 RMA 防火墙
- 排除提交故障
- 排除注册或序列号错误
- 排除报告错误
- 排除设备管理许可证错误
- 排除自动恢复防火墙配置问题
- 在关闭 Panorama HA 对等设备时完成内容更新
- 查看任务成功或失败状态
- 测试受管设备的策略匹配和连接
- 从 Panorama 10.0 降级

Panorama 系统问题故障排除

- 生成 Panorama 诊断文件
- 诊断 Panorama 挂起状态
- 监视文件系统完成性检查
- 管理用于软件和内容更新的 Panorama 存储
- 从 Panorama 高可用性部署的脑裂恢复

生成 Panorama 诊断文件

诊断文件有助于监视系统的活动和辨别 Panorama 上问题的可能原因。为了帮助 Palo Alto Networks 技术支持部门解决问题，支持代表可能会请求获取技术支持文件。以下步骤介绍了如何下载技术支持文件并将其上传到您的支持案例。

STEP 1 | 选择 **Panorama** > **Support**（Panorama > 支持），然后单击 **Generate Tech Support File**（生成技术支持文件）。

STEP 2 | 下载并将文件保存到您的计算机中。

STEP 3 | 将文件上传到 Palo Alto Networks 客户支持网站上您的案例中。

诊断 Panorama 挂起状态

如果 Panorama 处于挂起状态，请检查下列条件：

- 序列号 — 验证每台 Panorama 虚拟设备的序列号是否唯一。如果使用相同序列号来创建两个或多个 Panorama 实例，则将会挂起使用相同序列号的所有实例。
- 模式 — 如果在高可用性 (HA) 配置中部署 Panorama 虚拟设备，请验证两个 HA 对端设备处于相同模式：Panorama 模式或传统模式。
- **HA** 优先级 — 验证您是否将一台对端设备的高可用性优先级设置设为主要，而将另一台对端设备的高可用性优先级设置设为辅助。如果两台对端设备的优先级设置相同，则会将序列号数值较高的 Panorama 对端设备置入挂起状态。
- **Panorama** 软件版本 — 验证两台 Panorama 高可用性对端设备是否运行相同的 Panorama 软件版本（主版本号和子版本号）。

监视文件系统完成性检查

Panorama 定期执行文件系统完整性检查 (FSCK)，以防止 Panorama 系统文件损坏。此检查在八次重新启动后或在最后一次执行文件系统完整性检查 90 天后发生。如果 Panorama 正在运行文件系统完整性检查，Web 界面和安全外壳 (SSH) 登录屏幕将显示一则提示正在进行文件系统完整性检查的警告。您此时无法登录，直到该过程完成。完成此过程所需的时间随存储系统大小不同而不同；可能需要数小时之后才可以返回登录 Panorama，具体时间取决于存储系统的大小。

在 Panorama 或受管防火墙上成功下载并安装 PAN-OS 软件更新后，该软件更新将在软件安装过程中 Panorama 或受管防火墙重新启动后接受验证，以确保 PAN-OS 软件的完整性。这样可确保现在运行的软件更新是已知良好的，且 Panorama 或受管防火墙不会因远程或物理漏洞利用而受到威胁。

要查看文件系统完整性检查的进度，请访问 Panorama 的控制台并查看检查状态。

© 2019 Palo Alto Networks, Inc.

管理用于软件和内容更新的 Panorama 存储

您可以安装 Panorama 的内容和软件更新和使用 Panorama 将更新部署到防火墙、日志收集器和 WildFire 设备。您无法配置 Panorama 上的可用空间量来存储更新。当分配的存储容量达到 90% 时，Panorama 会提醒您释放空间（删除已存储的更新）以便下载新内容或上传新内容。更新的最大数量是全局设置，对 Panorama 存储的所有更新都适用。您必须访问 CLI 以配置此设置。默认值为每种类型两项更新。

- 修改每种类型的更新的最大数量。

  访问 Panorama CLI，然后输入以下命令，其中 *<number>* 可以是 2 至 64 之间的任意一个数字：

```
> set max-num-images count <number>
```

- 查看 Panorama 当前存储的更新的数量。

  输入：

```
> show max-num-images
```

- 使用 Web 界面删除更新，从而在 Panorama 上释放空间。
  1. 选择要删除的更新类型：
     - 防火墙或日志收集器更新：

       PAN-OS/Panorama 软件映像 — 选择 **Panorama** > **Device Deployment**（设备部署）> **Software**（软件）。

       GlobalProtect™ 代理/应用软件更新 — 选择 **Panorama** > **Device Deployment**（设备部署）> **GlobalProtect Client**（**GlobalProtect** 客户端）。

       内容更新 — 选择 **Panorama** > **Device Deployment**（设备部署）> **Dynamic Updates**（动态更新）。
     - Panorama 软件映像 — 选择 **Panorama** > **Software**（Panorama > 软件）。
     - Panorama 内容更新 — 选择 **Panorama** > **Dynamic Updates**（Panorama > 动态更新）。
  2. 单击映像或更新的最右列中的 **X** 图标。

- 使用 CLI 删除更新，从而在 Panorama 上释放空间。

  按版本删除软件映像：

```
> delete software version <version_number>
```

  删除内容更新：

```
> delete content update <filename>
```

从 Panorama 高可用性部署的脑裂恢复

在高可用性 (HA) 设置中配置 Panorama 时，受管防火墙已同时连接到主动和被动 Panorama 高可用性对端设备。当主动和被动 Panorama 对端设备之间的连接失败时，在被动 Panorama 接管为主动对端设备之前，将检查是否有任何防火墙同时连接到主动和被动对端设备。如果有一个防火墙连接到这两台对端设备，则不会触发故障转移。

© 2019 Palo Alto Networks, Inc.

在以下罕见情况下，我们称之为脑裂：当一组防火墙连接到主动对端设备，一组防火墙连接到被动对端设备，但没有一个防火墙同时连接到这两台对端设备时，触发故障转移。当发生脑裂时，会出现以下情况：

- Panorama 对端设备既不知道另一个对端设备的状态，也不知道其高可用性角色。
- 两台 Panorama 对端设备都成为主动设备，并管理一组唯一的防火墙。

要解决脑裂问题，请调试网络问题，并恢复 Panorama 高可用性对端设备之间的连接。

但是，如果需要更改防火墙的配置，而不恢复对端设备之间的连接，下面提供了几种可选方法：

- 在两台 Panorama 对端设备上手动添加相同的配置更改内容。此方法可确保在重新建立链接时配置同步。
- 如果需要仅在一个 Panorama 位置添加/更改配置，则在重新建立 Panorama 对端设备之间的链接后，更改和同步配置（确保从做出更改的对端设备开始同步）。要同步对端设备，选择 **Dashboard**（仪表盘）选项卡，然后在 High Availability（高可用性）小部件中，单击 **Sync to peer**（同步到对端设备）。
- 如果需要在每个位置仅对连接的防火墙添加/更改配置，则可以在每台 Panorama 对端设备上独立更改配置。由于对端设备已断开连接，因此没有复制内容，并且每台对端设备现在具有完全不同的配置文件（它们不同步）。因此，要确保在恢复连接时每台对端设备上的配置更改不丢失，就不能让配置自动重新同步。要解决此问题，请从每台 Panorama 对端设备导出配置，然后使用外部对比和合并工具手动合并这些更改。在整合这些更改后，可以在主要 Panorama 上导入此统一的配置文件，然后与对端设备同步导入的配置文件。

© 2019 Palo Alto Networks, Inc.

日志存储和连接问题故障排除

仅 *M-Series* 设备支持迁移日志。请参阅 从 Panorama 虚拟设备迁移到不同的管理程序 以迁移 *Panorama* 虚拟设备。

- 验证 Panorama 端口使用情况
- 解决收集器组的零日志存储
- 在 M 系列设备上更换故障磁盘
- 替换 ESXi 服务器上的虚拟磁盘
- 替换 vCloud Air 上的虚拟磁盘
- 将日志迁移到日志收集器模式下的新 M 系列设备
- 将日志迁移到 Panorama 模式下的新 M 系列设备
- 将日志迁移到高可用性配置中 Panorama 模式下的新 M 系列设备型号
- 将日志迁移到高可用性的 Panorama 模式下的新 M 系列设备型号
- 非高可用性 Panorama 出现故障/RMA 时迁移日志收集器
- 重新生成 M 系列设备 RAID 对的元数据
- 查看日志查询作业

验证 Panorama 端口使用情况

为了确保 Panorama 能够与受管防火墙、日志收集器、WildFire 设备和设备群集及其高可用性 (HA) 对端设备通信，请使用下表验证必须在网络上开放的端口。Panorama 使用 TCP 协议进行端口通信。

默认情况下，Panorama 使用管理 (MGT) 接口管理设备（防火墙、日志收集器、WildFire 设备和设备群集），收集日志，与收集器组进行通信以及将软件和内容更新部署到设备。但是，您可以选择将日志收集和收集器组通信功能分配到运行 Panorama 6.1 到 7.1 的 M-600、M-500 或 M-200 设备上的 Eth1 或 Eth2 接口。如果设备运行 Panorama 8.0 或更高版本，则可以将任何功能分配给 M-600、M-500 或 M-200 设备上的 Eth1、Eth2、Eth3、Eth4 或 Eth5 接口。不管您将哪个功能分配到哪个接口，下表中列出的端口都适用。例如，如果您将日志收集分配到 MGT 接口，而将收集器组通信分配到 Eth2，则 MGT 会使用端口 3978，而 Eth2 会使用端口 28270。（对于所有这些功能，Panorama 虚拟设备只能使用 MGT 接口。）

建立连接的通信系统和方向	Panorama 5.x 所用端口	Panorama 6.x 至 7.x 所用端口	Panorama 8.x 及更高版本所用端口	说明
Panorama 和 Panorama (HA) 方向：每台对端设备均从自身发起与另一台对端设备的连接	28	28	28	如果已启用加密，则适用于高可用性连接和同步。 用于收集器组中日志收集器之间的通信，以便进行日志分发。
Panorama 和 Panorama (HA) 方向：每台对端设备均从自身发起与另一台对端设备的连接	28769 和 28260 (5.1) 28769 和 49160 (5.0)	28260 和 28769	28260 和 28769	如果未启用加密，则适用于高可用性连接和同步。
Panorama 和受管防火墙 方向：由防火墙发起	3978	3978	3978	双向连接，在这种情况下可以将日志从防火墙转发到 Panorama，并将配置更改从

© 2019 Palo Alto Networks, Inc.

建立连接的通信系统和方向	Panorama 5.x 所用端口	Panorama 6.x 至 7.x 所用端口	Panorama 8.x 及更高版本所用端口	说明
				Panorama 推送到受管防火墙。此外，也可以通过同一连接发送上下文切换命令。
Panorama 和日志收集器 方向：由日志收集器发起	3978	3978	3978	适用于管理和日志收集/报告。 适用于在 Panorama 模式下 Panorama 上的本地日志收集器之间的通信，也适用于与分布式日志收集部署中的日志收集器通信。
Panorama 和受管设备（防火墙、日志收集器、WildFire 设备和设备群集） 方向： • 由运行 PAN-OS 8.x 或更高版本的受管设备启动。 • 由 Panorama 为运行 PAN-OS 7.x 或更早发行版的设备启动。	3978	3978	28443	运行 PAN-OS 8.x 或更高版本的设备使用端口 28443 从 Panorama 检索软件和内容更新文件。 运行 7.x 或更低版本的设备不会从 Panorama 检索更新文件；Panorama 将更新文件通过端口 3978 推送到设备。 支持 WildFire 设备和设备群集的 Panorama 管理需要在受管 WildFire 设备上安装 PAN-OS 8.0.1 或更高版本。我们建议 Panorama 运行 8.0.1 或更高版本管理 WildFire 设备和设备群集。
日志收集器到日志收集器 方向：每个日志收集器均从自身发起与收集器组中其他日志收集器的连接	49190	28270	28270	适用于在日志收集器之间分发块和所有二进制数据。
Panorama 至 Cortex 数据湖	NA	NA	444 *8.0.5* 版本及更高版本。	用于设置与 Cortex 数据湖的安全通信通道。 受管防火墙使用端口 3978 与 与 Cortex 数据湖通信。

解决收集器组的零日志存储

如果没有为日志收集器中的日志记录启用磁盘对，则收集器组的日志存储容量可能会显示为 0MB。要启用磁盘对，请为收集器组中的每个日志收集器执行以下步骤。

© 2019 Palo Alto Networks, Inc.

STEP 1 | 添加 RAID 磁盘对。

1. 选择 **Panorama** > **Managed Collectors**（受管收集器），然后单击收集器名称。
2. 选择 **Disks**（磁盘），**Add**（添加）每个 RAID 磁盘对，然后单击 **OK**（确定）。

STEP 2 | 将更改提交到 Panorama，并将更改推送到收集器组。

1. 选择 **Commit**（提交）> **Commit and Push**（提交并推送）和推送范围中的 **Edit Selections**（编辑选择）。
2. 选择 **Collector Groups**（收集器组），选择您所修改的收集器组，然后单击 **OK**（确定）。
3. **Commit and Push**（提交并推送）更改。

STEP 3 | 验证日志收集器和磁盘对的状态。

1. 选择 **Panorama** > **Managed Collectors**（Panorama > 受管收集器），核实每个日志收集器的配置是否已与 Panorama 同步。

   配置状态列应显示 **In Sync**（同步），运行时间状态列应显示 **connected**（已连接）。
2. 单击每个日志收集器最后一列的 **Statistics**（统计信息），验证磁盘对是否为 **Enabled**（已启用）和 **Available**（可用）。

在 M 系列设备上更换故障磁盘

如果 M 系列设备上的磁盘出现故障，您必须更换此磁盘，并在 RAID 1 阵列中重新配置它。有关详细信息，请参阅《M 系列设备硬件参考指南》。

替换 ESXi 服务器上的虚拟磁盘

在将虚拟磁盘添加到在 VMware ESXi 服务器上运行的 Panorama 虚拟设备后，您不能调整其大小。由于传统模式下的 Panorama 虚拟设备只允许一个日志存储位置，必须按照如下所示更换虚拟磁盘以修改日志存储容量。在 Panorama 模式下，您可以简单地添加另一个磁盘（最多 12 个）扩展 Panorama 虚拟设备上的日志存储容量。

在传统模式下的 *Panorama* 虚拟设备上，更换现有磁盘时会丢失此磁盘上的日志。有关保留现有日志的选项，请参阅当在传统模式下在 Panorama 虚拟设备上添加存储时保留现有日志。

STEP 1 | 移除旧虚拟磁盘。

1. 访问 VMware vSphere Client，然后选择 **Virtual Machines**（虚拟机）选项卡。
2. 右击 Panorama 虚拟设备，然后选择 **Power**（电源）> **Power Off**（关闭电源）。
3. 右击 Panorama 虚拟设备，然后选择 **Edit Settings**（编辑设置）。
4. 在 **Hardware**（硬件）选项卡中选择虚拟磁盘，单击 **Remove**（删除）。
5. 选择一个移除选项，单击 **OK**（确定）。

STEP 2 | 添加新虚拟磁盘。

1. 向 ESXi 服务器上的 Panorama 添加虚拟磁盘。

   运行 ESXi 5.5 及更高版本的 Panorama 支持容量达 8TB 的虚拟磁盘。运行更低版本 ESXi 的 Panorama 支持容量达 2TB 的虚拟磁盘。
2. 在 vSphere Client 中，右击 Panorama 虚拟设备，然后选择 **Power** > **Power On**（电源 > 开启电源）。

   重新启动过程可能需要几分钟时间，并且将会显示 `cache data unavailable` 的消息。

STEP 3 | 核实修改后的日志存储容量正确无误。

1. 登录到 Panoram 虚拟设备。

© 2019 Palo Alto Networks, Inc.

2. 选择 **Panorama** > **Setup** > **Management**（Panorama > 设置 > 管理），然后验证“Logging and Reporting Settings（日志记录和报告设置）”部分 Log Storage（日志存储）是否已准确显示修改后的日志存储容量。

替换 vCloud Air 上的虚拟磁盘

在将虚拟磁盘添加到在 VMware vCloud Air 服务器上运行的 Panorama 虚拟设备后，您不能调整其大小。由于传统模式下的 Panorama 虚拟设备只允许一个日志存储位置，必须按照如下所示更换虚拟磁盘以修改日志存储容量。在 Panorama 模式下，您可以简单 向 vCloud Air 中的 Panorama 添加虚拟磁盘（最多 12 个）。

在传统模式下的 *Panorama* 虚拟设备上，更换现有磁盘时会丢失此磁盘上的日志。有关保留现有日志的选项，请参阅当在传统模式下在 Panorama 虚拟设备上添加存储时保留现有日志。

STEP 1 | 移除旧虚拟磁盘。

1. 访问 vCloud Air Web 控制台，然后选择您的 **Virtual Private Cloud OnDemand**（按需虚拟私有云）区域。
2. 在 **Virtual Machines**（虚拟机）选项卡中选择 Panorama 虚拟设备。
3. 选择 **Actions** > **Edit Resources**（操作 > 编辑资源）。
4. 为您要移除的虚拟磁盘单击 **x**。

STEP 2 | 添加新虚拟磁盘。

1. **Add another disk**（添加其他磁盘）。
2. 将 **Storage**（存储器）设置为 8TB，将存储层设置为 **Standard**（标准）或 **SSD-Accelerated**（**SSD** 加速）。
3. **Save**（保持）更改。

STEP 3 | 重新启动 Panorama。

1. 登录到 Panoram 虚拟设备。
2. 选择 **Panorama** > **Setup** > **Operations**（Panorama > 设置 > 操作），然后单击 **Reboot Panorama**（重新启动 Panorama）。

STEP 4 | 核实修改后的日志存储容量正确无误。

1. 在 Panoram 虚拟设备重新启动后登录到此设备。
2. 选择 **Panorama** > **Setup** > **Management**（Panorama > 设置 > 管理），然后验证“Logging and Reporting Settings（日志记录和报告设置）”部分 Log Storage（日志存储）是否已准确显示修改后的日志存储容量。

将日志迁移到日志收集器模式下的新 M 系列设备

如果您需要更换日志收集器模式下的 M-600、M-500、 M-200 或 M-100 系列设备（专用日志收集器），您可以通过将其 RAID 磁盘转移到新 M 系列设备来迁移它之前从防火墙收集的日志。此过程可以让您在 M-Series 设备发生系统故障之后恢复日志，或者把日志视为硬件升级的一部分而加以迁移（从 M-100 设备迁移到 M-500 设备）。

不支持通过从任何 M 系列设备中删除日志记录磁盘并将其加载到 *M-600 Panorama* 管理服务器来迁移日志。如要迁移到 *M-600* 设备，请设置 M-600 设备、配置日志转发到新 M-600 设备以及将 M 系列设备配置为受管日志收集器直至您不再需要访问 *M* 系列设备上存储的日志。

STEP 1 | 执行将用作专用日志收集器的新 M 系列设备的初始设置。

1. 将 M 系列设备安装到机架上。有关说明，请参阅《M 系列设备硬件参考指南》。
2. 执行 M 系列设备的初始配置。

© 2019 Palo Alto Networks, Inc.

配置接口时，仅配置管理 *(MGT)* 接口。切换到日志收集器模式（稍后在此过程中）可删除任何其他接口的配置。如果日志收集器使用除 *MTG* 以外的接口，则在配置日志收集器时进行添加（请参阅步骤2）。

3. 注册 Panorama。
4. 只有当新 M 系列设备的硬件型号与旧 M 系列设备的硬件型号相同时，才可以按如下步骤购买和激活 Panorama 支持许可证或转移许可证。如果新 M 系列设备的型号与旧 M 系列设备的型号不同，则必须购买新许可证。
   1. 登录到 Palo Alto Networks 客户支持站点。
   2. 选择 **Assets**（资产）选项卡，然后单击 **Spares**（备件）链接。
   3. 单击新 M 系列设备的 Serial Number（序列号）。
   4. 单击 **Transfer Licenses**（转移许可证）。
   5. **Select**（选择）旧 M 系列设备，然后单击 **Submit**（提交）。
5. 激活防火墙管理许可证。如果您将日志从 M-100 设备迁移到 M-500 设备，则应输入与迁移许可证相关联的身份验证代码。
6. 安装 Panorama 的内容和软件更新。有关软件版本的重要详细信息，请参阅 Panorama、日志收集器、防火墙和 WildFire 的版本兼容性。
7. 从 Panorama 模式切换到日志收集器模式：
   1. 访问日志收集器 CLI，切换到日志收集器模式：

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

   2. 输入 **Y** 确认模式更改。M 系列设备重新启动。如果重新启动进程终止了终端模拟软件会话，重新连接 M 系列设备以显示 Panorama 登录提示。

      如果系统显示 ***CMS Login***提示符，按 *Enter* 键，而不输入用户名或密码。

8. 使用日志收集器 CLI 启用日志收集器和 Panorama 管理服务器之间的连接。<IPaddress1> 是主要 Panorama 的 MGT 接口，<IPaddress2> 是辅助 Panorama 的 MGT 接口。

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

STEP 2 | 在 Panorama 管理服务器上，将新日志收集器添加为受管收集器。

对于所有涉及需要序列号的命令的步骤，您必须键入完整的序列号；按下“*Tab*”键即可填写完整的序列号。

1. 使用 Panorama Web 界面或使用以下 CLI 命令，将日志收集器配置为受管收集器：

```
> configure
# set log-collector <LC_serial_number> deviceconfig system hostname
 <LC_hostname>
# exit
```

如果旧日志收集器将 *MGT* 接口以外的接口用于日志收集和收集器组通信，您必须在将新日志收集器配置为受管收集器时在新日志收集器上定义这些接口（*Panorama* > *Managed Collectors*（受管收集器）> *Interfaces*（接口））。

© 2019 Palo Alto Networks, Inc.

2. 核实日志收集器已连接上 Panorama，且其磁盘对的状态为“存在/可用”。

```
> show log-collector serial-number <log-collector_SN>
```

磁盘对在此阶段的恢复过程中将显示为 Disabled（禁用）。

3. 将更改提交到 Panorama。不可在此时就将更改提交到收集器组。

```
> configure
# commit
# exit
```

STEP 3 | 从旧日志收集器中移除 RAID 磁盘。

1. 按下电源按钮以关闭旧日志收集器，直到系统关闭。
2. 移除磁盘对。有关详细信息，请参阅《M 系列设备硬件参考指南》中的磁盘更换程序。

STEP 4 | 准备磁盘进行迁移。



生成每个磁盘对的元数据后，需重新构建索引。因此，根据数据大小，此过程需要较长时间才能完成。若要加快这一过程，您可以启动多个 *CLI* 会话并在每一个会话中运行元数据再生命令，为每一个磁盘对同时完成此过程。有关详细信息，请参阅重新生成 M 系列设备 RAID 对的元数据。

1. 将磁盘插入新日志收集器。有关详细信息，请参阅《M 系列设备硬件参考指南》中的磁盘更换程序。



M-100 设备的磁盘载体与 *M-500* 设备的磁盘载体不兼容。因此，在这些硬件型号之间执行迁移时，必须将每个磁盘从其旧载体上旋下，并在将磁盘插入新设备中之前将磁盘插入新载体。

您必须维持磁盘对的关联。尽管您可以把磁盘对从旧设备上的 A1/A2 插槽置入到新设备上的 B1/B2 插槽，但您必须保持磁盘对处于同一插槽中；否则，Panorama 可能无法成功地恢复数据。

2. 为每个磁盘对运行以下 CLI 命令即可启用磁盘对：

```
> request system raid add <slot> force no-format
```

例如：

```
> request system raid add A1 force no-format
> request system raid add A2 force no-format
```

Force 和 **no-format** 是必需的命令参数。**Force** 参数使磁盘对与新日志收集器相关联。**No-format** 参数则防止驱动器的重新格式化，并保留存储在磁盘上的日志。

3. 生成每个磁盘对的元数据。

```
> request metadata-regenerate slot <slot_number>
```

例如：

```
> request metadata-regenerate slot 1
```

STEP 5 | 将没有磁盘的日志收集器添加到收集器组。

© 2019 Palo Alto Networks, Inc.

从此时开始，仅提交在 *Panorama* 和日志收集器上完成迁移过程所需的提交。暂缓进行任何其他更改。

1. 访问 Panorama CLI。
2. 覆盖 Panorama 限制以允许将没有磁盘的日志收集器添加到收集器组：**request log-migration-set-start**

STEP 6 | 迁移日志。

对于此步骤，您必须使用 *Panorama CLI*，而不是 *Web* 界面。

您必须将新日志收集器分配到包含了旧日志收集器的收集器组。

1. 将新日志收集器分配到收集器组，然后将更改提交到 Panorama。

```
> configure
# set log-collector-group <collector_group_name> logfwd-setting collectors
 <new_LC_serial_number>
# commit
# exit
```

2. 对于每个磁盘对，应将日志从旧日志收集器迁移到新日志收集器，并使磁盘对与新日志收集器相关联。

```
> request log-migration from <old_LC_serial_number> old-disk-pair
 <log_disk_pair> to <new_LC_serial_number> new-disk-pair <log_disk_pair>
```

例如：

```
> request log-migration from 003001000010 old-disk-pair A to 00300100038
 new-disk-pair A
```

STEP 7 | 重新配置收集器组。

1. 使用 Web 界面，将新日志收集器分配到转发日志的防火墙（**Panorama** > **Collector Groups**（收集器组）> **Device Log Forwarding**（设备日志转发））。在防火墙首选项列表中，向新日志收集器给予与旧日志收集器相同的优先级。

您不能使用 *CLI* 更改防火墙首选项列表的优先级分配。

2. 从收集器组中删除旧日志收集器。

```
> configure
# delete log-collector-group <group_name> logfwd-setting collectors
 <old_LC_serial_number>
```

例如：

```
# delete log-collector-group DC-Collector-Group logfwd-setting collectors
 003001000010
```

3. 从 Panorama 配置中删除旧日志收集器，并将更改提交到 Panorama。

© 2019 Palo Alto Networks, Inc.

```
# delete log-collector <old_LC_serial_number>
# commit
# exit
```

4. 提交收集器组更改，以使受管防火墙可以将日志发送到新日志收集器。

```
> commit-all log-collector-config log-collector-
group <collector_group_name>
```

例如：

```
> commit-all log-collector-config log-collector-group DC-Collector-Group
```

STEP 8 | 在新的专用日志收集器上生成新密钥。

需要此命令才能将新的日志收集器添加到收集器组，并且只应为要替换的日志收集器的收集器组运行。此步骤会删除现有的 *RSA* 密钥，并允许 *Panorama* 创建新的 *RSA* 密钥。

1. 访问 Panorama CLI。
2. 删除新的日志收集器上的所有 RSA 密钥：

   request logdb update-collector-group-after-replace collector-group *<collector-group-name>*

   该过程可能需要 10 分钟才能完成。

STEP 9 | 确认收集器组中所有日志收集器的 SearchEngine Status（SearchEngine 状态）为 Active（活动）状态。

在收集器组中的所有日志收集器的 *SearchEngine Status*（*SearchEngine* 状态）变为 *Active*（活动）状态前，请勿继续操作。否则，这将会导致清除替换的日志收集器中的日志。

1. 访问 Panorama CLI。
2. 通过运行以下命令显示日志收集器详细信息：
   - 在所有日志收集器的 Panorama 上：

     show log-collector all

     或者，您可以在每个专用日志收集器上运行以下命令：

     show log-collector detail

3. 确认 SearchEngine Status（SearchEngine 状态）为 Active（活动）状态。

```
Redistribution status:       none
```

```
Last commit-all: commit succeeded, current ring version 1
```

```
SearchEngine status:     Active
```


© 2019 Palo Alto Networks, Inc.

```
md5sum 4e5055a359f7662fab8f8c4f57e24525 updated at 2017/06/14 09:58:19
```

STEP 10 | 在新的日志收集器上，使用新的日志收集器序列号替换以前的日志收集器序列号。

您必须使用新的日志收集器序列号替换旧的日志收集器序列号，以便新的日志收集器不会出现清除问题，从而导致日志收集器无法在必要时从迁移的日志中清除旧数据。

1. 访问日志收集器 CLI。
2. 使用新的日志收集器序列号替换旧的日志收集器序列号：

   request log-migration-update-logger from *<old-log-collector-serial-number>* to *<new-log-collector-serial-number>*

将日志迁移到 Panorama 模式下的新 M 系列设备

如果您需要更换 Panorama 模式（Panorama 管理服务器）下的 M-600、M-500、 M-200 或 M-100 系列设备，您可以通过将其 RAID 磁盘转移到新 M 系列设备来迁移它之前从防火墙收集的日志。移动磁盘可以让您在 M 系列设备发生系统故障之后恢复日志，或者把日志视为硬件升级的一部分而加以迁移（从 M-100 设备迁移到 M-500 设备）。

不支持通过从任何 M 系列设备中删除日志记录磁盘并将其加载到 *M-600 Panorama* 管理服务器来迁移日志。如要迁移到 *M-600* 设备，请设置 M-600 设备、配置日志转发到新 M-600 设备以及将 M 系列设备配置为受管日志收集器直至您不再需要访问 *M* 系列设备上存储的日志。

此迁移程序涵盖以下情况，您可以使用收集器组中受管收集器（日志收集器）更换未在 HA 配置中的单个 M 系列设备。

STEP 1 | 如果您想要保留旧 M 系列设备 SSD 中的任何日志，请将它们转发到外部目标。

SSD 存储 Panorama 和日志收集器所生成的系统和配置日志。您无法在 M 系列设备之间移动 SSD。

配置从 Panorama 到外部目标的日志转发。

STEP 2 | 从 Panorama 模式下的已停用 M 系列设备导出 Panorama 配置。

1. 登录到 Panorama 设备，然后选择 **Panorama** > **Setup**（设置）> **Operations**（操作）。
2. 单击 **Save named Panorama configuration snapshot**（保存已命名的 **Panorama** 配置快照），输入 **Name**（名称）以标识该配置，然后单击 **OK**（确定）。
3. 单击 **Export named Panorama configuration snapshot**（导出已命名的 **Panorama** 配置快照），选择您刚才所保存配置的 **Name**（名称），然后单击 **OK**（确定）。Panorama 会向您的客户端系统将配置导出为 XML 文件。

STEP 3 | 从旧 M 系列设备中移除 RAID 磁盘。

1. 按下电源按钮以关闭旧日志收集器，直到系统关闭。
2. 移除磁盘对。有关详细信息，请参阅《M 系列设备硬件参考指南》中的磁盘更换程序。

STEP 4 | 执行新 M 系列设备的初始设置。

1. 将 M 系列设备安装到机架上。有关说明，请参阅《M 系列设备硬件参考指南》。
2. 执行 M 系列设备的初始配置。
3. 注册 Panorama。
4. 只有当新 M 系列设备的硬件型号与旧 M 系列设备的硬件型号相同时，才可以按如下步骤购买和激活 Panorama 支持许可证或转移许可证。如果新 M 系列设备的型号与旧 M 系列设备的型号不同，则必须购买新许可证。

   1. 登录到 Palo Alto Networks 客户支持站点。

© 2019 Palo Alto Networks, Inc.

2. 选择 **Assets**（资产）选项卡，然后单击 **Spares**（备件）链接。
3. 单击新 M 系列设备的 Serial Number（序列号）。
4. 单击 **Transfer Licenses**（转移许可证）。
5. **Select**（选择）旧 M 系列设备，然后单击 **Submit**（提交）。

5. 激活防火墙管理许可证。如果您是在将日志从 M-100 设备迁移到 M-500 设备，则应输入与迁移许可证相关联的身份验证代码。
6. 安装 Panorama 的内容和软件更新。有关软件版本的重要详细信息，请参阅 Panorama、日志收集器、防火墙和 WildFire 的版本兼容性。

STEP 5 | 加载您从已停用的 M 系列设备导出到 Panorama 模式下新的 M 系列设备的 Panorama 配置快照。

1. 登录到 Panorama Web 界面在新的 M 系列设备上，选择**Panorama** > **Setup**（设置）> **Operations**（操作）。
2. 单击 **Import named Panorama configuration snapshot**（导入已命名 **Panorama** 配置快照），**Browse**（浏览）到您从已停用的 M 系列设备导出的配置文件，然后单击 **OK**（确定）。
3. 单击 **Load named Panorama configuration snapshot**（加载已命名的 **Panorama** 配置快照），选择刚才导入的配置的 **Name**（名称），选择 **Decryption Key**（解密密钥）（Panorama 的主秘钥），然后单击 **OK**（确定）。Panorama 将使用加载的配置覆盖其当前待选配置。在加载配置文件时，Panorama 会显示任何出现的错误。如果出现错误，请将错误保存到本地文件中。解决每一个错误，以确保迁移的配置有效。

   要替换 *RMA Panorama*，请务必在您加载已命名的 *Panorama* 配置快照时 *Retain Rule UUIDs*（保留规则 *UUID*）。如果未选择此选项，*Panorama* 将从配置快照中删除先前所有规则 *UUID*，并将新 *UUID* 分配给 *Panorama* 上的规则，这意味着与先前 *UUID* 相关的信息将不会被保留，例如，策略规则点击数。
4. 根据需要执行任何其他配置更改。

   如果旧 *M* 系列设备将 *MGT* 接口以外的接口用于 *Panorama* 服务（如日志收集），则您必须在新 *M* 系列设备的定义这些接口（*Panorama* > *Setup*（设置）> *Interfaces*（接口））。
5. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），然后选择 **Validate Commit**（验证提交）。在继续操作之前，解决任何错误。
6. 将更改 **Commit**（提交）到 Panorama 配置。

STEP 6 | 将磁盘插入新 M 系列设备。有关详细信息，请参阅《M 系列设备硬件参考指南》中的磁盘更换程序。

M-100 设备的磁盘载体与 *M-500* 设备的磁盘载体不兼容。因此，在这些硬件型号之间执行迁移时，必须将每个磁盘从其旧载体上旋下，并在将磁盘插入新设备中之前将磁盘插入新载体。

您必须维持磁盘对的关联。尽管您可以把磁盘对从旧设备上的 A1/A2 插槽置入到新设备上的 B1/B2 插槽，但您必须保持磁盘对处于同一插槽中；否则，Panorama 可能无法成功地恢复数据。

STEP 7 | 联系 Palo Alto Networks 客户支持，将从已停用的 M 系列设备获取的日志收集器组元数据复制到新的 M 系列设备，并重启 mgmtsrvr 进程。

STEP 8 | 如果 M 系列设备是收集器组的一部分，请确认已停用的 M 系列设备序列号仍是正确的收集器组的一部分：

```
debug log-collector-group show name <Log Collector Group name>
```

如果已停用的 M 系列设备序列号不再是正确的收集器组的一部分，则在上一步中复制的技术支持文件夹是不正确的。请再次联系 Palo Alto Networks 客户支持将技术支持文件夹复制到正确的位置。

© 2019 Palo Alto Networks, Inc.

STEP 9 | 准备磁盘进行迁移。



生成每个磁盘对的元数据后，需重新构建索引。因此，根据数据大小，此过程需要较长时间才能完成。若要加快这一过程，您可以启动多个 *CLI* 会话并在每一个会话中运行元数据再生命令，为每一个磁盘对同时完成此过程。有关详细信息，请参阅重新生成 M 系列设备 RAID 对的元数据。

1. 将磁盘插入新 M 系列设备。有关详细信息，请参阅《M 系列设备硬件参考指南》中的磁盘更换程序。

   M-100 设备的磁盘载体与 *M-500* 设备的磁盘载体不兼容。因此，在这些硬件型号之间执行迁移时，必须将每个磁盘从其旧载体上旋下，并在将磁盘插入新设备中之前将磁盘插入新载体。

   您必须维持磁盘对的关联。尽管您可以把磁盘对从旧设备上的 A1/A2 插槽置入到新设备上的 B1/B2 插槽，但您必须保持磁盘对处于同一插槽中；否则，Panorama 可能无法成功地恢复数据。
2. 为每个磁盘对运行以下 CLI 命令即可启用磁盘对：

   ```
   admin> request system raid add <slot> force no-format
   ```

   例如：

   ```
   admin> request system raid add A1 force no-format
   admin> request system raid add A2 force no-format
   ```

   Force 和 **no-format** 是必需的命令参数。**Force** 参数使磁盘对与新设备相关联。**No-format** 参数则防止驱动器的重新格式化，并保留存储在磁盘上的日志。
3. 生成每个磁盘对的元数据。

   此步骤可能最多需要 *6* 小时的时间，具体取决于磁盘上的日志数据量。

   ```
   admin> request metadata-regenerate slot <slot_number>
   ```

   例如：

   ```
   admin> request metadata-regenerate slot 1
   ```

STEP 10 | 在新 M 系列设备上配置本地日志收集器。



对于所有涉及需要序列号的命令的步骤，您必须键入完整的序列号；按下“*Tab*”键即可填写完整的序列号。

切勿在此时启用新 M 系列设备上的磁盘。当您成功迁移日志时，Panorama 会自动启用磁盘。

1. 使用 Panorama Web 界面或使用以下 CLI 命令，将本地日志收集器配置为受管收集器：

   ```
   admin> configure
   admin# set log-collector <log-collector_SN> deviceconfig system hostname
    <LC_hostname>
   admin# exit
   ```


© 2019 Palo Alto Networks, Inc.

2. 核实本地日志收集器已连接上 Panorama，且其磁盘对的状态为“存在/可用”。

```
admin> show log-collector serial-number <log-collector_SN>
```

   磁盘对在此阶段的恢复过程中将显示为 Disabled（禁用）。
3. 将更改提交到 Panorama。不可在此时就将更改提交到收集器组。

```
admin> configure
admin# commit
```

STEP 11 | 将没有磁盘的日志收集器添加到收集器组。

从此时开始，仅提交在 *Panorama* 和日志收集器上完成迁移过程所需的提交。暂缓进行任何其他更改。

1. 访问新的 M 系列设备的 Panorama CLI。
2. 覆盖 Panorama 限制以允许将没有磁盘的日志收集器添加到收集器组：**request log-migration-set-start**
3. 提交已覆盖的限制：

```
admin> configure
admin# commit force
```

STEP 12 | 迁移日志。

1. 访问新的 M 系列设备的 Panorama CLI。
2. 将新本地日志收集器添加为收集器组成员，然后将更改提交到 Panorama。

```
admin# set log-collector-group <collector_group_name> logfwd-setting
 collectors <SN_managed_collector>
admin# commit
admin# exit
```

   旧的本地日志收集器仍会显示在成员列表中，因为您尚未将其从配置中删除。
3. 对于每一个磁盘对，应将日志迁移到新设备。

```
admin> request log-migration from <old_LC_serial_number> old-disk-pair
 <log_disk_pair> to <new_LC_serial_number> new-disk-pair <log_disk_pair>
```

   例如：

```
admin> request log-migration from 003001000010 old-disk-pair A to
 00300100038 new-disk-pair A
```

4. 将更改提交到 Panorama。

```
admin> configure
admin# commit
```

STEP 13 | 重新配置收集器组。

© 2019 Palo Alto Networks, Inc.

1. 登录到 Panorama Web 界面 在新的 M 系列设备上，将新日志收集器分配到转发日志的防火墙（**Panorama** > **Collector Groups**（收集器组）> **Device Log Forwarding**（设备日志转发））。在防火墙首选项列表中，向新日志收集器给予与旧日志收集器相同的优先级。

   您不能使用 *CLI* 更改防火墙首选项列表的优先级分配。

2. 访问新的 M 系列设备的 Panorama CLI。
3. 从收集器组中删除旧日志收集器。

```
admin# delete log-collector-group <group_name> logfwd-setting collectors
 <old_LC_serial_number>
```

   例如：

```
admin# delete log-collector-group DC-Collector-Group logfwd-setting
 collectors 003001000010
```

4. 从 Panorama 配置中删除旧日志收集器，并将更改提交到 Panorama。

```
admin# delete log-collector <old_LC_serial_number>
admin# commit
admin# exit
```

5. 提交收集器组更改，以使受管防火墙可以将日志发送到新日志收集器。

```
admin> commit-all log-collector-config log-collector-
group <collector_group_name>
```

   例如：

```
admin> commit-all log-collector-config log-collector-group DC-Collector-
Group
```

STEP 14 | 在新的日志收集器上生成新密钥。

需要此命令才能将新的日志收集器添加到收集器组，并且只应为要替换的日志收集器的收集器组运行。此步骤会删除现有的 *RSA* 密钥，并允许 *Panorama* 创建新的 *RSA* 密钥。

1. 访问新的 M 系列设备的 Panorama CLI。
2. 删除新的日志收集器上的所有 RSA 密钥：

   ```
   request logdb update-collector-group-after-replace collector-group
   <collector-group-name>
   ```

   该过程可能需要 10 分钟才能完成。

STEP 15 | 确认收集器组中所有日志收集器的 SearchEngine Status（SearchEngine 状态）为 Active（活动）状态。

在收集器组中的所有日志收集器的 *SearchEngine Status*（*SearchEngine* 状态）变为 *Active*（活动）状态前，请勿继续操作。否则，这将会导致清除替换的日志收集器中的日志。

© 2019 Palo Alto Networks, Inc.

1. 访问新的 M 系列设备的 Panorama CLI。
2. 通过运行以下命令显示日志收集器详细信息：
   - 在所有日志收集器的 Panorama 上：

     show log-collector all

     或者，您可以在每个专用日志收集器上运行以下命令：

     ```
     show log-collector detail
     ```
3. 确认 SearchEngine Status（SearchEngine 状态）为 Active（活动）状态。

```
Redistribution status:       none
```

```
Last commit-all: commit succeeded, current ring version 1
```

```
SearchEngine status:     Active
```

```
md5sum 4e5055a359f7662fab8f8c4f57e24525 updated at 2017/06/14 09:58:19
```

STEP 16 | 在新的日志收集器上，使用新的日志收集器序列号替换以前的日志收集器序列号。

您必须使用新的日志收集器序列号替换旧的日志收集器序列号，以便新的日志收集器不会出现清除问题，从而导致日志收集器无法在必要时从迁移的日志中清除旧数据。

1. 访问日志收集器 CLI。
2. 使用新的日志收集器序列号替换旧的日志收集器序列号：

   request log-migration-update-logger from *<old-log-collector-serial-number>* to *<new-log-collector-serial-number>*

将日志迁移到高可用性配置中 Panorama 模式下的新 M 系列设备型号

如果您需要采用与被更换的 M 系列设备不相同的 M 系列设备更换 Panorama 模式（Panorama 管理服务器）下的 M-600、M-500、 M-200 或 M-100 系列设备，您可以通过将其 RAID 磁盘转移到新 M 系列设备来迁移它之前从防火墙收集的日志。移动磁盘可以让您把日志视为硬件升级的一部分而进行迁移（从 M-100 设备迁移到 M-500 设备）。您可以将 M-100 设备迁移至 M-500 设备以及从其迁回。M-100 和 M-500 设备无法迁移到 M-200 或 M-600 设备，或从其迁回。



不支持通过从任何 M 系列设备中删除日志记录磁盘并将其加载到 *M-600 Panorama* 管理服务器来迁移日志。如要迁移到 *M-600* 设备，请设置 M-600 设备、配置日志转发到新 M-600 设备以及将 M 系列设备配置为受管日志收集器直至您不再需要访问 *M* 系列设备上存储的日志。

此迁移程序涵盖以下情况：

- 一台 Panorama 高可用性对端设备具有一个收集器组中的受管收集器（日志收集器）。

© 2019 Palo Alto Networks, Inc.

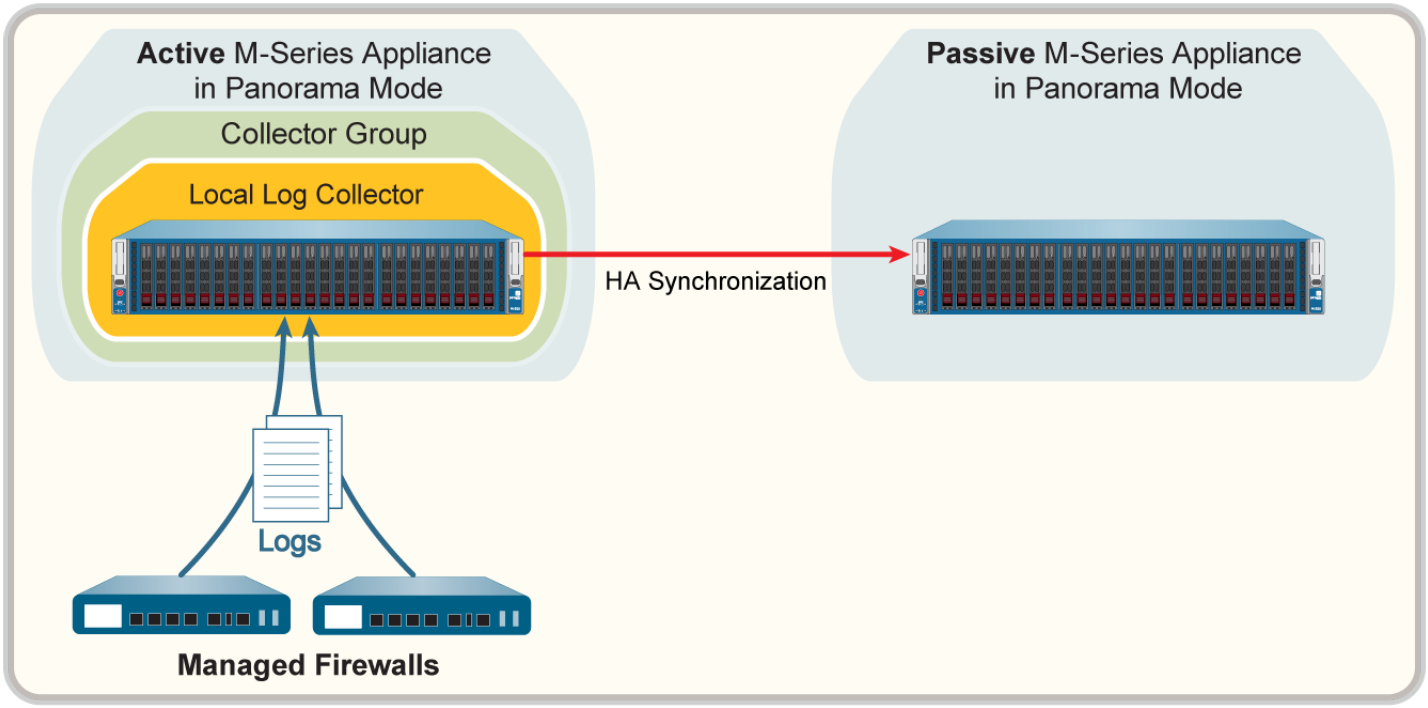


图 **30:** 具有收集器组的 **Panorama HA** 对端设备

- 两台 Panorama 高可用性对端设备都具有属于单个收集器组的受管收集器。有关详细信息，请参阅每个收集器组多个本地日志收集器。
- 两台 Panorama 高可用性对端设备都各有一个收集器，且每一个收集器都已分配到一个单独的收集器组。有关详细信息，请参阅每个收集器组一个本地日志收集器。

STEP 1 | 如果您想要保留旧 M 系列设备 SSD 中的任何日志，请将它们转发到外部目标。

SSD 存储 Panorama 和日志收集器所生成的系统和配置日志。您无法在 M 系列设备之间移动 SSD。

配置从 Panorama 到外部目标的日志转发。

STEP 2 | 从 Panorama 模式下已停用的主要 M 系列设备导出 Panorama 配置。

1. 登录到 Panorama Web 界面在正在更换的 M 系列设备上，选择 **Panorama** > **Setup**（设置）> **Operations**（操作）。
2. 单击 **Save named Panorama configuration snapshot**（保存已命名的 **Panorama** 配置快照），输入 **Name**（名称）以标识该配置，然后单击 **OK**（确定）。
3. 单击 **Export named Panorama configuration snapshot**（导出已命名的 **Panorama** 配置快照），选择您刚才所保存配置的 **Name**（名称），然后单击 **OK**（确定）。Panorama 会向您的客户端系统将配置导出为 XML 文件。

STEP 3 | 从旧 M 系列设备中移除 RAID 磁盘。

1. 按下电源按钮以关闭旧日志收集器，直到系统关闭。
2. 移除磁盘对。有关详细信息，请参阅《M 系列设备硬件参考指南》中的磁盘更换程序。

STEP 4 | 执行新 M 系列设备的初始设置。

对 HA 配置中的每个新 M 系列设备重复此步骤。

1. 将 M 系列设备安装到机架上。有关说明，请参阅《M 系列设备硬件参考指南》。
2. 执行 M 系列设备的初始配置。
3. 注册 Panorama。

© 2019 Palo Alto Networks, Inc.

4. 只有当新 M 系列设备的硬件型号与旧 M 系列设备的硬件型号相同时，才可以按如下步骤购买和激活 Panorama 支持许可证或转移许可证。如果新 M 系列设备的型号与旧 M 系列设备的型号不同，则必须购买新许可证。
   1. 登录到 Palo Alto Networks 客户支持站点。
   2. 选择 **Assets**（资产）选项卡，然后单击 **Spares**（备件）链接。
   3. 单击新 M 系列设备的 Serial Number（序列号）。
   4. 单击 **Transfer Licenses**（转移许可证）。
   5. **Select**（选择）旧 M 系列设备，然后单击 **Submit**（提交）。
5. 激活防火墙管理许可证。如果您是在将日志从 M-100 设备迁移到 M-500 设备，则应输入与迁移许可证相关联的身份验证代码。
6. 安装 Panorama 的内容和软件更新。有关软件版本的重要详细信息，请参阅 Panorama、日志收集器、防火墙和 WildFire 的版本兼容性。
7. 设置 Panorama 高可用性。新 M 系列设备必须具有与您正在更换的高可用性对端设备相同的优先级。

STEP 5 | 加载您从已停用的主要 M 系列设备导出到 Panorama 模式下新的主要 M 系列设备的 Panorama 配置快照。

1. 登录到 Panorama Web 界面在新的 M 系列设备上，选择**Panorama** > **Setup**（设置）> **Operations**（操作）。
2. 单击 **Import named Panorama configuration snapshot**（导入已命名 **Panorama** 配置快照），**Browse**（浏览）到您从已停用的 M 系列设备导出的配置文件，然后单击 **OK**（确定）。
3. 单击 **Load named Panorama configuration snapshot**（加载已命名的 **Panorama** 配置快照），选择刚才导入的配置的 **Name**（名称），选择 **Decryption Key**（解密密钥）（Panorama 的主秘钥），然后单击 **OK**（确定）。Panorama 将使用加载的配置覆盖其当前待选配置。在加载配置文件时，Panorama 会显示任何出现的错误。如果出现错误，请将错误保存到本地文件中。解决每一个错误，以确保迁移的配置有效。

   要替换 *RMA Panorama*，请务必在您加载已命名的 *Panorama* 配置快照时 *Retain Rule UUIDs*（保留规则 *UUID*）。如果未选择此选项，*Panorama* 将从配置快照中删除先前所有规则 *UUID*，并将新 *UUID* 分配给 *Panorama* 上的规则，这意味着与先前 *UUID* 相关的信息将不会被保留，例如，策略规则点击数。
4. 根据需要执行任何其他配置更改。

   如果旧 *M* 系列设备将 *MGT* 接口以外的接口用于 *Panorama* 服务（如日志收集），则您必须在新 *M* 系列设备的定义这些接口（*Panorama* > *Setup*（设置）> *Interfaces*（接口））。
5. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），然后选择 **Validate Commit**（验证提交）。在继续操作之前，解决任何错误。
6. 将更改 **Commit**（提交）到 Panorama 配置。提交后，Panorama 配置将在 HA 对端设备之间同步。

STEP 6 | 将磁盘插入新 M 系列设备。有关详细信息，请参阅《M 系列设备硬件参考指南》中的磁盘更换程序。

对 HA 配置中的每个新 M 系列设备重复此步骤。

M-100 设备的磁盘载体与 *M-500* 设备的磁盘载体不兼容。因此，在这些硬件型号之间执行迁移时，必须将每个磁盘从其旧载体上旋下，并在将磁盘插入新设备中之前将磁盘插入新载体。

您必须维持磁盘对的关联。尽管您可以把磁盘对从旧设备上的 A1/A2 插槽置入到新设备上的 B1/B2 插槽，但您必须保持磁盘对处于同一插槽中；否则，Panorama 可能无法成功地恢复数据。

© 2019 Palo Alto Networks, Inc.

STEP 7 | 联系 Palo Alto Networks 客户支持，将从已停用的 M 系列设备获取的日志收集器组元数据复制到新的 M 系列设备，并重启 mgmtsrvr 进程。

STEP 8 | 如果 M 系列设备是收集器组的一部分，请确认已停用的 M 系列设备序列号仍是正确的收集器组的一部分：

```
debug log-collector-group show name <Log CollectorGroup name>
```

如果已停用的 M 系列设备序列号不再是正确的收集器组的一部分，则在上一步中复制的技术支持文件夹是不正确的。请再次联系 Palo Alto Networks 客户支持将技术支持文件夹复制到正确的位置。

STEP 9 | 准备磁盘进行迁移。



生成每个磁盘对的元数据后，需重新构建索引。因此，根据数据大小，此过程需要较长时间才能完成。若要加快这一过程，您可以启动多个 *CLI* 会话并在每一个会话中运行元数据再生命令，为每一个磁盘对同时完成此过程。有关详细信息，请参阅重新生成 M 系列设备 RAID 对的元数据。

1. 为每个磁盘对运行以下 CLI 命令即可启用磁盘对：

```
admin> request system raid add <slot> force no-format
```

例如：

```
admin> request system raid add A1 force no-format
admin> request system raid add A2 force no-format
```

Force 和 **no-format** 是必需的命令参数。**Force** 参数使磁盘对与新设备相关联。**No-format** 参数则防止驱动器的重新格式化，并保留存储在磁盘上的日志。

2. 生成每个磁盘对的元数据。



此步骤可能最多需要 *6* 小时的时间，具体取决于磁盘上的日志数据量。

```
admin> request metadata-regenerate slot <slot_number>
```

例如：

```
admin> request metadata-regenerate slot 1
```

STEP 10 | 在新 M 系列设备上配置本地日志收集器。



对于所有涉及需要序列号的命令的步骤，您必须键入完整的序列号；按下“*Tab*”键即可填写完整的序列号。

切勿在此时启用新 M 系列设备上的磁盘。当您成功迁移日志时，Panorama 会自动启用磁盘。

1. 使用 Panorama Web 界面或使用以下 CLI 命令，将本地日志收集器配置为受管收集器：

```
admin> configure
admin# set log-collector <log-collector_SN> deviceconfig system hostname
 <LC_hostname>
admin# exit
```


© 2019 Palo Alto Networks, Inc.

2. 将更改提交到 Panorama。不可在此时就将更改提交到收集器组。

```
admin> configure
admin# commit
```

3. 核实本地日志收集器已连接上 Panorama，且其磁盘对的状态为“存在/可用”。

```
admin> show log-collector serial-number <log-collector_SN>
```

磁盘对在此阶段的恢复过程中将显示为 Disabled（禁用）。

STEP 11 | 将没有磁盘的日志收集器添加到收集器组。

从此时开始，仅提交在 *Panorama* 和日志收集器上完成迁移过程所需的提交。暂缓进行任何其他更改。

1. 访问新的 M 系列设备的 Panorama CLI。
2. 覆盖 Panorama 限制以允许将没有磁盘的日志收集器添加到收集器组：**request log-migration-set-start**
3. 将更改提交到 Panorama。

```
admin> configure
admin# commit force
```

STEP 12 | 迁移日志。

1. 访问新的 M 系列设备的 Panorama CLI。
2. 将新本地日志收集器添加为收集器组成员，然后将更改提交到 Panorama。

```
admin# set log-collector-group <collector_group_name> logfwd-setting
 collectors <SN_managed_collector>
admin# commit
admin# exit
```

旧的本地日志收集器仍会显示在成员列表中，因为您尚未将其从配置中删除。

3. 对于每一个磁盘对，应将日志迁移到新设备。

```
admin> request log-migration from <old_LC_serial_number> old-disk-pair
 <log_disk_pair> to <new_LC_serial_number> new-disk-pair <log_disk_pair>
```

例如：

```
admin> request log-migration from 003001000010 old-disk-pair A to
 00300100038 new-disk-pair A
```

4. 将更改提交到 Panorama。

```
admin> configure
admin# commit
```

STEP 13 | 重新配置收集器组。

© 2019 Palo Alto Networks, Inc.

1. 登录到 Panorama Web 界面在新的 M 系列设备上，将新日志收集器分配到转发日志的防火墙（**Panorama** > **Collector Groups**（收集器组）> **Device Log Forwarding**（设备日志转发））。在防火墙首选项列表中，向新日志收集器给予与旧日志收集器相同的优先级。

   您不能使用 *CLI* 更改防火墙首选项列表的优先级分配。

2. 访问新的 M 系列设备的 Panorama CLI。
3. 从收集器组中删除旧日志收集器。

```
admin# delete log-collector-group <group_name> logfwd-setting collectors
 <old_LC_serial_number>
```

例如：

```
admin# delete log-collector-group DC-Collector-Group logfwd-setting
 collectors 003001000010
```

4. 从 Panorama 配置中删除旧日志收集器，并将更改提交到 Panorama。

```
admin# delete log-collector <old_LC_serial_number>
admin# commit
admin# exit
```

5. 提交收集器组更改，以使受管防火墙可以将日志发送到新日志收集器。

```
admin> commit-all log-collector-config log-collector-
group <collector_group_name>
```

例如：

```
admin> commit-all log-collector-config log-collector-group DC-Collector-
Group
```

STEP 14 | 在新的日志收集器上生成新密钥。

需要此命令才能将新的日志收集器添加到收集器组，并且只应为要替换的日志收集器的收集器组运行。此步骤会删除现有的 *RSA* 密钥，并允许 *Panorama* 创建新的 *RSA* 密钥。

1. 访问新的 M 系列设备的 Panorama CLI。
2. 删除新的日志收集器上的所有 RSA 密钥：

   ```
   request logdb update-collector-group-after-replacecollector-group
   <collector-group-name>
   ```

   该过程可能需要 10 分钟才能完成。

STEP 15 | 确认收集器组中所有日志收集器的 SearchEngine Status（SearchEngine 状态）为 Active（活动）状态。

在收集器组中的所有日志收集器的 *SearchEngine Status*（*SearchEngine* 状态）变为 *Active*（活动）状态前，请勿继续操作。否则，这将会导致清除替换的日志收集器中的日志。

© 2019 Palo Alto Networks, Inc.

1. 访问新的 M 系列设备的 Panorama CLI。
2. 通过运行以下命令显示日志收集器详细信息：
   - 在所有日志收集器的 Panorama 上：

     show log-collector all

     或者，您可以在每个专用日志收集器上运行以下命令：

     ```
     show log-collector detail
     ```
3. 确认 SearchEngine Status（SearchEngine 状态）为 Active（活动）状态。

```
Redistribution status:       none
```

```
Last commit-all: commit succeeded, current ring version 1
```

```
SearchEngine status:     Active
```

```
md5sum 4e5055a359f7662fab8f8c4f57e24525 updated at 2017/06/14 09:58:19
```

STEP 16 | 在新的日志收集器上，使用新的日志收集器序列号替换以前的日志收集器序列号。

您必须使用新的日志收集器序列号替换旧的日志收集器序列号，以便新的日志收集器不会出现清除问题，从而导致日志收集器无法在必要时从迁移的日志中清除旧数据。

1. 访问日志收集器 CLI。
2. 使用新的日志收集器序列号替换旧的日志收集器序列号：

   request log-migration-update-logger from *<old-log-collector-serial-number>* to *<new-log-collector-serial-number>*

STEP 17 | 设置新的辅助 Panorama 高可用性对端设备。

1. 如果您想要保留旧 M 系列设备 SSD 中的任何日志，请将它们转发到外部目标。
2. 从旧 M 系列设备中移除 RAID 磁盘。
3. 执行新 M 系列设备的初始设置。
4. 将磁盘插入新 M 系列设备。
5. 要将日志从旧 M 系列设备迁移到新 M 系列设备，则重复步骤 7 到 16。
6. 设置 Panorama 高可用性。新 M 系列设备必须具有与您正在更换的高可用性对端设备相同的优先级。
7. 登录到 Panorama Web 界面在主要 HA 对端设备上，单击 **Dashboard**（仪表盘）> **High Availability**（高可用性）> **Sync to peer**（同步到对端设备）以同步 M 系列设备高可用性对端设备的配置。

将日志迁移到高可用性的 Panorama 模式下的新 M 系列设备型号

如果您需要采用与被更换的 M 系列设备完全相同的 M 系列设备更换 Panorama 模式（Panorama 管理服务器）下高可用性 (HA) 配置中部署的 M-600、M-500、 M-200 或 M-100 系列设备，您可以通过将其 RAID 磁盘转移到新 M 系列设备来迁移它之前从防火墙收集的日志。通过移动磁盘，您可以在 M 系列设备发生系统故障后恢复日志。

此迁移程序涵盖以下情况：

- 一台 Panorama 高可用性对端设备具有一个收集器组中的受管收集器（日志收集器）。

© 2019 Palo Alto Networks, Inc.

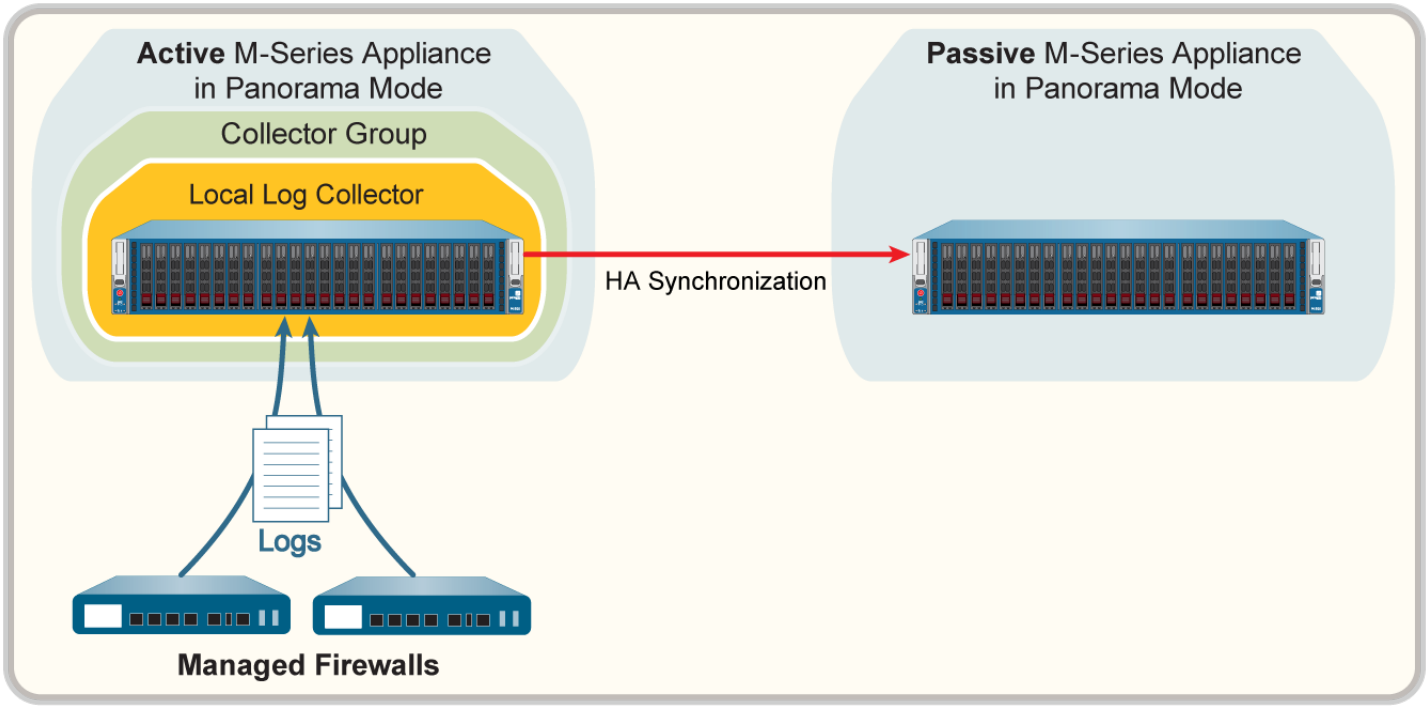


图 **31:** 具有收集器组的 **Panorama HA** 对端设备

- 两台 Panorama 高可用性对端设备都具有属于单个收集器组的受管收集器。有关详细信息，请参阅每个收集器组多个本地日志收集器。
- 两台 Panorama 高可用性对端设备都各有一个收集器，且每一个收集器都已分配到一个单独的收集器组。有关详细信息，请参阅每个收集器组一个本地日志收集器。

STEP 1 | 如果您想要保留旧 M 系列设备 SSD 中的任何日志，请将它们转发到外部目标。

SSD 存储 Panorama 和日志收集器所生成的系统和配置日志。您无法在 M 系列设备之间移动 SSD。

配置从 Panorama 到外部目标的日志转发。

STEP 2 | 从旧 M 系列设备中移除 RAID 磁盘。

1. 按下电源按钮以关闭旧日志收集器，直到系统关闭。
2. 移除磁盘对。有关详细信息，请参阅《M 系列设备硬件参考指南》中的磁盘更换程序。

STEP 3 | 执行新 M 系列设备的初始设置。

1. 将 M 系列设备安装到机架上。有关说明，请参阅《M 系列设备硬件参考指南》。
2. 执行 M 系列设备的初始配置。

   如果旧 *M* 系列设备将 *MGT* 接口以外的接口用于 *Panorama* 服务（如日志收集），则您必须在新 *M* 系列设备的初始配置期间定义这些接口（*Panorama* > *Setup*（设置）> *Interfaces*（接口））。
3. 注册 Panorama。
4. 只有当新 M 系列设备的硬件型号与旧 M 系列设备的硬件型号相同时，才可以按如下步骤购买和激活 Panorama 支持许可证或转移许可证。如果新 M 系列设备的型号与旧 M 系列设备的型号不同，则必须购买新许可证。
   1. 登录到 Palo Alto Networks 客户支持站点。
   2. 选择 **Assets**（资产）选项卡，然后单击 **Spares**（备件）链接。
   3. 单击新 M 系列设备的 Serial Number（序列号）。

© 2019 Palo Alto Networks, Inc.

4. 单击 **Transfer Licenses**（转移许可证）。
5. **Select**（选择）旧 M 系列设备，然后单击 **Submit**（提交）。

5. 激活防火墙管理许可证。如果您是在将日志从 M-100 设备迁移到 M-500 设备，则应输入与迁移许可证相关联的身份验证代码。
6. 安装 Panorama 的内容和软件更新。有关软件版本的重要详细信息，请参阅 Panorama、日志收集器、防火墙和 WildFire 的版本兼容性。
7. 根据需要执行任何其他配置更改。



如果旧 *M* 系列设备将 *MGT* 接口以外的接口用于 *Panorama* 服务（如日志收集），则您必须在新 *M* 系列设备的定义这些接口（*Panorama* > *Setup*（设置）> *Interfaces*（接口））。

8. 设置 Panorama 高可用性。新 M 系列设备必须具有与您正在更换的高可用性对端设备相同的优先级。

STEP 4 | 将磁盘插入新 M 系列设备。有关详细信息，请参阅《M 系列设备硬件参考指南》中的磁盘更换程序。



M-100 设备的磁盘载体与 *M-500* 设备的磁盘载体不兼容。因此，在这些硬件型号之间执行迁移时，必须将每个磁盘从其旧载体上旋下，并在将磁盘插入新设备中之前将磁盘插入新载体。

您必须维持磁盘对的关联。尽管您可以把磁盘对从旧设备上的 A1/A2 插槽置入到新设备上的 B1/B2 插槽，但您必须保持磁盘对处于同一插槽中；否则，Panorama 可能无法成功地恢复数据。

STEP 5 | 如果 M 系列设备是收集器组的一部分，请确认已停用的 M 系列设备序列号仍是正确的收集器组的一部分：

```
debug log-collector-group show name <Log CollectorGroup name>
```

STEP 6 | 准备磁盘进行迁移。



生成每个磁盘对的元数据后，需重新构建索引。因此，根据数据大小，此过程需要较长时间才能完成。若要加快这一过程，您可以启动多个 *CLI* 会话并在每一个会话中运行元数据再生命令，为每一个磁盘对同时完成此过程。有关详细信息，请参阅重新生成 M 系列设备 RAID 对的元数据。

1. 为每个磁盘对运行以下 CLI 命令即可启用磁盘对：

```
admin> request system raid add <slot> force no-format
```

例如：

```
admin> request system raid add A1 force no-format
admin> request system raid add A2 force no-format
```

Force 和 **no-format** 是必需的命令参数。**Force** 参数使磁盘对与新设备相关联。**No-format** 参数则防止驱动器的重新格式化，并保留存储在磁盘上的日志。

2. 生成每个磁盘对的元数据。

```
admin> request metadata-regenerate slot <slot_number>
```

例如：

© 2019 Palo Alto Networks, Inc.

```
admin> request metadata-regenerate slot 1
```

STEP 7 | 在新 M 系列设备上配置本地日志收集器。

对于所有涉及需要序列号的命令的步骤，您必须键入完整的序列号；按下“*Tab*”键即可填写完整的序列号。

切勿在此时启用新 M 系列设备上的磁盘。当您成功迁移日志时，Panorama 会自动启用磁盘。

1. 使用 Panorama Web 界面或使用以下 CLI 命令，将本地日志收集器配置为受管收集器：

```
admin> configure
admin# set log-collector <log-collector_SN> deviceconfig system hostname
 <LC_hostname>
admin# exit
```

2. 将更改提交到 Panorama。不可在此时就将更改提交到收集器组。

```
admin> configure
admin# commit
```

3. 核实本地日志收集器已连接上 Panorama，且其磁盘对的状态为“存在/可用”。

```
admin> show log-collector serial-number <log-collector_SN>
```

磁盘对在此阶段的恢复过程中将显示为 Disabled（禁用）。

STEP 8 | 将没有磁盘的日志收集器添加到收集器组。

从此时开始，仅提交在 *Panorama* 和日志收集器上完成迁移过程所需的提交。暂缓进行任何其他更改。

1. 访问 Panorama CLI。
2. 覆盖 Panorama 限制以允许将没有磁盘的日志收集器添加到收集器组：**request log-migration-set-start**
3. 提交已覆盖的限制：

```
admin> configure
admin# commit force
```

STEP 9 | 迁移日志。

1. 访问 Panorama CLI。
2. 将新本地日志收集器添加为收集器组成员，然后将更改提交到 Panorama。

```
admin# set log-collector-group <collector_group_name> logfwd-setting
 collectors <SN_managed_collector>
admin# commit
admin# exit
```

旧的本地日志收集器仍会显示在成员列表中，因为您尚未将其从配置中删除。

3. 对于每一个磁盘对，应将日志迁移到新设备。

© 2019 Palo Alto Networks, Inc.

```
admin> request log-migration from <old_LC_serial_number> old-disk-pair
 <log_disk_pair> to <new_LC_serial_number> new-disk-pair <log_disk_pair>
```

例如：

```
admin> request log-migration from 003001000010 old-disk-pair A to
 00300100038 new-disk-pair A
```

4. 将更改提交到 Panorama。

```
admin> configure
admin# commit
```

STEP 10 | 重新配置收集器组。

1. 使用 Web 界面，将新日志收集器分配到转发日志的防火墙（**Panorama** > **Collector Groups**（收集器组）> **Device Log Forwarding**（设备日志转发））。在防火墙首选项列表中，向新日志收集器给予与旧日志收集器相同的优先级。

   您不能使用 *CLI* 更改防火墙首选项列表的优先级分配。

2. 从收集器组中删除旧日志收集器。

```
admin# delete log-collector-group <group_name> logfwd-setting collectors
 <old_LC_serial_number>
```

例如：

```
admin# delete log-collector-group DC-Collector-Group logfwd-setting
 collectors 003001000010
```

3. 从 Panorama 配置中删除旧日志收集器，并将更改提交到 Panorama。

```
admin# delete log-collector <old_LC_serial_number>
admin# commit
admin# exit
```

4. 同步 M 系列设备高可用性对端设备的配置。

```
admin> request high-availability sync-to-remote running-config
```

5. 提交收集器组更改，以使受管防火墙可以将日志发送到新日志收集器。

```
admin> commit-all log-collector-config log-collector-
group <collector_group_name>
```

例如：

```
admin> commit-all log-collector-config log-collector-group DC-Collector-
Group
```


© 2019 Palo Alto Networks, Inc.

STEP 11 | 在新的日志收集器上生成新密钥。

需要此命令才能将新的日志收集器添加到收集器组，并且只应为要替换的日志收集器的收集器组运行。此步骤会删除现有的 *RSA* 密钥，并允许 *Panorama* 创建新的 *RSA* 密钥。

1. 访问 Panorama CLI。
2. 删除新的日志收集器上的所有 RSA 密钥：

   request logdb update-collector-group-after-replacecollector-group *<collector-group-name>*

   该过程可能需要 10 分钟才能完成。

STEP 12 | 确认收集器组中所有日志收集器的 SearchEngine Status（SearchEngine 状态）为 Active（活动）状态。

在收集器组中的所有日志收集器的 *SearchEngine Status*（*SearchEngine* 状态）变为 *Active*（活动）状态前，请勿继续操作。否则，这将会导致清除替换的日志收集器中的日志。

1. 访问 Panorama CLI。
2. 通过运行以下命令显示日志收集器详细信息：
   - 在所有日志收集器的 Panorama 上：

     show log-collector all

   或者，您可以在每个专用日志收集器上运行以下命令：

   ```
   show log-collector detail
   ```

3. 确认 SearchEngine Status（SearchEngine 状态）为 Active（活动）状态。

```
Redistribution status:       none
```

```
Last commit-all: commit succeeded, current ring version 1
```

```
SearchEngine status:     Active
```

```
md5sum 4e5055a359f7662fab8f8c4f57e24525 updated at 2017/06/14 09:58:19
```

STEP 13 | 在新的日志收集器上，使用新的日志收集器序列号替换以前的日志收集器序列号。

您必须使用新的日志收集器序列号替换旧的日志收集器序列号，以便新的日志收集器不会出现清除问题，从而导致日志收集器无法在必要时从迁移的日志中清除旧数据。

1. 访问日志收集器 CLI。
2. 使用新的日志收集器序列号替换旧的日志收集器序列号：

   request log-migration-update-logger from *<old-log-collector-serial-number>* to *<new-log-collector-serial-number>*

© 2019 Palo Alto Networks, Inc.

非高可用性 Panorama 出现故障/RMA 时迁移日志收集器

如果未部署在高可用性 (HA) 配置中的 Panorama 管理服务器发生系统故障，则使用此程序在替用 Panorama 上恢复配置，并恢复对受管专用日志收集器上日志的访问权限。允许的迁移情境因 Panorama 管理服务器型号而异：

旧/故障 Panorama	新/更换 Panorama
Panorama 虚拟设备	• Panorama 虚拟设备 • M-200 设备 • M-500 设备 • M-600 设备
M-100 设备	• Panorama 虚拟设备 • M-200 设备 • M-500 设备 • M-600 设备
M-500 设备	• Panorama 虚拟设备 • M-200 设备 • M-500 设备 • M-600 设备

Panorama 会保留映射了专用日志收集器存储日志时所用分段和分区的环形文件。Panorama 模式下的 M 系列设备会将环形文件存储在其内部 SSD 中；而 Panorama 虚拟设备则会将环形文件保存在其内部磁盘中。当系统故障发生时，非高可用性 Panorama 无法自动恢复环形文件。因此，当您更换 Panorama 时，您必须恢复用于访问专用日志收集器上日志的环形文件。

此过程要求在系统故障发生之前，备份并导出 Panorama 配置。

Palo Alto Networks 建议您在高可用性配置中部署 *Panorama*。主动 *Panorama* 对端设备会自动将环形文件同步到高可用性配置中的被动对端设备，即使您必须更换一个对端设备，也能由此保持对专用日志收集器上日志的访问权限。

STEP 1 | 执行新 Panorama 设备的初始设置。

1. 根据您的需求设置 M 系列设备 或设置 Panorama 虚拟设备。如果您正在设置新的 M 系列设备，有关如何将新的 M 系列设备安装到机架上的说明，请参阅 《M 系列设备硬件参考指南》 。
2. 执行 M 系列设备的初始配置或执行 Panorama 虚拟设备的初始配置。

   如果旧 *M* 系列设备将 *MGT* 接口以外的接口用于 *Panorama* 服务（如日志收集），则您必须在新 *M* 系列设备的初始配置期间定义这些接口（*Panorama* > *Setup*（设置）> *Interfaces*（接口））。*Panorama* 虚拟设备不支持 *MGT* 接口以外的接口。
3. 注册 Panorama。
4. 只有当新 Panorama 设备与旧设备的型号相同时，才可以按如下步骤转移许可证。否则，您必须购买新许可证。
   1. 登录到 Palo Alto Networks 客户支持站点。
   2. 选择 **Assets**（资产）选项卡，然后单击 **Spares**（备件）链接。
   3. 单击新 M 系列设备的 Serial Number（序列号）。
   4. 单击 **Transfer Licenses**（转移许可证）。
   5. **Select**（选择）旧设备，然后单击 **Submit**（提交）。

© 2019 Palo Alto Networks, Inc.

5. 激活 Panorama 支持许可证。
6. 激活防火墙管理许可证。
7. 安装 Panorama 的内容和软件更新。

M-500 设备要求使用 *Panorama 7.0* 或更高版本。*M-200* 和 *M-600* 设备要求使用 *Panorama 8.1*。有关软件版本的重要详细信息，请参阅 Panorama、日志收集器、防火墙和 WildFire 的版本兼容性。

STEP 2 | 将配置从旧 Panorama 恢复到替用 Panorama。

1. 登录到新 Panorama，然后选择 **Panorama** > **Setup**（设置）> **Operations**（操作）。
2. 单击 **Import named Panorama configuration snapshot**（导入已命名 **Panorama** 配置快照），**Browse**（浏览）到备份配置文件，然后单击 **OK**（确定）。
3. 单击 **Load named Panorama configuration snapshot**（加载已命名的 **Panorama** 配置快照），选择您导入的文件 **Name**（名称），单击 **OK**（确定）。

要替换 *RMA Panorama*，请务必在您加载已命名的 *Panorama* 配置快照时 *Retain Rule UUIDs*（保留规则 *UUID*）。如果未选择此选项，*Panorama* 将从配置快照中删除先前所有规则 *UUID*，并将新 *UUID* 分配给 *Panorama* 上的规则，这意味着与先前 *UUID* 相关的信息将不会被保留，例如，策略规则点击数。

4. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。
5. 选择 **Panorama** > **Managed Collectors**（Panorama > 受管收集器），然后核实“Connected（已连接）”列显示了专用日志收集器的复选标记。

   如果专用日志收集器并未显示，您必须按下一步所述，重新配置它及其收集器组。否则，请跳转至下一步获取环形文件，以恢复对专用日志收集器所存储日志的访问权限。。

STEP 3 | 如果 Panorama 缺失专用日志收集器和收集器组，则重新配置它们。

1. 访问专用日志收集器的 CLI，并输入以下命令以显示其收集器组的名称。
   1. 输入命令：

```
> request fetch ring from log-collector <serial_number>
```

   将显示以下错误：

```
Server error: Failed to fetch ring info from <serial_number>
```

   2. 输入命令：

```
> less mp-log ms.log
```

   将显示以下错误：

```
Dec04 11:07:08 Error:
 pan_cms_convert_resp_ring_to_file(pan_ops_cms.c:3719): Current
 configuration does not contain group CA-Collector-Group
```

   在本例中，此错误消息表明，缺失收集器组的名称为 CA-Collector-Group。
2. 配置收集器组，然后将专用日志收集器分配给它。

```
> configure
# set log-collector-group <collector-group-name>
```


© 2019 Palo Alto Networks, Inc.

```
# set log-collector-group <collector-group-name> logfwd-setting
collector <serial-number>
```

3. 将更改提交到 Panorama，而不是收集器组。

```
# commit
# exit
```

STEP 4 | 获取环形文件，以恢复对专用日志收集器所存储日志的访问权限。

1. 访问新 Panorama 的 CLI。
2. 获取环形文件：

```
> request fetch ring from log-collector <serial-number>
```

例如：

```
> request fetch ring from log-collector 009201000343
```



如果您不知道专用日志收集器的序列号，请登录到其 *CLI*，然后输入操作命令 ***show system info***。

3. 将更改提交到收集器组。

```
> commit-all log-collector-config log-collector-group <collector-group-
name>
```

重新生成 M 系列设备 RAID 对的元数据

当 M-600、M-500 或 M-200 设备发生系统故障且您需要以物理方式将磁盘从一台设备移动到另一台设备时，必须重新生成元数据。需要使用元数据才能找到磁盘上的日志；当用户发出日志查询时，此查询需查阅此元数据才能访问请求的日志数据。

对于 M 系列设备中的每一个已配置 RAID 磁盘对，您必须访问设备 CLI 并执行以下命令，以重新生成元数据：

```
> request metadata-regenerate slot <slot_number>
```

例如：

```
> request metadata-regenerate slot 1
```

RAID 磁盘的大小决定了元数据的重新生成需要花费多长时间。平均而言，每 100 GB 需要花费 1 小时。当您运行此命令时，CLI 会话将会锁定，直至此命令完全执行完毕。您可以使用多个 CLI 会话以节省时间。例如，若要更换总日志数据大小为 4TB 的 4 个 1TB 驱动器 RAID 磁盘对，应启动 4 个 CLI 会话，并在每个会话中运行命令，以在大约 10 小时之内为所有磁盘对/插槽同时重新生成元数据。

在重新生成元数据时，这些磁盘所属的收集器组不可用，而且磁盘对也不可用于任何记录或报告操作（写/查询）。但是，您可以执行其他任务，例如处理新防火墙的连接或在受管防火墙上管理配置更改。Panorama 管理的以及不构成此 RMA 过程一部分的所有其他收集器组可以照常执行分配的记录和报告功能。

© 2019 Palo Alto Networks, Inc.

查看日志查询作业

您可以查看日志查询作业以调查并更好地了解为什么查询日志数据花费的时间超出预期。首先，必须先显示在 Panorama 上运行的所有日志查询作业。识别需要调查的日志查询作业后，使用作业 ID 查看有关查询的详情，以更好地了解日志查询为什么会出现问题。在 Panorama 上查询日志数据时，随着执行新的日志查询作业，详细的作业 ID 信息将被覆盖。

STEP 1 | 登录到 Panorama 命令行界面。

STEP 2 | 查看 Panorama 上执行的日志查询作业。

CLI 输出包括有关每个已执行日志查询的一般信息，例如作业 ID、运行查询的时间、查询状态、查询的日志数据库、查询的日志数、查询返回结果所花费的时间（以毫秒为单位）、执行查询的管理员以及应用至查询的所有筛选器。

```
admin@Panorama> show query jobs
```

```
admin@bingdot34> show query jobs

ID        Enqueue Time         State       Database  nlogs     Runtime(ms)    Us
er            Filter
------------------------------------------------------------------------------
------------------------------------------------------------------------
42        2020/01/02 14:35:46  COMPLETE    threat    110       166.27         ad
min           ((((receive_time leq 'now')) and (((subtype eq 'file')) or ((subty
pe eq 'data')))) and ((receive_time in 'last-hour')))


41        2020/01/02 14:35:46  COMPLETE    system    110       163.84         ad
min           (((receive_time leq now)) and (receive_time in last-hour))

40        2020/01/02 14:35:46  COMPLETE    config    110       158.23         ad
min           (((receive_time leq now)) and (receive_time in last-hour))

39        2020/01/02 14:35:36  COMPLETE    config    110       162.58         ad
min           (((receive_time leq now)) and (receive_time in last-hour))

38        2020/01/02 14:35:36  COMPLETE    system    110       172.68         ad
min           (((receive_time leq now)) and (receive_time in last-hour))

37        2020/01/02 14:35:36  COMPLETE    threat    110       188.80         ad
min           ((((receive_time leq 'now')) and (((subtype eq 'file')) or ((subty
pe eq 'data')))) and ((receive_time in 'last-hour')))
```

STEP 3 | 使用作业 ID 查看有关特定作业的详细日志查询信息。

```
admin@Panorama> show query jobid <Job ID>
```

```
admin@bingdot34> show query jobid 42

Serial          ID        State     Num Req   Num Proc  RTT(Max)      Avg Recs/R
TTSoftware Ver    CG                                Last Update Time
------------------------------------------------------------------------------
------------------------------------------------------------------------
LOGDB           42        DONE      110       0         0.00      0.00
9.2.0           LOCAL                             2020/01/02 14:35:46

PODABCD12       42        FAILED    110       0         0.00      0.00
9.2.0           PODABCD12                         2020/01/02 14:35:46
```


© 2019 Palo Alto Networks, Inc.

替换 RMA 防火墙

为尽量减少在退货授权 (RMA) 上的受管防火墙中恢复配置时的工作，请将旧防火墙的序列号替换为 Panorama 上的新防火墙的序列号。为了随后可以在替用防火墙上恢复配置，您可以导入先前生成并从防火墙导出的防火墙状态，也可以使用 Panorama 为运行 PAN-OS v5.0 和更高版本的受管防火墙生成局部设备状态。通过替换序列号和导入防火墙状态，您可以恢复使用 Panorama 对设备的管理。

- 为防火墙生成局部设备状态
- 开始 RMA 防火墙替换之前
- 替换后还原防火墙配置

为防火墙生成局部设备状态

当您使用 Panorama 生成局部设备状态时，它会复制受管防火墙的配置，大型 VPN (LSVPN) 设置有一些例外。您可以通过防火墙配置的两个方面创建局部设备状态：

- Panorama 管理的集中配置 — Panorama 维护推送到防火墙的共享策略规则和模板的快照。
- 防火墙上的本地配置 — 在防火墙上提交配置更改后，防火墙会将其本地配置文件的一个副本发送到 Panorama。Panorama 会保存此文件并用其来编译局部设备状态包。



在 *LSVPN* 设置中，您在 *Panorama* 上生成的局部设备状态包与您从防火墙导出的版本不同（选择 *Device* > *Setup* > *Operations*（设备 > 设置 > 操作），然后单击 *Export device state*（导出设备状态））。如果手动运行设备状态导出或者安排了 *XML API* 脚本将文件导出到远程服务器，则可以在设备替换工作流程中使用导出的设备状态。

如果没有导出设备状态，则您在此替换工作流程中生成的设备状态将不会包含在动态配置信息，例如证书详细信息和注册的防火墙，这些都是恢复用作 *LSVPN* 门户网站的防火墙功能的完整配置时所必需的。有关详细信息，请参阅开始 RMA 防火墙替换之前。

Panorama 不会保存设备状态；您可以根据请求在替换后还原防火墙配置中使用列出的 CLI 命令生成该状态。

开始 RMA 防火墙替换之前

- 您将替换的防火墙必须运行的是 PAN-OS 5.0.4 或更新版本。对于运行较低 PAN-OS 版本的防火墙，Panorama 无法生成 *device state*（设备状态）。
- 请记录关于您将替换的防火墙的以下详细信息：
  - 序列号 — 您必须在 Palo Alto Networks 客户支持网站上输入序列号才能将许可证从旧防火墙转移到替用防火墙。您还可能需要在 Panorama 上输入该信息，以便将针对旧序列号的所有引用替换为替用防火墙的新序列号。
  - （推荐）**PAN-OS** 版本和内容数据库版本 — 安装相同的软件和内容数据库版本，包括 URL 数据库供应商可让您在替用防火墙上创建相同的状态。如果决定安装最新版本的内容数据库，则需要注意其中的差异，因为数据库进行了更新和补充。要确定防火墙上安装的版本，请访问 Panorama 上存储的防火墙系统日志。
- 准备要部署的替用防火墙。在导入设备状态包和恢复配置之前，必须：
  - 验证替用防火墙是否具有与旧防火墙相同的型号，并且支持相似的操作功能。考虑以下操作功能：是否替用防火墙必须有多个虚拟系统、支持巨帧、或在 CC 或 FIPS 模式下运行？
  - 配置网络访问，传输许可证并安装适当的 PAN-OS 和内容数据库版本。
- 必须使用 Panorama CLI 来完成这个防火墙替换过程，所以您的管理员账户必须有超级用户或 Panorama 管理员用户角色。
- 如果您具有 LSVPN 配置并且要替换部署为卫星或 LSVPN 门户网站的 Palo Alto Networks 防火墙，恢复 LSVPN 连接性时所需的动态配置信息在恢复 Panorama 上生成的局部设备状态时不可用。如果您根据建

© 2019 Palo Alto Networks, Inc.

议频繁生成和导出 LSVPN 配置中防火墙的设备状态，请使用您先前从防火墙本身导出的设备状态，而不是 Panorama 上生成的设备状态。

如果没有从防火墙手动导出设备状态并且需要在 Panorama 上生成局部设备状态，则所缺少的动态配置将会以如下方式影响防火墙替换过程：

- 如果要替换的防火墙是 **GlobalProtect** 门户，并且该设备使用卫星的序列号进行了显式配置（**Network** > **GlobalProtect** > **Portals** > **Satellite Configuration**（网络 > GlobalProtect > 门户网站 > 卫星配置）），则在恢复防火墙配置时，尽管动态配置已经丢失，但门户网站防火墙仍然可以成功验证卫星。成功认证之后将会填充动态配置信息，LSVPN 连接也将重新恢复。
- 如果要更换卫星防火墙，卫星防火墙将无法连接和验证到门户网站。这种连接失败之所以会发生，要么是因为防火墙上未显式配置序列号（**Network** > **GlobalProtect** > **Portals** > **Satellite Configuration**（网络 > GlobalProtect > 门户网站 > 卫星配置）），或者是因为尽管显式配置了序列号，但所替换的防火墙的序列号与旧防火墙的序列号不匹配。要在导入设备状态包之后恢复连接，卫星设备管理员必须登录到防火墙并输入用于验证到门户网站的凭据（用户名和密码）。进行此验证后，门户网站上将会生成 LSVPN 连接所需的动态配置。

但是，如果防火墙在高可用性配置中进行了配置，则在恢复配置之后，防火墙将会自动同步正在运行的配置及其对端设备，并获得无缝运行所需的最新动态配置。

替换后还原防火墙配置

要在新防火墙上还原防火墙配置，您将先在新防火墙上执行初始配置，包括设置操作模式，以及升级 PAN-OS 软件与内容发布版本以匹配旧防火墙上安装的的软件和内容。然后，您将从 Panorama 导出旧防火墙的设备状态，将它导入新防火墙。最后，您将返回 Panorama 验证新防火墙是否已连接，然后将此防火墙与 Panorama 同步。

STEP 1 | 在新防火墙上执行初始配置并验证网络连接。

使用串行端口连接或安全外壳 (SSH) 连接来添加 IP 地址、DNS 服务器 IP 地址，并验证新防火墙可以访问 Palo Alto Networks 更新服务器。

STEP 2 | （可选）在新防火墙上设置操作模式，使其与旧防火墙上的操作模式匹配。

此任务需要串行端口连接。

1. 输入以下 CLI 命令以访问防火墙的维护模式：

```
> debug system maintenance-mode
```

2. 对于操作模式，从主菜单中选择 **Set FIPS Mode**（设置 FIPS 模式）或 **Set CCEAL 4 Mode**（设置 CCEAL 4 模式）。

STEP 3 | 在新防火墙上检索许可证。

输入以下命令来检索许可证：

```
> request license fetch
```

STEP 4 | （可选）将新防火墙的操作状态与旧防火墙的操作状态进行匹配。例如，针对曾经支持多 vsys 功能的防火墙启用多虚拟系统（多 vsys）功能。

输入与防火墙设置有关的命令：

```
> set system setting multi-vsys on
> set system setting jumbo-frame on
```


© 2019 Palo Alto Networks, Inc.

STEP 5 | 在新防火墙上升级 PAN-OS 版本。

必须升级到旧防火墙上安装的 PAN-OS 版本。必须升级内容更新版本到旧防火墙上安装的版本或更高版本。

输入以下命令：

1. 要升级内容发布版本：

```
> request content upgrade download latest
> request content upgrade install version latest
```

2. 要升级防病毒发布版本：

```
> request anti-virus upgrade download latest
> request anti-virus upgrade install version latest
```

3. 要升级 PAN-OS 软件版本：

```
> request system software download version <version>
> request system software install version <version>
```

STEP 6 | 前往 Panorama CLI，使用安全复制 (SCP) 或 TFTP 将设备状态包从旧防火墙导出到计算机（在 Web 界面中无法执行此操作）。



如果您从防火墙手动导出了设备状态，可跳过此步骤。

导出命令会以 tar 打包文件格式生成设备状态包，并将其导出到指定的位置。此设备状态不包含 LSVPN 动态配置（卫星信息和证书详细信息）。

输入以下任一命令：

```
> scp export device-state device <old serial#> to <login> @ <serverIP>:
 <path>
```

或者

```
> tftp export device-state device <old serial#> to <login> @ <serverIP>:
 <path>
```

STEP 7 | 使用 Panorama 上的新替用防火墙的序列号来替代旧防火墙的序列号。

通过替换 Panorama 上的序列号，在恢复防火墙上的配置之后，新防火墙将可以连接到 Panorama。

1. 在操作模式下输入以下命令：

```
> replace device old <old SN#> new <new SN#>
```

2. 进入配置模式，并提交更改。

```
> configure
# commit
```

3. 退出配置模式。

© 2019 Palo Alto Networks, Inc.

```
# exit
```

STEP 8 | 在新防火墙上，导入设备状态并提交更改。

1. 访问新防火墙的 Web 界面。
2. 选择 **Device** > **Setup** > **Operations**（设备 > 设置 > 操作）并单击“Configuration Management（配置管理）”部分的 **Import Device State**（导入设备状态）链接。
3. 浏览并找到文件，然后单击 **OK**（确定）。
4. 将更改 **Commit**（提交）到防火墙上正在运行的配置。

STEP 9 | 使用 Panorama 核实是否已成功地恢复了防火墙配置。

1. 访问 Panorama Web 接口并选择 **Panorama** > **Managed Devices**（受管设备）。
2. 核实新防火墙的 Connected（已连接）列具有复选标记。

STEP 10 | 将防火墙与 Panorama 同步。

1. 访问 Panorama Web 界面，选择 Push Scope（推送范围）中的 **Commit**（提交） > **Commit and Push**（提交并推送）和 **Edit Selections**（编辑选择）。
2. 选择 **Device Groups**（设备组），选择包含防火墙的设备组，然后选择 **Include Device and Network Templates**（包含设备和网络模板）。
3. 选择 **Collector Groups**（收集器组），然后选择包含防火墙的收集器组。
4. 单击 **OK**（确定）保存对推送范围所作的更改。
5. **Commit and Push**（提交并推送）更改。



如果您需要针对安装新防火墙之后旧防火墙仍在运行的这段时间生成报告，您必须为每个防火墙序列号生成单独的查询，因为在 *Panorama* 上替换序列号并不会覆盖日志中的信息。

© 2019 Palo Alto Networks, Inc.

排除提交故障

如果 Panorama 发生提交或推送操作故障，请检查以下状况：

症状	条件	解决方案
模板或设备组推送故障	防火墙上已禁用从 Panorama 接收模板和设备组配置更改这一功能。	访问防火墙 Web 界面，选择 **Device**（设备）> **Setup**（设置），编辑 Panorama Settings（Panorama 设置），然后单击 **Enable Device and Network Template**（启用设备和网络模板）和 **Enable Panorama Policy and Objects**（启用 **Panorama** 策略和对象）。
Panorama 提交故障或模板、设备组或收集器组推送故障	Panorama 管理服务器所具有的软件版本早于其管理的专用日志收集器或防火墙所具有的版本。	升级 Panorama 管理服务器，使其软件版本与受管防火墙、日志收集器、WildFire 设备和设备群集的软件版本相同或者高于后者。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。

© 2019 Palo Alto Networks, Inc.

排除注册或序列号错误

在 M-600、M-500 或 M-200 设备上，如果 **Panorama** > **Support**（支持）页面不显示支持许可证详情，或即使是在您注册 Panorama 之后，**Panorama** > **Setup**（设置）> **Management**（管理）页面仍对 **Serial Number**（序列号）显示 Unknown（未知），则请执行以下步骤：

STEP 1 | 记录下您下达 Panorama 购买订单时， Palo Alto Network 发送给您的订单执行电子邮件中提供的 Panorama 序列号。

STEP 2 | 选择 **Panorama** > **Setup** > **Management**（Panorama > 设置 > 管理），然后编辑“General Settings（常规设置）”。

STEP 3 | 输入 **Serial Number**（序列号），然后单击 **OK**（确定）。

STEP 4 | 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

© 2019 Palo Alto Networks, Inc.

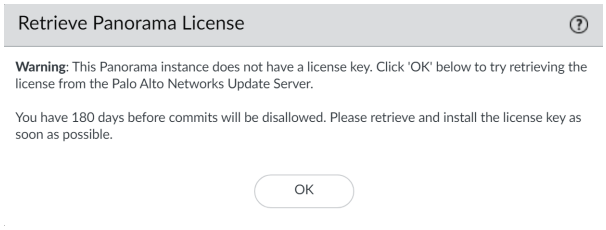
排除报告错误

如果 Panorama 未能生成报告，或者报告缺失预期的数据，则其内容版本（例如，应用程序数据库）可能与受管收集器和防火墙上的内容版本并不相同。Panorama 上的内容版本必须与受管收集器和防火墙上的内容版本相同，或者低于后者。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。

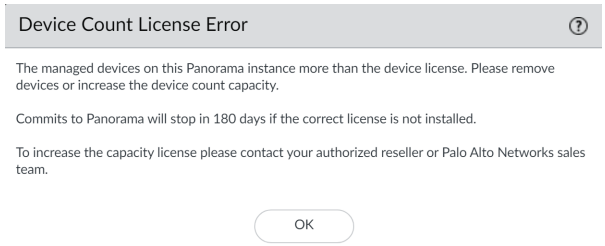
© 2019 Palo Alto Networks, Inc.

排除设备管理许可证错误

更新到 PAN-OS 8.1 后，Panorama 虚拟设备将检查是否已成功安装设备管理许可证。如果尚未成功安装设备管理许可证，或 Panorama 虚拟设备管理的防火墙数量超出设备管理许可证限制，则必须在 180 天内安装有效的设备管理许可证。如果未安装有效的设备管理许可证，则每次您登录到 Panorama Web 界面时均会显示以下警告：



如果 Panorama 虚拟设备管理的防火墙数量超出设备管理许可证限制，则每次您登陆到 Panorama Web 界面时均会显示以下警告：



要解决这些问题，请安装有效的设备管理许可证：

STEP 1 | 要购买适当的设备管理许可证，请联系您的 Palo Alto Networks 销售代表或授权分销商。

STEP 2 | 登录到 Panorama Web 界面。

STEP 3 | 根据 Panorama 虚拟设备是在线或离线来激活/检索设备管理许可证。

- 在 Panorama 虚拟设备连接到互联网时激活/检索防火墙管理许可证。
- 在 Panorama 虚拟设备未连接到互联网时激活/检索防火墙管理许可证。

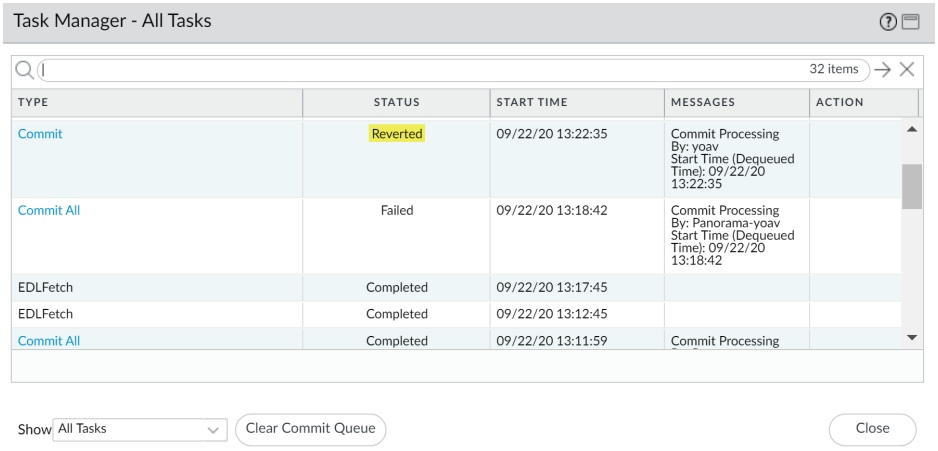
© 2019 Palo Alto Networks, Inc.

排除自动恢复防火墙配置问题

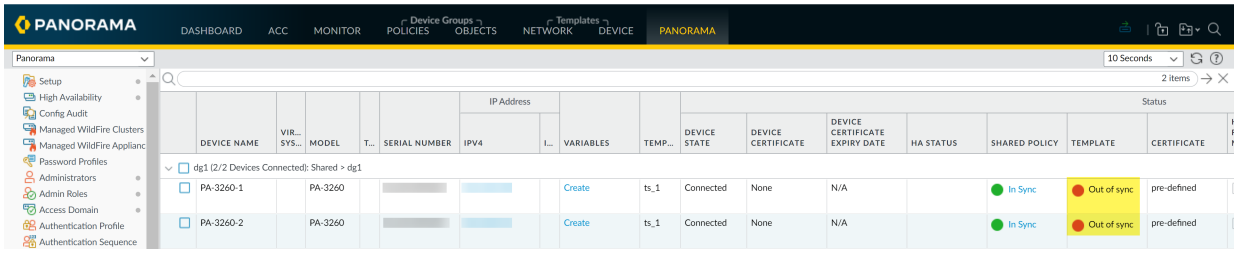
如果您的受管防火墙会因导致 Panorama™ 管理服务器与防火墙之间连接中断的配置更改而自动恢复其配置，则您可以对不同步的防火墙进行故障排除，以确定已实施哪些更改并确定最后配置推送了哪些内容导致防火墙恢复其配置。

STEP 1 | 验证受管防火墙是否自动恢复到最后运行的配置。

- 在防火墙上
  1. 启动防火墙 Web 界面。
  2. 单击 **Tasks**（任务）（Web 界面的右下角）。
  3. 验证最后一次提交操作（从 Panorama 推送或本地提交）是否显示 `Reverted`（已恢复）状态。

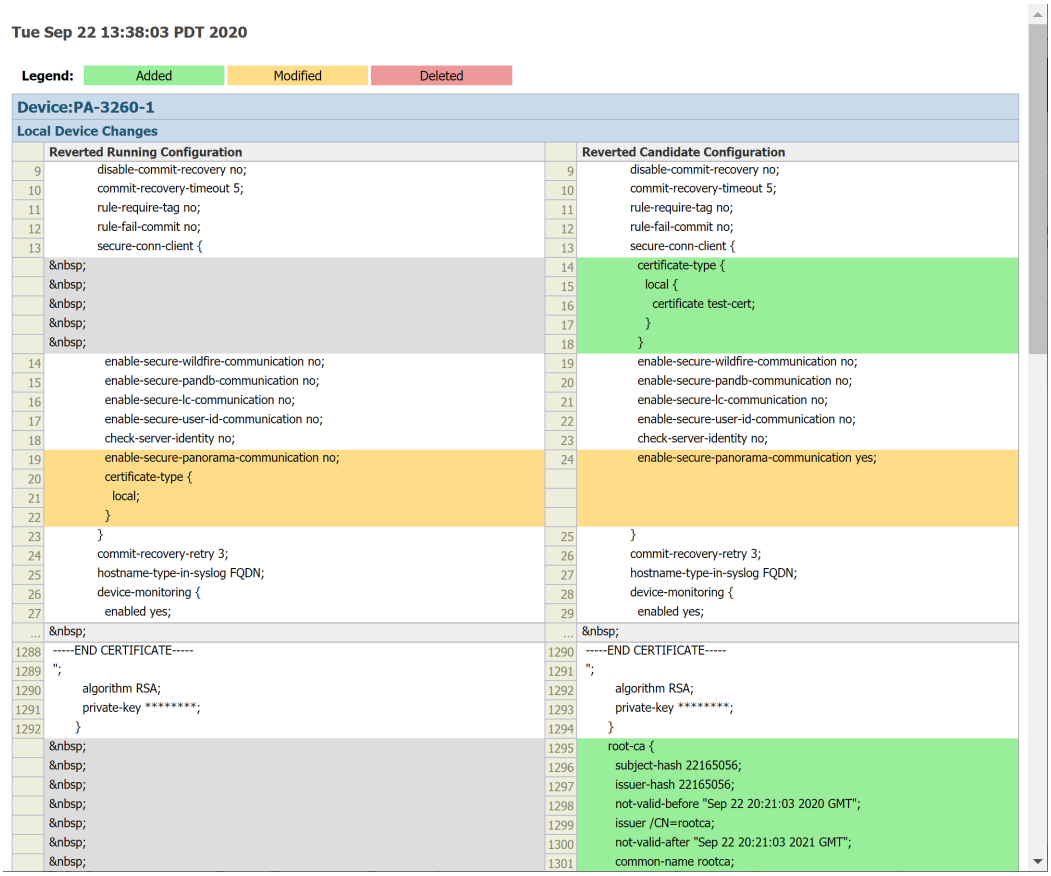


- 在 Panorama 上
  1. 登录到 Panorama Web 界面。
  2. 选择 **Panorama** > **Managed Devices**（受管设备）> **Summary**（摘要）。
  3. 查看共享策略和模板同步状态。如果您最近从 Panorama 推送了配置到受管防火墙并且被恢复，则共享策略或模板会显示为 `Out of Sync`（不同步）（取决于所进行的配置更改）。



STEP 2 | 在受管防火墙的 Last Merged Diff（最后合并差异）列中，显示最后合并配置差异（ ）以将当前运行的配置与恢复的配置进行比较。在本示例中，从 Panorama 推送的策略规则拒绝受管防火墙与 Panorama 之间的所有流量，这导致防火墙配置自动恢复。

© 2019 Palo Alto Networks, Inc.



Tue Sep 22 13:38:03 PDT 2020

Legend: Added Modified Deleted

Device:PA-3260-1

Local Device Changes

	Reverted Running Configuration		Reverted Candidate Configuration
9	disable-commit-recovery no;	9	disable-commit-recovery no;
10	commit-recovery-timeout 5;	10	commit-recovery-timeout 5;
11	rule-require-tag no;	11	rule-require-tag no;
12	rule-fail-commit no;	12	rule-fail-commit no;
13	secure-conn-client {	13	secure-conn-client {
		14	certificate-type {
		15	local {
		16	certificate test-cert;
		17	}
		18	}
14	enable-secure-wildfire-communication no;	19	enable-secure-wildfire-communication no;
15	enable-secure-pandb-communication no;	20	enable-secure-pandb-communication no;
16	enable-secure-lc-communication no;	21	enable-secure-lc-communication no;
17	enable-secure-user-id-communication no;	22	enable-secure-user-id-communication no;
18	check-server-identity no;	23	check-server-identity no;
19	enable-secure-panorama-communication no;	24	enable-secure-panorama-communication yes;
20	certificate-type {		
21	local;		
22	}		
23	}	25	}
24	commit-recovery-retry 3;	26	commit-recovery-retry 3;
25	hostname-type-in-syslog FQDN;	27	hostname-type-in-syslog FQDN;
26	device-monitoring {	28	device-monitoring {
27	enabled yes;	29	enabled yes;
...		...	
1288	-----END CERTIFICATE-----	1290	-----END CERTIFICATE-----
1289	";	1291	";
1290	algorithm RSA;	1292	algorithm RSA;
1291	private-key ********;	1293	private-key ********;
1292	}	1294	}
		1295	root-ca {
		1296	subject-hash 22165056;
		1297	issuer-hash 22165056;
		1298	not-valid-before "Sep 22 20:21:03 2020 GMT";
		1299	issuer /CN=rootca;
		1300	not-valid-after "Sep 22 20:21:03 2021 GMT";
		1301	common-name rootca;

STEP 3 | 在重新推送配置之前，请按需修改配置对象，以确保不会中断受管防火墙与 Panorama 之间的连接。

© 2019 Palo Alto Networks, Inc.

在关闭 Panorama HA 对等设备时完成内容更新

如果在 Panorama™ 处于高可用性 (HA) 配置时将内容更新部署到受管设备，Panorama 会均衡 HA 对等设备之间的内容更新工作，以减少每个 Panorama 上的负载。如果 HA 对等设备在内容更新时变得无法访问，对于通常由宕机的 HA 对等设备推送内容更新的受管设备，内容更新作业将会失败。计划和手动内容更新时会出现这种情况。要完成内容更新，必须手动将内容更新推送到这些受管设备，

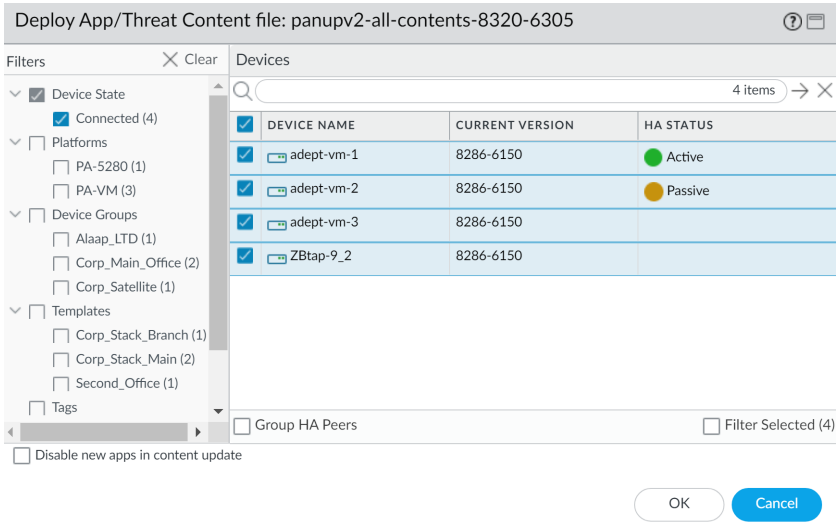
STEP 1 | 登录到 Panorama 命令行界面并禁用内容更新的负载均衡：

```
admin> set dlsrvr distribute no
```

STEP 2 | 登录到 Panorama Web 界面。

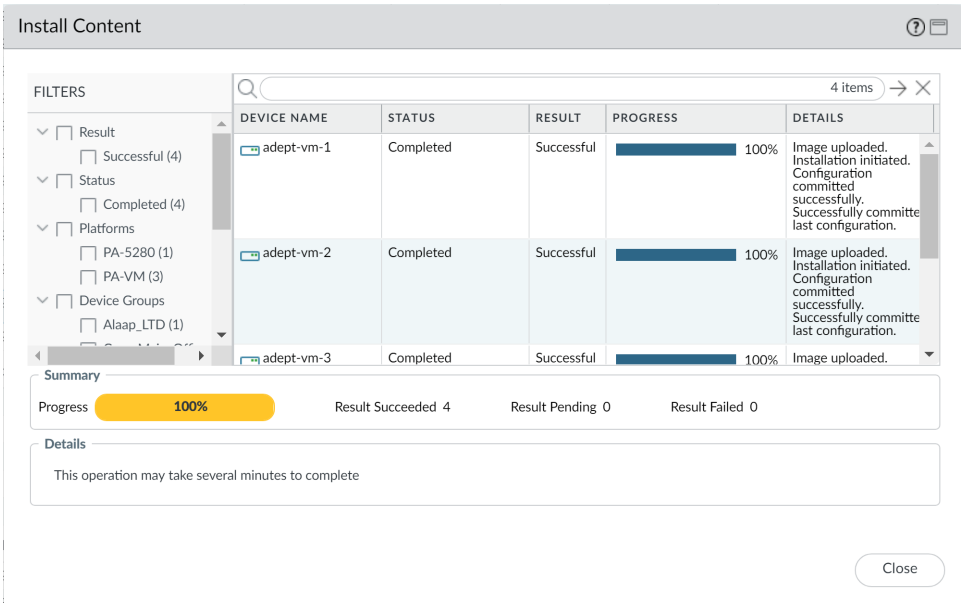
STEP 3 | 选择 **Panorama** > **Device Deployment** > **Dynamic Updates**（Panorama > 设备部署 > 动态更新），然后 **Install**（安装）动态更新。

STEP 4 | 选择内容更新失败的受管设备，并单击 **OK**（确定）。



STEP 5 | 检查内容更新是否被成功推送到选定的受管设备，

© 2019 Palo Alto Networks, Inc.



STEP 6 | 登录到 Panorama 命令行界面并启用内容更新的负载均衡：

```
admin> set dlsrvr distribute yes
```


© 2019 Palo Alto Networks, Inc.

查看任务成功或失败状态

单击 Panorama Web 接口右下角的任务管理器图标 

可查看任务是否成功。任务管理器还会显示一条可帮助调试问题的详细消息。有关详细信息，请参阅使用 Panorama 任务管理器。

© 2019 Palo Alto Networks, Inc.

测试受管设备的策略匹配和连接

成功将设备组和模板堆栈配置推送到防火墙后，日志收集器和 WF-500 设备将测试正确的流量是否与推送到受管设备的策略规则匹配，且您的防火墙是否可以成功连接到所有适当的网络资源。

- 排除策略规则流量匹配问题
- 排除网络资源连接问题

排除策略规则流量匹配问题

要对受管防火墙执行策略匹配测试，请测试受管设备的策略规则配置，确保正在运行的配置可通过允许和拒绝正确的流量来适当地保护您的网络。与已配置规则匹配的流量结果生成后，您可以 **Export to PDF**（导出至 **PDF**），以进行审核。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 选择 **Panorama** > **Managed Devices**（受管设备）> **Troubleshooting**（故障排除）以执行策略匹配。

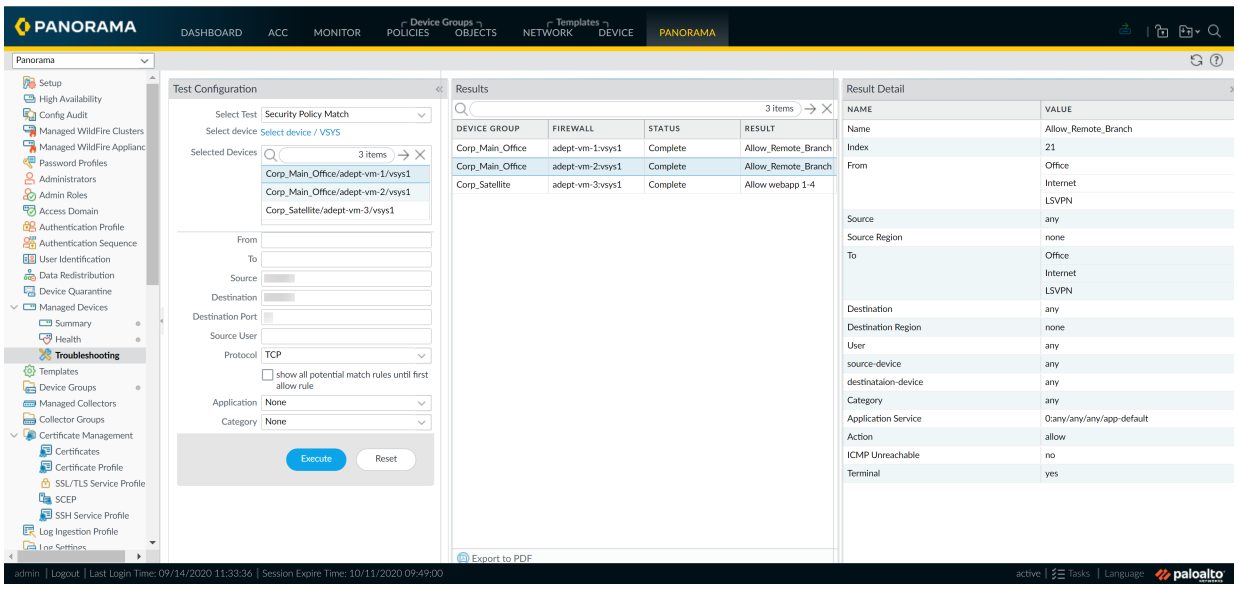
此外，您还可以通过 *Policies*（策略）选项卡运行策略匹配测试。

STEP 3 | 输入所需的信息，以执行策略匹配测试。在本示例中，执行的是安全策略匹配测试。

1. 从 **Select Test**（选择测试）下拉列表中选择 **Security Policy Match**（安全策略匹配）。
2. **Select device/VSYS**（选择设备/VSYS），并选择要进行测试的受管防火墙。
3. 输入流量的源 IP 地址。
4. 输入流量目标设备的目标 IP 地址。
5. 输入流量使用的协议 IP。
6. 必要时，输入安全策略规则测试所需的任何其他信息。

STEP 4 | **Execute**（执行）安全策略匹配测试。

STEP 5 | 选择安全策略匹配结果，以查看与测试标准匹配的策略规则。



© 2019 Palo Alto Networks, Inc.

排除网络资源连接问题

对受管防火墙执行连接测试，确保您的受管设备已连接到所有适当的网络资源。测试受管设备的设备配置，确保使用中的配置能正确保护您的网络（允许您验证这些推送到受管设备的配置仍允许这些设备连接到日志收集器、已配置的外部动态列表、以及 Palo Alto Networks 更新服务器等资源）。此外，您还可以执行路由、WildFire®、威胁库、ping、以及 traceroute 连接测试，以验证 Panorama™ 和受管设备是否可以访问对网络操作和安全至关重要的任何外部网络资源。结果生成后，您可以 **Export to PDF**（导出至 **PDF**），以进行审核。

Ping 连接测试仅在运行 *PAN-OS 9.0* 或更高版本的防火墙中受支持。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 选择 **Panorama** > **Managed Devices**（受管设备）> **Troubleshooting**（故障排除）以执行连接测试。

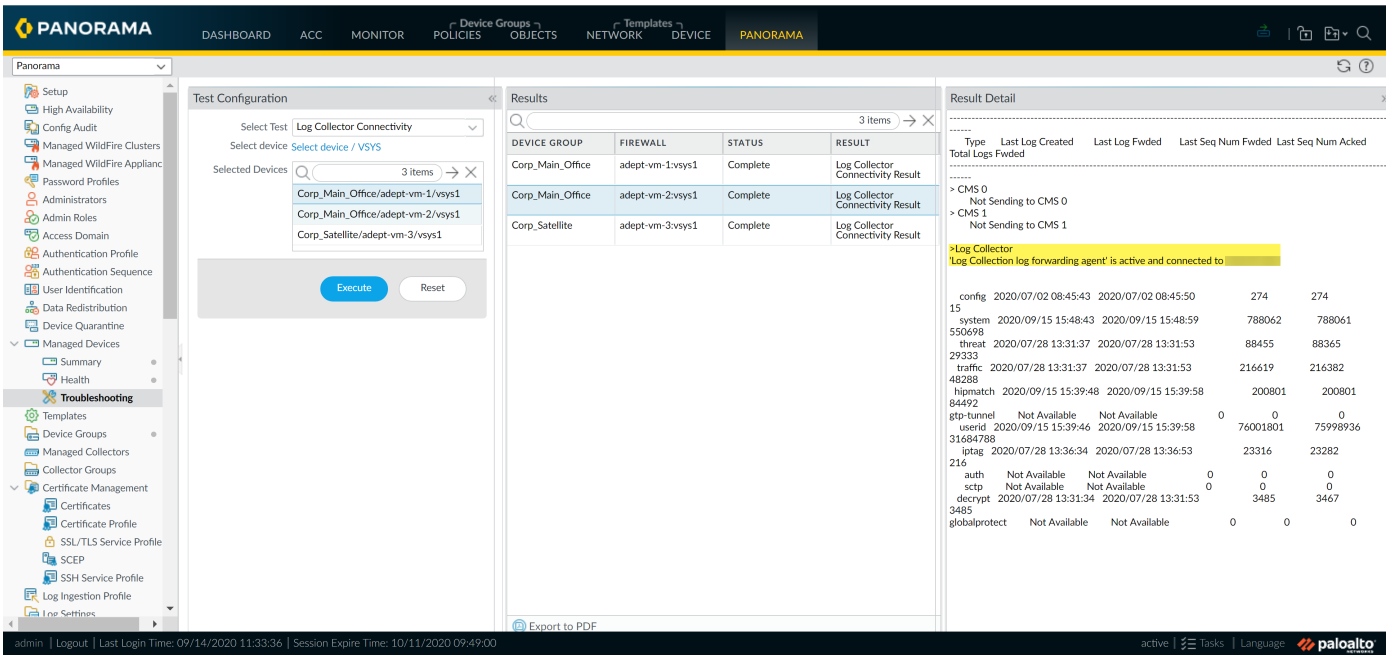
此外，您还可以通过 *Policies*（策略）选项卡运行策略匹配测试。

STEP 3 | 输入执行连接测试所需的信息。在本示例中，执行的是日志收集器连接测试。

1. 从 **Select Test**（选择测试）下拉列表中选择 **Log Collector Connectivity**（日志收集器连接）。
2. **Select device/VSYS**（选择设备/**VSYS**），并选择要进行测试的受管防火墙。
3. 必要时，输入连接测试所需的任何其他信息。

STEP 4 | **Execute**（执行）日志收集器连接测试。

STEP 5 | 选择日志收集器连接测试，以查看选中设备的日志收集器连接状态。



© 2019 Palo Alto Networks, Inc.

从 Panorama 10.0 降级

PAN-OS®10.0 引入了为专用日志收集器和 WildFire 设备配置本地和 Panorama 管理员的功能、通过以太网接口转发日志的功能、针对物理隔离 Panorama™ 管理服务器的自动动态更新、对策略优化器中的筛选后规则执行操作的功能，以及用于监视、ACC、按需报告的额外 60 天和 90 天筛选器。但是，这些功能与运行 PAN-OS 9.1 或更早版本的 Panorama 不兼容。在将运行 Panorama 10.0 版的日志收集器和 Panorama 降级到更早功能版本之前，应先根据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。

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/降级考虑因素以确保您在降级后考虑所有功能和配置设置将不同或不可用。

STEP 1 | 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 2 | 如果您针对专用日志收集器配置了身份验证，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 3 | 降级运行 PAN-OS 10.0 版的每个防火墙。

如果降级多个防火墙，请在开始降级前将各防火墙特定 *PAN-OS 9.1* 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 9.1.0*，请下载 *`PanOS_220- 9.1.0`* 或 *`PanOS_3000- 9.1.0`* 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））。
2. 找到您打算降级的每个型号或系列防火墙的 PAN-OS 9.1 映像。如果尚未下载映像，请 **Download**（下载）。

非 **HA** 防火墙

Install（安装）（Action（操作）列）相应 PAN-OS 9.1 版本，选择您打算降级的所有防火墙，并且选择 **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：

© 2019 Palo Alto Networks, Inc.

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 4 | 降级运行 Panorama 10.0 的各日志收集器。

1. **Check Now**（立即检查）可用的映像（**Panorama** > **Device Deployment**（设备部署）> **Software**（软件））。
2. 找到 Panorama 9.1 映像。如果尚未下载映像，请 **Download**（下载）（Action（操作）列）。
3. 下载完成后，在运行 Panorama 10.0 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 5 | 降级 Panorama。

1. **Check Now**（立即检查）可用的映像（**Panorama** > **Device Deployment**（设备部署）> **Software**（软件））。
2. 找到 Panorama 9.1 映像。如果尚未下载映像，请 **Download**（下载）。
3. 下载完成后，在 Panorama 上 **Install**（安装）映像。
4. 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 6 | 将 Panorama 日志迁移到 PAN-OS 8.1 日志格式。

在迁移期间，*ACC* 或监控选项卡中不会显示日志数据。此外，在迁移未完成之前，新的日志数据不会转发到日志收集器。

1. 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
```


© 2019 Palo Alto Networks, Inc.

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。

2. 开始将每个日志收集器上的日志迁移到先前格式。

   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> 开始
```

3. 查看日志迁移状态以估计完成将所有现有日志迁移到先前格式所需的时间。

```
admin@FC-M500-1> request logdb migrate lc serial-number <ser_num> 状态
 Slot: all
Migration State: In Progress
Percent Complete: 0.04
Estimated Time Remaining: 451 hour(s) 47 min(s)
```


© 2019 Palo Alto Networks, Inc.