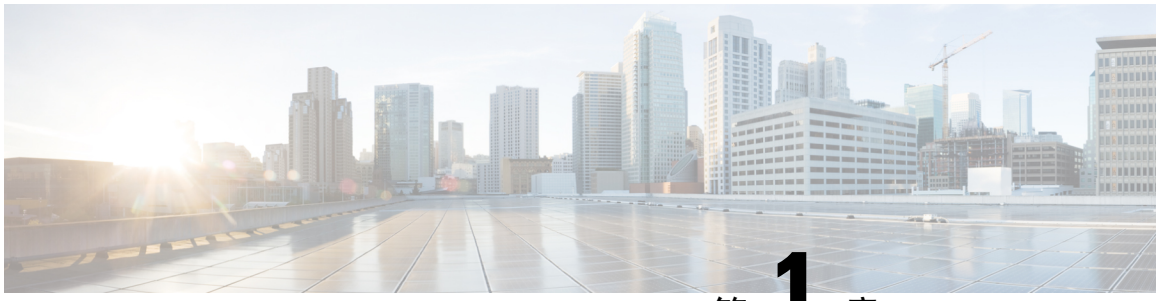
适用于 Tetration 的思科 Firepower 管理中心补救模块，版本 1.0.1 快速入门指南

首次发布日期: 2018 年 8 月 1 日

上次修改日期: 2018 年 9 月 20 日

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

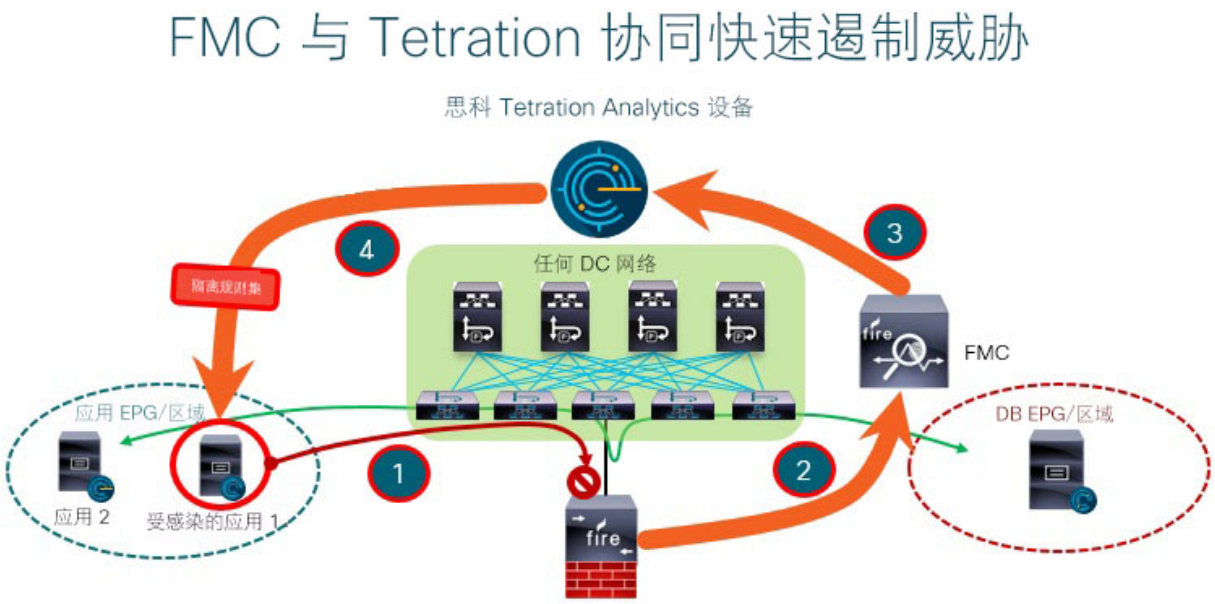


第 1 章

简介

概述

借助适用于 Tetration 的思科 Firepower 管理中心 (FMC) 补救模块，当 FMC 检测到从受感染的主机对您的网络发起的攻击时，Tetration Analytics (TA) 实施代理可以隔离发起攻击的主机，这样任何流量都无法再进出该主机。下图显示了安装补救模块时 FMC 和 Tetration 之间的关系：



图中还显示了隔离网络攻击的整体过程：

步骤 1 一旦主机中的某个应用受到感染，主机就会对您的网络发起攻击。Firepower 设备（物理或虚拟）上运行的思科 Firepower 威胁防御 (FTD) 会在线阻止攻击 。

步骤 2 系统会生成包括感染相关信息的入侵事件并向负责管理 FTD 的 FMC 报告。

步骤 3 攻击会触发 FMC 上的补救模块使用北向 API 来请求 Tetration 隔离受感染的主机。

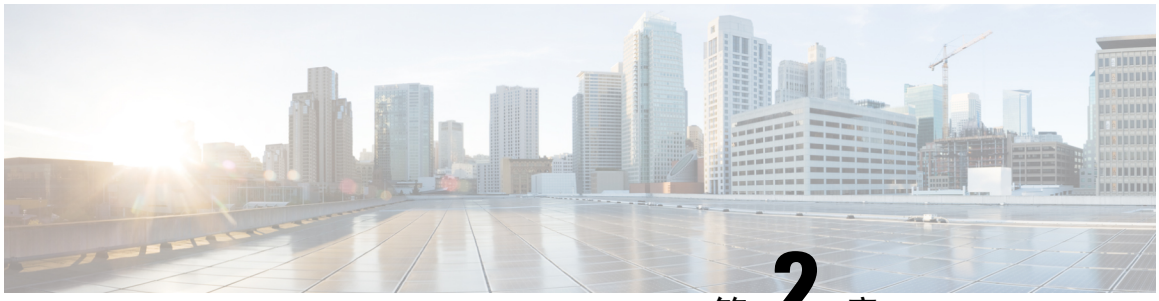
步骤 4 Tetration 会将隔离请求发送至受感染的主机上的实施代理，从而快速遏制受感染的应用工作负载。

必备条件

- 在 TA 中预定义绝对策略，以丢弃进出任何标注了“隔离”的主机的所有流量。如果您想要隔离部分流量，请在 TA 中自定义该策略，以只拒绝部分类型的流量，而不是全部类型的流量。有关更多信息，请在 TA GUI 中参阅《用户指南》。
- Tetration 代理是在 Linux 或 Windows 等主机操作系统中运行的软件。作为实施代理，它们还能够在所安装的主机上设置防火墙规则。在您想要保护的网络主机上安装实施代理。有关更多信息，请参阅思科 Tetration Analytics 的《软件代理安装指南》。

相关文档

- Firepower 管理中心配置指南
- 思科 Tetration Analytics



第 2 章

执行安装

执行安装

要下载并安装适用于 Tetration 的思科 Firepower 管理中心补救模块，请完成以下步骤：

步骤 1 使用网络浏览器下载补救模块：

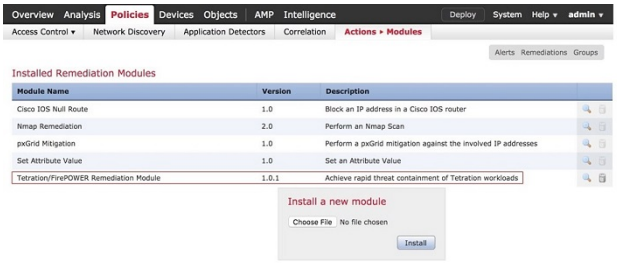
https://software.cisco.com/download/home/286259687/type

步骤 2 将补救模块安装到 FMC 上：

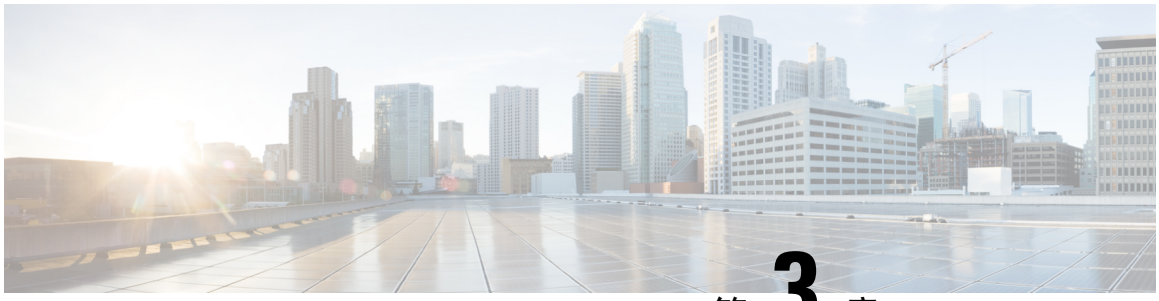
1. 在 FMC GUI 中，导航至**策略 > 操作 > 模块**。
2. 在**安装新模块**对话框中，点击**选择文件**，如下图所示。
3. 选择第 1 步中已下载的补救模块的文件。
4. 点击**安装**。

   注释 如果系统显示访问错误消息，请清除错误消息并重复第 2 步。

在成功安装后，已安装的补救模块的列表中会显示适用于 Tetration 的思科 Firepower 管理中心补救模块：



执行安装



第 3 章

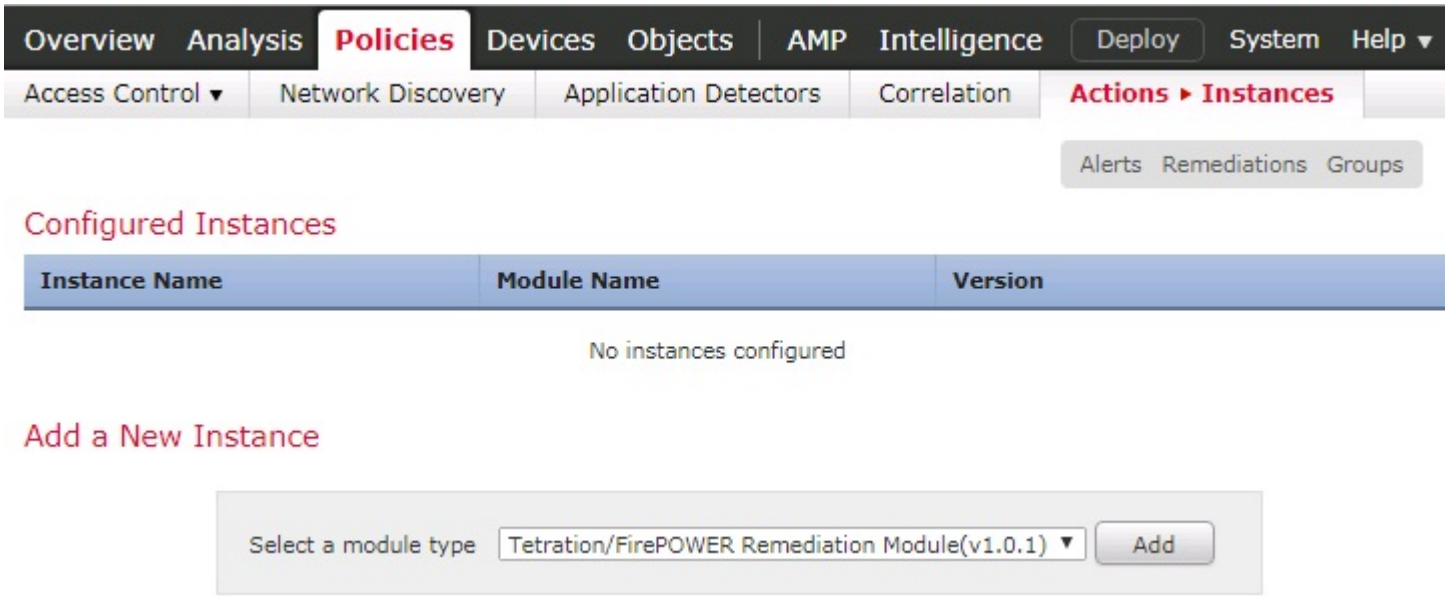
配置

配置

要配置 FMC 上安装的补救模块，请在 FMC GUI 中完成以下程序：

步骤 1 为您的网络中每个 Tetration Analytics (TA) 服务器补救模块创建实例：

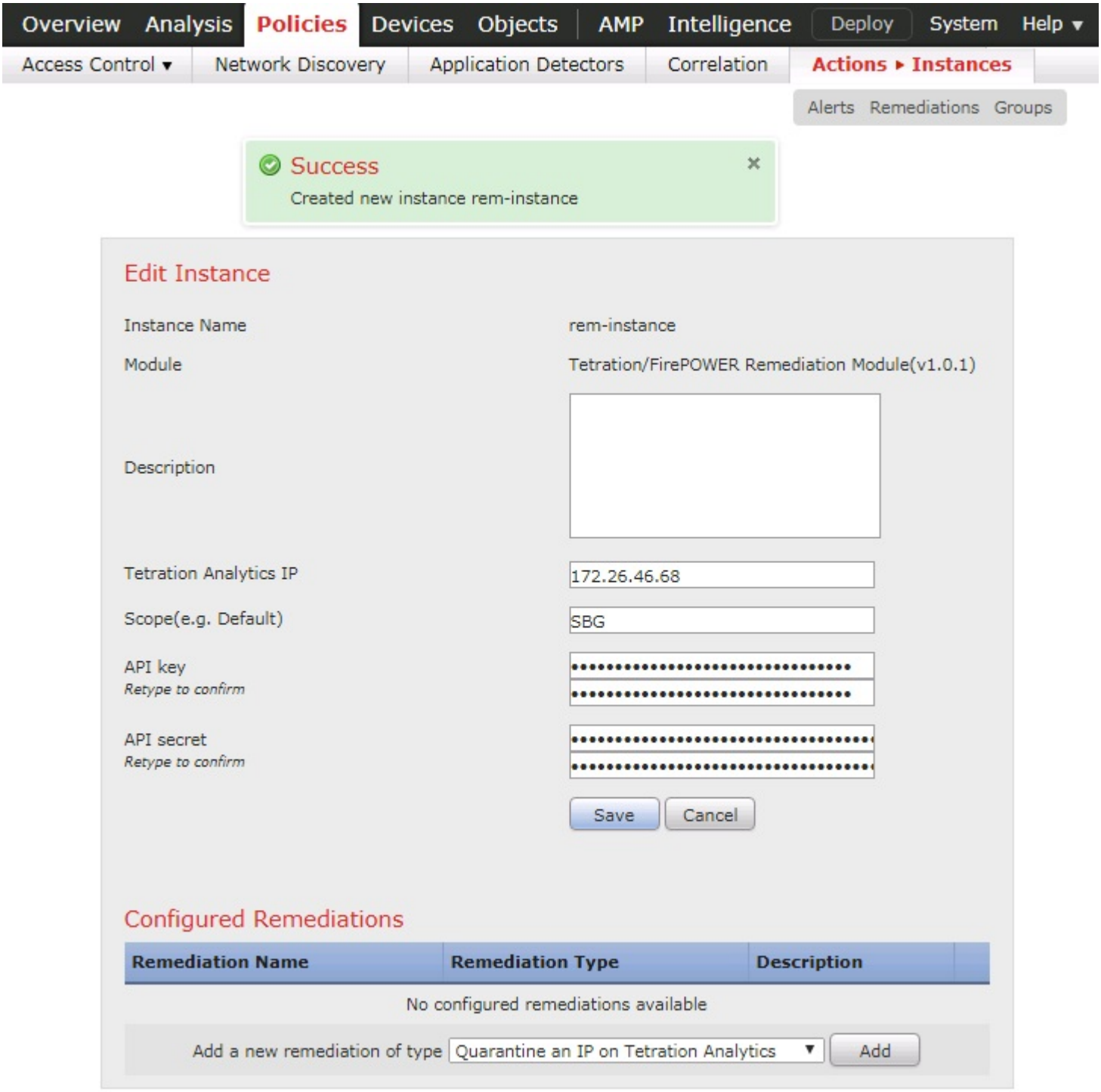
1. 导航至**策略 > 操作 > 实例**。
2. 在下拉列表中选择补救模块，然后点击**添加**。



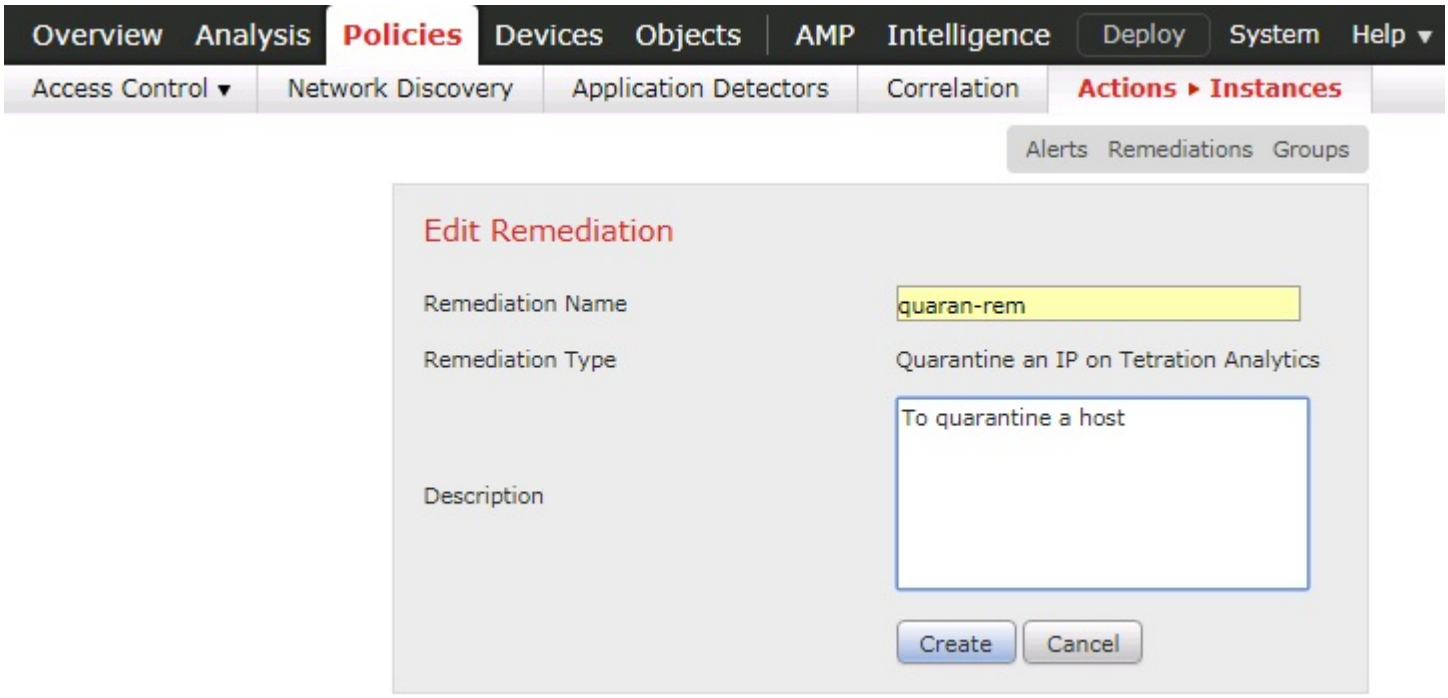
3. 输入**实例名称**（在此示例中，为 **`rem-instance`**）。
4. 输入 TA 服务器的 IP 地址、API 密钥、API 密码和可能发起攻击的主机所在的范围。点击**创建**。

配置

注释　此时，系统不会根据 TA 服务器验证 API 密钥和密码。必须先由站点管理员、客户支持或根范围所有者角色在 TA 中创建 API 密钥和密码。复制该信息在此处使用。有关更多详细信息，请参阅 TA API 配置指南。

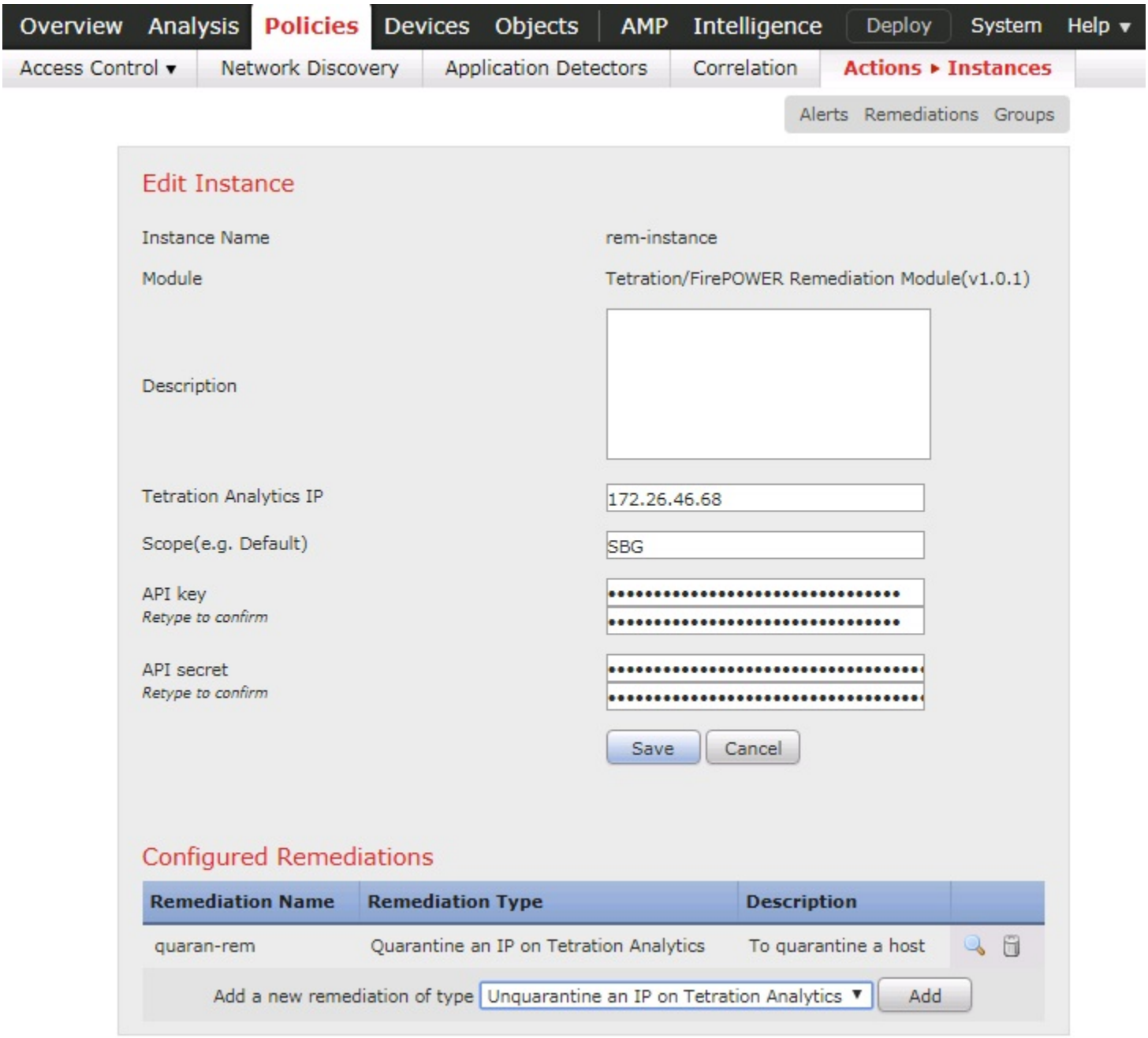


5. 在**已配置的补救**下，选择补救类型（在此示例中，为**在 Tetration Analytics 上隔离 IP**），然后点击**添加**以添加新补救。
6. 输入**补救名称**（在此示例中，为 **quaran-rem**），然后点击**创建**。



7. 表中会随后显示您刚配置的补救。点击**保存**。

配置



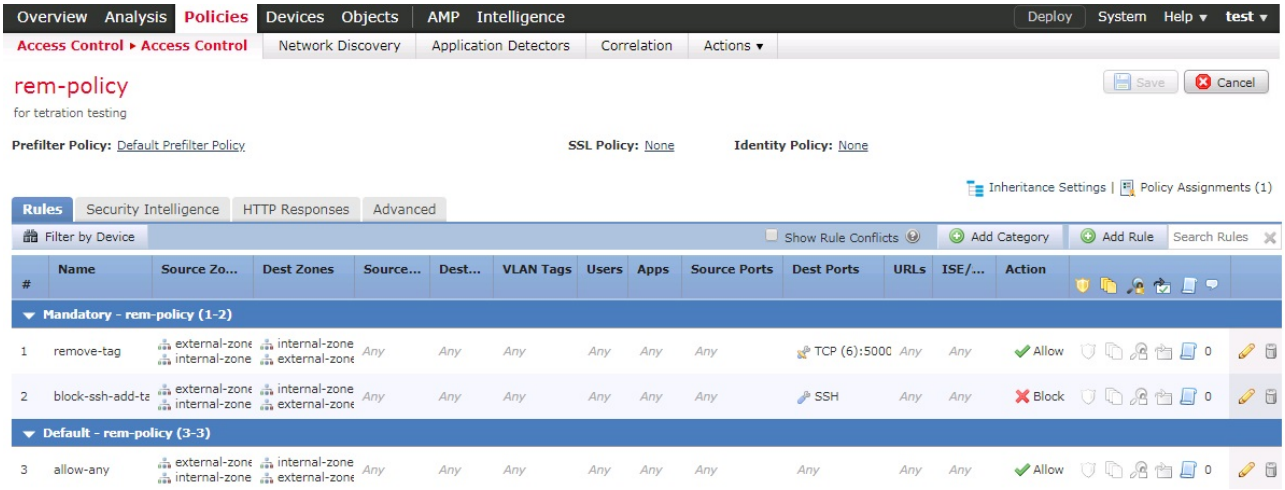
步骤 2 配置访问控制策略（在此示例中，为 **rem-policy**）：

1. 导航至**策略 > 访问控制 > 规则**。
2. 点击**添加规则**（例如，**block-ssh-add-tag**）。
3. 对于**操作**，选择**阻止**。
4. 在**端口**选项卡中，从目的端口的协议列表中选择 **SSH**，然后点击**添加**。

5. 点击**保存**。
6. 在**日志记录**选项卡中，选择**在连接开始时记录**。

   重要事项 确保对访问规则启用了日志记录，以便 FMC 接收事件通知。

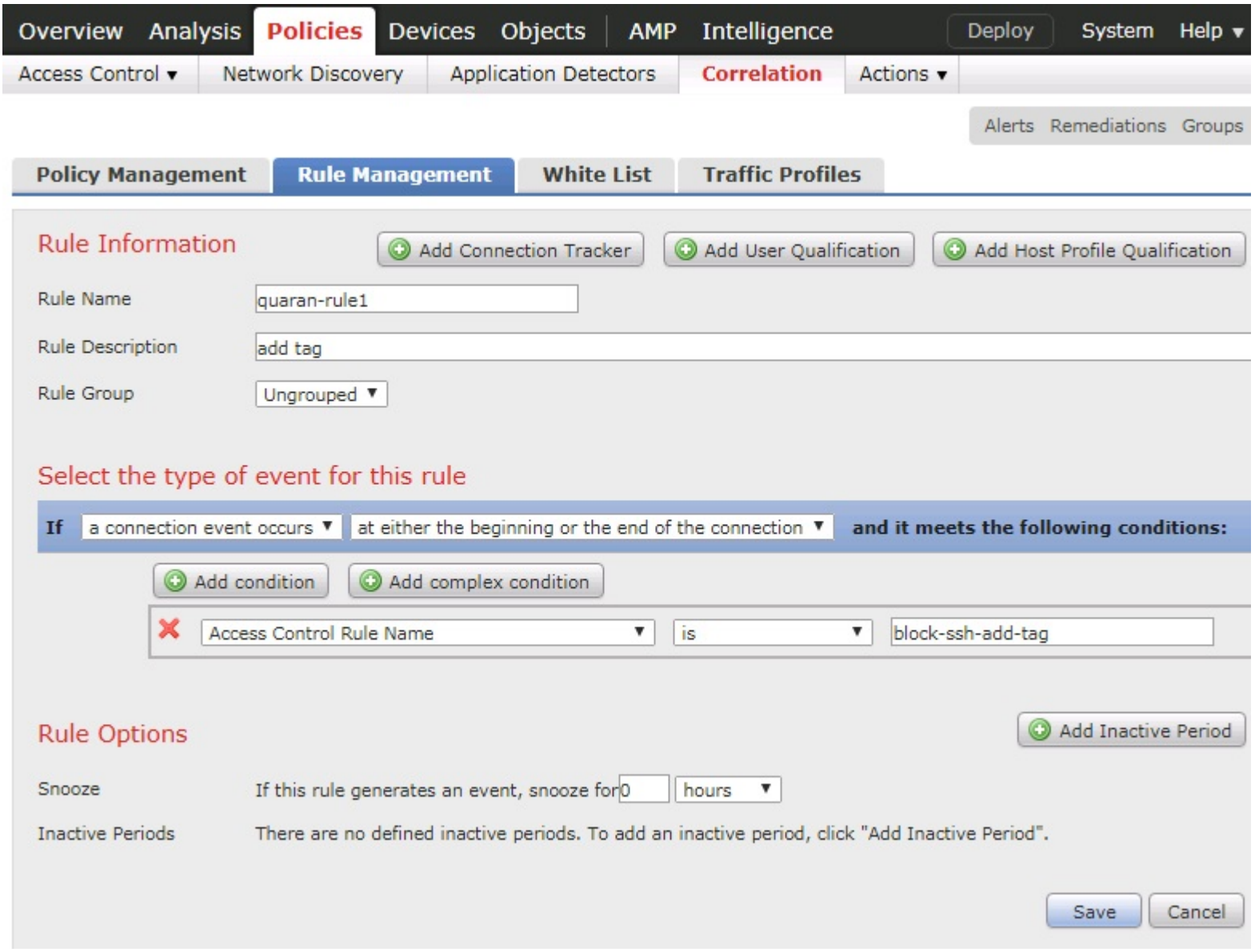
7. 点击**保存**。



步骤 3 配置关联规则：

1. 导航至**策略 > 关联 > 规则管理**。
2. 输入**规则名称**（在此示例中，为 **`quaran-rule1`**）和说明 （可选）。
3. 在**为此规则选择事件类型**部分中，选择**连接事件发生**和**连接开始或结束时**。
4. 点击**添加条件**，然后将运算符从 **OR** 更改为 **AND**。
5. 在下拉列表中，选择**访问控制规则名称**、**是**，然后输入您之前在第 2 步中配置的访问控制规则名称（在此示例中，为 **`block-ssh-add-tag`**）。

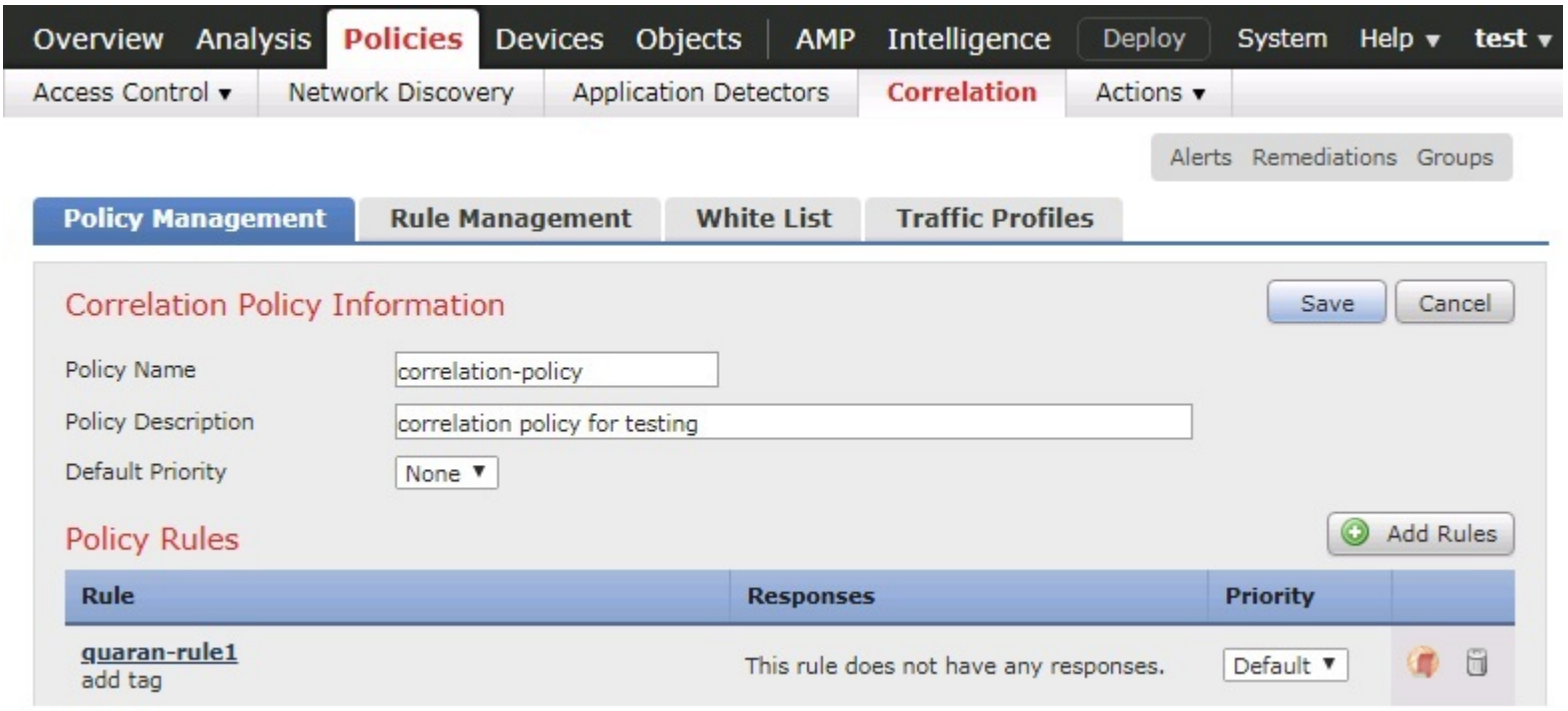
配置



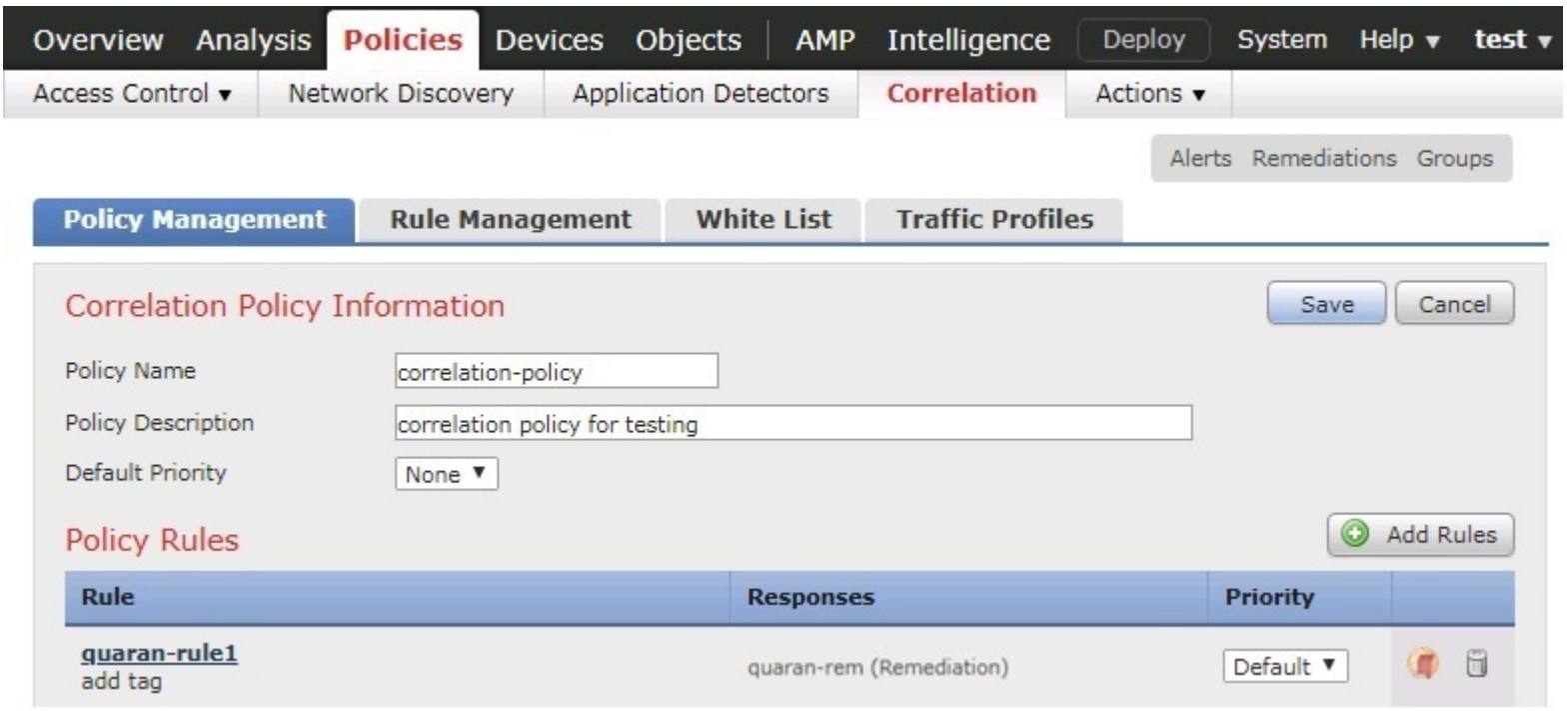
6. 点击**保存**。

步骤 4 将补救模块的实例作为响应与关联规则进行关联：

1. 导航至**策略 > 关联 > 策略管理**。
2. 点击**创建策略**。
3. 输入**策略名称**（在此示例中，为 **correlation-policy**）和说明（可选）。
4. 从**默认优先级**下拉列表中选择策略的优先级。选择**无**可仅使用规则优先级。
5. 点击**添加规则**，选择您之前在第 3 步中配置的关联规则（在此示例中，为 **quaran-rule1**），然后点击**添加**。

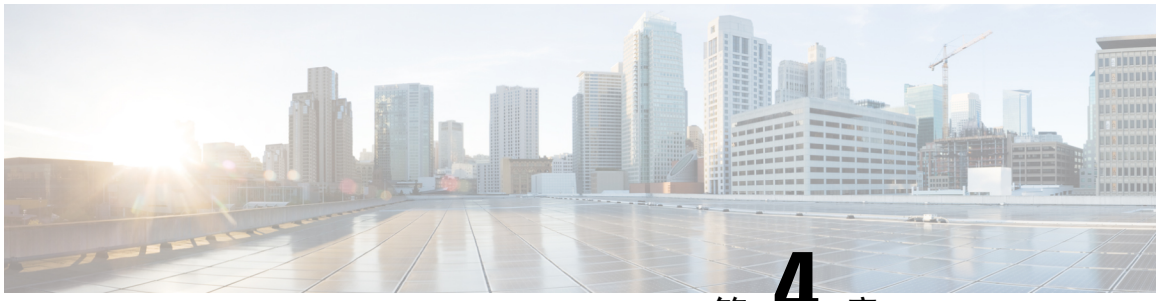


6. 点击规则旁边的**响应**图标，然后将响应（在此示例中，为 **quaran-rem**）分配给该规则。点击**更新**。



7. 点击**保存**。

配置



第 4 章

验证

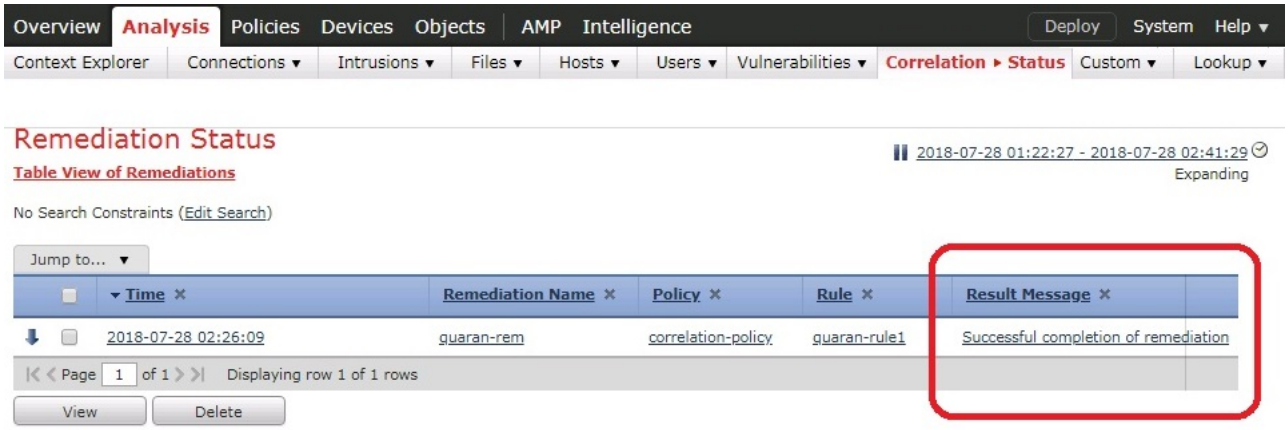
验证

由于补救可能因各种原因失败，请执行以下步骤以验证补救是否成功：

步骤 1 在相关的关联规则触发补救模块后，请在 FMC GUI 中查看执行补救的状态。

步骤 2 导航至**分析> 关联 > 状态**。

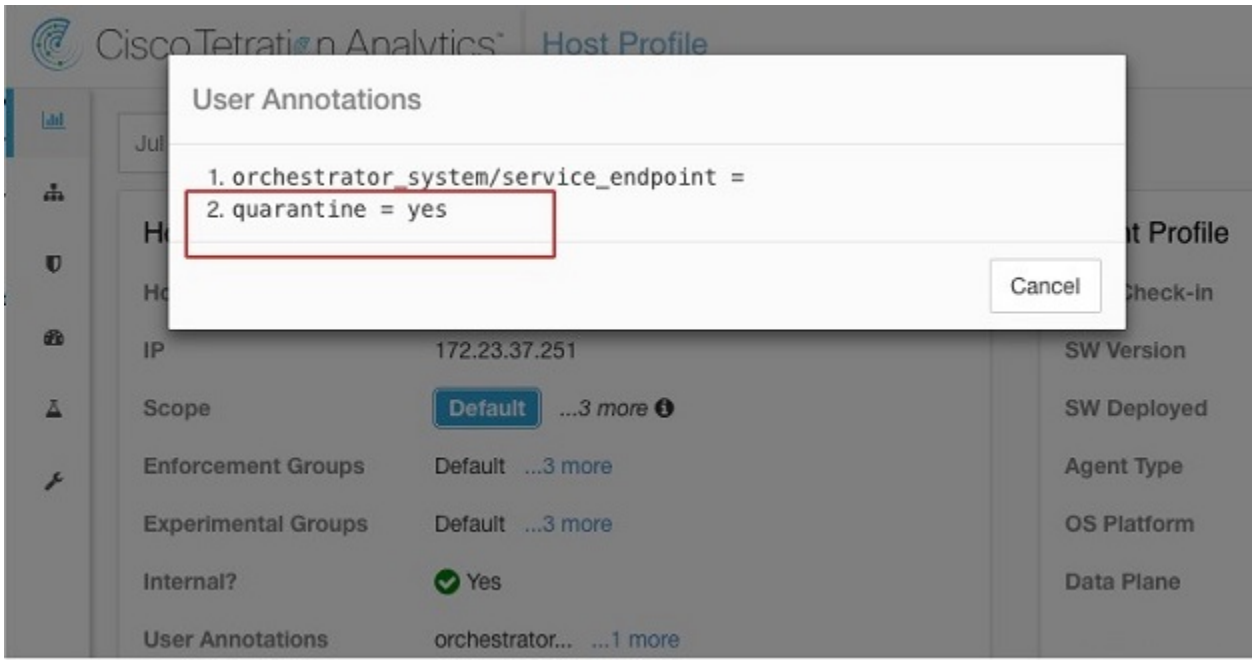
步骤 3 在“补救状态”表中，找到您的策略所在的行，并查看结果消息。



步骤 4 在完成补救后，请转至 TA GUI：

1. 导航至**可视性 > 资产搜索**。
2. 输入受感染的主机的 IP 地址，然后点击**搜索**。
3. 在用户注释中，您应该会看到受感染的主机的 IP 地址部分有**隔离 = 是**注释。

验证



下一步做什么

在清理隔离的主机且它不再受到感染后，您可以使用 Tetration（建议）将**隔离 = 是**注释改回为**隔离 = 否**，如下所示：

- 例如，如果不再受到感染的隔离的主机是 172.21.208.11 且在**默认**范围内，请创建 CSV 文件，如下所示：

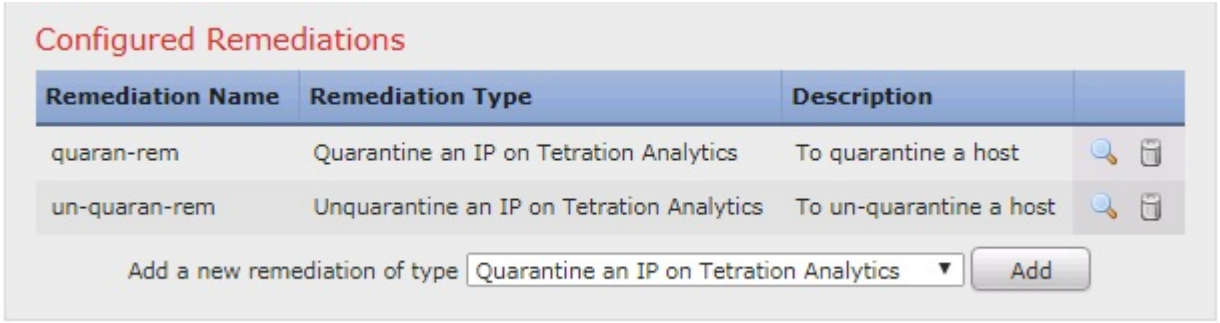
```
IP,VRF,quarantine
172.21.208.11,Default,no
```

- 导航至**应用 > 资产上传**。有关如何将您的 CSV 文件上传至 Tetration 的说明，请参阅 Tetration 服务器上的在线帮助用户指南：

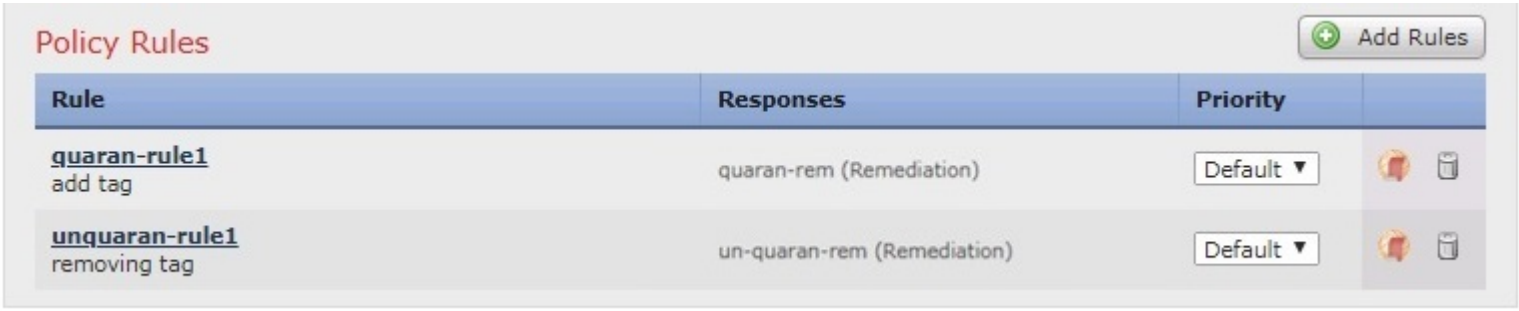
  `https://<your-Tetration-server-IP-address>/documentation/ui/inventory/user_annotations.html`

或者，使用 FMC 补救模块删除隔离（出于安全考虑，不建议在生产网络中使用），如下所示：

- （请参阅“配置：第 1 步”）添加使用“取消隔离”补救类型的新补救。编辑同一实例，并在**已配置的补救**下，选择并添加“取消隔离”补救类型（在此示例中，为 **un-quaran-rem**）。



- （请参阅“配置：第 2 步”）将访问控制策略（在此示例中，为 **remove-tag**）添加至可用于触发“取消隔离”补救的同一策略（在此示例中，为 **rem-policy**）。
- （请参阅“配置：第 3 步”）添加使用访问控制规则（在此示例中，为 **unquaran-rule1**）的关联规则（在此示例中，为 **remove-tag**）。
- （请参阅“配置：第 4 步”）将“取消隔离”响应（在此示例中，为 **un-quaran-rem**）分配至该关联规则（在此示例中，为 **unquaran-rule1**）。



- 在该规则匹配后，“取消隔离”补救会被触发以删除隔离注释。

验证