



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

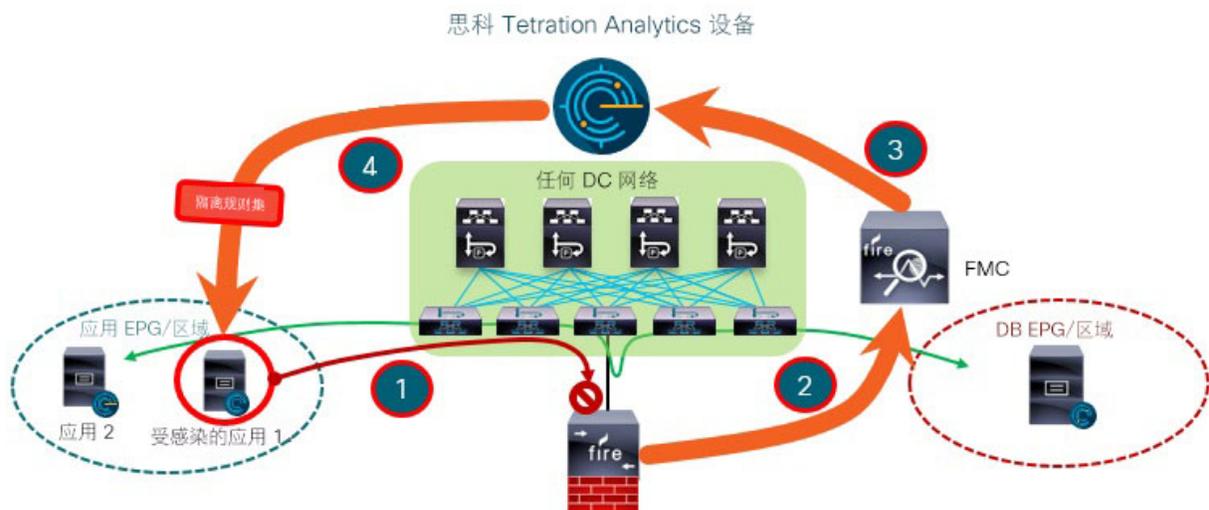
简介

- 概述，第 1 页
- 必备条件，第 2 页
- 相关文档，第 2 页

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：

FMC 与 Tetration 协同快速遏制威胁



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。在您想要保护的網絡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，第 3 页

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：

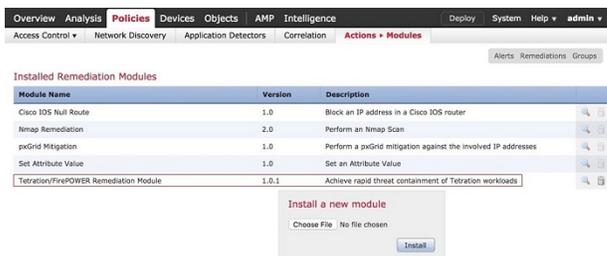
<https://software.cisco.com/download/home/286259687/type>

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：





第 3 章

配置

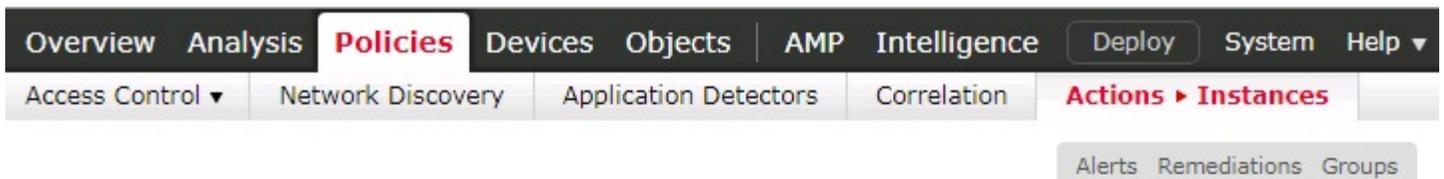
- [配置](#)，第 5 页

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。



Configured Instances

Instance Name	Module Name	Version
---------------	-------------	---------

No instances configured

Add a New Instance

Select a module type

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**。

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](#)。

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy System Help ▾

Access Control ▾ Network Discovery Application Detectors Correlation **Actions ▸ Instances**

Alerts Remediations Groups

✔ Success ✕

Created new instance rem-instance

Edit Instance

Instance Name: rem-instance

Module: Tetration/FirePOWER Remediation Module(v1.0.1)

Description:

Tetration Analytics IP:

Scope(e.g. Default):

API key
Retype to confirm:

API secret
Retype to confirm:

Configured Remediations

Remediation Name	Remediation Type	Description
No configured remediations available		

Add a new remediation of type

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。

The screenshot shows the Tetration Analytics web interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', 'Intelligence', 'Deploy', 'System', and 'Help'. Below this, a secondary navigation bar contains 'Access Control', 'Network Discovery', 'Application Detectors', 'Correlation', and 'Actions > Instances'. A sub-menu for 'Alerts Remediations Groups' is visible. The main content area displays the 'Edit Remediation' dialog box with the following fields:

- Remediation Name:** quaran-rem
- Remediation Type:** Quarantine an IP on Tetration Analytics
- Description:** To quarantine a host

At the bottom of the dialog are 'Create' and 'Cancel' buttons.

7. 表中会随后显示您刚配置的补救。点击保存。

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy System Help ▾

Access Control ▾ Network Discovery Application Detectors Correlation **Actions ▸ Instances**

Alerts Remediations Groups

Edit Instance

Instance Name rem-instance

Module Tetration/FirePOWER Remediation Module(v1.0.1)

Description

Tetration Analytics IP 172.26.46.68

Scope(e.g. Default) SBG

API key
Retype to confirm

API secret
Retype to confirm

Save Cancel

Configured Remediations

Remediation Name	Remediation Type	Description
quaran-rem	Quarantine an IP on Tetration Analytics	To quarantine a host

Add a new remediation of type **Unquarantine an IP on Tetration Analytics** Add

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。

The screenshot shows the FMC interface for configuring a policy named 'rem-policy'. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Policies' section is active, showing 'Access Control' and 'Access Control' sub-sections. The policy is titled 'rem-policy' and is used for 'tetration testing'. It has a 'Prefilter Policy' of 'Default Prefilter Policy', an 'SSL Policy' of 'None', and an 'Identity Policy' of 'None'. The 'Rules' tab is selected, showing a table of rules. The table has columns for '#', 'Name', 'Source Zones', 'Dest Zones', 'Source...', 'Dest...', 'VLAN Tags', 'Users', 'Apps', 'Source Ports', 'Dest Ports', 'URLs', 'ISE/...', and 'Action'. There are three rules listed:

#	Name	Source Zones	Dest Zones	Source...	Dest...	VLAN Tags	Users	Apps	Source Ports	Dest Ports	URLs	ISE/...	Action
Mandatory - rem-policy (1-2)													
1	remove-tag	external-zone internal-zone	internal-zone external-zone	Any	Any	Any	Any	Any	Any	TCP (6):5000	Any	Any	Allow
2	block-ssh-add-tag	external-zone internal-zone	internal-zone external-zone	Any	Any	Any	Any	Any	Any	SSH	Any	Any	Block
Default - rem-policy (3-3)													
3	allow-any	external-zone internal-zone	internal-zone external-zone	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow

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**）。

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy System Help ▾

Access Control ▾ Network Discovery Application Detectors **Correlation** Actions ▾ Alerts Remediations Groups

Policy Management **Rule Management** White List Traffic Profiles

Rule Information

Rule Name

Rule Description

Rule Group

Select the type of event for this rule

If at either the beginning or the end of the connection ▾ and it meets the following conditions:

is

Rule Options

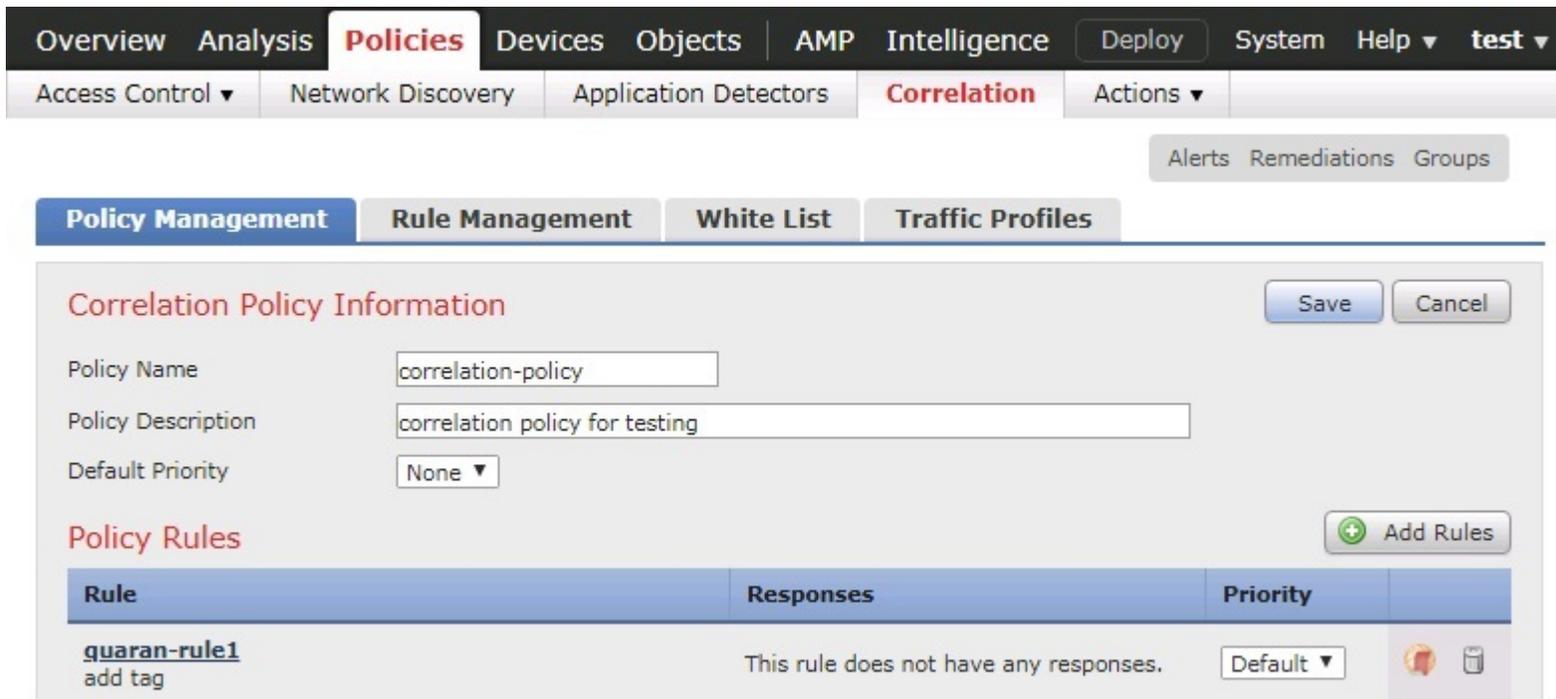
Snooze If this rule generates an event, snooze for hours ▾

Inactive Periods There are no defined inactive periods. To add an inactive period, click "Add Inactive Period".

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。



Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy System Help test

Access Control Network Discovery Application Detectors **Correlation** Actions Alerts Remediations Groups

Policy Management Rule Management White List Traffic Profiles

Correlation Policy Information

Policy Name: correlation-policy

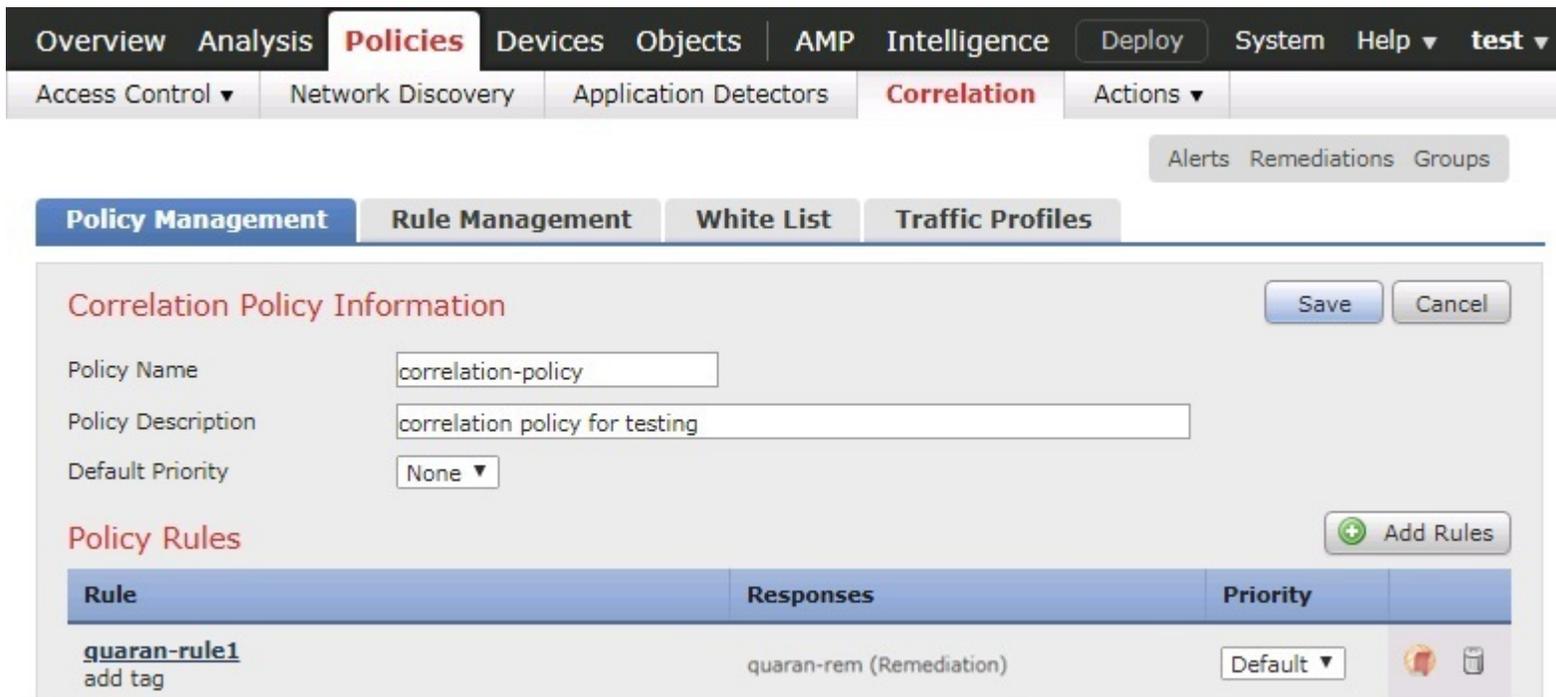
Policy Description: correlation policy for testing

Default Priority: None

Policy Rules

Rule	Responses	Priority
quaran-rule1 add tag	This rule does not have any responses.	Default

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。



Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy System Help test

Access Control Network Discovery Application Detectors **Correlation** Actions Alerts Remediations Groups

Policy Management Rule Management White List Traffic Profiles

Correlation Policy Information

Policy Name: correlation-policy

Policy Description: correlation policy for testing

Default Priority: None

Policy Rules

Rule	Responses	Priority
quaran-rule1 add tag	quaran-rem (Remediation)	Default

7. 点击保存。



第 4 章

验证

• 验证，第 13 页

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。

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help

Context Explorer Connections Intrusions Files Hosts Users Vulnerabilities Correlation Status Custom Lookup

Remediation Status

2018-07-28 01:22:27 - 2018-07-28 02:41:29 Expanding

Table View of Remediations

No Search Constraints (Edit Search)

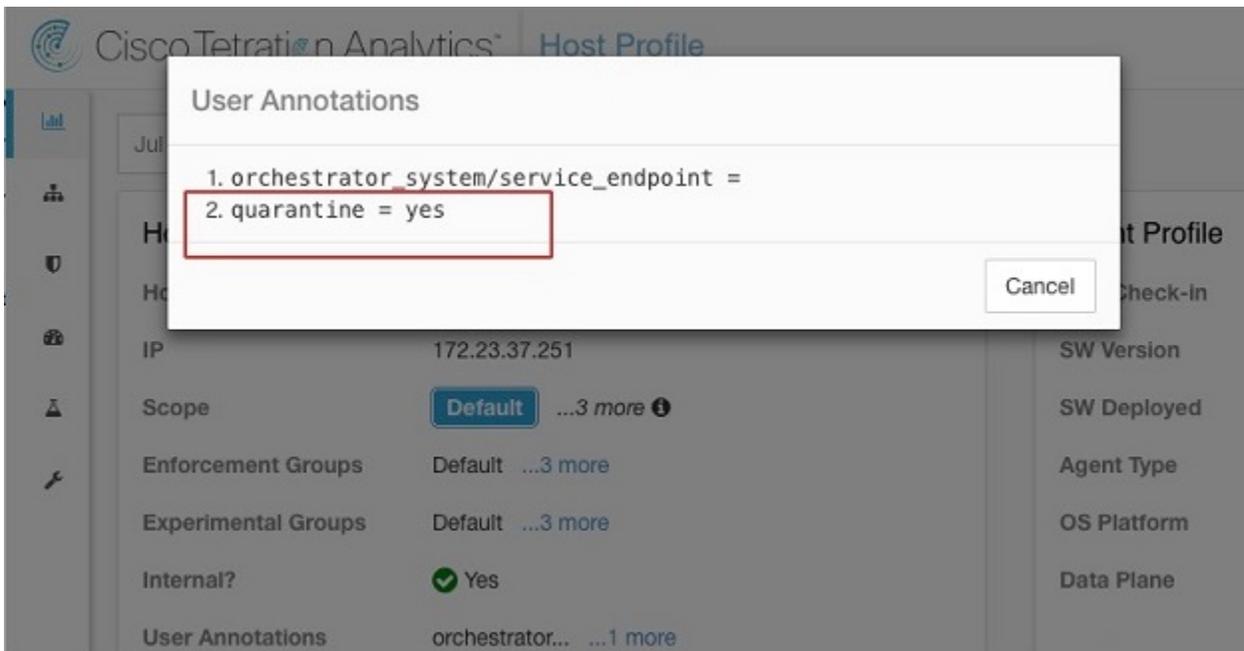
Jump to...	Time	Remediation Name	Policy	Rule	Result Message
	2018-07-28 02:26:09	guaran-rem	correlation-policy	guaran-rule1	Successful completion of remediation

<< Page 1 of 1 >> Displaying row 1 of 1 rows

View Delete

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。



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**）。

Configured Remediations

Remediation Name	Remediation Type	Description	
quaran-rem	Quarantine an IP on Tetration Analytics	To quarantine a host	 
un-quaran-rem	Unquarantine an IP on Tetration Analytics	To un-quarantine a host	 

Add a new remediation of type

- （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**）。

Policy Rules

Rule	Responses	Priority	
<u>quaran-rule1</u> add tag	quaran-rem (Remediation)	Default ▾	 
<u>unquaran-rule1</u> removing tag	un-quaran-rem (Remediation)	Default ▾	 

- 在该规则匹配后，“取消隔离”补救会被触发以删除隔离注释。

