



修復の検証

次のセクションでは、修復プロセスが成功したかどうかを確認する手順について説明します。

- [修復の検証 \(1 ページ\)](#)

修復の検証

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関連ルールによってトリガーされた後、修復実行のステータスを確認します。FMC Web インターフェイスで、[分析 (Analysis)] > [相関 (Correlation)] > [ステータス (Status)] に移動します。

ステップ 2 [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。

Firepower Management Center
Analysis / Correlation / Status

Deploy | DC-North-South | admin

Bookmark This Page | Reporting | View Bookmarks | Search

2022-02-23 06:47:00 - 2022-04-22 07:54:27
Expanding

No Search Constraints (Edit Search)

Table View of Remediations

Jump to...

	Remediation Name x	Policy x	Rule x	Result Message x	Domain x
2022-03-31 14:56:34	quarantine-fmc	correlation-policy	quaran-rule-1	Successful completion of remediation	Global DC-North-South

Page 1 of 1 | Displaying row 1 of 1 rows

View Delete
View All Delete All

ステップ 3 修復が完了したら、次の手順を実行します。

1. Cisco Secure Workload ユーザーインターフェイスで、[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。

3. [ユーザー注釈 (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。

The screenshot shows the 'Scopes and Inventory' interface. On the left, there are scope filters: Default (internal) with 453 inventory items, Internet with 266, IoT-Devices with 0, and Quarantine-FMC with 2. The main area shows a query for '* quarantine = yes' under the 'All Inventory' tab. Below the query, there are tabs for Services, Pods, Workloads, and IP Addresses. The IP Addresses tab is active, showing a table with 2 items. The table has columns for Address, Location, Service, and Quarantine. The Quarantine column shows 'yes' for both items, which are highlighted with a red box.

Address	* Location	* Service	* Quarantine
192.168.110.2	Contractors		yes
192.168.10.35	DC		yes

次のタスク

隔離されたホストをクリーンアップし、感染がなくなったら、次のいずれかのアクションを実行して隔離の注釈を削除できます。

- (推奨) Secure Workload を使用して、「**quarantine = yes**」という注釈を「**quarantine = no**」に戻します。
 1. たとえば、感染がなくなった隔離されたホストが 172.21.208.11 で、デフォルトの範囲内であれば、次のような CSV ファイルを作成します。






```
IP,VRF,quarantine
172.21.208.11,Default,no
```
 2. [アプリケーション (Applications)] > [インベントリアップロード (Inventory Upload)] に移動し、Cisco Secure Workload に CSV ファイルをアップロードします。Cisco Secure Workload に CSV ファイルをアップロードする方法の詳細については、[関連資料](#) のセクションを参照してください。
- FMC 修復モジュールを使用して隔離の注釈を削除します。



重要 この方法は、セキュリティ上の懸念から、実稼働ネットワークでは推奨されません。

1. (「設定」セクションのステップ 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 (この例では **unquarantine-fmc**) を選択して追加します。

Configured Remediations

Remediation Name	Remediation Type	Description	
quarantine-fmc	Quarantine an IP on Secure Workload		 
unquarantine-fmc	Unquarantine an IP on Secure Workload		 

Add a new remediation of type

- （「設定」セクションのステップ 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」セクションのステップ 3 を参照）アクセスコントロールルール（この例では **remove-tag**）を使用する関連ルール（この例では **unquaran-rule1**）を追加します。
- （「設定」セクションのステップ 4B を参照）隔離解除応答（この例では **un-quaran-rem**）を関連ルール（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、隔離の注釈が削除されます。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。