设置用户界面

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。

设置用户界面

开始之前

- 要完成此配置，您需要一台设备，例如具有以太网端口和互联网接入的笔记本电脑。
- 您需要使用以太网电缆将设备连接到 Cisco Secure Workload 集群中的最高服务器。
- Google Chrome 是设置门户的唯一受支持浏览器，这是此流程的一部分所必需的。
- （可选）从版本 3.6 及更高版本开始，您可以在双栈模式下配置集群，这允许将 IPv4 和 IPv6 用于某些安全工作负载组件之间以及 Cisco Secure Workload 与网络服务（例如 NTP 和 DNS）之间的通信。（无论是否启用双协议栈模式，Cisco Secure Workload 都已处理 IPv6 流量。）您只能在部署或升级期间启用此支持。

  如果您正在考虑启用对 IPv6 的支持，请参阅 双栈模式（IPv6 支持）的要求和限制，第 1 页。

重要事项 在以下程序的所有字段中输入 IPv4 地址，除非字段名称明确指出 IPv6。

步骤 1 使用 IP 地址 2.2.2.1/30 (255.255.255.252) 配置互联网设备。

步骤 2 使用以太网电缆将互联网设备上的以太网端口连接到 Cisco Secure Workload 集群顶部最高层服务器上的 LOM 端口 2 (LAN2)。

步骤 3 在互联网设备上，打开 Chrome 浏览器并转至 http://2.2.2.2:9000。

注释 Chrome 浏览器是使用此流程测试的唯一浏览器。

系统将打开“设置诊断”页面。

步骤 4 如果“诊断”页面中存在错误，请在继续执行此程序之前检查集群设备之间的布线连接是否断开或电缆布线不正确。完成后，返回步骤 2。

有关正确的布线，请参阅 C1-Workload 集群设备布线 和 C1-Workload-M 集群设备布线 。

步骤 5 点击**继续**。

系统将打开“RPM 上传”页面。

注释 如果改为打开“站点配置”页面，请输入以下 URL 以打开“RPM 上传”页面：

`http://2.2.2.2:9000 /upload`

步骤 6 将 RPM 文件上传到 Cisco Secure Workload 云。

您必须按以下顺序上传文件：

- tetration_os_rpminstall_k9
- tetration_os_UcsFirmware_k9
- tetration_os_adhoc_k9
- tetration_os_mother_rpm_k9
- tetration_os_base_rpm_k9

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

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_k9-2.1.1.31-1.el6.x86_64.rpm` 文件后看到错误，请等待大约 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。该错误是由于协调器重新启动造成的，不构成问题。

d) 对每个 RPM 重复这些步骤。

完成 RPM 上传后，系统将打开“站点配置”页面。

步骤 7 使用“站点配置”页面设置新站点，如下所示：

- 点击 **常规**。
  1. 在 **站点名称** 字段中，输入唯一的集群名。
  2. 在 **SSH 公共密钥** 字段中，粘贴身份验证密钥。

注释　　生成可用于集群 SSH 访问的您自己的 SSH 密钥对。

我们强烈建议您将 SSH 密钥保存在安全、持久且可访问的位置，以便使用 ta_guest 访问进行故障排除或恢复集群。

3. 点击**下一步**。

- 点击 **电邮**。

1. 填写必填的电邮地址。
2. 点击**下一步**。

- 点击 **L3**。

输入每个请求的地址。带有 * 的字段为必填字段。

除非字段名称指定 IPv6，否则输入所有地址为 IPv4。

（可选）如果要安装 3.6 或更高版本的软件：要启用双协议栈模式（同时支持 IPv4 和 IPv6），请执行以下操作：

1. 选择 IPv6 复选框。
2. 以 CIDR 符号输入枝叶 1 和枝叶 2 交换机的 IPv6 地址。
3. 输入枝叶 1 和枝叶 2 IPv6 默认网关。
4. 点击**下一步**。

- 点击**网络 (Network)**。

除非字段名称指定 IPv6，否则输入所有地址为 IPv4。

1. 在 **内部网络 IP 地址** 字段中，粘贴协调器部署输出中的地址。
2. 在 **外部网络 IP 地址** 字段中，粘贴协调器部署输出中的地址。
3. 在 **外部网关 IP 地址** 字段中，粘贴协调器部署输出中的地址。
4. 在 **DNS 解析器 IP 地址** 字段中，粘贴协调器部署输出中的地址。
5. 在 **DNS 域** 字段中，输入您的 DNS 域（例如，`cisco.com`）。
6. （软件版本 3.6 或更高版本）如果在 L3 页面上启用了 IPv6，则会自动选择 **IPv6** 。

   如果选择 IPv6，则必须指定为 Cisco Secure Workload 保留的 IPv6 地址：

   - 输入 **外部 IPv6 网络**。

     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。

   - 如果要仅对某些地址使用 IPv6，请在 **外部 IPv6 IP** 字段中输入这些地址。

注释
- 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。

7. 点击**下一步**。

- 点击 **服务**。
  1. 在 **NTP 服务器** 字段中，输入协调器部署输出中以空格分隔的 NTP 服务器名称或 IP 地址列表。
  2. 在 **SMTP 服务器** 字段中，输入 Cisco Secure Workload 可用于发送邮件的 SMTP 服务器的名称或 IP 地址。此服务器必须可由 Cisco Secure Workload 访问。
  3. 在 **SMTP 端口** 字段中，输入 SMTP 服务器的端口号。AWS 限制使用端口 25 和 465。您必须正确配置账户或使用端口 587。
  4. （可选）在 **SMTP 用户名** 字段中，输入 SMTP 身份验证的用户名。
  5. （可选）在 **SMTP 密码** 字段中，输入 SMTP 身份验证的密码。
  6. （可选）在 **HTTP 代理服务器** 字段中，输入可供 Cisco Secure Workload 用于访问互联网上的外部服务的 HTTP 代理服务器的名称或 IP 地址。
  7. （可选）在 **HTTP 代理端口** 字段中，输入 HTTP 代理服务器的端口号。
  8. （可选）在 **HTTPS 代理服务器** 字段中，输入可供 Cisco Secure Workload 用于访问互联网上的外部服务的 HTTPS 代理服务器的名称或 IP 地址。
  9. （可选）在 **HTTPs 代理端口** 字段中，输入 HTTPs 代理服务器的端口号。
  10. （可选）在 **系统日志服务器** 字段中，输入可供 Cisco Secure Workload 用于发送警报的系统日志服务器的名称或 IP 地址。
  11. （可选）在 **系统日志端口** 字段中，输入系统日志服务器的端口号。
  12. （可选）在 **系统日志严重性** 字段中，输入系统日志消息的严重性级别。可能的值包括信息、通知、警告、错误、关键、警报和应急。
  13. 点击**下一步**。
- 点击 **UI**。
  1. 在 **UI VRRP VRID** 字段中，输入 **77**，除非您需要唯一的 VRID。
  2. 在 **UI FQDN** 字段中，输入您访问集群的完全限定域名。
  3. 将 **UI Airbrake Key** 字段留空。
  4. 点击**下一步**。

     Tetration (Cisco Secure Workload) 验证您的配置设置并显示设置的状态。
- 点击 **高级**。

1. 在 **外部 IP** 字段中，输入 IPv4 地址。
2. 点击**继续**。

步骤 8 如果有任何失败，请点击 **返回** 并编辑配置（请参阅步骤 7）。

注释 离开此页面后，您将无法在设置 GUI 中修改这些设置。但是，您可以稍后从 GUI 中的公司页面修改设置。

步骤 9 如果没有记录您的配置失败，并且您不需要进行任何更改，请点击 **继续**。

根据您指定的设置配置 Cisco Secure Workload。此过程需要一到两个小时，您无需进行任何交互。

下一步做什么

如果您部署了软件版本 3.6 或更高版本，并且启用了 IPv6 连接：

- 您可以使用 IPv4 或 IPv6 访问 Cisco Secure Workload Web 门户。
- 默认情况下，软件席座使用 IPv4 与 Cisco Secure Workload 集群通信，即使集群已启用支持 IPv6。如果您希望受支持的席座为此目的使用 IPv6，则必须在 Cisco Secure Workload Web 门户的 **平台 > 集群配置** 页面上配置 **传感器 VIP FQDN** 字段。有关重要说明，请参阅用户指南，可从 Cisco Secure Workload Web 门户获取在线帮助，也可从 https://www.cisco.com/c/en/us/support/security/tetration/products-installation-and-configuration-guides-list.html获取。

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。