Cisco Secure Workload 升级指南

上次修改日期: 2024 年 9 月 3 日

Cisco Secure Workload 支持的升级路径

表 *1: Cisco Secure Workload* 支持的升级路径

自	至	升级类型
3.9.1.10 3.9.1.1	3.9.1.25	补丁升级
3.9.1.1	3.9.1.10	补丁升级
3.8.1.39 3.8.1.36 3.8.1.19 3.8.1.1	3.9.1.1	主要版本升级
3.8.1.39 3.8.1.36 3.8.1.19 3.8.1.1	3.8.1.44	补丁升级
3.8.1.36 3.8.1.19 3.8.1.1	3.8.1.39	补丁升级
3.8.1.19 3.8.1.1	3.8.1.36	补丁升级
3.8.1.1	3.8.1.19	补丁升级
3.7.1.59 3.7.1.51 3.7.1.39	3.8.1.1	主要版本升级

自	至	升级类型
3.7.1.51 3.7.1.39 3.7.1.22 3.7.1.5	3.7.1.59	补丁升级
3.7.1.39 3.7.1.22 3.7.1.5	3.7.1.51	补丁升级
3.7.1.22 3.7.1.5	3.7.1.39	补丁升级
3.7.1.5	3.7.1.22	补丁升级
3.6.x	3.7.1.5	主要版本升级
3.6.1.x	任何更高版本的 3.6 补丁	补丁升级
3.5.1.x （Tetration 品牌）	3.6.1.5	主要版本升级
低于 3.6 的版本。	任何低于 3.6 的版本。 请参阅此处提供的《 思科 *Tetration* 升级指南》 中的详细信息。	-

双栈模式（IPv6 支持）的要求和限制

在物理硬件上运行的 Cisco Secure Workload 集群可以配置为使用 IPv6 和 IPv4 进行某些进出集群的通信。

注释

- 安装或升级到 3.6.1.5、3.7.1.5、3.8.1.1 和 3.9.1.1 版本时，可以使用双栈模式（IPv6 支持）功能。但是，当您安装或升级到修补程序版本时，启用该功能的选项不可用。
- 代理使用 IPv4 与集群通信，除非您将其配置为使用 IPv6。有关详细信息，请参阅 Cisco Secure Workload 用户指南。

限制

如果您正在考虑启用双堆栈模式，请注意以下事项：

- 您只能在初始部署或升级到主要版本期间启用 IPv6 连接（在修补程序升级期间无法启用此功能）。
- 仅物理硬件或裸机集群支持双堆栈模式。
- 不支持纯 IPv6 模式。
- 为集群启用双堆栈模式后，您无法恢复到仅 IPv4 模式。
- （适用于版本 3.8 或更早版本）如果启用了双堆栈连接，则不支持数据 Backup and Restore (DBR)。
- 请勿为使用联合身份验证配置的集群启用双堆栈模式。
- 以下功能始终且仅使用 IPv4（请注意，即使 IPv6 已启用，IPv4 也始终处于启用状态）：
  - （适用于版本 3.9.1.1, 3.8.1.1, 3.7.1.5 和 3.6.x）在 AIX 代理上实施
  - （仅适用于版本 3.6.x）与集群的硬件代理通信
  - （仅适用于版本 3.6.x）用于数据流注入、资产扩充或警报通知的连接器

要求

- 在为集群启用双堆栈模式之前，请为 FQDN 配置 A 和 AAAA DNS 记录。
- 外部服务（例如 NTP、SMTP 和 DNS）必须可通过 IPv4 和 IPv6 实现，以实现冗余。
- 要为集群配置双堆栈模式，请执行以下操作：
  - 两个集群枝叶交换机必须在两个不同的网络上分配可路由的 IPv6 地址，以实现冗余，并且必须为每个网络提供默认网关。
  - 对于 39RU 集群，需要具有至少 29 个主机地址空间的站点可路由 IPv6 网络。
  - 对于 8RU 集群，需要具有至少 20 个主机地址空间的站点可路由 IPv6 网络。
  - 站点可路由 IPv6 网络的前三个主机地址保留给思科安全工作负载集群 HSRP 配置，不得由任何其他设备使用。

升级到 Cisco Secure Workload 版本 3.9.x

升级到 Cisco Secure Workload 版本 3.9.1.38

您可以从 3.9.1.1、3.9.1.10、3.9.1.25 和 3.9.1.28 版本升级到此版本。

开始之前

⚠

注意 如果任何节点当前处于停用状态或任何服务运行状况不正常，请勿升级。在继续之前，请联系思科技术支持中心 (TAC) 以修复任何问题。

- 下载安装包：

  在浏览器中，前往 https://software.cisco.com/download/home/286309796/type/286309874/release/3.9.1.38。

  下载以下 RPM：`tetration_os_patch_k9-3.9.1.38-1.noarch.rpm`

- 确保**客户支持 (Customer Support)** 级别的帐户已上传 SSH 密钥以进行故障排除。
- 您必须以具有站点管理员或客户支持权限的用户身份执行以下程序。
- Google Chrome 和 Microsoft Edge 是支持升级的浏览器。

过程

步骤 1 检查系统运行状况。如果服务不正常，则无法执行升级。

a) 在 Secure Workload UI 的导航窗格中，选择**故障排除 (Troubleshoot)** > **服务状态 (Service Status)**。

b) 在图中查找红色圆圈，表示服务不正常。

或者，要查看服务运行状况的表格视图，请点击图形顶部的列表按钮，点击**全部展开 (Expand All)**，然后向下滚动页面以查看所有服务的状态。

c) 如果服务不正常，请执行必要的修复，使服务恢复正常运行后再继续升级。

步骤 2 从导航窗格中，依次选择**平台 (Platform)** > **升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。在继续之前，请按照屏幕上的说明排除预先检查发现的问题（如有）。

步骤 3 确保已选择**补丁升级 (Patch Upgrade)**。（这是补丁升级。）

步骤 4 点击**发送升级链接 (Send Upgrade Link)**。

步骤 5 查找包含以下主题的电子邮件消息：

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

此邮件包含您必须用于执行升级的超链接。

步骤 6 在电子邮件中，点击**补丁升级 (Patch Upgrade)** > **集群 (Cluster)** 链接以打开 Secure Workload 设置 UI。

步骤 7 点击**选择文件 (Choose File)**。

步骤 8 选择已下载的补丁 RPM，然后点击**打开 (Open)**。

步骤 9 要启动升级，请点击**上传 (Upload)** 以上传 RPM。在此过程中，您将暂时失去与 Secure Workload 设置 UI 的连接。

注释 您必须等待几分钟，重新获得对 Secure Workload UI 的访问权限后才能查看升级结果。如果升级存在问题，系统将显示红色横幅。

步骤 10 点击**书本**图标以查看日志。

步骤 11 验证升级：

a) 在浏览器中打开 Secure Workload UI。

b) 在导航窗格中，点击**平台 (Platform)** > **升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

c) 点击**历史记录 (History)**。
d) 验证**状态 (Status)** 列下的状态是否为**成功 (Succeeded)**。

步骤 12 如果升级成功，请点击**禁用补丁升级链接 (Disable Patch Upgrade Link)**。

升级到 Cisco Secure Workload 版本 3.9.1.28

您可以从 3.9.1.1、3.9.1.10 和 3.9.1.25 版本升级到此版本。

开始之前

注意 如果任何节点当前处于停用状态或任何服务运行状况不正常，请勿升级。在继续之前，请联系思科技术支持中心 (TAC) 以修复任何问题。

- 下载安装包：

  在浏览器中，前往 https://software.cisco.com/download/home/286309796/type/286309874/release/3.9.1.28。

  下载以下 RPM：`tetration_os_patch_k9-3.9.1.28-1.noarch.rpm`

- 确保**客户支持 (Customer Support)** 级别的帐户已上传 SSH 密钥以进行故障排除。
- 您必须以具有站点管理员或客户支持权限的用户身份执行以下程序。
- Google Chrome 和 Microsoft Edge 是支持升级的浏览器。

过程

步骤 1 检查系统运行状况。如果服务不正常，则无法执行升级。

a) 在 Secure Workload UI 的导航窗格中，选择**故障排除 (Troubleshoot)** > **服务状态 (Service Status)**。
b) 在图中查找红色圆圈，表示服务不正常。

   或者，要查看服务运行状况的表格视图，请点击图形顶部的列表按钮，点击**全部展开 (Expand All)**，然后向下滚动页面以查看所有服务的状态。

c) 如果服务不正常，请执行必要的修复，使服务恢复正常运行后再继续升级。

步骤 2 从导航窗格中，依次选择**平台 (Platform)** > **升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

步骤 3 按照屏幕上的指示操作。

在继续之前，请对通过预先检查识别的问题（如有）进行故障排除。

确保已选择**补丁升级 (Patch Upgrade)**。（这是补丁升级。）

点击**发送升级链接 (Send Upgrade Link)**。

步骤 4 查找包含以下主题的电子邮件消息：

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

此消息包含您必须用于执行升级的超链接。

步骤 5 在电子邮件消息中，点击**补丁升级 (Patch Upgrade)** 链接打开 Secure Workload 设置 UI。

步骤 6 点击**选择文件 (Choose File)**。

步骤 7 选择已下载的补丁 RPM，然后点击**打开 (Open)**。

步骤 8 点击**上传 (Upload)**。

上传 RPM 会启动升级。

在此过程中，您将暂时失去与设置 UI 的连接。

步骤 9 等待几分钟，重新获得对 UI 的访问权限后才能查看升级结果。

如果升级存在问题，系统将显示红色横幅。点击书本图像以查看日志。

步骤 10 验证升级：

a) 在浏览器中打开 Secure Workload UI。

b) 在导航窗格中，点击**平台 (Platform)** > **升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

c) 点击**历史记录 (History)**。

d) 验证**状态 (Status)** 列下的状态是否为**成功 (Succeeded)**。

步骤 11 如果升级成功，请点击**禁用补丁升级链接 (Disable Patch Upgrade Link)**。

升级到 Cisco Secure Workload 版本 3.9.1.25

您可以从 3.9.1.1 或 3.9.1.10 版本升级到此版本。

开始之前

⚠

注意 如果任何节点当前处于停用状态或任何服务运行状况不正常，请勿升级。在继续之前，请联系思科技术支持中心 (TAC) 以修复任何问题。

- 下载安装包：

  在浏览器中，前往 https://software.cisco.com/download/home/286309796/type/286309874/release/3.9.1.25。

  下载以下 RPM：`tetration_os_patch_k9-3.9.1.25-1.noarch.rpm`

- 确保**客户支持 (Customer Support)** 级别的帐户已上传 SSH 密钥以进行故障排除。
- 您必须以具有站点管理员或客户支持权限的用户身份执行以下程序。
- Google Chrome 和 Microsoft Edge 是支持升级的浏览器。

过程

步骤 1 检查系统运行状况。如果服务不正常，则无法执行升级。

a) 在 Secure Workload UI 的导航窗格中，选择**故障排除 (Troubleshoot)** > **服务状态 (Service Status)**。

b) 在图中查找红色圆圈，表示服务不正常。

或者，要查看服务运行状况的表格视图，请点击图形顶部的列表按钮，点击**全部展开 (Expand All)**，然后向下滚动页面以查看所有服务的状态。

c) 如果服务不正常，请执行必要的修复，使服务恢复正常运行后再继续升级。

步骤 2 从导航窗格中，依次选择**平台 (Platform)** > **升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

步骤 3 按照屏幕上的指示操作。

在继续之前，请对通过预先检查识别的问题（如有）进行故障排除。

确保已选择**补丁升级 (Patch Upgrade)**。（这是补丁升级。）

点击**发送升级链接 (Send Upgrade Link)**。

步骤 4 查找包含以下主题的电子邮件消息：

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

此消息包含您必须用于执行升级的超链接。

步骤 5 在电子邮件消息中，点击**补丁升级 (Patch Upgrade)** 链接打开 Secure Workload 设置 UI。

步骤 6 点击**选择文件 (Choose File)**。

步骤 7 选择已下载的补丁 RPM，然后点击**打开 (Open)**。

步骤 8 点击**上传 (Upload)**。

上传 RPM 会启动升级。

在此过程中，您将暂时失去与设置 UI 的连接。

步骤 9 等待几分钟，重新获得对 UI 的访问权限后才能查看升级结果。

如果升级存在问题，系统将显示红色横幅。点击书本图像以查看日志。

步骤 10 验证升级：

a) 在浏览器中打开 Secure Workload UI。

b) 在导航窗格中，点击**平台 (Platform)** > **升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

c) 点击**历史记录 (History)**。

d) 验证**状态 (Status)** 列下的状态是否为**成功 (Succeeded)**。

步骤 11 如果升级成功，请点击**禁用补丁升级链接 (Disable Patch Upgrade Link)**。

升级到 Cisco Secure Workload 版本 3.9.1.10

您可以从 3.9.1.1 版本升级到此版本。

开始之前

⚠

注意 如果任何节点当前处于停用状态或任何服务运行状况不正常，请勿升级。在继续之前，请联系思科技术支持中心 (TAC) 以修复任何问题。

- 下载安装包：

  在浏览器中，前往 https://software.cisco.com/download/home/286309796/type/286309874/release/3.9.1.10。

  下载以下 RPM：`tetration_os_patch_k9-3.9.1.10-1.noarch.rpm`

- 确保**客户支持 (Customer Support)** 级别的帐户已上传 SSH 密钥以进行故障排除。
- 您必须以具有站点管理员或客户支持权限的用户身份执行以下程序。
- Google Chrome 和 Microsoft Edge 是支持升级的浏览器。

过程

步骤 1 检查系统运行状况。如果服务不正常，则无法执行升级。

a) 在 Secure Workload UI 的导航窗格中，选择**故障排除 (Troubleshoot)** > **服务状态 (Service Status)**。

b) 在图中查找红色圆圈，表示服务不正常。

或者，要查看服务运行状况的表格视图，请点击图形顶部的列表按钮，点击**全部展开 (Expand All)**，然后向下滚动页面以查看所有服务的状态。

c) 如果服务不正常，请执行必要的修复，使服务恢复正常运行后再继续升级。

步骤 2 从导航窗格中，依次选择**平台 (Platform)** > **升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

步骤 3 按照屏幕上的指示操作。

在继续之前，请对通过预先检查识别的问题（如有）进行故障排除。

确保已选择**补丁升级 (Patch Upgrade)**。（这是补丁升级。）

点击**发送升级链接 (Send Upgrade Link)**。

步骤 4 查找包含以下主题的电子邮件消息：

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

此消息包含您必须用于执行升级的超链接。

步骤 5 在电子邮件消息中，点击**补丁升级 (Patch Upgrade)** 链接打开 Secure Workload 设置 UI。

步骤 6 点击**选择文件 (Choose File)**。

步骤 7 选择已下载的补丁 RPM，然后点击**打开 (Open)**。

步骤 8 点击**上传 (Upload)**。

上传 RPM 会启动升级。

在此过程中，您将暂时失去与设置 UI 的连接。

步骤 9 等待几分钟，重新获得对 UI 的访问权限后才能查看升级结果。

如果升级存在问题，系统将显示红色横幅。点击书本图像以查看日志。

步骤 10 验证升级：

a) 在浏览器中打开 Secure Workload UI。

b) 在导航窗格中，点击**平台 (Platform) > 升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

c) 点击**历史记录 (History)**。

d) 验证**状态 (Status)** 列下的状态是否为**成功 (Succeeded)**。

步骤 11 如果升级成功，请点击**禁用补丁升级链接 (Disable Patch Upgrade Link)**。

升级到 Cisco Secure Workload 版本 3.9.1.1

您可以从任何 3.8 版本升级到此版本。但建议您先升级到最新的 3.8.1.x 补丁版本，然后再升级到此版本。

开始之前

注意 如果任何节点处于停用状态或任何服务运行状况不正常，请勿升级。在继续之前，请联系思科技术支持中心 (TAC) 以修复任何问题。

- Kubernetes AKS 外部协调器 - 升级后，AKS 外部协调器将处于只读状态；如果要在升级后进行更改，请创建新的 Azure 连接器并启用**托管 Kubernetes 服务 (Managed Kubernetes services)** 选项。
- FMC 外部协调器 - 升级后，FMC 外部协调器将迁移到连接器。
- 确保客户支持 *(Customer Support)* 级别的帐户已上传 SSH 密钥以进行故障排除。
- 您必须以具有站点管理员或客户支持权限的用户身份执行以下程序。
- Google Chrome 和 Microsoft Edge 是支持升级的浏览器。
- 如果配置了 ISE 连接器，请验证其 TLS 证书是否有主体备用名称 (SAN) 部分。升级后，ISE 连接器将无法连接到提供传统仅 CN TLS 证书的 ISE 端点。在使用 SAN 扩展重新生成 ISE TLS 证书之前，请勿继续升级。
- **许可**
  - 如果您的 Cisco Secure Workload 部署没有有效的思科智能许可证（或在评估期之外），则必须在升级前注册有效许可证。
  - 管理许可证需要站点管理权限。
  - 要查看许可证的状态，请执行以下操作：在 Cisco Secure Workload UI 中，依次选择**管理 (Manage) > 服务设置 (Service Settings) > 许可证 (Licenses)**。如果您的集群许可证注册不合

规，您会在UI上看到一个横幅。有关获取和注册许可证的信息，请在Cisco Secure Workload UI 中选择**帮助 (Help)** > **页面级帮助 (Page-level Help)**，然后搜索 智能许可证。

过程

步骤 1 转到 https://software.cisco.com/download/home/286309796/type 并下载适用于您的部署的 RPM 文件。

- 对于 8-RU 或 39-RU 系统，请下载以下 RPM：
  - tetration_os_UcsFirmware_k9-3.9.1.1-1.x86_64.rpm
  - tetration_os_base_rpm_k9-3.9.1.1-1.el7.x86_64.rpm
  - tetration_os_adhoc_k9-3.9.1.1-1.el6.x86_64.rpm
  - tetration_os_mother_rpm_k9-3.9.1.1-1.el6.x86_64.rpm
  - tetration_os_rpminstall_k9-3.9.1.1-1.noarch.rpm
  - tetration_os_enforcement_k9-3.9.1.1-1.el6.x86_64.rpm
  - tetration_os_nxos_k9-3.9.1.1-1.x86_64.rpm
- 对于虚拟系统，请下载以下 RPM：
  - tetration_os_ova_k9-3.9.1.1-1.noarch.rpm
  - tetration_os_adhoc_k9-3.9.1.1-1.el6.x86_64.rpm
  - tetration_os_mother_rpm_k9-3.9.1.1-1.el6.x86_64.rpm
  - tetration_os_rpminstall_k9-3.9.1.1-1.noarch.rpm
  - tetration_os_enforcement_k9-3.9.1.1-5.el6.x86_64.rpm

步骤 2 验证下载的 RPM 的 MD5 校验和与 Cisco.com 上的 MD5 校验和是否一致。

步骤 3 检查系统运行状况。如果服务不正常，则无法执行升级。

a) 在 Secure Workload UI 的导航窗格中，选择**故障排除 (Troubleshoot)** > **服务状态 (Service Status)**。

b) 在图中查找红色圆圈，表示服务不正常。

或者，要查看服务运行状况的表格视图，请点击图形顶部的列表按钮，点击**全部展开 (Expand All)**，然后向下滚动页面以查看所有服务的状态。

c) 如果服务不正常，请执行必要的修复，使服务恢复正常运行后再继续升级。

步骤 4 集群快照有助于在升级期间对问题（如有）进行故障排除。从导航窗格中选择**故障排除 (Troubleshoot)** > **快照 (Snapshots)** > **创建快照 (Create Snapshot)** > **经典快照 (Classic Snapshot)**。

a) 不要更改默认设置。

b) 在**注释 (Comments)** 字段中，输入有关快照的注释。

c) 点击**创建快照 (Create Snapshot)**。

步骤 5 从导航窗格中，依次选择**平台 (Platform)** > **升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

步骤 6 在**升级 (Upgrade)** 选项卡下，按照屏幕上的说明执行操作。确保不要跳过任何步骤。

注释 在**选择操作 (Select Operation)** 下，为此升级选择**升级 (Upgrade)**。不要选择**补丁升级 (Patch Upgrade)** 选项。

步骤 7 点击**发送升级链接 (Send Upgrade Link)**。

登录的站点管理员或客户支持用户会收到一封主题如下的电子邮件：

```
[Tetration Analytics] Upgrade Initiation Link
```

步骤 8 点击电子邮件中收到的链接。或者，您可以通过导航到**故障排除 (Troubleshoot)** > **维护资源管理器 (Maintenance Explorer)** 并输入以下信息来获取升级 URL：

- 快照操作：**POST**
- 快照主机：**orchestrator.service.consul**
- 快照路径：**upgrade_url**

注释 Google Chrome 和 Microsoft Edge 是支持此升级的 Web 浏览器。

系统将显示 Cisco Secure Workload 设置门户。

步骤 9 在 Cisco Secure Workload 设置门户中，上传 RPM 文件：

a) 点击**选择文件 (Choose File)**。
b) 导航并选择 **tetration_os_rpminstall_k9-3.9.1.1-1.noarch.rpm**，然后点击**打开 (Open)**。
c) 点击**上传 (Upload)**。
d) 成功上传 **tetration_os_rpminstall_k9-3.9.1.1-1.noarch.rpm** 文件后，点击**安装 (Install)**。
安装 **tetration_os_rpminstall_k9-3.9.1.1-1.noarch.rpm** 文件后，将加载相关的RPM 文件，并且可以暂存这些RPM 文件进行部署。您可以查看当前部署的 RPM 文件和暂存的 RPM 文件的版本。
e) 根据您的集群部署，对相关 RPM 文件重复步骤 **a** 至 **c** 。有关 RPM 文件列表，请参阅步骤 1。
上传每个 RPM 文件时，页面上的 RPM 文件列表不会更新。这是预期行为。如果在上传 **tetration_os_mother_rpm_k9-3.9.1.1-1.el6.x86_64.rpm** 文件后看到错误，请等待 5 至 10 分钟，然后重新加载页面。现在应该可以查看已上传 RPM 的列表了。

注释 如果要从 3.8.1.1 升级到此版本，请按以下顺序上传 RPM 文件。上传 **tetration_os_mother_rpm_k9-3.9.1.1-1.el6.x86_64.rpm** 文件后，页面会刷新，您会注意到上传的RPM文件已暂存。您现在可以上传其他 RPM 文件。

- 对于 8-RU 或 39-RU 系统：
  1. tetration_os_rpminstall_k9-3.9.1.1-1.noarch.rpm
  2. tetration_os_UcsFirmware_k9-3.9.1.1-1.x86_64.rpm
  3. tetration_os_nxos_k9-3.9.1.1-1.x86_64.rpm
  4. tetration_os_adhoc_k9-3.9.1.1-1.el6.x86_64.rpm
  5. tetration_os_mother_rpm_k9-3.9.1.1-1.el6.x86_64.rpm

- 对于虚拟系统：
  1. tetration_os_rpminstall_k9-3.9.1.1-1.noarch.rpm
  2. tetration_os_adhoc_k9-3.9.1.1-1.el6.x86_64.rpm
  3. tetration_os_mother_rpm_k9-3.9.1.1-1.el6.x86_64.rpm

以绿色突出显示的行表示已成功上传 RPM。如果有任何问题，请点击**状态 (Status)** 以查看日志。

步骤 10 点击**安装 (Install)** 以部署 RPM 文件。

步骤 11 点击**继续 (Continue)**。
系统将显示**站点配置 (Site Config)** 门户。

注释 从 Cisco Secure Workload 版本 3.8 及更高版本开始，无法在使用 Cisco Secure Workload 设置 UI 的站点配置的任何文本字段中输入非 ASCII 字符。

步骤 12 （可选）在**常规 (General)** 下，更改 SSH 公钥，然后点击**下一步 (Next)**。

步骤 13 （可选）在**电子邮件 (Email)** 下，更改 UI 管理员或管理员邮件地址，然后点击**下一步 (Next)**。

步骤 14 （可选）在 **L3**下，启用集群以便在升级后的某些集群连接中除使用 IPv4 外还使用 IPv6 地址。要启用 IPv6：

a) 选中 **IPv6** 复选框。
b) 以 CIDR 符号输入枝叶 1 和枝叶 2 交换机的 IPv6 地址。
c) 输入枝叶 1 和枝叶 2 IPv6 默认网关。
d) 点击**下一步 (Next)**。

如果在此页面上启用 IPv6，则还必须在**网络 (Network)** 页面上配置 IPv6 字段，如步骤 15 所述。

有关双堆叠模式的要求和限制，请参阅双栈模式（IPv6 支持）的要求和限制，第 2 页。

步骤 15 在**网络 (Network)** 下：

a) 如有必要，请更改 **CIMC 内部网络**、**CIMC 内部网络网关**、**DNS 解析器**和 **DNS 域**的值。

注释 不要更改或删除现有的**外部网络**值。但可以添加更多 IPv4 网络。

b) 如果在L3页面启用了IPv6，**IPv6**复选框将自动被选中。通过执行以下任务，指定为Cisco Secure Workload保留的IPv6地址：

1. 输入采用CIDR表示法的IPv6外部网络。
2. （可选）要将IPv6仅用于指定地址，请输入单个外部IPv6 IP。

注释
- **IPv6 外部网络 (IPv6 External Network)** 字段中的前三个IPv6地址始终保留给Cisco Secure Workload集群的交换机，不应用于任何其他目的。
- 对于39-RU集群，请确保IPv6外部网络或外部IPv6 IP列表中至少有29个IPv6地址。
- 对于8-RU集群，请确保IPv6外部网络或外部IPv6 IP列表中至少有20个IPv6地址可用。

c) 点击**下一步 (Next)**。

步骤 16 （可选）在**服务 (Service)** 下，更改现有NTP和SMTP值，然后点击**下一步 (Next)**。

步骤 17 在**安全 (Security)** 下，启用或禁用**代理连接的SSL强密码 (Strong SSL Ciphers for Agent Connections)**，然后点击**下一步 (Next)**。

注释 您无法更改**UI**、**高级 (Advanced)** 和**恢复 (Recovery)** 选项卡下的值。

在**恢复 (Recovery)** 下，如果集群被配置为备用集群，则集群将以备用模式部署，其中包括较少的功能（仅支持热待机模式）。

步骤 18 点击**继续 (Continue)**。
在升级过程中，Cisco Secure Workload会执行某些验证任务，以确保：
- RPM版本正确。
- 集群运行正常。
- 您提供的站点信息有效。
- 交换机配置正确，可以升级到较新版本的NX-OS软件。
- 系统将验证信息字段。
- 在部署开始前同步NTP。
- 名称节点和辅助名称节点未处于故障转换状态。

如果必须升级集群交换机，检查可能需要几分钟到一个小时。完成检查后，您将收到一封主题为：`TETRATION CLUSTER MyCluster: Verify Token` 的电子邮件。邮件中包含所需的令牌以便继续升级。复制电子邮件中的令牌。

步骤 19 在Cisco Secure Workload Setup门户中，将令牌粘贴到**验证令牌 (Validation Token)** 字段中，然后点击**继续 (Continue)**。

注释　不哟啊选中**忽略实例停止故障 (Ignore instance stop failures)** 复选框，除非思科 TAC 要求这样做。

升级进程已启动。在 3.9.1.1、3.8.1.1 和 3.7.1.5 版本中，协调器虚拟机将先于其他组件升级。这可能需要 30 到 60 分钟，在此期间，进度条会从 0% 变为 100%。协调器升级完成后，其余组件也将升级，进度条将从 0% 重新开始。当绿色进度条达到 100% 时，就表示升级已完成。所有实例均显示**已部署 (Deployed)** 状态。

步骤 20　验证升级：

a) 在浏览器中打开 Secure Workload UI。
b) 从导航窗格中，依次选择**平台 (Platform)** > **升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。
c) 点击**历史记录 (History)**。
d) 验证**状态 (Status)** 列下的状态是否为**成功 (Succeeded)**。

下一步做什么

升级后，请进行更改，以便从该版本的增强功能中获益：

- 如果已启用 IPv6，则可以使用 IPv4 或 IPv6 地址访问 Cisco Secure Workload UI。默认情况下，代理继续使用 IPv4 连接到集群。如果希望软件代理能够使用 IPv6 与集群通信，请执行以下操作：

  1. 从导航窗格中，依次选择**平台 (Platform)** > **集群配置 (Cluster Configuration)**。
  2. 按照《Cisco Secure Workload 用户指南》中的说明配置**传感器 VIP FQDN (Sensor VIP FQDN)** 设置。

- 有关范围内改进的普通 Kubernetes 工作负载集群的信息，请参阅升级到版本 3.9、3.8 和 3.7：在策略发现中启用改进的 Kubernetes 工作负载集群，第 36 页。

升级到 Cisco Secure Workload 版本 3.8.x

升级到 Cisco Secure Workload 版本 3.8.1.53

您可以从 3.8.1.1、3.8.1.19、3.8.1.36 或 3.8.1.39 版本升级到此版本。

开始之前

⚠

注意　如果任何节点当前处于停用状态或任何服务运行状况不正常，请勿升级。在继续之前，请联系思科技术支持中心 (TAC) 以修复任何问题。

- 下载安装包：

  在浏览器中，前往 https://software.cisco.com/download/home/286309796/type/286309874/release/3.8.1.53。

下载以下 RPM：`tetration_os_patch_k9-3.8.1.53-1.noarch.rpm`

- 确保**客户支持 (Customer Support)** 级别的帐户已上传 SSH 密钥以进行故障排除。
- 您必须以具有站点管理员或客户支持权限的用户身份执行以下程序。
- Google Chrome 和 Microsoft Edge 是支持升级的浏览器。

过程

步骤 1 检查系统运行状况。如果任何服务运行不正常，则无法执行升级。

a) 在 Secure Workload UI 的导航窗格中，选择**故障排除 (Troubleshoot)** > **服务状态 (Service Status)**。

b) 在图中查找红色圆圈，表示服务不正常。

或者，要查看服务运行状况的表格视图，请点击图形顶部的列表按钮，点击**全部展开 (Expand All)**，然后向下滚动页面以查看所有服务的状态。

c) 如果任何服务运行不正常，请在继续升级之前执行任何必要的修复以使服务正常运行。

步骤 2 从导航窗格中，依次选择**平台 (Platform)** > **升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

步骤 3 按照屏幕上的指示操作。

在继续之前，请对预先检查确定的任何问题进行故障排除。

确保已选择**补丁升级 (Patch Upgrade)**。（这是补丁升级。）

点击**发送升级链接 (Send Upgrade Link)**。

步骤 4 查找包含以下主题的电子邮件消息：

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

此消息包含您必须用于执行升级的超链接。

步骤 5 在电子邮件消息中，点击**补丁升级 (Patch Upgrade)** 链接打开 Secure Workload 设置 UI。

步骤 6 点击**选择文件 (Choose File)**。

步骤 7 选择已下载的补丁 RPM，然后点击**打开 (Open)**。

步骤 8 点击**上传 (Upload)**。

上传 RPM 会启动升级。

在此过程中，您将暂时失去与设置 UI 的连接。

步骤 9 等待几分钟，重新获得对 UI 的访问权限并查看升级结果。

如果升级存在问题，系统将显示红色横幅。点击书本图像以查看日志。

步骤 10 验证升级：

a) 在浏览器中打开 Secure Workload UI。

b) 在导航窗格中，点击**平台 (Platform)** > **升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

c) 点击**历史记录 (History)**。

d) 验证“状态”(Status) 列是否显示**成功 (Succeeded)**。

步骤 11 如果升级成功，请点击**禁用补丁升级链接 (Disable Patch Upgrade Link)**。

升级到 Cisco Secure Workload 版本 3.8.1.39

您可以从 3.8.1.1、3.8.1.19 或 3.8.1.36 版本升级到此版本。

开始之前

注意 如果任何节点当前处于停用状态或任何服务运行状况不正常，请勿升级。在继续之前，请联系思科技术支持中心 (TAC) 以修复任何问题。

- 下载安装包：

  在浏览器中，前往 https://software.cisco.com/download/home/286309796/type/286309874/release/3.8.1.39。

  下载以下 RPM：`tetration_os_patch_k9-3.8.1.39-1.noarch.rpm`

- 确保**客户支持 (Customer Support)** 级别的帐户已上传 SSH 密钥以进行故障排除。
- 您必须以具有站点管理员或客户支持权限的用户身份执行以下程序。
- Google Chrome 和 Microsoft Edge 是支持升级的浏览器。

过程

步骤 1 检查系统运行状况。如果任何服务运行不正常，则无法执行升级。

a) 在 Secure Workload UI 的导航窗格中，选择**故障排除 (Troubleshoot)** > **服务状态 (Service Status)**。

b) 在图中查找红色圆圈，表示服务不正常。

或者，要查看服务运行状况的表格视图，请点击图形顶部的列表按钮，点击**全部展开 (Expand All)**，然后向下滚动页面以查看所有服务的状态。

c) 如果任何服务运行不正常，请在继续升级之前执行任何必要的修复以使服务正常运行。

步骤 2 从导航窗格中，依次选择**平台 (Platform)** > **升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

步骤 3 按照屏幕上的指示操作。

在继续之前，请对预先检查确定的任何问题进行故障排除。

确保已选择**补丁升级 (Patch Upgrade)**。（这是补丁升级。）

点击**发送升级链接 (Send Upgrade Link)**。

步骤 4 查找包含以下主题的电子邮件消息：

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

此消息包含您必须用于执行升级的超链接。

步骤 5 在电子邮件消息中，点击**补丁升级 (Patch Upgrade)** 链接打开 Secure Workload 设置 UI。

步骤 6 点击**选择文件 (Choose File)**。

步骤 7 选择已下载的补丁 RPM，然后点击**打开 (Open)**。

步骤 8 点击**上传 (Upload)**。

上传 RPM 会启动升级。

在此过程中，您将暂时失去与设置 UI 的连接。

步骤 9 等待几分钟，重新获得对 UI 的访问权限并查看升级结果。

如果升级存在问题，系统将显示红色横幅。点击书本图像以查看日志。

步骤 10 验证升级：

a) 在浏览器中打开 Secure Workload UI。

b) 在导航窗格中，点击**平台 (Platform) > 升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

c) 点击**历史记录 (History)**。

d) 验证“状态”(Status) 列是否显示**成功 (Succeeded)**。

步骤 11 如果升级成功，请点击**禁用补丁升级链接 (Disable Patch Upgrade Link)**。

升级到 Cisco Secure Workload 版本 3.8.1.36

您可以从 3.8.1.1 或 3.8.1.19 版本升级到此版本。

开始之前

注意 如果任何节点当前处于停用状态或任何服务运行状况不正常，请勿升级。在继续之前，请联系思科技术支持中心 (TAC) 以修复任何问题。

- 下载安装包：

  在浏览器中，前往 https://software.cisco.com/download/home/286309796/type/286309874/release/3.8.1.36。

  下载以下 RPM：`tetration_os_patch_k9-3.8.1.36-1.noarch.rpm`

- 确保**客户支持 (Customer Support)** 级别的帐户已上传 SSH 密钥以进行故障排除。
- 您必须以具有站点管理员或客户支持权限的用户身份执行以下程序。
- Google Chrome 和 Microsoft Edge 是支持升级的浏览器。

过程

步骤 1 检查系统运行状况。如果任何服务运行不正常，则无法执行升级。

a) 在 Secure Workload UI 的导航窗格中，选择**故障排除 (Troubleshoot)** > **服务状态 (Service Status)**。

b) 在图中查找红色圆圈，表示服务不正常。

或者，要查看服务运行状况的表格视图，请点击图形顶部的列表按钮，点击**全部展开 (Expand All)**，然后向下滚动页面以查看所有服务的状态。

c) 如果任何服务运行不正常，请在继续升级之前执行任何必要的修复以使服务正常运行。

步骤 2 从导航窗格中，依次选择**平台 (Platform)** > **升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

步骤 3 按照屏幕上的指示操作。

在继续之前，请对预先检查确定的任何问题进行故障排除。

确保已选择**补丁升级 (Patch Upgrade)**。（这是补丁升级。）

点击**发送升级链接 (Send Upgrade Link)**。

步骤 4 查找包含以下主题的电子邮件消息：

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

此消息包含您必须用于执行升级的超链接。

步骤 5 在电子邮件消息中，点击**补丁升级 (Patch Upgrade)** 链接打开 Secure Workload 设置 UI。

步骤 6 点击**选择文件 (Choose File)**。

步骤 7 选择已下载的补丁 RPM，然后点击**打开 (Open)**。

步骤 8 点击**上传 (Upload)**。

上传 RPM 会启动升级。

在此过程中，您将暂时失去与设置 UI 的连接。

步骤 9 等待几分钟，重新获得对 UI 的访问权限并查看升级结果。

如果升级存在问题，系统将显示红色横幅。点击书本图像以查看日志。

步骤 10 验证升级：

a) 在浏览器中打开 Secure Workload UI。

b) 在导航窗格中，点击**平台 (Platform)** > **升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

c) 点击**历史记录 (History)**。

d) 验证“状态”(Status) 列是否显示**成功 (Succeeded)**。

步骤 11 如果升级成功，请点击**禁用补丁升级链接 (Disable Patch Upgrade Link)**。

升级到 Cisco Secure Workload 版本 3.8.1.19

您可以从 3.8.1.1 版本升级到此版本。

开始之前

⚠

注意 如果任何节点当前处于停用状态或任何服务运行状况不正常，请勿升级。在继续之前，请联系思科技术支持中心 (TAC) 以修复任何问题。

- 下载安装包：

  在浏览器中，前往 https://software.cisco.com/download/home/286309796/type/286309874/release/3.8.1.19。

  下载以下 RPM：`tetration_os_patch_k9-3.8.1.19-1.noarch.rpm`

- 确保**客户支持 (Customer Support)** 级别的帐户已上传 SSH 密钥以进行故障排除。
- 您必须以具有站点管理员或客户支持权限的用户身份执行以下程序。
- Google Chrome 和 Microsoft Edge 是支持升级的浏览器。

过程

步骤 1 检查系统运行状况。如果任何服务运行不正常，则无法执行升级。

a) 在 Secure Workload UI 的导航窗格中，选择**故障排除 (Troubleshoot)** > **服务状态 (Service Status)**。

b) 在图中查找红色圆圈，表示服务不正常。

或者，要查看服务运行状况的表格视图，请点击图形顶部的列表按钮，点击**全部展开 (Expand All)**，然后向下滚动页面以查看所有服务的状态。

c) 如果任何服务运行不正常，请在继续升级之前执行任何必要的修复以使服务正常运行。

步骤 2 从导航窗格中，依次选择**平台 (Platform)** > **升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

步骤 3 按照屏幕上的指示操作。

在继续之前，请对预先检查确定的任何问题进行故障排除。

确保已选择**补丁升级 (Patch Upgrade)**。（这是补丁升级。）

点击**发送升级链接 (Send Upgrade Link)**。

步骤 4 查找包含以下主题的电子邮件消息：

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

此消息包含您必须用于执行升级的超链接。

步骤 5 在电子邮件消息中，点击**补丁升级 (Patch Upgrade)** 链接打开 Secure Workload 设置 UI。

步骤 6 点击**选择文件 (Choose File)**。

步骤 7 选择已下载的补丁 RPM，然后点击**打开 (Open)**。

步骤 8 点击**上传 (Upload)**。

上传 RPM 会启动升级。

在此过程中，您将暂时失去与设置 UI 的连接。

步骤 9 等待几分钟，重新获得对 UI 的访问权限并查看升级结果。

如果升级存在问题，系统将显示红色横幅。点击书本图像以查看日志。

步骤 10 验证升级：

a) 在浏览器中打开 Secure Workload UI。

b) 在导航窗格中，点击**平台 (Platform) > 升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

c) 点击**历史记录 (History)**。

d) 验证“状态”(Status) 列是否显示**成功 (Succeeded)**。

步骤 11 如果升级成功，请点击**禁用补丁升级链接 (Disable Patch Upgrade Link)**。

升级到 Cisco Secure Workload 版本 3.8.1.1

您必须先升级到最新的 3.7.1.x 补丁版本，然后才能升级到此版本。

开始之前

注意 如果任何节点当前处于停用状态或任何服务运行状况不正常，请勿升级。在继续之前，请联系思科技术支持中心 (TAC) 以修复任何问题。

请注意这些问题：

- Kubernetes AKS 外部协调器 - 升级后，AKS 外部协调器将处于只读状态；如果要在升级后进行更改，请创建新的 Azure 连接器并启用**托管 Kubernetes 服务 (Managed Kubernetes services)** 选项。
- FMC 外部协调器 - 升级后，FMC 外部协调器将迁移到连接器。
- 确保“客户支持”级别的帐户已上传 SSH 密钥以进行故障排除。
- 您必须以具有站点管理员或客户支持权限的用户身份执行以下程序。
- Google Chrome 和 Microsoft Edge 是支持升级的浏览器。
- 如果配置了 ISE 连接器，请验证其 TLS 证书是否有主体备用名称 (SAN) 部分。升级后，ISE 连接器将无法连接到提供传统仅 CN TLS 证书的 ISE 端点。在使用 SAN 扩展重新生成 ISE TLS 证书之前，请勿继续升级。
- 许可
  - 如果您的 Cisco Secure Workload 部署当前没有有效的思科智能许可证（或在评估期之外），则必须在升级前注册有效许可证。
  - 管理许可证需要站点管理权限。

- 要查看许可证的状态，请执行以下操作：在 Cisco Secure Workload Web 门户中，依次选择**管理 (Manage)** > **服务设置 (Service Settings)** > **许可证 (Licenses)**。如果您的集群许可证注册不合规，您将在 UI 上看到一个横幅。有关获取和注册许可证的信息，请在 Cisco Secure Workload Web 门户中选择**帮助 (Help)** > **页面级帮助 (Page-level Help)**，然后搜索智能许可证。

过程

步骤 1 从 Cisco.com 下载适用于您的部署的 RPM 文件：

a) 前往 https://software.cisco.com/download/home/286309796/type。

b) 根据需要下载：

- 对于 8-RU 或 39-RU 系统，请下载以下 RPM：
  - tetration_os_UcsFirmware_k9-3.8.1.1-1.x86_64.rpm
  - tetration_os_base_rpm_k9-3.8.1.1-1.el7.x86_64.rpm
  - tetration_os_adhoc_k9-3.8.1.1-1.el6.x86_64.rpm
  - tetration_os_mother_rpm_k9-3.8.1.1-1.el6.x86_64.rpm
  - tetration_os_rpminstall_k9-3.8.1.1-1.noarch.rpm
  - tetration_os_enforcement_k9-3.8.1.1-1.el6.x86_64.rpm
  - tetration_os_nxos_k9-3.8.1.1-1.x86_64.rpm
- 对于虚拟系统，请下载以下 RPM：
  - tetration_os_ova_k9-3.8.1.1-1.noarch.rpm
  - tetration_os_adhoc_k9-3.8.1.1-1.el6.x86_64.rpm
  - tetration_os_mother_rpm_k9-3.8.1.1-1.el6.x86_64.rpm
  - tetration_os_rpminstall_k9-3.8.1.1-1.noarch.rpm
  - tetration_os_enforcement_k9-3.8.1.1-5.el6.x86_64.rpm

c) 验证下载的 RPM 的 MD5 校验和与 CCO 中的 MD5 校验和是否一致。

步骤 2 检查系统运行状况。如果任何服务运行不正常，则无法执行升级。

a) 在 Secure Workload UI 的导航窗格中，选择**故障排除 (Troubleshoot)** > **服务状态 (Service Status)**。

b) 在图中查找表示服务不正常的红色圆圈。

或者，要查看服务运行状况的表格视图，请点击图形顶部的列表按钮，点击**全部展开 (Expand All)**，然后向下滚动页面以查看所有服务的状态。

c) 如果任何服务运行不正常，请在继续升级之前执行任何必要的修复以使服务正常运行。

步骤 3 从导航窗格中，依次选择**平台 (Platform)** > **升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

步骤 4 在**升级 (Upgrade)** 选项卡下，按照屏幕上显示的说明操作。确保不要跳过任何步骤。

注释 在**选择操作 (Select Operation)** 下，选择**升级 (Upgrade)**。不要选择“补丁升级”(Patch Upgrade) 选项。

步骤 5 点击**发送升级链接 (Send Upgrade Link)**。

使用站点管理员或客户支持角色登录的用户将收到一封包含超链接的电子邮件，您必须使用它执行升级。电子邮件的主题为：

```
[Tetration Analytics] Upgrade Initiation Link
```

打开电子邮件并复制**升级集群 (Upgrade Cluster)** URL。

或者，您可以通过点击**故障排除 (Troubleshoot)** > **维护资源管理器 (Maintenance Explorer)** 并输入以下信息来获取升级 URL：

- 快照操作：**POST**
- 快照主机：**orchestrator.service.consul**
- 快照路径：**upgrade_url**

步骤 6 在浏览器中，将升级 URL 粘贴到地址字段中，然后按 **Enter** 键。

系统将显示 Cisco Secure Workload 设置门户。请注意，Google Chrome 和 Microsoft Edge 是升级支持的 Web 浏览器。

步骤 7 在 Cisco Secure Workload 设置门户中，您必须以特定顺序上传 RPM，具体取决于您的设置。要上传 RPM 文件，请执行以下操作：

a) 点击**选择文件 (Choose File)**。
b) 导航并选择 RPM 文件，然后点击**打开 (Open)**。
c) 点击**上传 (Upload)**。
d) 对每个 RPM 文件重复步骤 **a** 至 **c**。
在上传每个 RPM 时，页面上的 RPM 列表不会更新，这在意料之中。如果在上传 *tetration_os_mother_rpm_k9-3.8.1.1-1.el6.x86_64.rpm* 文件后看到错误，请等待 5 至 10 分钟，然后重新加载页面。现在应该可以查看已上传 RPM 的列表了。

对于 8-RU 或 39-RU 系统，请按给定顺序上传以下文件：

- tetration_os_rpminstall_k9-3.8.1.1-1.noarch.rpm
- tetration_os_UcsFirmware_k9-3.8.1.1-1.x86_64.rpm
- tetration_os_nxos_k9-3.8.1.1-1.x86_64.rpm
- tetration_os_adhoc_k9-3.8.1.1-1.el6.x86_64.rpm
- tetration_os_mother_rpm_k9-3.8.1.1-1.el6.x86_64.rpm
- tetration_os_enforcement_k9-3.3.8.1.1-1.el6.x86_64.rpm

- tetration_os_base_rpm_k9-3.3.8.1.1-1.el7.x86_64.rpm

对于虚拟系统，以给定顺序上传以下文件：

- tetration_os_rpminstall_k9-3.8.1.1-1.noarch.rpm
- tetration_os_adhoc_k9-3.8.1.1-1.el6.x86_64.rpm
- tetration_os_mother_rpm_k9-3.8.1.1-1.el6.x86_64.rpm
- tetration_os_enforcement_k9-3.3.8.1.1-1.el6.x86_64.rpm
- tetration_os_ova_k9-3.8.1.1-1.noarch.rpm

步骤 8 点击**继续 (Continue)**。
系统将显示**站点配置 (Site Config)** 门户。

注释 从 Cisco Secure Workload 版本 3.8 及更高版本开始，不允许在使用 Cisco Secure Workload 设置用户界面的站点配置的任何文本字段中输入非 ASCII 字符。

步骤 9 （可选）在**常规 (General)** 下，更改 SSH 公钥，然后点击**下一步 (Next)**。

步骤 10 （可选）在**电子邮件 (Email)** 下，更改 UI 管理员或管理员邮件地址，然后点击**下一步 (Next)**。

步骤 11 （可选）在 **L3**下，启用集群以便在升级后的某些集群连接中除使用 IPv4 外还使用 IPv6 地址。要启用 IPv6：

a) 选中 **IPv6** 复选框。
b) 以 CIDR 符号输入枝叶 1 和枝叶 2 交换机的 IPv6 地址。
c) 输入枝叶 1 和枝叶 2 IPv6 默认网关。
d) 点击**下一步 (Next)**。

如果在此页面上启用 IPv6，则还必须在**网络 (Network)** 页面上配置 IPv6 字段，如下一步所述。

重要事项 有关双堆叠模式的要求和限制，请参阅双栈模式（IPv6 支持）的要求和限制，第 2 页。

步骤 12 在**网络 (Network)** 下：

a) 如有必要，请更改 **CIMC 内部网络**、**CIMC 内部网络网关**、**DNS 解析器**和 **DNS 域**的值。
b) **重要提示**！不要更改或删除现有的**外部网络**值。但可以添加其他 IPv4 网络。
c) 如果在 L3 页面启用了 IPv6，**IPv6** 复选框将自动被选中。指定为 Cisco Secure Workload 保留的 IPv6 地址：

1. 输入采用 CIDR 表示法的 IPv6 外部网络。
2. （可选）要将 IPv6 仅用于指定地址，请输入单个外部 IPv6 IP。

注释
- IPv6 外部网络字段中的前 3 个 IPv6 地址始终保留给 Cisco Secure Workload 集群的交换机，不应用于任何其他目的。
- 对于 39 RU 集群，请确保 IPv6 外部网络或外部 IPv6 IP 列表中至少有 29 个 IPv6 地址。
- 对于 8 RU 集群，请确保 IPv6 外部网络或外部 IPv6 IP 列表中至少有 20 个 IPv6 地址可用。

d) 点击**下一步 (Next)**。

步骤 13 （可选）在**服务 (Service)** 下，更改 NTP 和 SMTP 值，然后点击**下一步 (Next)**。

步骤 14 在**安全 (Security)** 下，启用或禁用“代理连接的 SSL 强密码”(Strong SSL Ciphers for Agent Connections)，然后点击**下一步 (Next)**。

您无法更改**UI**、**高级 (Advanced)** 和**恢复 (Recovery)** 选项卡下的值。

在**恢复 (Recovery)** 下，如果集群被配置为备用集群，则集群将以备用模式部署，其中包括较少的功能（仅支持热备模式）。

步骤 15 点击**继续 (Continue)**。
在升级过程中执行以下检查，以确保：
- RPM 版本正确
- 集群运行正常
- 您提供的站点信息有效
- 交换机配置正确，可以升级到较新版本的 NX-OS 软件
- 信息字段已验证
- 在部署开始前同步 NTP
- 名称节点和辅助名称节点未处于故障转换状态

如果需要升级集群交换机，检查可能需要几分钟到一个小时。完成检查后，您将收到一封主题为：`TETRATION CLUSTER MyCluster: Verify Token` 的电子邮件。邮件中包含所需的令牌以便继续升级。复制电子邮件中的令牌。

步骤 16 在 Cisco Secure Workload Setup 门户中，将令牌粘贴到**验证令牌 (Validation Token)** 字段中，然后点击**继续 (Continue)**。

重要事项 请勿选中**忽略实例停止故障 (Ignore instance stop failures)** 复选框，除非思科员工明确指示这样做。

升级进程已启动。在 3.8.1.1 和 3.7.1.5 版本中，协调器虚拟机将先于其他组件升级。这可能需要 30 到 60 分钟，在此期间，进度条将从 0 变为 100%。协调器升级完成后，其余组件也将升级，而进度条将从0%重新开始。当绿色进度条达到100％时，升级完成。所有实例都显示“已部署”(Deployed) 状态。

步骤 17 验证升级：

a) 在浏览器中打开 Secure Workload UI。

b) 在左导航窗格中，点击**平台 (Platform)** > **升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

c) 点击**历史记录 (History)**。

d) 验证**状态 (Status)** 列下的状态是否为**成功 (Succeeded)**。

下一步做什么

升级后，请进行更改，以便从该版本的增强功能中获益：

- 如果启用了 IPv6，则可以使用 IPv4 或 IPv6 地址访问 Cisco Secure Workload 网络界面。默认情况下，代理继续使用 IPv4 连接到集群。如果希望软件代理能够使用 IPv6 与集群通信，请执行以下操作：

  1. 从导航窗格中，依次选择**平台 (Platform)** > **集群配置 (Cluster Configuration)**。
  2. 按照 Cisco Secure Workload Web 门户上提供的《用户指南》中的说明配置**传感器 VIP FQDN (Sensor VIP FQDN)** 设置。

- 有关范围内改进的普通 Kubernetes 工作负载集群的信息，请参阅升级到版本 3.9、3.8 和 3.7：在策略发现中启用改进的 Kubernetes 工作负载集群，第 36 页。

升级到 Cisco Secure Workload 版本 3.7.x

升级到 Cisco Secure Workload 版本 3.7.1.59

您可以从 3.7.1.5、3.7.1.22、3.7.1.39 或 3.7.1.51 版本升级到此版本。

开始之前

注意 如果任何节点当前处于停用状态或任何服务运行状况不正常，请勿升级。在继续之前，请联系思科技术支持中心 (TAC) 以修复任何问题。

- 下载安装包：

  在浏览器中，前往 https://software.cisco.com/download/home/286309796/type/286309874/release/3.7.1.59。

  下载以下 RPM：`tetration_os_patch_k9-3.7.1.59-1.noarch.rpm`

- 确保**客户支持 (Customer Support)** 级别的帐户已上传 SSH 密钥以进行故障排除。
- 您必须以具有站点管理员或客户支持权限的用户身份执行以下程序。
- Google Chrome 是本次升级唯一支持的浏览器。

过程

步骤 1 检查系统运行状况。如果任何服务运行不正常，则无法执行升级。

a) 在 Secure Workload Web 界面中，从窗口左侧的导航菜单中选择**故障排除 (Troubleshoot) > 服务状态 (Service Status)**。

b) 在图中查找红色圆圈，表示服务不正常。

或者，要查看服务运行状况的表格视图，请点击图形顶部的列表按钮，点击**全部展开 (Expand All)**，然后向下滚动页面以查看所有服务的状态。

c) 如果任何服务运行不正常，请在继续升级之前执行任何必要的修复以使服务正常运行。

步骤 2 在 Secure Workload Web 界面中，从窗口左侧的菜单中点击**平台 (Platform)** > **升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

步骤 3 按照所示说明进行操作。

在继续之前解决预先检查中发现的任何问题。

确保已选择**补丁升级 (Patch Upgrade)**。（这是补丁升级。）

点击**发送升级链接 (Send Upgrade Link)**。

步骤 4 查找包含以下主题的电子邮件消息：

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

此消息包含您必须用于执行升级的超链接。

步骤 5 在电子邮件消息中，点击**补丁升级 <Cluster> (Patch Upgrade <Cluster>)** 链接打开 Secure Workload 设置用户界面。您必须使用 Google Chrome 浏览器。

步骤 6 点击**选择文件 (Choose File)**。

步骤 7 导航到您在上面下载的补丁 RPM，选择它，然后点击**打开 (Open)**。

步骤 8 点击**上传 (Upload)**。

上传 RPM 将启动升级。

在此过程中，您将暂时失去与设置用户界面的连接。

步骤 9 等待几分钟，重新获得对 Web 界面的访问权限并查看升级结果。

如果升级存在问题，系统会显示红色横幅。点击书本图像以查看日志。

步骤 10 验证升级：

a) 在浏览器中打开 Secure Workload Web 界面。

b) 从左侧的黑色导航菜单中，依次选择**平台 (Platform)** > **升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

c) 点击**历史记录 (History)**。

d) 验证“状态”(Status) 列是否显示**成功 (Succeeded)**。

步骤 11 如果升级成功，请点击**禁用补丁升级链接 (Disable Patch Upgrade Link)**。

升级到 Cisco Secure Workload 版本 3.7.1.51

您可以从 3.7.1.5、3.7.1.22 或 3.7.1.39 版本升级到此版本。

开始之前

注意 如果任何节点当前处于停用状态或任何服务运行状况不正常，请勿升级。在继续之前，请联系思科技术支持中心 (TAC) 以修复任何问题。

- 下载安装包：

  在浏览器中，前往 https://software.cisco.com/download/home/286309796/type/286309874/release/3.7.1.51。

  下载以下 RPM：`tetration_os_patch_k9-3.7.1.51-1.noarch.rpm`

- 确保**客户支持 (Customer Support)** 级别的帐户已上传 SSH 密钥以进行故障排除。
- 您必须以具有站点管理员或客户支持权限的用户身份执行以下程序。
- Google Chrome 是本次升级唯一支持的浏览器。

过程

步骤 1 检查系统运行状况。如果任何服务运行不正常，则无法执行升级。

a) 在 Secure Workload Web 界面中，从窗口左侧的导航菜单中选择**故障排除 (Troubleshoot)** > **服务状态 (Service Status)**。

b) 在图中查找红色圆圈，表示服务不正常。

或者，要查看服务运行状况的表格视图，请点击图形顶部的列表按钮，点击**全部展开 (Expand All)**，然后向下滚动页面以查看所有服务的状态。

c) 如果任何服务运行不正常，请在继续升级之前执行任何必要的修复以使服务正常运行。

步骤 2 在 Secure Workload Web 界面中，从窗口左侧的菜单中点击**平台 (Platform)** > **升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

步骤 3 按照所示说明进行操作。

在继续之前解决预先检查中发现的任何问题。

确保已选择**补丁升级 (Patch Upgrade)**。（这是补丁升级。）

点击**发送升级链接 (Send Upgrade Link)**。

步骤 4 查找包含以下主题的电子邮件消息：

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

此消息包含您必须用于执行升级的超链接。

步骤 5 在电子邮件消息中，点击**补丁升级 <Cluster> (Patch Upgrade <Cluster>)** 链接打开 Secure Workload 设置用户界面。您必须使用 Google Chrome 浏览器。

步骤 6 点击**选择文件 (Choose File)**。

步骤 7 导航到您在上面下载的补丁 RPM，选择它，然后点击**打开 (Open)**。

步骤 8 点击**上传 (Upload)**。

上传 RPM 将启动升级。

在此过程中，您将暂时失去与设置用户界面的连接。

步骤 9 等待几分钟，重新获得对 Web 界面的访问权限并查看升级结果。

如果升级存在问题，系统会显示红色横幅。点击书本图像以查看日志。

步骤 10 验证升级：

a) 在浏览器中打开 Secure Workload Web 界面。

b) 从左侧的黑色导航菜单中，依次选择**平台 (Platform) > 升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

c) 点击**历史记录 (History)**。

d) 验证“状态”(Status) 列是否显示**成功 (Succeeded)**。

步骤 11 如果升级成功，请点击**禁用补丁升级链接 (Disable Patch Upgrade Link)**。

升级到 Cisco Secure Workload 版本 3.7.1.39

您可以从 3.7.1.5 或 3.7.1.22 版本升级到此版本。

开始之前

注意 如果任何节点当前处于停用状态或任何服务运行状况不正常，请勿升级。在继续之前，请联系思科技术支持中心 (TAC) 以修复任何问题。

- 下载安装包：

  在浏览器中，前往 https://software.cisco.com/download/home/286309796/type/286309874/release/3.7.1.39。

  下载以下 RPM：`tetration_os_patch_k9-3.7.1.39-1.noarch.rpm`

- 确保“客户支持”级别的帐户已上传 SSH 密钥以进行故障排除。
- 您必须以具有站点管理员或客户支持权限的用户身份执行以下程序。
- Google Chrome 是本次升级唯一支持的浏览器。

过程

步骤 1 检查系统运行状况。如果任何服务运行不正常，则无法执行升级。

a) 在 Secure Workload Web 界面中，从窗口左侧的导航菜单中选择**故障排除 (Troubleshoot) > 服务状态 (Service Status)**。

b) 在图中查找红色圆圈，表示服务不正常。

或者，要查看服务运行状况的表格视图，请点击图形顶部的列表按钮，点击**全部展开 (Expand All)**，然后向下滚动页面以查看所有服务的状态。

c) 如果任何服务运行不正常，请在继续升级之前执行任何必要的修复以使服务正常运行。

步骤 2 在 Secure Workload Web 界面中，从窗口左侧的菜单中点击**平台 (Platform) > 升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

步骤 3 按照所示说明进行操作。

在继续之前解决预先检查中发现的任何问题。

确保已选择**补丁升级 (Patch Upgrade)**。（这是补丁升级。）

点击**发送升级链接 (Send Upgrade Link)**。

步骤 4 查找包含以下主题的电子邮件消息：

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

此消息包含您必须用于执行升级的超链接。

步骤 5 在电子邮件消息中，点击**补丁升级 <Cluster> (Patch Upgrade <Cluster>)** 链接打开 Secure Workload 设置用户界面。您必须使用 Google Chrome 浏览器。

步骤 6 点击**选择文件 (Choose File)**。

步骤 7 导航到您在上面下载的补丁 RPM，选择它，然后点击**打开 (Open)**。

步骤 8 点击**上传 (Upload)**。

上传 RPM 将启动升级。

在此过程中，您将暂时失去与设置用户界面的连接。

步骤 9 等待几分钟，重新获得对 Web 界面的访问权限并查看升级结果。

如果升级存在问题，系统会显示红色横幅。点击书本图像以查看日志。

步骤 10 验证升级：

a) 在浏览器中打开 Secure Workload Web 界面。

b) 从左侧的黑色导航菜单中，依次选择**平台 (Platform) > 升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

c) 点击**历史记录 (History)**。

d) 验证“状态”(Status) 列是否显示**成功 (Succeeded)**。

步骤 11 如果升级成功，请点击**禁用补丁升级链接 (Disable Patch Upgrade Link)**。

升级到 Cisco Secure Workload 版本 3.7.1.22

您可以从版本 3.7.1.5 升级到此版本。

开始之前

⚠

注意 如果任何节点当前处于停用状态或任何服务运行状况不正常，请勿升级。在继续之前，请联系思科技术支持中心 (TAC) 以修复任何问题。

- 下载安装包：

  在浏览器中，前往 https://software.cisco.com/download/home/286309796/type/286309874/release/3.7.1.22。

  下载以下 RPM：`tetration_os_patch_k9-3.7.1.22-1.noarch.rpm`

- 确保“客户支持”级别的帐户已上传 SSH 密钥以进行故障排除。
- 您必须以具有站点管理员或客户支持权限的用户身份执行以下程序。
- Google Chrome 是本次升级唯一支持的浏览器。

过程

步骤 1 检查系统运行状况。如果任何服务运行不正常，则无法执行升级。

a) 在 Secure Workload Web 界面中，从窗口左侧的导航菜单中选择**故障排除 (Troubleshoot)** > **服务状态 (Service Status)**。

b) 在图中查找红色圆圈，表示服务不正常。

或者，要查看服务运行状况的表格视图，请点击图形顶部的列表按钮，点击**全部展开 (Expand All)**，然后向下滚动页面以查看所有服务的状态。

c) 如果任何服务运行不正常，请在继续升级之前执行任何必要的修复以使服务正常运行。

步骤 2 在 Secure Workload Web 界面中，从窗口左侧的菜单中点击**平台 (Platform)** > **升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

步骤 3 按照所示说明进行操作。

在继续之前解决预先检查中发现的任何问题。

确保已选择**补丁升级 (Patch Upgrade)**。（这是补丁升级。）

点击**发送升级链接 (Send Upgrade Link)**。

步骤 4 查找包含以下主题的电子邮件消息：

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

此消息包含您必须用于执行升级的超链接。

步骤 5 在电子邮件消息中，点击**补丁升级 <Cluster> (Patch Upgrade <Cluster>)** 链接打开 Secure Workload 设置用户界面。您必须使用 Google Chrome 浏览器。

步骤 6 点击**选择文件 (Choose File)**。

步骤 7 导航到您在上面下载的补丁 RPM，选择它，然后点击**打开 (Open)**。

步骤 8 点击**上传 (Upload)**。

上传 RPM 将启动升级。

在此过程中，您将暂时失去与设置用户界面的连接。

步骤 9 等待几分钟，重新获得对 Web 界面的访问权限并查看升级结果。

如果升级存在问题，系统会显示红色横幅。点击书本图像以查看日志。

步骤 10 验证升级：

a) 在浏览器中打开 Secure Workload Web 界面。

b) 从左侧的黑色导航菜单中，依次选择**平台 (Platform) > 升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

c) 点击**历史记录 (History)**。

d) 验证“状态”(Status) 列是否显示**成功 (Succeeded)**。

步骤 11 如果升级成功，请点击**禁用补丁升级链接 (Disable Patch Upgrade Link)**。

升级到 Cisco Secure Workload 版本 3.7.1.5

您可以从任何 3.6 版本升级到此版本，但建议先升级到最新的 3.6.1.x 补丁版本，再升级到此版本。

开始之前

注意 如果任何节点当前处于停用状态或任何服务运行状况不正常，请勿升级。在继续之前，请联系思科技术支持中心 (TAC) 以修复任何问题。

请注意这些问题：

- Kubernetes AKS 外部协调器 - 升级后，AKS 外部协调器将处于只读状态；如果要在升级后进行更改，请创建新的 Azure 连接器并启用**托管 Kubernetes 服务 (Managed Kubernetes services)** 选项。
- 确保“客户支持”级别的帐户已上传 SSH 密钥以进行故障排除。
- 您必须以具有站点管理员或客户支持权限的用户身份执行以下程序。
- Google Chrome 是此升级唯一支持的浏览器。

- 如果配置了 ISE 连接器，请验证其 TLS 证书是否有主体备用名称 (SAN) 部分。升级后，ISE 连接器将无法连接到提供传统仅 CN TLS 证书的 ISE 端点。在使用 SAN 扩展重新生成 ISE TLS 证书之前，请勿继续升级。
- 许可
  - 如果您的 Cisco Secure Workload 部署当前没有有效的许可证（或在评估期之外），则必须在升级前注册有效许可证。
  - 管理许可证需要站点管理权限。
  - 要查看许可证的状态，请执行以下操作：在 Cisco Secure Workload Web 门户中，依次选择**监控 (Monitoring)** > **许可证 (Licenses)**。如果您的集群许可证注册不合规，您将看到带有**执行操作 (Take action)** 链接的横幅。有关获取和注册许可证的信息，请在 Cisco Secure Workload Web 门户中选择**帮助 (Help)** > **页面级帮助 (Page-level Help)**，然后搜索许可证。

过程

步骤 1 从 Cisco.com 下载适用于您的部署的 RPM 文件：

a) 前往 https://software.cisco.com/download/home/286309796/type。

b) 根据需要下载：

- 对于 8-RU 或 39-RU 系统，请下载以下 RPM：
  - tetration_os_UcsFirmware_k9-3.7.1.5-1.x86_64.rpm
  - tetration_os_base_rpm_k9-3.7.1.5-1.el7.x86_64.rpm
  - tetration_os_adhoc_k9-3.7.1.5-1.el6.x86_64.rpm
  - tetration_os_mother_rpm_k9-3.7.1.5-1.el6.x86_64.rpm
  - tetration_os_rpminstall_k9-3.7.1.5-1.noarch.rpm
  - tetration_os_enforcement_k9-3.7.1.5-1.el6.x86_64.rpm
  - tetration_os_nxos_k9-3.7.1.5-1.x86_64.rpm
- 对于虚拟系统，请下载以下 RPM：
  - tetration_os_ova_k9-3.7.1.5-1.noarch.rpm
  - tetration_os_adhoc_k9-3.7.1.5-1.el6.x86_64.rpm
  - tetration_os_mother_rpm_k9-3.7.1.5-1.el6.x86_64.rpm
  - tetration_os_rpminstall_k9-3.7.1.5-1.noarch.rpm
  - tetration_os_enforcement_k9-3.7.1.5-5.el6.x86_64.rpm

c) 验证下载的 RPM 的 MD5 校验和与 CCO 中的 MD5 校验和是否一致。

步骤 2 检查系统运行状况。如果任何服务运行不正常，则无法执行升级。

a) 在 Secure Workload Web 界面中，点击**设置 (Settings)**，然后选择**维护 (Maintenance)**。

b) 在左侧窗格中，选择**服务状态 (Service Status)**。

c) 在图中查找红色圆圈，表示服务不正常。

或者，要查看服务运行状况的表格视图，请点击图形顶部的列表按钮，点击**全部展开 (Expand All)**，然后向下滚动页面以查看所有服务的状态。

d) 如果任何服务运行不正常，请在继续升级之前执行任何必要的修复以使服务正常运行。

步骤 3 在左侧导航菜单中，选择**维护 (Maintenance)** > **升级 (Upgrade)**。

步骤 4 如有必要，请点击**升级 (Upgrade)** 选项卡。

步骤 5 按照屏幕上显示的指示操作。确保不要跳过任何步骤。

使用**升级 (Upgrade)** 选项，而不是补丁升级选项。

步骤 6 点击**发送升级链接 (Send Upgrade Link)**。

使用站点管理员或客户支持角色登录的用户将收到一封包含超链接的电子邮件，您必须使用它执行升级。电子邮件的主题为：

```
[Tetration Analytics] Upgrade Initiation Link
```

打开电子邮件并复制**升级集群 (Upgrade Cluster)** URL。

或者，您可以通过输入以下信息，从 **维护 (Maintenance)** > **浏览 (Explore)** 页面获取升级 URL：

- 快照操作：**POST**
- 快照主机：**orchestrator.service.consul**
- 快照路径：**upgrade_url**

步骤 7 在 Google Chrome 中，将升级 URL 粘贴到地址字段中，然后按 **Enter** 键。

系统将显示 Cisco Secure Workload 设置门户。请注意，Google Chrome 是升级中唯一支持的 Web 浏览器。

步骤 8 在 Cisco Secure Workload 设置门户中，您必须以特定顺序上传 RPM，具体取决于您的设置。要上传 RPM 文件，请执行以下操作：

a) 点击**选择文件 (Choose File)**。

b) 导航并选择 RPM 文件，然后点击**打开 (Open)**。

c) 点击**上传 (Upload)**。

d) 对每个 RPM 文件重复步骤 **a** 至 **c**。
在上传每个 RPM 时，页面上的 RPM 列表不会更新，这在意料之中。如果在上传 *tetration_os_mother_rpm_k9-3.7.1.5-1.el6.x86_64.rpm* 文件后看到错误，请等待 5 至 10 分钟，然后重新加载页面。现在应该可以查看已上传 RPM 的列表了。

对于 8-RU 或 39-RU 系统，请按给定顺序上传以下文件：

- tetration_os_rpminstall_k9-3.7.1.5-1.noarch.rpm

- tetration_os_UcsFirmware_k9-3.7.1.5-1.x86_64.rpm
- tetration_os_nxos_k9-3.7.1.5-1.x86_64.rpm
- tetration_os_adhoc_k9-3.7.1.5-1.el6.x86_64.rpm
- tetration_os_mother_rpm_k9-3.7.1.5-1.el6.x86_64.rpm
- tetration_os_enforcement_k9-3.7.1.5-1.el6.x86_64.rpm
- tetration_os_base_rpm_k9-3.7.1.5-1.el7.x86_64.rpm

对于虚拟系统，以给定顺序上传以下文件：

- tetration_os_rpminstall_k9-3.7.1.5-1.noarch.rpm
- tetration_os_adhoc_k9-3.7.1.5-1.el6.x86_64.rpm
- tetration_os_mother_rpm_k9-3.7.1.5-1.el6.x86_64.rpm
- tetration_os_enforcement_k9-3.7.1.5-1.el6.x86_64.rpm
- tetration_os_ova_k9-3.7.1.5-1.noarch.rpm

步骤 9 点击**继续 (Continue)**。
系统将显示**站点配置 (Site Config)** 门户。

步骤 10 （可选）在**常规 (General)** 下，更改 SSH 公钥，然后点击**下一步 (Next)**。

步骤 11 （可选）在**电子邮件 (Email)** 下，更改 UI 管理员或管理员邮件地址，然后点击**下一步 (Next)**。

步骤 12 （可选）在 **L3**下，启用集群以便在升级后的某些集群连接中除使用 IPv4 外还使用 IPv6 地址。要启用 IPv6：

a) 选中 **IPv6** 复选框。
b) 以 CIDR 符号输入枝叶 1 和枝叶 2 交换机的 IPv6 地址。
c) 输入枝叶 1 和枝叶 2 IPv6 默认网关。
d) 点击**下一步 (Next)**。

如果在此页面上启用 IPv6，则还必须在**网络 (Network)** 页面上配置 IPv6 字段，如下一步所述。

重要事项 有关双堆叠模式的要求和限制，请参阅双栈模式（IPv6 支持）的要求和限制，第 2 页。

步骤 13 在**网络 (Network)** 下：

a) 如有必要，请更改 **CIMC 内部网络**、**CIMC 内部网络网关**、**DNS 解析器**和 **DNS 域**的值。
b) **重要提示！**不要更改或删除现有的**外部网络**值。但可以添加其他 IPv4 网络。
c) 如果在 L3 页面启用了 IPv6，**IPv6** 复选框将自动被选中。指定为 Cisco Secure Workload 保留的 IPv6 地址：

1. 输入采用 CIDR 表示法的 IPv6 外部网络。
2. （可选）要将 IPv6 仅用于指定地址，请输入单个外部 IPv6 IP。

请注意：

- IPv6 外部网络字段中的前 3 个 IPv6 地址始终保留给 Cisco Secure Workload 集群的交换机，不应用于任何其他目的。
- 对于 39 RU 集群，请确保 IPv6 外部网络或外部 IPv6 IP 列表中至少有 29 个 IPv6 地址。
- 对于 8 RU 集群，请确保 IPv6 外部网络或外部 IPv6 IP 列表中至少有 20 个 IPv6 地址可用。

d) 点击**下一步 (Next)**。

步骤 14 （可选）在**服务 (Service)** 下，更改 NTP 和 SMTP 值，然后点击**下一步 (Next)**。

如果需要更改系统日志值（如有），请使用 TAN 设备。

步骤 15 在**安全 (Security)** 下，启用或禁用“代理连接的 SSL 强密码”(Strong SSL Ciphers for Agent Connections)，然后点击**下一步 (Next)**。

您无法更改**UI**、**高级 (Advanced)** 和**恢复 (Recovery)** 选项卡下的值。

在**恢复 (Recovery)** 下，如果集群被配置为备用集群，则集群将以备用模式部署，其中包括较少的功能（仅支持热备模式）。

步骤 16 点击**继续 (Continue)**。
在升级过程中执行以下检查，以确保：

- RPM 版本正确
- 集群运行正常
- 您提供的站点信息有效
- 交换机配置正确，可以升级到较新版本的 NX-OS 软件
- 信息字段已验证
- 在部署开始前同步 NTP
- 名称节点和辅助名称节点未处于故障转换状态

如果需要升级集群交换机，检查可能需要几分钟到一个小时。完成检查后，您将收到一封主题为：`TETRATION CLUSTER MyCluster: Verify Token` 的电子邮件。邮件中包含所需的令牌以便继续升级。复制电子邮件中的令牌。

步骤 17 在 Cisco Secure Workload Setup 门户中，将令牌粘贴到**验证令牌 (Validation Token)** 字段中，然后点击**继续 (Continue)**。

重要事项 请勿选中**忽略实例停止故障 (Ignore instance stop failures)** 复选框，除非思科员工明确指示这样做。

升级进程已启动。在 3.7.1.5 版本中，协调器虚拟机将先于其他组件升级。这可能需要 30 到 60 分钟，在此期间，进度条将从 0 变为 100%。协调器升级完成后，其余组件也将升级，而进度条将从 0% 重新开始。当绿色进度条达到 100％ 时，升级完成。所有实例都显示“已部署”(Deployed) 状态。

步骤 18 验证升级：

a) 在浏览器中打开 Secure Workload Web 界面。
b) 从左侧的黑色导航菜单中，依次选择**平台 (Platform) > 升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。
c) 点击**历史记录 (History)**。
d) 验证“状态”(Status) 列是否显示**成功 (Succeeded)**。

步骤 19 如果升级成功，请点击**禁用补丁升级链接 (Disable Patch Upgrade Link)**。

下一步做什么

升级后，请进行更改，以便从该版本的增强功能中获益：

- 请参阅后续操作，第 50 页。
- 有关范围内改进的普通 Kubernetes 工作负载集群的信息，请参阅升级到版本 3.9、3.8 和 3.7：在策略发现中启用改进的 Kubernetes 工作负载集群，第 36 页。

升级到版本 3.9、3.8 和 3.7：在策略发现中启用改进的 Kubernetes 工作负载集群

此功能仅适用于普通 Kubernetes（在协调器配置中，“K8s 管理器类型”(K8s Manager Type) 为“无”(None)。）

如果已经配置了 Kubernetes 外部协调器，则可以启用 3.9、3.8 和 3.7 版中的增强功能，通过使用集群的 Kubernetes 标签元数据来提高针对 Kubernetes 工作负载的 ADM 集群结果的准确性。

要启用此增强功能，请在升级后对每个普通的 Kubernetes 协调器执行以下两项操作：

- 在普通 Kubernetes 外部协调器配置中（在**管理 (Manage) > 外部协调器 (External Orchestrators)** 下），启用**用于策略发现集群 (Use for policy discovery clustering)** 并保存更改。
- 将以下权限添加到绑定到服务帐户的 ClusterRole。

资源	Kubernetes 动词
replicationcontrollers	[get list watch]
replicasets	[get list watch]
deployments	[get list watch]
daemonsets	[get list watch]
statefulsets	[get list watch]
jobs	[get list watch]
cronjobs	[get list watch]

包含这些权限的示例 clusterrole.yaml（您的版本可能略有不同）：

```
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
```

```
metadata:
  name: tetration.read.only
rules:
  - apiGroups:
    - ""
      resources:
        - nodes
        - services
        - endpoints
        - namespaces
        - pods
        - replicationcontrollers
        - ingresses
      verbs:
        - get
        - list
        - watch
  - apiGroups:
    - extensions
    - networking.k8s.io
      resources:
        - ingresses
      verbs:
        - get
        - list
        - watch
  - apiGroups:
    - apps
      resources:
        - replicasets
        - deployments
        - statefulsets
        - daemonsets
      verbs:
        - get
        - list
        - watch
  - apiGroups:
    - batch
      resources:
        - jobs
        - cronjobs
      verbs:
        - get
        - list
        - watch
```

升级到 Cisco Secure Workload 版本 3.6.x

升级到 Cisco Secure Workload 版本 3.6.1.47

您可以从较早的 3.6 版本升级到此版本。

开始之前

注意 如果任何节点当前处于停用状态或任何服务运行状况不正常，请勿升级。在继续之前，请联系思科技术支持中心 (TAC) 以修复任何问题。

- 下载安装包：

  在浏览器中，前往 https://software.cisco.com/download/home/286309796/type/286309874/release/3.6.1.47。

  下载以下 RPM：`tetration_os_patch_k9-3.6.1.47-1.noarch.rpm`

- 在执行升级之前，您应备份系统。有关详细信息，请参阅用户指南中有关数据备份和恢复(DBR)的信息，包括有关升级的小节。
- 确保“客户支持”级别的帐户已上传 SSH 密钥以进行故障排除。
- 您必须以具有站点管理员或客户支持权限的用户身份执行以下程序。
- Google Chrome 是本次升级唯一支持的浏览器。

过程

步骤 1 检查系统运行状况。如果任何服务运行不正常，则无法执行升级。

a) 在 Secure Workload Web 界面中，从窗口左侧的导航菜单中选择**故障排除 (Troubleshoot)** > **服务状态 (Service Status)**。

b) 在图中查找红色圆圈，表示服务不正常。

或者，要查看服务运行状况的表格视图，请点击图形顶部的列表按钮，点击**全部展开 (Expand All)**，然后向下滚动页面以查看所有服务的状态。

c) 如果任何服务运行不正常，请在继续升级之前执行任何必要的修复以使服务正常运行。

步骤 2 在 Secure Workload Web 界面中，从窗口左侧的菜单中点击**平台 (Platform)** > **升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

步骤 3 按照所示说明进行操作。

在继续之前解决预先检查中发现的任何问题。

确保已选择**补丁升级 (Patch Upgrade)**。（这是补丁升级。）

点击**发送升级链接 (Send Upgrade Link)**。

步骤 4 查找包含以下主题的电子邮件消息：

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

此消息包含您必须用于执行升级的超链接。

步骤 5 在电子邮件消息中，点击**补丁升级 <Cluster> (Patch Upgrade <Cluster>)** 链接打开 Secure Workload 设置用户界面。您必须使用 Google Chrome 浏览器。

步骤 6 点击**选择文件 (Choose File)**。

步骤 7 导航到您在上面下载的补丁 RPM，选择它，然后点击**打开 (Open)**。

步骤 8 点击**上传 (Upload)**。

上传 RPM 将启动升级。

在此过程中，您将暂时失去与设置用户界面的连接。

步骤 9 等待几分钟，重新获得对 Web 界面的访问权限并查看升级结果。

如果升级存在问题，系统会显示红色横幅。点击书本图像以查看日志。

步骤 10 验证升级：

a) 在浏览器中打开 Secure Workload Web 界面。

b) 从左侧的黑色导航菜单中，依次选择**平台 (Platform) > 升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

c) 点击**历史记录 (History)**。

d) 验证“状态”(Status) 列是否显示**成功 (Succeeded)**。

步骤 11 如果升级成功，请点击**禁用补丁升级链接 (Disable Patch Upgrade Link)**。

升级到 Cisco Secure Workload 版本 3.6.1.36

您可以从较早的 3.6 版本升级到此版本。

开始之前

注意 如果任何节点当前处于停用状态或任何服务运行状况不正常，请勿升级。在继续之前，请联系思科技术支持中心 (TAC) 以修复任何问题。

- 下载安装包：

  在浏览器中，前往 https://software.cisco.com/download/home/286309796/type/286309874/release/3.6.1.36。

  下载以下 RPM：`tetration_os_patch_k9-3.6.1.36-1.noarch.rpm`

- 在执行升级之前，您应备份系统。有关详细信息，请参阅用户指南中有关数据备份和恢复 (DBR) 的信息，包括有关升级的小节。
- 确保“客户支持”级别的帐户已上传 SSH 密钥以进行故障排除。
- 您必须以具有站点管理员或客户支持权限的用户身份执行以下程序。
- Google Chrome 是本次升级唯一支持的浏览器。

过程

步骤 1 检查系统运行状况。如果任何服务运行不正常，则无法执行升级。

a) 在 Secure Workload Web 界面中，从窗口左侧的导航菜单中选择**故障排除 (Troubleshoot) > 服务状态 (Service Status)**。

b) 在图中查找红色圆圈，表示服务不正常。

或者，要查看服务运行状况的表格视图，请点击图形顶部的列表按钮，点击**全部展开 (Expand All)**，然后向下滚动页面以查看所有服务的状态。

c) 如果任何服务运行不正常，请在继续升级之前执行任何必要的修复以使服务正常运行。

步骤 2 在 Secure Workload Web 界面中，从窗口左侧的菜单中点击**平台 (Platform)** > **升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

步骤 3 按照所示说明进行操作。

在继续之前解决预先检查中发现的任何问题。

确保已选择**补丁升级 (Patch Upgrade)**。（这是补丁升级。）

点击**发送升级链接 (Send Upgrade Link)**。

步骤 4 查找包含以下主题的电子邮件消息：

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

此消息包含您必须用于执行升级的超链接。

步骤 5 在电子邮件消息中，点击**补丁升级 <Cluster> (Patch Upgrade <Cluster>)** 链接打开 Secure Workload 设置用户界面。您必须使用 Google Chrome 浏览器。

步骤 6 点击**选择文件 (Choose File)**。

步骤 7 导航到您在上面下载的补丁 RPM，选择它，然后点击**打开 (Open)**。

步骤 8 点击**上传 (Upload)**。

上传 RPM 将启动升级。

在此过程中，您将暂时失去与设置用户界面的连接。

步骤 9 等待几分钟，重新获得对 Web 界面的访问权限并查看升级结果。

如果升级存在问题，系统会显示红色横幅。点击书本图像以查看日志。

步骤 10 验证升级：

a) 在浏览器中打开 Secure Workload Web 界面。

b) 从左侧的黑色导航菜单中，依次选择**平台 (Platform)** > **升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

c) 点击**历史记录 (History)**。

d) 验证“状态”(Status) 列是否显示**成功 (Succeeded)**。

步骤 11 如果升级成功，请点击**禁用补丁升级链接 (Disable Patch Upgrade Link)**。

升级到 Cisco Secure Workload 版本 3.6.1.21

您可以从较早的 3.6 版本升级到此版本。

开始之前

注意 如果任何节点当前处于停用状态或任何服务运行状况不正常，请勿升级。在继续之前，请联系思科技术支持中心 (TAC) 以修复任何问题。

- 下载安装包：

  在浏览器中，前往 https://software.cisco.com/download/home/286309796/type/286309874/release/3.6.1.21。

  下载以下 RPM：`tetration_os_patch_k9-3.6.1.21-1.noarch.rpm`

- 在执行升级之前，您应备份系统。有关详细信息，请参阅用户指南中有关数据备份和恢复 (DBR) 的信息，包括有关升级的小节。
- 确保“客户支持”级别的帐户已上传 SSH 密钥以进行故障排除。
- 您必须以具有站点管理员或客户支持权限的用户身份执行以下程序。
- Google Chrome 是本次升级唯一支持的浏览器。

过程

步骤 1 检查系统运行状况。如果任何服务运行不正常，则无法执行升级。

a) 在 Secure Workload Web 界面中，从窗口左侧的导航菜单中选择**故障排除 (Troubleshoot)** > **服务状态 (Service Status)**。

b) 在图中查找红色圆圈，表示服务不正常。

或者，要查看服务运行状况的表格视图，请点击图形顶部的列表按钮，点击**全部展开 (Expand All)**，然后向下滚动页面以查看所有服务的状态。

c) 如果任何服务运行不正常，请在继续升级之前执行任何必要的修复以使服务正常运行。

步骤 2 在 Secure Workload Web 界面中，从窗口左侧的菜单中点击**平台 (Platform)** > **升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

步骤 3 按照所示说明进行操作。

在继续之前解决预先检查中发现的任何问题。

确保已选择**补丁升级 (Patch Upgrade)**。（这是补丁升级。）

点击**发送升级链接 (Send Upgrade Link)**。

步骤 4 查找包含以下主题的电子邮件消息：

`[Tetration][<cluster_name>] Patch Upgrade Initiation Link`

此消息包含您必须用于执行升级的超链接。

步骤 5 在电子邮件消息中，点击**补丁升级 <Cluster> (Patch Upgrade <Cluster>)** 链接打开 Secure Workload 设置用户界面。您必须使用 Google Chrome 浏览器。

步骤 6 点击**选择文件 (Choose File)**。

步骤 7 导航到您在上面下载的补丁 RPM，选择它，然后点击**打开 (Open)**。

步骤 8 点击**上传 (Upload)**。

上传 RPM 将启动升级。

在此过程中，您将暂时失去与设置用户界面的连接。

步骤 9 等待几分钟，重新获得对 Web 界面的访问权限并查看升级结果。

如果升级存在问题，系统会显示红色横幅。点击书本图像以查看日志。

步骤 10 验证升级：

a) 在浏览器中打开 Secure Workload Web 界面。

b) 从左侧的黑色导航菜单中，依次选择**平台 (Platform) > 升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

c) 点击**历史记录 (History)**。

d) 验证“状态”(Status) 列是否显示**成功 (Succeeded)**。

步骤 11 如果升级成功，请点击**禁用补丁升级链接 (Disable Patch Upgrade Link)**。

升级到 Cisco Secure Workload 版本 3.6.1.17

您可以从版本 3.6.1.5 升级到版本 3.6.1.17。

开始之前

注意 如果任何节点当前处于停用状态或任何服务运行状况不正常，请勿升级。在继续之前，请联系思科技术支持中心 (TAC) 以修复任何问题。

- 下载安装包：

  在浏览器中，前往 https://software.cisco.com/download/home/286309796/type/286309874/release/3.6.1.17。

  下载以下 RPM：`tetration_os_patch_k9-3.6.1.17-1.noarch.rpm`

- 在执行升级之前，您应备份系统。有关详细信息，请参阅用户指南中有关数据备份和恢复 (DBR) 的信息，包括有关升级的小节。
- 确保“客户支持”级别的帐户已上传 SSH 密钥以进行故障排除。
- 您必须以具有站点管理员或客户支持权限的用户身份执行以下程序。
- Google Chrome 是本次升级唯一支持的浏览器。

过程

步骤 1 检查系统运行状况。如果任何服务运行不正常，则无法执行升级。

a) 在 Secure Workload Web 界面中，从窗口左侧的导航菜单中选择**故障排除 (Troubleshoot) > 服务状态 (Service Status)**。

b) 在图中查找红色圆圈，表示服务不正常。

或者，要查看服务运行状况的表格视图，请点击图形顶部的列表按钮，点击**全部展开 (Expand All)**，然后向下滚动页面以查看所有服务的状态。

c) 如果任何服务运行不正常，请在继续升级之前执行任何必要的修复以使服务正常运行。

步骤 2 在 Secure Workload Web 界面中，从窗口左侧的菜单中点击**平台 (Platform) > 升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

步骤 3 按照所示说明进行操作。

在继续之前解决预先检查中发现的任何问题。

确保已选择**补丁升级 (Patch Upgrade)**。（这是补丁升级。）

点击**发送升级链接 (Send Upgrade Link)**。

步骤 4 查找包含以下主题的电子邮件消息：

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

此消息包含您必须用于执行升级的超链接。

步骤 5 在电子邮件消息中，点击**补丁升级 <Cluster> (Patch Upgrade <Cluster>)** 链接打开 Secure Workload 设置用户界面。您必须使用 Google Chrome 浏览器。

步骤 6 点击**选择文件 (Choose File)**。

步骤 7 导航到您在上面下载的补丁 RPM，选择它，然后点击**打开 (Open)**。

步骤 8 点击**上传 (Upload)**。

上传 RPM 将启动升级。

在此过程中，您将暂时失去与设置用户界面的连接。

步骤 9 等待几分钟，重新获得对 Web 界面的访问权限并查看升级结果。

如果升级存在问题，系统会显示红色横幅。点击书本图像以查看日志。

步骤 10 验证升级：

a) 在浏览器中打开 Secure Workload Web 界面。

b) 从左侧的黑色导航菜单中，依次选择**平台 (Platform) > 升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

c) 点击**历史记录 (History)**。

d) 验证“状态”(Status) 列是否显示**成功 (Succeeded)**。

步骤 11 如果升级成功，请点击**禁用补丁升级链接 (Disable Patch Upgrade Link)**。

升级到 Cisco Secure Workload 版本 3.6.1.5

您可以从任何 3.5.1.x 版本升级到此版本，但建议先升级到最新的 3.5.1.x 补丁版本，再升级到此版本。

这些说明既适用于硬件部署，也适用于虚拟部署。

开始之前

⚠

注意 如果任何节点当前处于停用状态或任何服务运行状况不正常，请勿升级。在继续之前，请联系思科 Technical Assistance Center (TAC) 以修复任何问题。

其他前提条件：

- **许可**

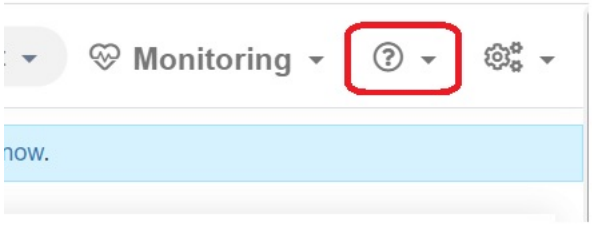
  如果您的 Tetration 部署当前没有有效许可证（或在评估期之外），则必须在升级前注册有效许可证。

  管理许可证需要站点管理权限。

  要查看许可证状态，请执行以下操作：

  在 Tetration Web 门户中，依次选择**监控 (Monitoring) > 许可证 (Licenses)**。如果您的集群许可证注册不合规，您将看到带有**执行操作 (Take action)** 链接的横幅。

  有关获取和注册许可证的信息，请点击此处以参阅 Tetration Web 门户中的《用户指南》：



  在用户指南中搜索“许可证”。

- **IPv6 支持（双堆栈模式）**

  （可选）在物理硬件上运行的 Cisco Secure Workload 集群可以配置为除使用 IPv4 外，还使用 IPv6 与集群或在集群内进行某些通信。（无论如何，Cisco Secure Workload 已出于策略目的处理 IPv6 流量。）

  只有在初始部署或升级到 3.6.1.5 版时才能启用此功能。

  如果您正在考虑启用双堆栈 (IPv6) 连接，请参阅双栈模式（IPv6 支持）的要求和限制，第 2 页。

- **其他功能**

  升级前可能需要采取行动的特定功能影响：

  - **Firepower 管理中心 (FMC) 集成：**

    如果升级 Cisco Secure Workload 并希望继续使用此集成，则必须先将 FMC 升级到所需版本。

    3.6 中的此集成与 3.5 实施存在显著差异。仔细阅读https://www.cisco.com/c/en/us/support/security/tetration/products-installation-and-configuration-guides-list.html中的《*Cisco Secure Workload* 和 *Firepower* 管理中心集成指南》，了解版本 3.6 的说明和要求。

    升级 Cisco Secure Workload 后，FMC 中的预过滤器策略将转换为访问控制策略，资产过滤器将转换为动态对象。

  - **AWS 连接器：**

    现有的 AWS 连接器将在升级时删除。升级后必须重新创建新的 AWS 云连接器。如有必要，请在升级前记录下已配置的信息。

  - Kubernetes EKS 外部协调器

    升级后，EKS 外部协调器将处于只读状态；如果要在升级后进行更改，请创建新的 AWS 连接器并启用**托管 Kubernetes 服务 (Managed Kubernetes services)** 选项。

  - **数据导出连接器：**

    此版本已删除对数据导出连接器（Alpha 版功能）的支持。如果配置了数据导出连接器；建议在升级到此版本之前禁用或删除它。

  - **其他更改：**

    其他不需要在升级前进行操作的行为更改在 3.6.1.5 版的发布说明中进行了说明，可从https://www.cisco.com/c/en/us/support/security/tetration/products-release-notes-list.html中获取。

- 此升级不需要任何新的公共可路由 IP 地址。
- 执行此升级需要客户支持权限。
- 确保具有客户支持权限的用户帐户已上传 SSH 密钥，以便进行故障排除。有关详细信息，请参阅 Tetration Web 门户提供的《用户指南》中的“导入 SSH 公钥”。
- 在执行升级之前，您应备份系统。有关详细信息，请参阅用户指南中有关数据备份和恢复 (DBR) 的信息，包括有关升级的小节。
- Google Chrome 浏览器是 Cisco Secure Workload 设置门户网站唯一支持的浏览器，该门户是本次升级所需的专用门户。

过程

步骤 1 从 Cisco.com 下载适用于您的部署的 RPM 文件：

a) 导航至 https://software.cisco.com/download/home/286309796/type。
b) 根据需要下载：
   - 对于 8-RU 或 39-RU 系统，请下载以下 RPM：
     - `tetration_os_UcsFirmware_k9-3.6.1.5.rpm`
     - `tetration_os_base_rpm_k9-3.6.1.5-1.el7.x86_64.rpm`
     - `tetration_os_adhoc_k9-3.6.1.5-1.el6.x86_64.rpm`
     - `tetration_os_mother_rpm_k9-3.6.1.5-1.el6.x86_64.rpm`
     - `tetration_os_rpminstall_k9-3.6.1.5-1.noarch.rpm`
     - `tetration_os_enforcement_k9-3.6.1.5-1.el6.x86_64.rpm`
   - 对于虚拟系统，请下载以下 RPM：
     - `tetration_os_ova_k9-3.6.1.5-1.el7.x86_64.rpm`
     - `tetration_os_adhoc_k9-3.6.1.5-1.el6.x86_64.rpm`
     - `tetration_os_mother_rpm_k9-3.6.1.5-1.el6.x86_64.rpm`
     - `tetration_os_rpminstall_k9-3.6.1.5-1.noarch.rpm`
     - `tetration_os_enforcement_k9-3.6.1.5-5.el6.x86_64.rpm`
c) 选中以确保每个 RPM 下载的 MD5 与 CCO 中的 MD5 匹配。

步骤 2 检查系统运行状况。如果任何服务运行不正常，则无法执行升级。
a) 在思科 Tetration GUI 中，点击设置按钮并选择**维护 (Maintenance)**。
b) 在左侧窗格中，点击**服务状态 (Service Status)**。
c) 在图中查找红色圆圈，表示服务不正常。

   或者，要查看服务运行状况的表格视图，请点击图形顶部的列表按钮，点击**全部展开 (Expand All)**，然后向下滚动页面以查看所有服务的状态。

d) 如果任何服务运行不正常，请在继续升级之前执行任何必要的修复以使服务正常运行。

步骤 3 在左侧导航菜单中，依次点击**维护 (Maintenance) > 升级 (Upgrade)**。

步骤 4 如有必要，请点击**升级 (Upgrade)** 选项卡。

步骤 5 按照屏幕上的步骤操作。不要跳过任何步骤。

使用**升级 (Upgrade)** 选项，而不是补丁升级选项。

步骤 6 点击**发送升级链接 (Send Upgrade Link)** 后，查找生成的电子邮件。

使用站点管理员或客户支持角色登录的用户将收到一封包含超链接的电子邮件，您必须使用它执行升级。邮件的主题为：

`[Tetration Analytics] 升级启动链接`

打开邮件并复制**升级集群 (Upgrade Cluster)** URL。

或者，您可以通过输入以下信息，从**维护 (Maintenance) > 浏览 (Explore)** 页面获取升级 URL：

- 快照操作：**POST**
- 快照主机：**orchestrator.service.consul**
- 快照路径：**upgrade_url**

步骤 7 打开新的 Google Chrome 浏览器选项卡，将升级 URL 粘贴到地址字段中，然后按 **Enter** 键。

这将打开 Cisco Secure Workload 设置门户，只有 Google Chrome 浏览器支持该界面。

步骤 8 在 Cisco Secure Workload 设置门户中，您必须以特定顺序上传 RPM，具体取决于您的设置。

对于 8-RU 或 39-RU 系统，请按给定顺序上传以下文件：

1. `tetration_os_rpminstall_k9-3.6.1.5-1.noarch.rpm`
2. `tetration_os_UcsFirmware_k9-3.6.1.5.rpm`
3. `tetration_os_adhoc_k9-3.6.1.5-1.el6.x86_64.rpm`
4. `tetration_os_mother_rpm_k9-3.6.1.5-1.el6.x86_64.rpm`
5. `tetration_os_enforcement_k9-3.6.1.5-1.el6.x86_64.rpm`
6. `tetration_os_base_rpm_k9-3.6.1.5-1.el7.x86_64.rpm`

对于虚拟系统，以给定顺序上传以下文件：

1. `tetration_os_rpminstall_k9-3.6.1.5-1.noarch.rpm`
2. `tetration_os_adhoc_k9-3.6.1.5-1.el6.x86_64.rpm`
3. `tetration_os_mother_rpm_k9-3.6.1.5-1.el6.x86_64.rpm`
4. `tetration_os_enforcement_k9-3.6.1.5-1.el6.x86_64.rpm`
5. `tetration_os_ova_k9-3.6.1.5-1.el7.x86_64.rpm`

要上传每个 RPM，请执行以下子步骤

a) 点击**选择文件 (Choose File)**。
b) 导航至 RPM，选择该文件，然后点击**打开 (Open)**。
c) 点击**上传 (Upload)**。

当您上传每个 RPM 时，页面上的 RPM 列表不会更新。这是预期行为。

如果在上传 `tetration_os_mother_rpm_k9-3.6.1.5-1.el6.x86_64.rpm` 文件后看到错误，只用等待大约 5 到 10 分钟，然后重新加载页面。重新加载页面后，您应该会看到已上传的 RPM 列表。

d) 对每个 RPM 重复这些子步骤。

步骤 9 点击**继续 (Continue)**。

系统将打开**站点配置 (Site Config)** 门户。

步骤 10 在**常规 (General)** 选项卡上：

（可选）更改 SSH 公钥。

步骤 11 点击**下一步 (Next)**。

步骤 12 在**电子邮件 (Email)** 选项卡上：

（可选）更改 UI 管理员电子邮件地址或管理警报电子邮件地址。

步骤 13 点击**下一步 (Next)**。

步骤 14 在 **L3** 选项卡上：

（可选）启用群集，使其在升级后的某些集群连接中除使用 IPv4 外还使用 IPv6。

重要提示！有关要求和限制，请参阅本程序前提条件中的链接。

要启用 IPv6：

a) 选中 **IPv6** 复选框。
b) 以 CIDR 符号输入枝叶 1 和枝叶 2 交换机的 **IPv6 地址**。
c) 输入枝叶 1 和枝叶 2 **IPv6 默认网关**。

如果在此页面上启用 IPv6，则还必须在下面的**网络 (Network)** 页面上配置 IPv6 字段。

步骤 15 点击**下一步 (Next)**。

步骤 16 在**网络 (Network)** 选项卡上：

- 如有必要，请更改 **CIMC 内部网络**、**CIMC 内部网络网关**、**DNS 解析器**和 **DNS 域**的值。
- **重要提示！**不要更改或删除现有的**外部网络**值。但可以添加其他 IPv4 网络。
- 如果在 L3 页面上启用了 IPv6：

  系统将自动选中 **IPv6** 复选框。

  指定为 Cisco Secure Workload 保留的 IPv6 地址：

  a. 输入**采用 CIDR 表示法的 IPv6 外部网络**。

  b.（可选）要将 IPv6 仅用于指定地址，请输入单个**外部 IPv6 IP**。

  请记住：

  - IPv6 外部网络字段中的前 3 个 IPv6 地址始终保留给 Cisco Secure Workload 集群的交换机，不应用于任何其他目的。
  - 对于 39 RU 集群，请确保 IPv6 外部网络或外部 IPv6 IP 列表中至少有 29 个 IPv6 地址。
  - 对于 8 RU 集群，请确保 IPv6 外部网络或外部 IPv6 IP 列表中至少有 20 个 IPv6 地址可用。

步骤 17 点击**下一步 (Next)**。

步骤 18 在**服务 (Service)** 选项卡上：

（可选）更改 NTP 和 SMTP 值。

如果需要更改系统日志值（如有），请使用 TAN 设备。

步骤 19 点击**下一步 (Next)**。

步骤 20 在**安全 (Security)** 选项卡上：

启用或禁用**代理连接的 SSL 强密码**。

步骤 21 点击**下一步 (Next)**。

您无法更改 **UI** 选项卡上的任何值。

步骤 22 点击**下一步 (Next)**。

您无法更改**高级 (Advanced)** 选项卡上的任何值。

步骤 23 点击**下一步 (Next)**。

步骤 24 在**恢复 (Recovery)** 选项卡上：

如果集群被配置为备用集群，则集群将以备用模式部署，其中包括较少的功能（仅支持热备模式）。

您无法更改此选项卡上的任何值。

步骤 25 点击**继续 (Continue)**。

升级过程开始。

升级过程会检查以确保：

- RPM 版本正确
- 集群运行正常
- 您提供的站点信息有效
- 交换机配置正确
- 信息字段已验证
- 在部署开始前同步 NTP
- 名称节点和辅助名称节点未处于故障转换状态

检查将需要几分钟。完成检查后，您将收到一封电子邮件，主题类似于以下示例：

```
TETRATION CLUSTER MyCluster: 验证令牌
```

邮件中包含所需的令牌以继续升级。

步骤 26 复制电子邮件正文中的令牌。

步骤 27 在 Cisco Secure Workload 设置门户中，将令牌粘贴到**验证令牌 (Validation Token)** 字段。

重要提示！请勿选中**忽略实例停止故障**复选框，除非思科员工明确指示这样做。

步骤 28 点击**继续 (Continue)**。

开始执行升级安装。当绿色进度条达到 100% 时，升级完成。所有实例都将显示“已部署”状态。

步骤 29 验证升级：

a) 在浏览器中打开 Cisco Secure Workload Web 门户。
b) 从左侧的黑色导航菜单中，依次选择**平台 (Platform) > 升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。
c) 点击**历史记录 (History)**。
d) 验证升级状态是否显示**成功 (Succeeded)**。

后续操作

如果已启用 IPv6：

- 您可以使用 IPv6 或 IPv4 访问 Cisco Secure Workload Web 界面。
- 默认情况下，软件代理继续使用 IPv4 连接到集群。如果希望软件代理能够与使用 IPv6 的集群通信，请执行以下操作：

  1. 在 Cisco Secure Workload UI 的左侧导航窗格中，点击**平台 (Platform)** > **集群配置 (Cluster Configuration)**。
  2. 配置**传感器 VIP FQDN (Sensor VIP FQDN)** 设置。有关详细信息，请参阅 Cisco.com 上提供的页面级帮助或《Secure Workload 用户指南》。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。