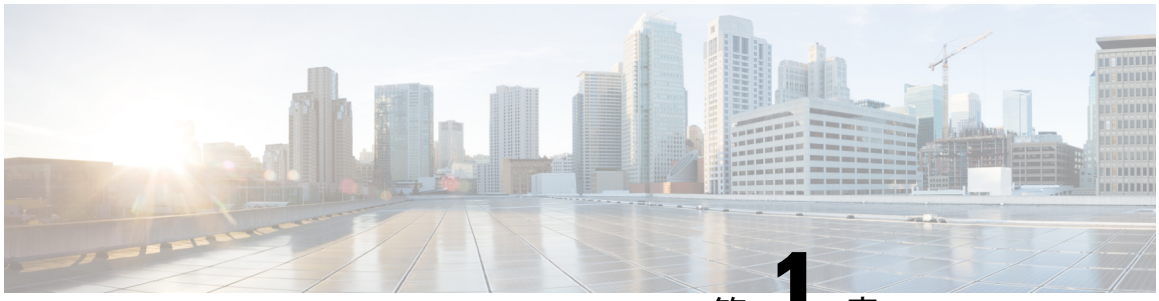
Cisco Firepower Management Center Remediation Module for Tetration バージョン 1.0.1 クイック スタート ガイド

初版：2018 年 8 月 1 日

最終更新：2018 年 8 月 20 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

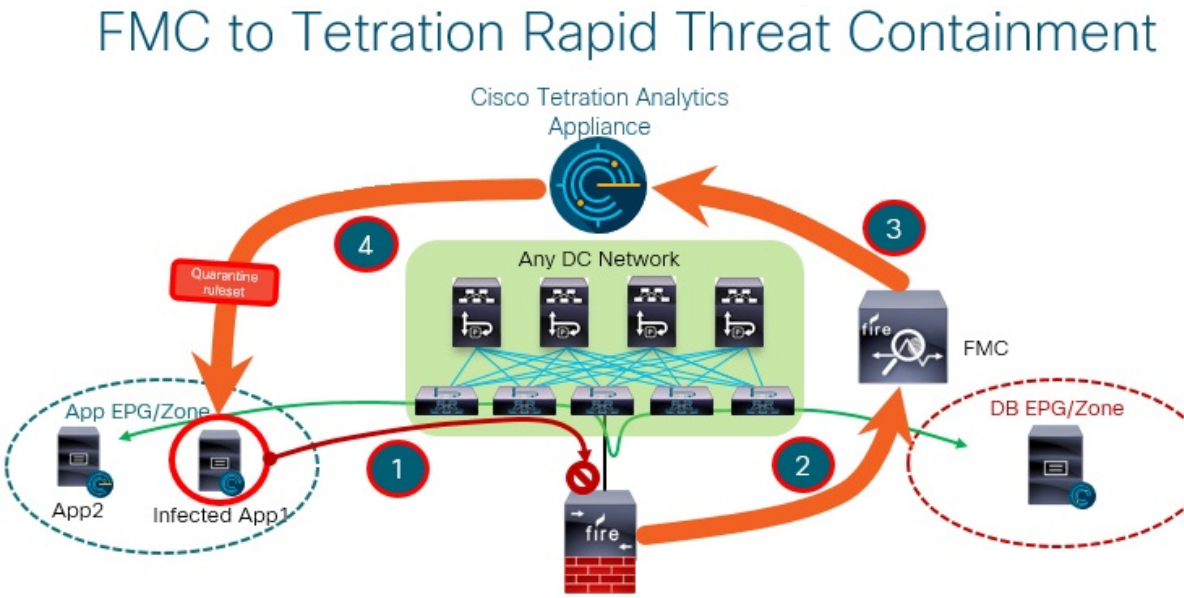


第 1 章

はじめに

概要

Cisco Firepower Management Center（FMC）Remediation Module for Tetration を使用すると、感染したホストからネットワークへの攻撃が FMC によって検出された場合に、Tetration Analytics（TA）エンフォースメント エージェントによって問題のあるホストを隔離でき、そのホストに対する以降のトラフィックの出入りを禁止できます。次の図は、この修復モジュールをインストールした場合の FMC と Tetration の関係を示しています。



この図は、ネットワーク攻撃を隔離する全体的なプロセスも示しています。

ステップ 1 感染したアプリケーションがあるホストは、ネットワークへの攻撃を開始します。攻撃は、Firepowerデバイス（物理または仮想）で実行されている Cisco Firepower Threat Defense（FTD）によってインラインでブロックされます。

ステップ 2 感染に関する情報を含む侵入イベントが生成され、FTD を管理する FMC に報告されます。

ステップ 3 攻撃によって、FMC 上の修復モジュールがトリガーされ、ノースバウンド API を使用して、感染したホストを隔離するよう Tetration に対して要求が送られます。

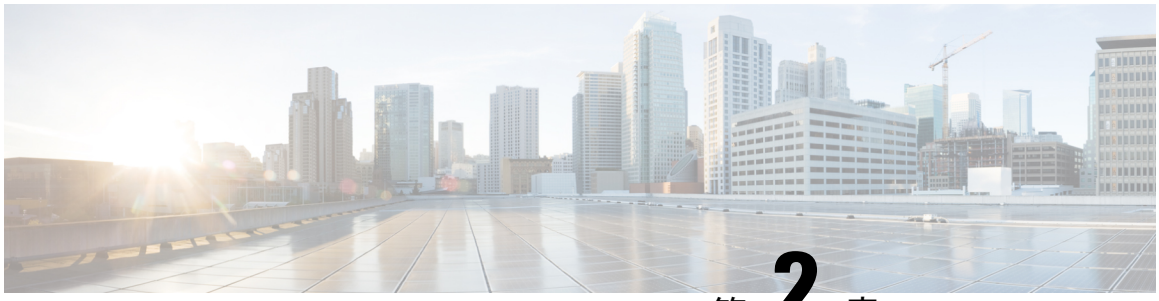
ステップ 4 Tetration は、感染したホスト上のエンフォースメント エージェントに隔離要求を送信することで、感染したアプリケーションのワークロードをすばやく封じ込めます。

前提条件

- 「隔離」という注釈が付けられたホストに出入りするすべてのトラフィックをドロップするために、TA で絶対ポリシーを事前定義します。部分隔離を希望する場合は、TA でポリシーをカスタマイズして、すべてではなく一部のタイプのトラフィックのみ拒否するようにします。詳細については、TA GUI でユーザ ガイドを参照してください。
- Tetration エージェントは、Linux、Windows などのホスト オペレーティング システム内で実行されるソフトウェアです。エンフォースメント エージェントとして、インストールされているホストに対してファイアウォール ルールを設定する機能があります。保護するネットワーク ホストに、エンフォースメント エージェントをインストールします。詳細については、『Cisco Tetration Analytics for the Software Agent Installation Guide』を参照してください。

関連資料

- Firepower Management Center 設定ガイド
- Cisco Tetration Analytics



第 2 章

インストール（Install）

インストール

Cisco Firepower Management Center Remediation Module for Tetration をダウンロードしてインストールするには、次の手順を実行します。

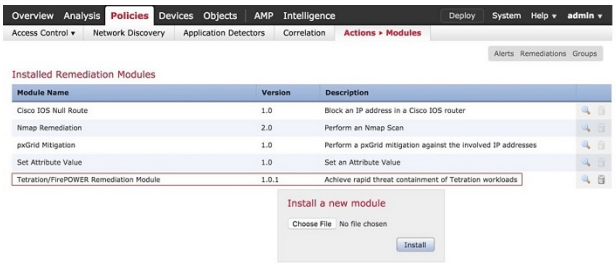
ステップ 1 Web ブラウザを使用して、この修復モジュールをダウンロードします。
https://software.cisco.com/download/home/286259687/type

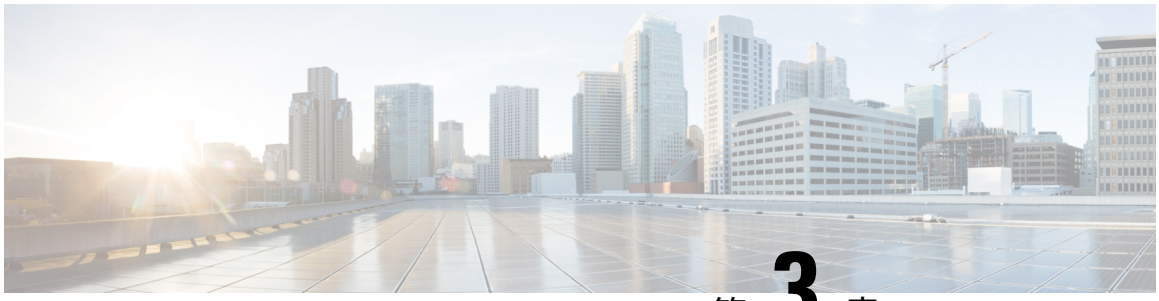
ステップ 2 FMC にこの修復モジュールをインストールします。

1. FMC GUI で、[ポリシー（Policies）] > [アクション（Actions）] > [モジュール（Modules）] に移動します。
2. 以下に示されているように、[新しいモジュールのインストール（Install a new module）] ダイアログボックスで、[ファイルの選択（Choose File）] をクリックします。
3. ステップ 1 でダウンロードした修復モジュールのファイルを選択します。
4. [Install（インストール）] をクリックします。

   （注） アクセス エラーメッセージを受信した場合、エラー メッセージをクリアし、ステップ 2 を繰り返します。

   インストールが成功すると、Cisco Firepower Management Center Remediation Module for Tetration が、インストールされている修復モジュールの一覧に表示されます。


Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help admin
Access Control Network Discovery Application Detectors Correlation Actions ▸ Modules
Alerts Remediations Groups
Installed Remediation Modules
Module Name
Version
Description
Cisco IOS Null Route
1.0
Block an IP address in a Cisco IOS router
Nmap Remediation
2.0
Perform an Nmap Scan
pxGrid Mitigation
1.0
Perform a pxGrid mitigation against the involved IP addresses
Set Attribute Value
1.0
Set an Attribute Value
Tetration/FirePOWER Remediation Module
1.0.1
Achieve rapid threat containment of Tetration workloads
Install a new module
Choose File
No file chosen
Install



第 3 章

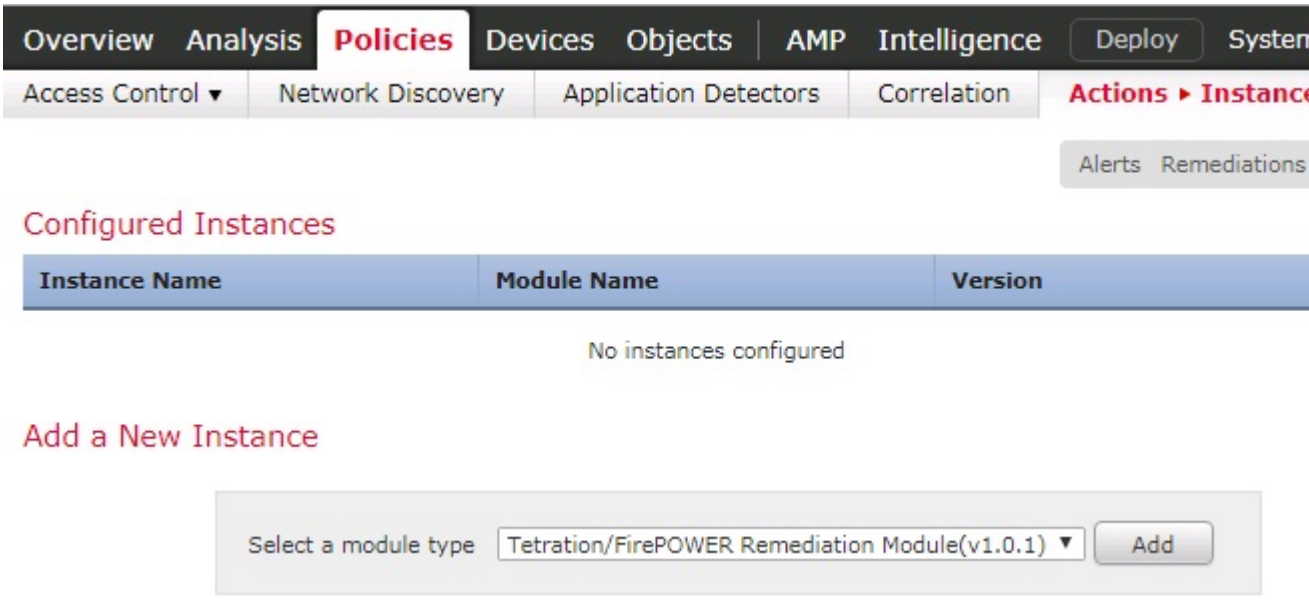
設定（Configure）

設定

FMC にインストールされた修復モジュールを設定するには、FMC GUI で次の手順を実行します。

ステップ 1 ネットワーク内の Tetration Analytics（TA）サーバごとに修復モジュールのインスタンスを作成します。

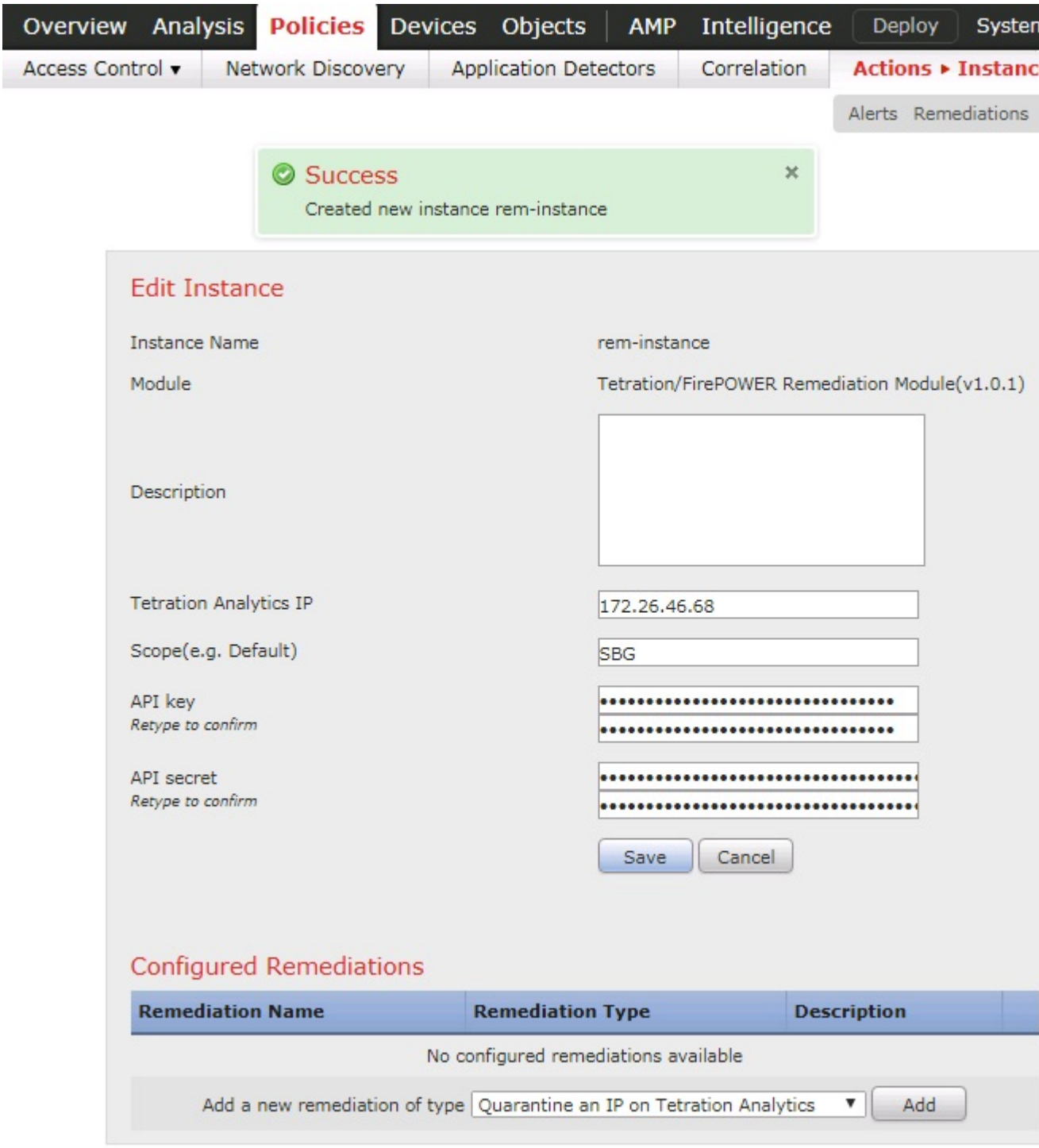
1. [ポリシー（Policies）] > [アクション（Actions）] > [インスタンス（Instances）] に移動します。
2. ドロップダウン リストから修復モジュールを選択し、[追加（Add）] をクリックします。



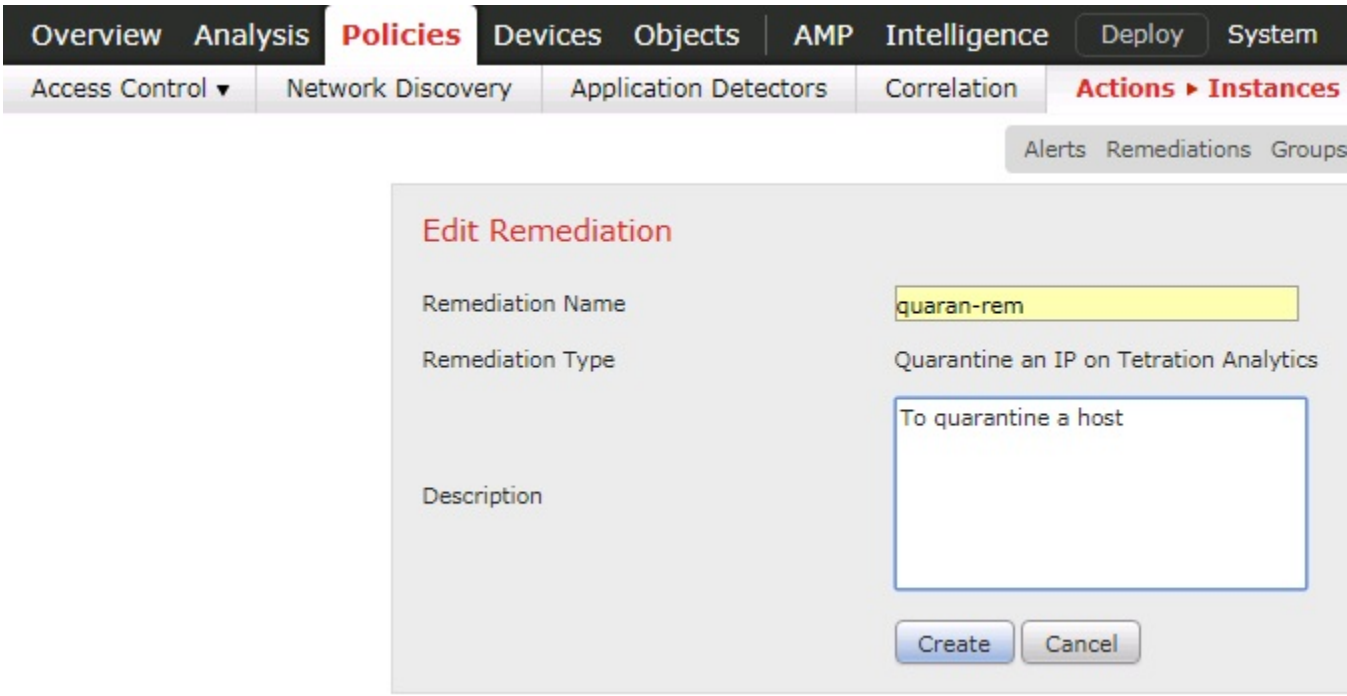
3. [インスタンス名（Instance Name）] を入力します（この例では、**rem-instance**）。

4. TA サーバの IP アドレス、API キー、API シークレット、および問題のある可能性のあるホストが含まれる範囲を入力します。[作成（Create）] をクリックします。

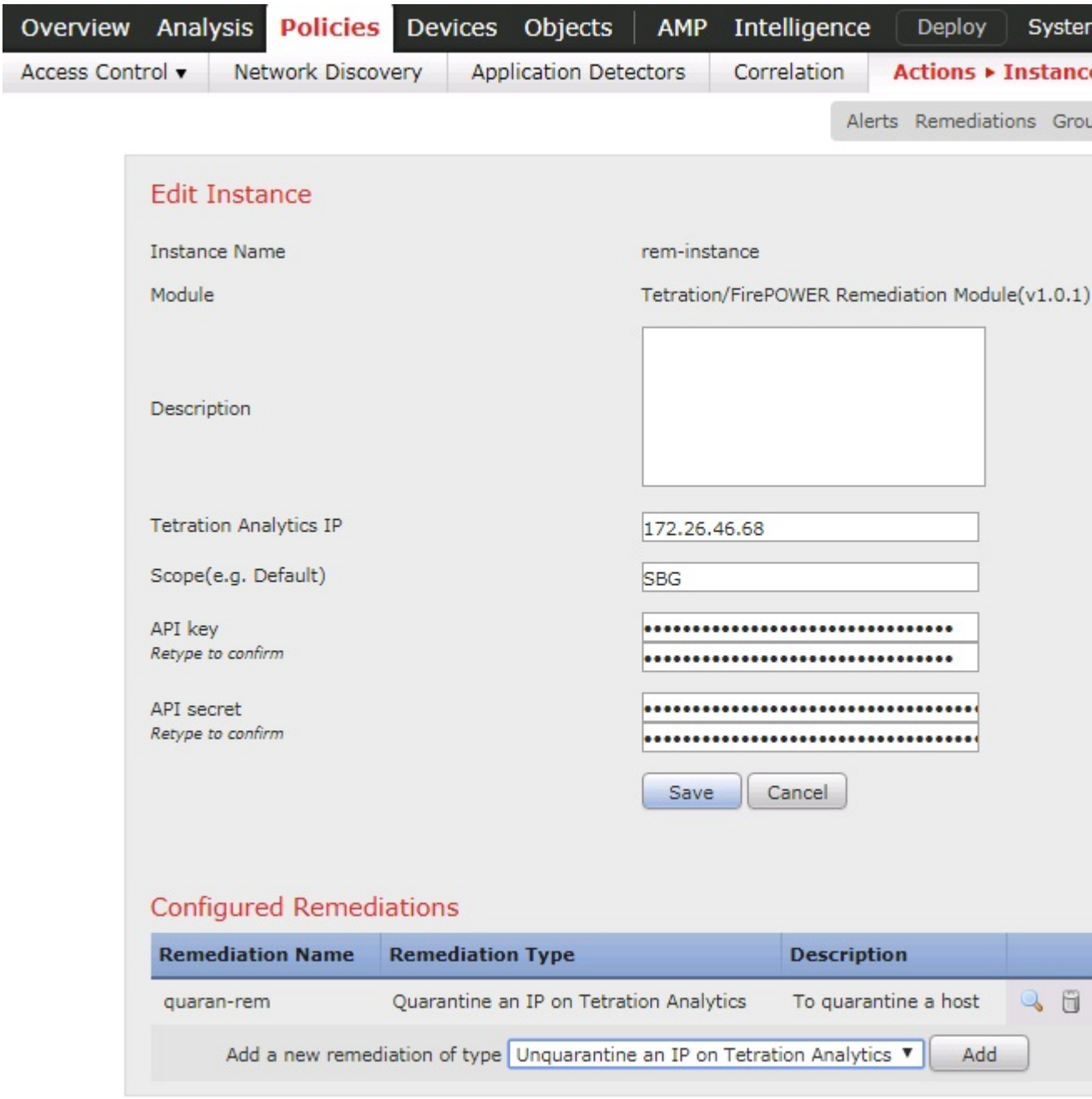
   （注） API キーとシークレットは、この時点では TA サーバに対して検証されません。サイト管理者、カスタマーサポート、またはルート スコープ オーナー ロールは、API キーとシークレットを TA で最初に作成しておく必要があります。ここで使用する情報をコピーします。詳細については、『 TA API Configuration Guide』を参照してください。



5. [設定されている修復（Configured Remediations）] で、修復のタイプを選択し（この例では、**Quarantine an IP on Tetration Analytics**）、[追加（Add）] をクリックして新しい修復を追加します。
6. [修復名（Remediation Name）] を入力し（この例では、**quaran-rem**）、[作成（Create）] をクリックします。



7. 設定した修復がテーブルに表示されます。[保存（Save）] をクリックします。



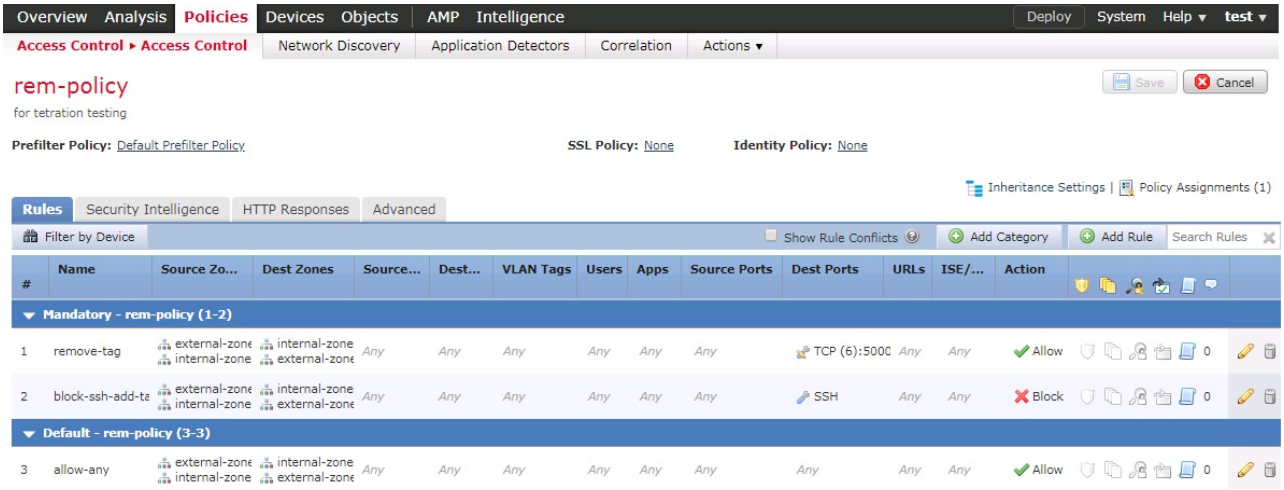
ステップ 2 アクセス制御ポリシーを設定します（この例では、**rem-policy**）。

1. [ポリシー（Policies）] > [アクセス制御（Access Control）] > [ルール（Rules）] に移動します。
2. [ルールの追加（Add Rule）] をクリックします（たとえば、**block-ssh-add-tag**）。
3. [アクション（Action）] で [ブロック（Block）] を選択します。

4. [ポート（Ports）] タブで、宛先ポートのプロトコルの一覧から [SSH] を選択し、[追加（Add）] をクリックします。
5. [保存（Save）] をクリックします。
6. [ロギング（Logging）] タブで、[接続開始時のログ（Log at Beginning of Connection）] を選択します。

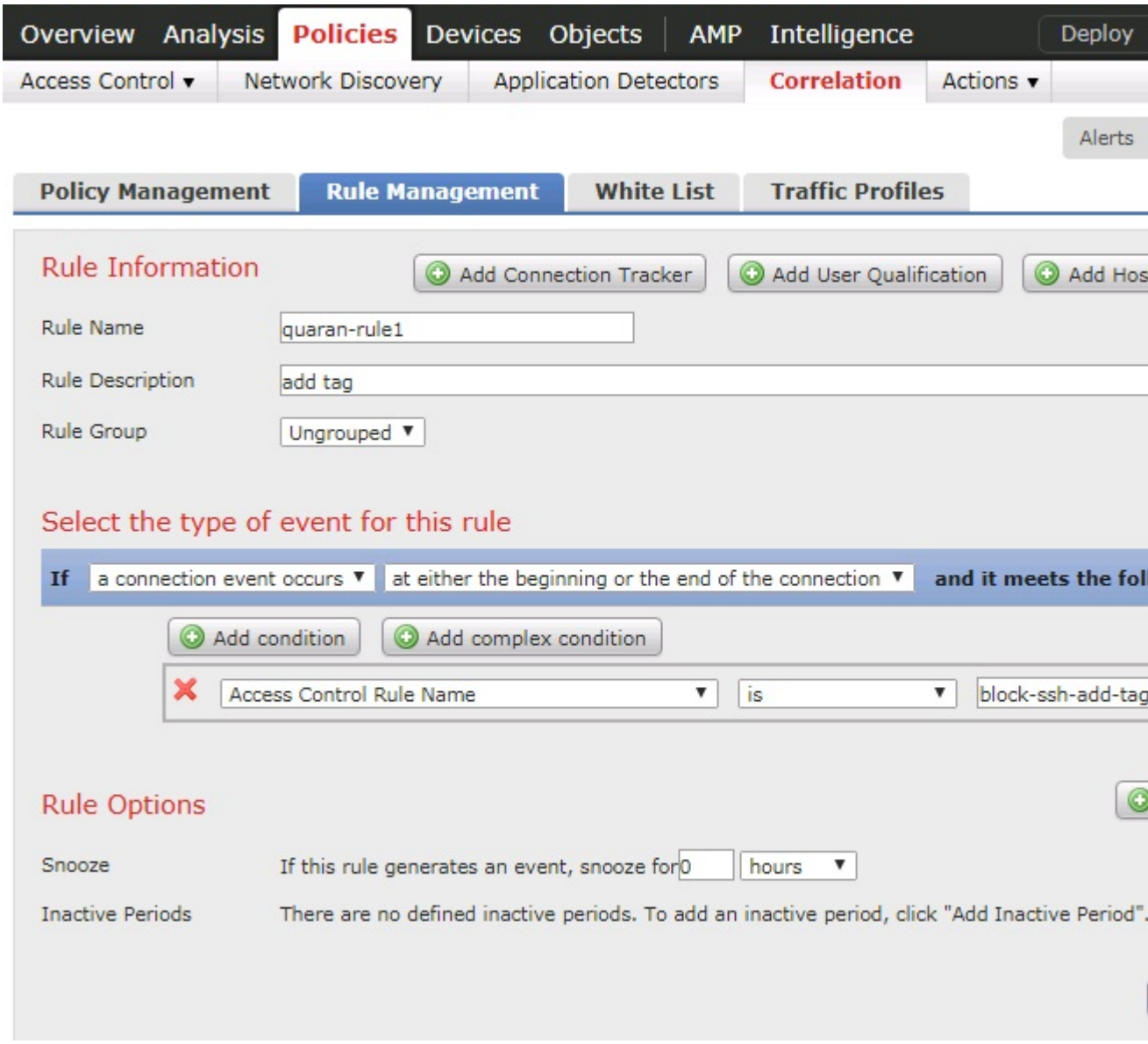
   重要　アクセスルールでロギングが有効になっていることを確認します。これにより、FMC はイベント通知を受信します。

7. [保存（Save）] をクリックします。



ステップ 3　相関ルールを設定します。

1. [ポリシー（Policies）] > [相関（Correlation）] > [ルールの管理（Rule Management）] に移動します。
2. [ルール名（Rule Name）] を入力し（この例では、**`quaran-rule1`**）、説明（オプション）を入力します。
3. [このルールのイベントタイプの選択（Select the type of event for this rule）] セクションで、[接続イベントの発生（a connection event occurs）] および [接続の開始時または終了時（at either the beginning or the end of the connection）] を選択します。
4. [条件を追加（Add condition）] をクリックし、演算子を **OR** から **AND** に変更します。
5. ドロップダウンリストで、[アクセスコントロールルール名（Access Control Rule Name）]、[は（is）] を選択し、ステップ 2 で設定したアクセス コントロール ルールの名前を入力します（この例では、**`block-ssh-add-tag`**）。

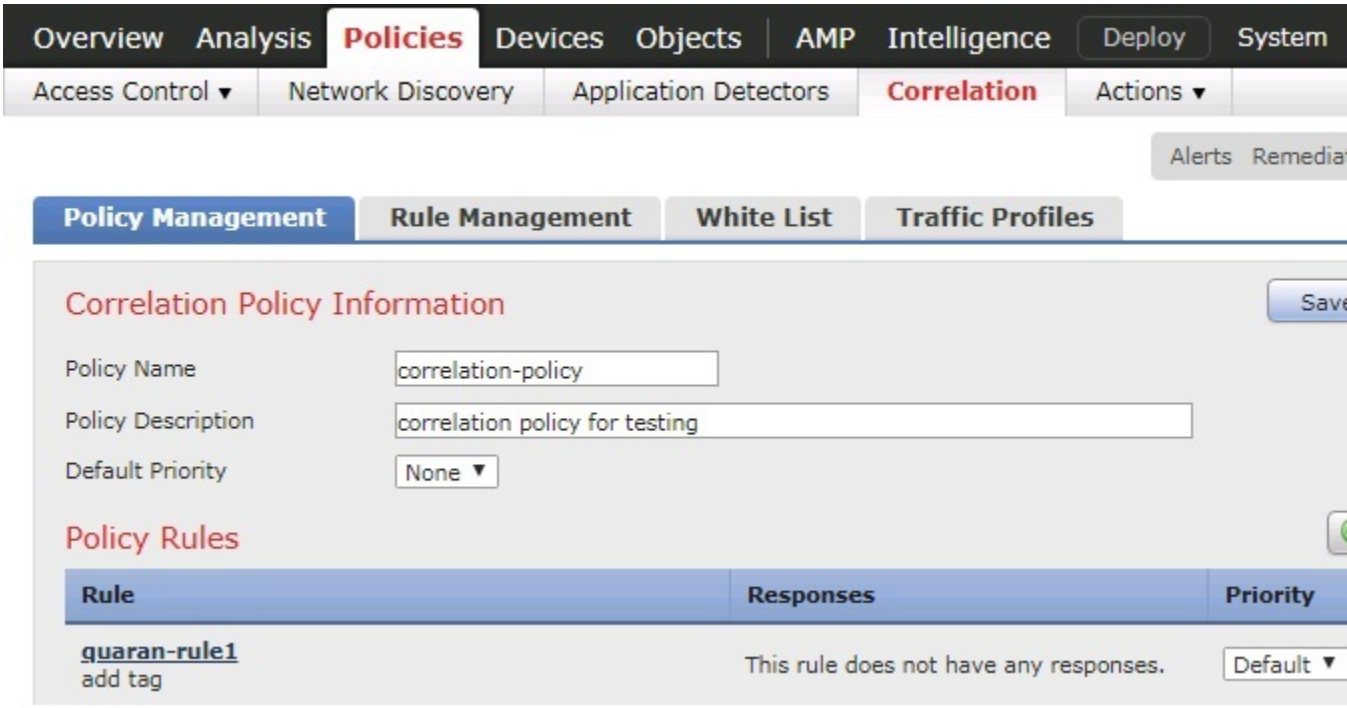


6. [保存（Save）] をクリックします。

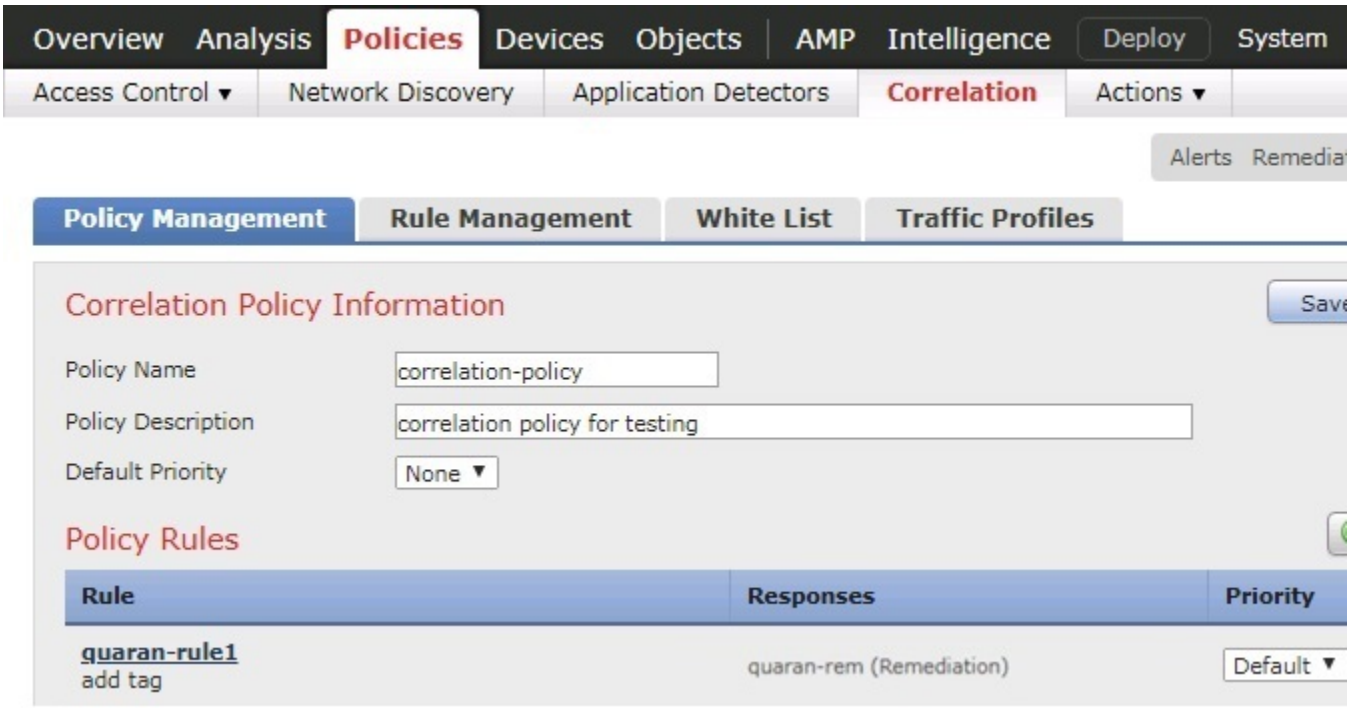
ステップ 4 相関ルールに、修復モジュールのインスタンスを応答としてアソシエートします。

1. [ポリシー（Policies）]>[相関（Correlation）]>[ポリシーの管理（Policy Management）] に移動します。
2. [ポリシーの作成（Create Policy）] をクリックします。
3. [ポリシー名（Policy Name）] を入力し（この例では、**`correlation-policy`**）、説明（オプション）を入力します。
4. [Default Priority] ドロップダウン リストから、ポリシーのプライオリティを選択します。[なし（None）] を選択して、ルールのプライオリティのみ使用します。

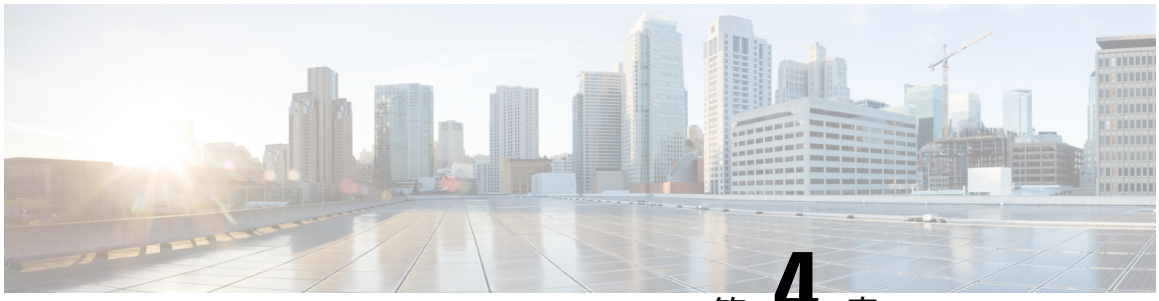
5. [ルールの追加（Add Rules）] をクリックし、ステップ 3 で設定した相関ルールを選択し（この例では、**quaran-rule1**）、[追加（Add）] をクリックします。



6. ルールの横にある [応答（Responses）] アイコンをクリックし、ルールに応答を割り当てます（この例では、**quaran-rem**）。[更新（Update）] をクリックします。



7. [保存（Save）] をクリックします。



第 4 章

検証

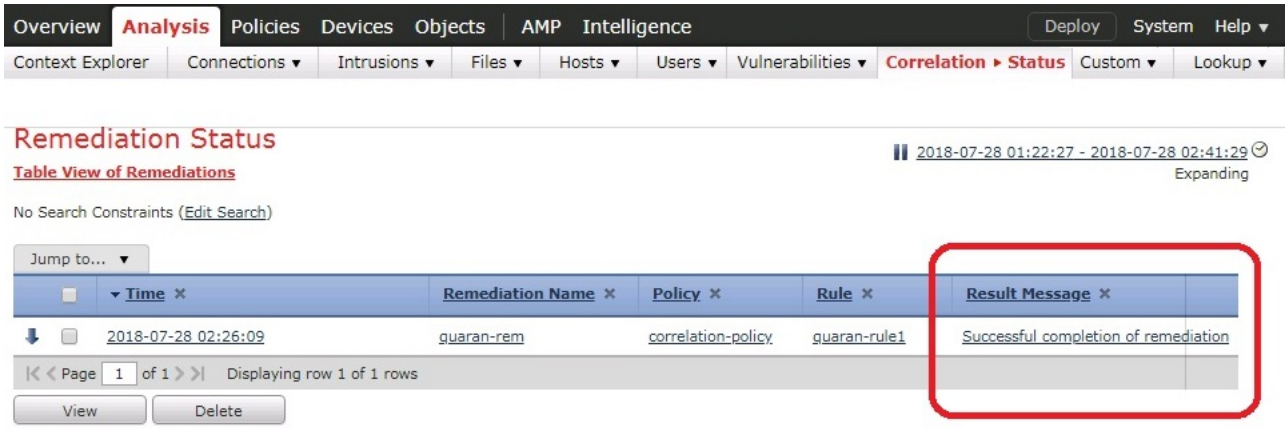
検証

修復はさまざまな理由で失敗することがあるため、次の手順を実行して、修復が成功したことを確認します。

ステップ 1 修復モジュールが関連付けられている相関ルールによってトリガーされた後、FMC GUI で修復実行のステータスを確認します。

ステップ 2 [分析（Analysis）] > [相関（Correlation）] > [ステータス（Status）] に移動します。

ステップ 3 [修復ステータス（Remediation Status）] テーブルで、ポリシーの行を見つけ、結果のメッセージを確認します。

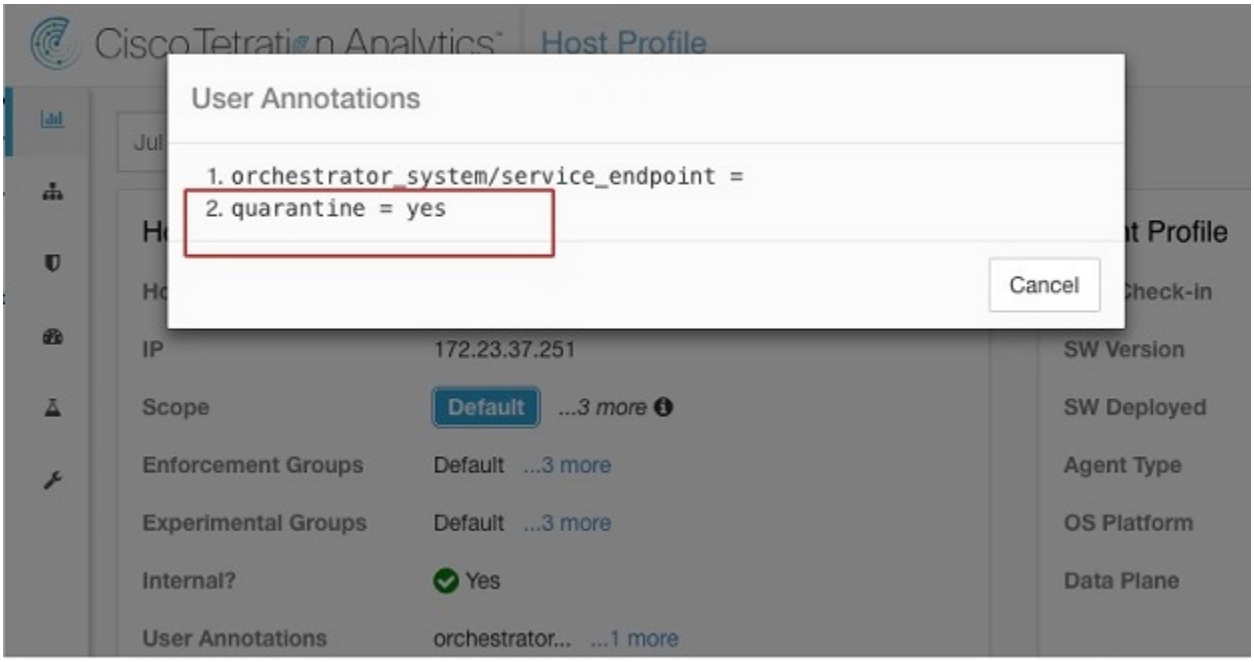


ステップ 4 修復が完了した後、TA GUI に移動します。

1. [可視性（Visibility）] > [インベントリ検索（Inventory Search）] に移動します。
2. 感染したホストの IP アドレスを入力し、[検索（Search）] をクリックします。

検証

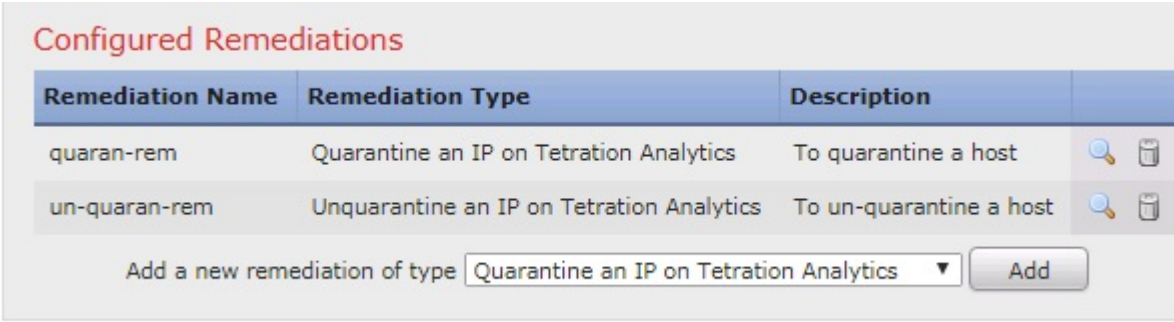
3. [ユーザ注釈（User Annotations）] で、感染したホストの IP アドレスに **quarantine = yes** という注釈が付けられていることを確認します。



次のタスク

隔離されたホストをクリーンにし、感染がなくなった後、TA GUI（推奨）を使用して **quarantine = yes** という注釈を **quarantine = no** に変更するか、または FMC 修復モジュールを使用して次のように隔離を解除します（セキュリティの問題のため、実稼働ネットワークでは非推奨）。

- （「設定：ステップ 1」を参照）隔離解除タイプの修復を使用する新しい修復を追加します。同じインスタンスを編集し、[設定されている修復（Configured Remediations）] で、隔離解除タイプの修復を選択し、追加します（この例では、**un-quaran-rem**）。



- （「設定：ステップ 2」を参照）隔離解除修復をトリガーするために使用できるアクセス コントロール ルール（この例では、**remove-tag**）を同じポリシー（この例では、**rem-policy**）に追加します。
- （「設定：ステップ 3」を参照）アクセス コントロール ルール（この例では、**remove-tag**）を使用する相関ルール（この例では、**unquaran-rule1**）を追加します。
- （「設定：ステップ 4」を参照）隔離解除応答（この例では、**un-quaran-rem**）を相関ルール（この例では、**unquaran-rule1**）に割り当てます。

- このルールに一致すると、隔離解除修復がトリガーされ、隔離注釈が削除されます。

検証