Tanium™ Network Quarantine ユーザガイド

バージョン 1.3.1

2022年01月04日

この文書の内容は予告なく変更されることがあります。また、本書に記載の内容は「現状のまま」提供されており、正確性には万全を期しておりますが、Taniumの顧客販売契約に規定されている保証を除き、明示または暗黙を問わずいかなる保証もしません。別段の規定がない限り、Taniumはいかなる責任も負いません。TaniumおよびそのサプライヤIは、Tanium Inc.がかかる損害の可能性を事前に通知されていたとしても、本書の使用または使用できないことから生じる、利益損失やデータ損失をはじめとする間接的損害や特別損害、結果的損害、および付随的損害に対して一切の責任を負いません。

本書で使用されているIPアドレスは、実際のアドレスであることを意図していません。本書に記載されている例、コマンド表示出力、ネットワークトポロジ図、およびその他の図は、例示の目的にのみ使用されています。例示コンテンツに実際のIPアドレスが使用されていたとしても、特別な意図はなく、偶然です。

最新のTanium製品のマニュアルについては、https://docs.tanium.com を参照してください。

この文書には、第三者が提供するコンテンツや製品(ハードウェアおよびソフトウェアを含む)、サービス(「第三者のアイテム」)に対するアクセス手段や、第三者のそうした情報そのものが含まれていることがあります。Tanium Inc.およびその関連会社は、(i)それらの第三者のアイテムに対して責任を負うものではなく、第三者のアイテムに関するすべての保証および責任を明示的に放棄し、(ii)お客様とTaniumとの間の有効な契約に明記されているのでない限り、かかる第三者のアイテムへのアクセスや、利用に起因する損失、費用または損害について責任を負いません。

また、この文書は、特定の第三者のアイテムの使用やTanium製品との組み合わせを求めるものでも、想定するものでもありません。そのような組み合わせによって生じた知的財産権の侵害について、Taniumおよびその関連会社は一切責任を負いません。第三者のアイテムとTanium製品の組み合わせが適切であるかどうか、また第三者の知的財産権を侵害しないかどうかの判定の責任はTaniumではなくお客様にあります。

Taniumは、Tanium Softwareの操作をより直感的にして、成功までの時間を短縮できるよう最高のアクセシビリティ基準の達成に全力で取り組んでいます。高いアクセシビリティ基準を確保するため、Taniumは米国連邦規則、特に1998年のリハビリテーション法の第508項に準拠しています。当社は、長年にわたって製品開発の過程でサードパーティのアクセシビリティ評価を実施してきました。最近では2019年9月、すべての主要製品モジュールについてWCAG 2.1/VPAT 2.3規格に対する包括的な監査を終了しました。Taniumは、見込み客を含むあらゆるお客様が大規模なソリューション計画立案プロセスの一環としてモジュール単位でVPATレポートを入手できるようにしています。

新製品や新機能を続々と提供する中、Taniumはテストを実施することでアクセシビリティ指針の徹底を図ります。Taniumは、問題の重要度と変更の範囲を踏まえ、実現可能な範囲でこの徹底に最大限の努力をすることをお約束します。これらの目標は、当社の既存のリソースとともに納品が計画されている機能およびリリースにも組み込まれます。

Taniumではお客様のご意見をお待ちしております。Taniumモジュールと有用な技術要件をもとに、ソリューションを使いやすくするためのご意見やご要望をお寄せください。Taniumのカスタマーコミュニティにとってアクセシビリティ要件は重要であり、当社は全体的な製品のロードマップの中でそうした要件に対する遵守を優先させることをお約束します。Taniumは当社の進捗とマイルストーンの透明性を維持し、この作業に関するさらなる質問や話し合いを歓迎します。詳細は、営業担当者にお問い合わせいただくか、Taniumサポート(support@tanium.com)またはaccessibility@tanium.comに電子メールでお問い合わせください。

Taniumは米国およびその他の国におけるTanium,Inc.の商標です。記載されているその他の社名、製品名、サービス名は各社の商標または登録商標です。

目次

Network Quarantineの概要

Network Quarantineでは、既存のネットワークアクセス制御(NAC)ソリューションを使用して、管理対象と非管理エンドポイントの両方の通信を制御することができます(非管理エンドポイントの制御には、TaniumTM Discoverが必要)。

NACデバイス

Network Quarantineサービスを使用すると、Tanium製品はエンドポイントを隔離するためにNACと通信できます。Network Quarantineでは、Cisco ISE (Identity Services Engine)を使用してMACアドレスに基づくブロックを行うことができます。

詳細については、NACの設定(15ページ)を参照してください。

自動ルール

ISEを使用する場合、自動化ルールを作成して、隔離する必要のあるエンドポイントを検索できます。自動化ルールは保存されたQuestionを使用して、違反を起こしているエンドポイントを特定します。その後、それらのエンドポイントを隔離できます。詳細については、検疫で自動ルールを使用する(21ページ)を参照してください。

製品の統合

Tanium Discover

Tanium DiscoverでNetwork Quarantineサービスを設定すると、Interface (インターフェイス)ページから直接、MACアドレスを検疫することもできます。詳細については、Tanium Discoverユーザーガイドを参照してください。

Tanium™ Connect

Network Quarantineは、NACが開始または停止するとき、またはエンドポイントが隔離されたときにイベントを生成します。これらのイベントに関する通知は、電子メール、セキュリティ情報およびイベント管理(SIEM)ソフトウェアなどの宛先へ、またはConnectで接続を作成してファイルへ送信できます。詳細については、通知の設定(25ページ)を参照してください。

はじめに

手順1: Network Quarantineをインストールする

Network Quarantineをインストールします。

詳細は、「Network Quarantineのインストール(13ページ)」を参照してください。

手順2: NACを設定する

NAC(ネットワークアクセス制御)ソリューションを設定します。

詳細については、NACの設定(15ページ)を参照してください。

手順3: (任意) 通知を設定する

(任意) NACの開始イベントと終了イベントまたはNACの検疫イベントに関する通知を設定します。

詳細については、通知の設定(25ページ)を参照してください。

手順4: エンドポイントを検疫する

エンドポイントを隔離します。

詳細は、「エンドポイントの隔離(21ページ)」を参照してください。

Tanium™ Discoverとの統合を設定する場合は、Discoverワークベンチからエンドポイントを隔離することもできます。

Network Quarantine要件

Network Quarantineをインストールおよび使用する前に要件を確認してください。

Taniumの依存関係

Network QuarantineはTanium Connectに含まれています。ライセンスについての詳細は、Taniumサポートにお問い合わせください。環境が以下の要件に適合していることを確認します。

コンポーネント	要件
Tanium™ Core Platform	バージョン7.3.314.4250以降
Taniumの製品	次のモジュールは任意ですが、併用するには、Network Quarantineが次の最小バージョンが必要です。 • Tanium Connect 4.7.4以降 • Tanium Discover 2.7.0以降

Tanium Module Server

Network Quarantineがインストールされると、Module Serverのホストコンピュータ上のサービスとして実行されます。Module Serverへの影響は最小限であり、使用状況によって異なります。

エンドポイント

サポートされているオペレーティングシステム

Tanium Clientサポートと同じです。Tanium Client Managementユーザガイド：クライアントのバージョンとホストシステムの要件を参照してください。

サードパーティのソフトウェア

Network Quarantineでは、pxGridがインストールされたCisco Identity Services Engine (ISE) 2.2以降を使用することができます。

ホストとネットワークセキュリティの要件

Network Quarantineを実行するには、特定のポートとプロセスが必要です。

ポート

Network Quarantineの通信には、以下のポートが必要です。

情報元	接続先	ポート	Protocol	目的
Module Server	Module Server (ループバック)	17467	TCP	内部使用、外部からアクセスできません。
	Cisco ISE	5222	TCP	特記のない限り、Cisco ISEへアクセス。

ユーザロールの要件

Network Quarantineユーザロールのアクセス権限

アクセス権限	Network Quarantine Administrator (管理者)	Network Quarantine Approver (承認者)	Network Quarantine Rule Author (ルール作成者)	Network Quarantine User (Network Quarantine ユーザー)	Network Quarantine Read Only User (Network Quarantine 読み取り専用ユーザー)	Network Quarantine Service Account (サービスアカウント)
Show Networkquarantine (Networkquarantineの表示) Network Quarantine共有サービスを表示する						
Network Quarantine Certificates Read (証明書の読み取り) 設定済み証明書の表示						
Network Quarantine Certificates Write (証明書の書き込み) 設定済みの証明書を追加または更新する						
Network Quarantine Nacs Read (Nacの読み取り) 設定済みのNACの表示						

Network Quarantineユーザロールのアクセス権限 (続き)

アクセス権限	Network Quarantine Administrator (管理者)	Network Quarantine Approver (承認者)	Network Quarantine Rule Author (ルール作成者)	Network Quarantine User (Network Quarantine ユーザー)	Network Quarantine Read Only User (Network Quarantine 読み取り専用ユーザー)	Network Quarantine Service Account (サービスアカウント)
Network Quarantine Nacs Write (Nacの書き込み) 設定済みのNACの追加または更新						
Network Quarantine Quarantines Read (隔離の読み取り) 隔離されたエンドポイントを表示する						
Network Quarantine Quarantines Write (隔離の書き込み) エンドポイントの隔離または隔離解除						
Network Quarantine Rules Evaluate (ルールの評価) ルールを評価するためにサービスアカウントを使用						
Network Quarantine Settings Read (設定の読み取り) サービス設定を表示する						
Network Quarantine Settings Write (設定の書き込み) サービスの設定を構成する						
Network Quarantine Nacauditlog Read (Nacauditlogの読み取り) 監査ログを表示する						

Network Quarantineユーザロールのアクセス権限 (続き)

アクセス権限	Network Quarantine Administrator (管理者)	Network Quarantine Approver (承認者)	Network Quarantine Rule Author (ルール作成者)	Network Quarantine User (Network Quarantine ユーザー)	Network Quarantine Read Only User (Network Quarantine 読み取り専用ユーザー)	Network Quarantine Service Account (サービスアカウント)
Network Quarantine Rules Run (ルールの実行) ルール評価プロセスを開始						
Network Quarantine Rules Read (ルールの読み取り) ルールと対象を表示						
Network Quarantine Rules Write (ルールの書き込み) ルールと対象を編集						
Network Quarantine Requests Read (要求の読み取り) 隔離要求を表示						
Network Quarantine Requests Approve (要求の読み取り) 隔離要求の承認						
Network Quarantine Requests Deny (要求の読み取り) 隔離要求の否定						
Network Quarantine Runs Read (実行の読み取り) ルール評価実行の表示						

Network QuarantineのMicro Adminと高度なユーザロールで提供されるアクセス権限

アクセス権限	ロールタイプ	アクセス許可用コンテンツセット	Network Quarantine Administrator (管理者)	Network Quarantine Approver (承認者)	Network Quarantine Rule Author (ルール作成者)	Network Quarantine User (Network Quarantine ユーザー)	Network Quarantine Read Only User (Network Quarantine 読み取り専用ユーザー)	Network Quarantine Service Account (サービスアカウント)
Read User (読み取りユーザ)	Micro Admin							
Read Computer Group (コンピュータグループの読み取り)	Micro Admin							
Execute Plugin (プラグインの実行)	詳細	Network Quarantine コンテンツセット						
Read Plugin (プラグインの読み取り)	詳細	Network Quarantine コンテンツセット						
Read Saved Question (保存されたQuestionの読み取り)	詳細	Network Quarantine コンテンツセット						
Read Sensor (センサーの読み取り)	詳細	予約、デフォルト、ベース、Network Quarantine コンテンツセット						
保存されたQuestionの書き込み	詳細	Network Quarantine コンテンツセット						

Network Quarantine用 のオプションロール

ロール	許 可 されるアクション
Connectユーザー	ログインしているユーザーの場 合 : • Network Quarantineイベント通 知 用 接 続 の設 定 サービスアカウントの場 合 : • Network Quarantineイベント通 知 の送 信

コンテンツセットとアクセス権 限についての詳 細および説 明については、Tanium Core Platformユーザガイド : ユーザとユーザグループを参 照してください。

Network Quarantineのインストール

[Tanium Solutions (Taniumソリューション)] ページを使用して、Network Quarantineをインストールし、自動または手動設定のいずれかを選択します。

- **デフォルト設定を使用した自動設定**(Tanium Core Platform 7.4.2以降のみ): Network Quarantineは、必要な依存関係およびその他の選択された製品と一緒にインストールされます。インストール後、Tanium Serverは推奨されるデフォルト設定を自動的に設定します。このオプションは、ほとんどのデプロイのベストプラクティスです。Network Quarantineの自動設定についての詳細は、「Network Quarantineのインポートおよび設定でデフォルトの設定を使用する(13ページ)」を参照してください。
- **カスタム設定を使用した手動設定**: Network Quarantineをインストールしたら、必要な設定を手動で設定する必要があります。このオプションは、Network Quarantineに推奨されるデフォルト設定とは異なる設定が必要な場合にのみ選択します。詳細については、Network Quarantineのインポートおよび設定でカスタム設定を使用する(13ページ)を参照してください。

使用を開始する前に

- リリースノートをお読みください。
- Network Quarantine要件(7ページ)をご確認ください。

Network Quarantineのインポートおよび設定でデフォルトの設定を使用する

Network Quarantineのインポートで自動構成を使用した場合、Network Quarantineサービスアカウントには、Network Quarantineモジュールのインポートに使用されたアカウントが設定されます。

Network Quarantineをインポートして、デフォルトの設定を使用するには、インポートの手順で**[Apply Tanium recommended configurations (Tanium推奨設定を適用)]** チェックボックスを選択します。手順については、以下を参照してください。Tanium Consoleユーザガイド: Taniumモジュールの管理を参照してください。インポート後、正しいバージョンがインストールされていることを確認します。Network Quarantineのバージョンを確認する(14ページ)を参照してください。

Network Quarantineのインポートおよび設定でカスタム設定を使用する

デフォルト設定を自動的に適用しないでNetwork Quarantineをインポートする手順については、以下を参照してください。Tanium Consoleユーザガイド: Taniumのコンテンツパックを管理するの手順に従ってください。インポート後、正しいバージョンがインストールされていることを確認します。Network Quarantineのバージョンを確認する(14ページ)を参照してください。

サービスアカウントを構成する

このサービスアカウントは、Network Quarantineのいくつかのバックグラウンド処理を実行するユーザです。このユーザには、次のロールとアクセス権が必要です。

- **Network Quarantine Service Account**ロール
- **Connect User**ロール - Connectで通知を送信
- 自動ルールで使用される保存済みQuestionへのアクセス権

Network Quarantineのアクセス権限についての詳細は、「ユーザロールの要件(8ページ)」を参照してください。

1. メインメニューから **[Administration (運用管理)] > [Shared Services (共有サービス)] > [Network Quarantine]** に移動して、Network Quarantineの**Overview (概要)**ページを開きます。
2. [Settings (設定)]をクリックして、**[Service Account (サービスアカウント)]**タブを開きます。
3. サービスアカウントの設定を更新し、**[Submit (送信)]** をクリックします。

Network Quarantineをアップグレードする

Network Quarantineをアップグレードする手順については、以下を参照してください。Tanium Consoleユーザガイド：Taniumモジュールの管理を参照してください。アップグレード後、正しいバージョンがインストールされていることを確認します。Network Quarantineのバージョンを確認する(14ページ)を参照してください。

Network Quarantineのバージョンを確認する

Network Quarantineのインポートまたはアップグレード後、正しいバージョンがインストールされていることを確認します。

1. ブラウザを更新します。
2. メインメニューから**[Administration (管理)] > [Shared Services (共有サービス)] > [Network Quarantine]** に移動して、Network Quarantineの **[Overview (概要)]** ページを開きます。
3. バージョン情報を表示するには、Info をクリックします。

次にやるべきこと

Network Quarantineの使用について詳しくは、はじめに(6ページ)を参照してください。

NACの設定

Cisco Identity Services Engine (ISE) pxGrid NACを設定します。NACの設定後、エンドポイントの隔離を開始できます。

NACの構成を作成または編集するには、Network Quarantine Administratorロールが必要です。ユーザロールの要件(8ページ)を参照してください。

Cisco Identity Services Engine(ISE) pxGrid NAC

Cisco ISE pxGrid NACを設定するには、自己署名証明書またはサーバ署名証明書を使用できます。NACを設定すると、ISEで設定されている適応型ネットワーク制御(ANC)ポリシーで、特定のMACアドレスを隔離できます。

ユーザーインターフェイス、またはSSHを使用して、ISEにログインすることができます。

サーバおよびクライアントの自己署名証明書の作成

ISEでは、サーバ認証とクライアント認証の両方で自己署名証明書を使用できます。

1. サーバから自己署名証明書を取得します。ISE UIで、**[Administration (管理)] > [Certificates(証明書)] > [System Certificates (システム証明書)]**に進みます。証明書が必要な場合は、UIから公開証明書をエクスポートします。
2. クライアント用に自己署名証明書を生成します。
   a. 以下を参照してください。Ciscoコミュニティ: pxGridを使用した証明書のデプロイ。
   b. ISEのUIで、**[Administration (運用管理)] > [Certificates (証明書)] > [System Certificates (システム証明書)]**に移動し、**[Trusted Certificates (信頼済み証明書)]** セクションに証明書をアップロードします。
3. pxGrid証明書を変更した場合は、ISEサーバを再起動してください。以下を参照してください。Cisco ISEクライアントコマンド：開始/停止コマンド。
4. Network Quarantineで証明書構成を作成するための、サーバ証明書、クライアント証明書、およびクライアントキーがあることを確認します。

署名付き証明書を生成する

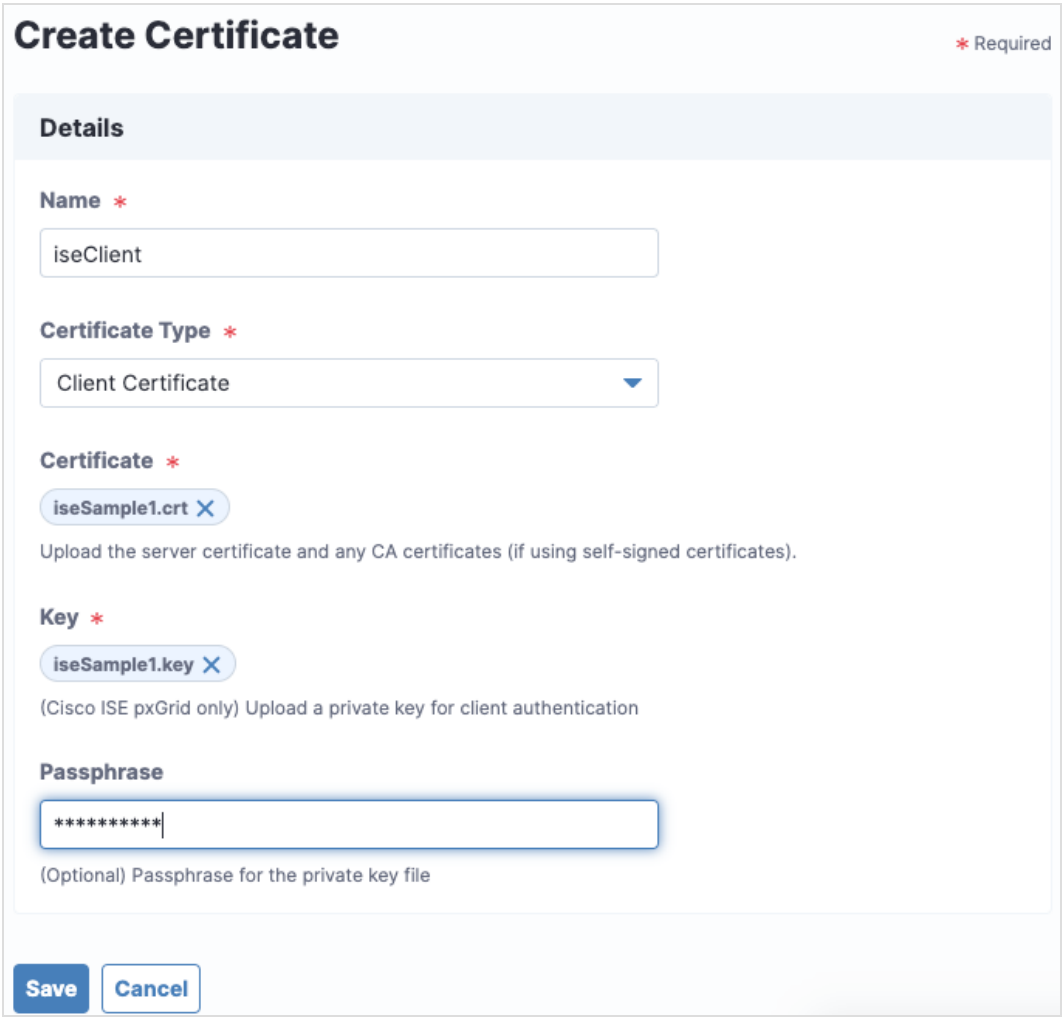
Network QuarantineでNACを設定した場合、pxGrid証明書を生成して、証明機関(CA)として提供します。

1. pxGrid UIで、**[Administration (管理)] > [pxGrid Services (pxGridサービス)] > [Certificates (証明書)]**に進みます。1つの証明書を生成します(証明書署名要求(CSR)なし)。Common Name (CN)には、IPアドレスなどの識別値を使用します。PEMダウンロード形式を選択します。証明書のパスワードを入力します。
2. **[Create (作成)]**をクリックして、サーバ証明書を含むZIPファイルをダウンロードします。このZIPファイルを解凍して、Network Quarantineで設定する必要があるサーバ証明書を取得します。

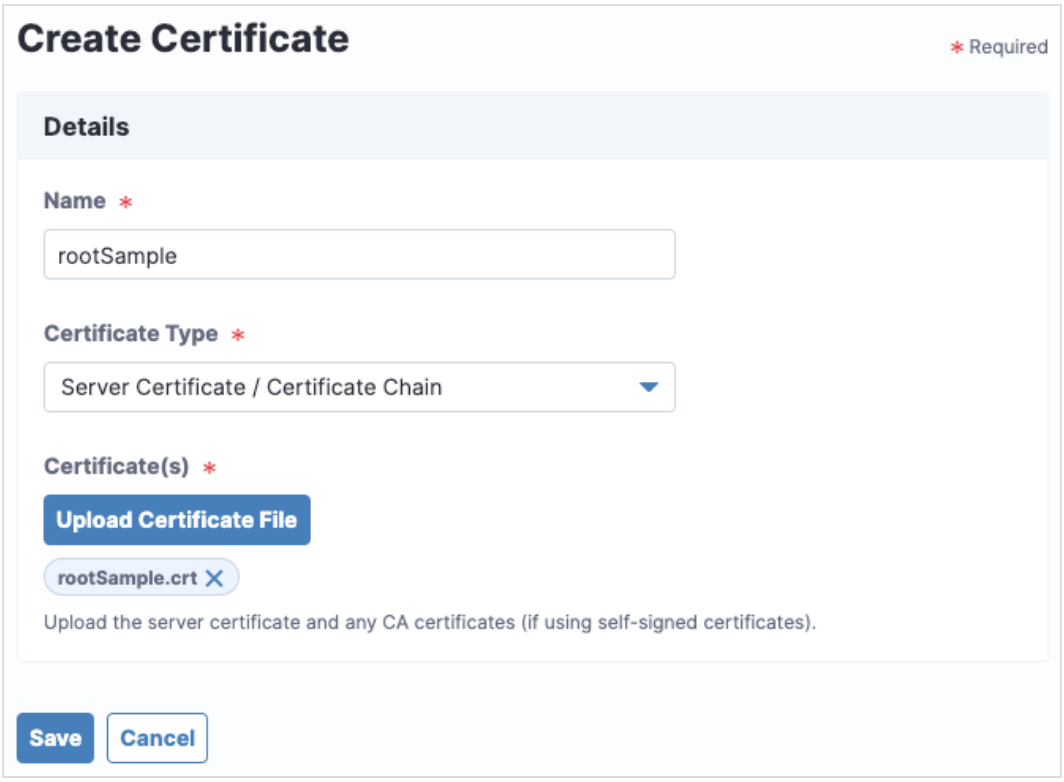
Network Quarantineで証明書を構成する

Network Quarantineでサーバ証明書とクライアント証明書を作成します。

1. Network Quarantineメニューから、**[Configuration (構成)] > [Certificates (証明書)]** に移動します。
2. クライアント証明書を作成します。
   a. **[Create Certificate (証明書の作成)]**をクリックします。
   b. 証明書の名前を指定します。
   c. **[Certificate Type (証明書タイプ)]**では、**[Client Certificate (クライアント証明書)]**を選択します。
   d. クライアント証明書とキーのファイルをアップロードします。
   e. 必要に応じて、秘密キーファイルのパスフレーズを指定します。
   f. **[Save (保存)]** をクリックします。



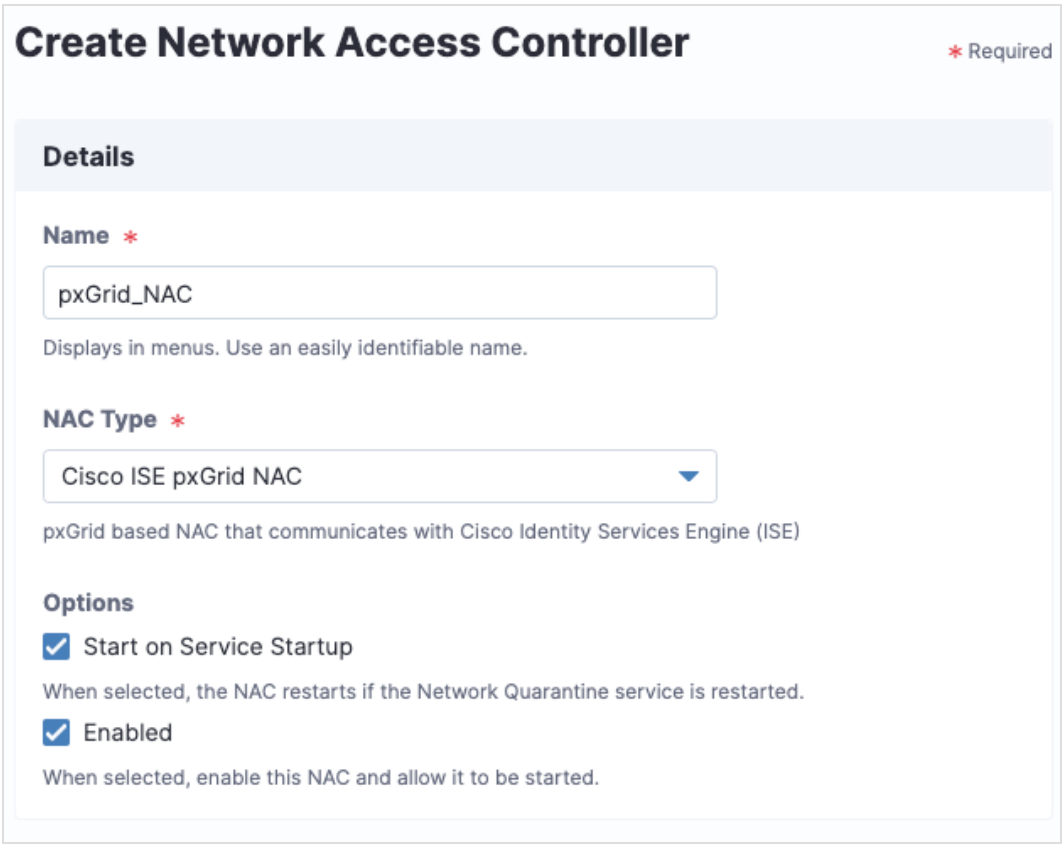
3. サーバ証明書を作成します。
    a. **[Create Certificate (証明書の作成)]**をクリックします。
    b. 証明書の名前を指定します。
    c. **[Certificate Type (証明書タイプ)]**では、**[Server Certificate / Certificate Chain (サーバ証明書/証明書チェーン)]**を選択します。
    d. pxGridウェブ管理UIで作成したpxGrid証明書をアップロードします。**[Save (保存)]** をクリックします。



pxGrid NACを設定する

1. Network Quarantineメニューから、**[Configuration (構成)] > [NAC] > [Create NAC (NACの作成)]** をクリックします。
2. 表示名を指定します。
3. NACタイプでは、**[Cisco ISE pxGrid NAC]**を選択します。

4. [**Options (オプション)**] セクションで [**Start on Service Startup (サービスの開始時に起動)**] を選択し、Network Quarantineサービスが再開したときにNACを再起動するようにします。[**Enabled (有効)**] を選択してNACを有効にして起動します。



5. Cisco ISE pxGrid NAC接続の詳細を指定します。

   a. **pxGridのユーザ名**と**pxGridのURI**を指定します。
   TaniumまたはCiscoサポートの指示なしに、デフォルトの**pxGrid Bind Resource**と**pxGrid Domain**、**pxGrid Capabilities**の値を変更しないでください。

   b. 自己署名証明書を使用する場合は、[**Check Server Identity (サーバIDの確認)**] の選択を解除します。

   c. [**Client Certificate (クライアント証明書)**] で、設定したクライアント証明書を選択します。

   d. [**Server Certificate Chain (サーバ証明書チェーン)**] で、設定したサーバ証明書を選択します。

6. (任意) [**IQ Timeout (IQのタイムアウト)**] と [**Refresh Interval (表示更新間隔)**] の設定を更新します。
7. NACを開始します。リストからNACを選択し、**[Start (開始)]**をクリックします。

NAC設定を編集するには、最初にNACを停止する必要があります。

次にやるべきこと

Network QuarantineでNACを設定すると、エンドポイントの検疫を開始することができます。エンドポイントの隔離 (21ページ)を参照してください。

エンドポイントの隔離

NACの設定後、エンドポイントを隔離する方法を設定できます。コンピュータグループに対する保存済みQuestionの結果に基づいて検疫を行う自動ルールを設定することも、MACアドレスを個別に選択することもできます。

検疫で自動ルールを使用する

自動化ルールは保存されたQuestionを使用してコンピュータグループに一連の条件をクエリします。エンドポイントが条件に一致したら、それは違反リストに追加されます。違反ページで、MACアドレスによってエンドポイントの隔離を選択できます。

Network Quarantineコンテンツセットに保存されたQuestionを追加する

自動化ルールを設定する前に、隔離するエンドポイントを選択するにあたり、どの保存されたQuestionを使用するかを決定する必要があります。たとえば、特定のパッチがインストールされていないエンドポイントを返す保存されたQuestionを作成することができます。

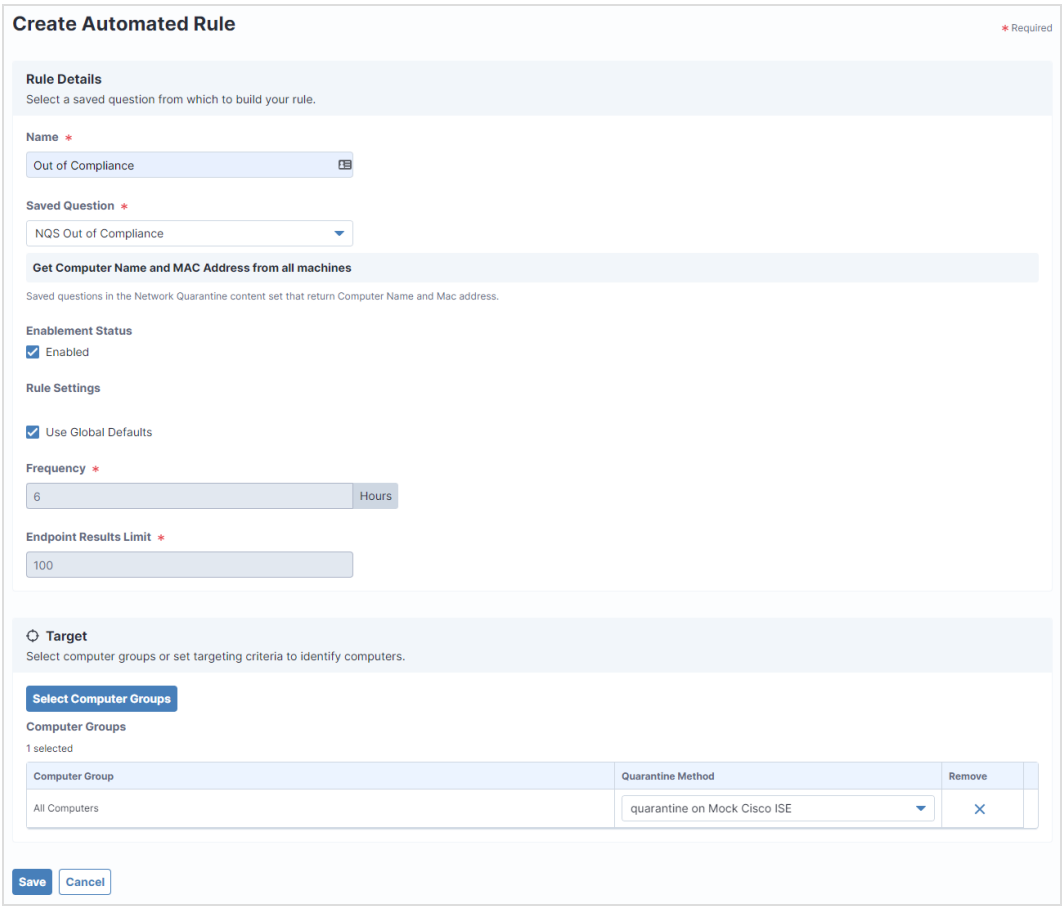
ルールに使用する保存されたQuestionは以下の要件を満たす必要があります：

- Network Quarantineコンテンツセットに属する
- コンピュータ名とMACアドレスセンサー用の列を返す
- Network Quarantineサービス用に設定したサービスアカウントユーザーがアクセスできる

保存されたQuestionをNetwork Quarantineコンテンツセットに追加するには、保存されたQestionを作成するときにコンテンツセットを選択するか、保存されたQuestionを編集してそれをコンテンツセットに追加できます。詳細については、Tanium Core Platformユーザガイド：保存済みQuestionを編集するを参照してください。

自動化ルールを作成する

1. Network Quarantineメニューで、**[Automated Rules (自動化ルール)] > [Add rule (ルールを追加)]**をクリックします。
2. ルールの名前を入力し、ルールに使用する保存済みQuestionを選択します。



3. **[Enabled (有効)]**を選択して、指定した頻度でルールを実行できるようにします。
4. 頻度とエンドポイント結果の制限にカスタム設定を使用するには、**[Use Global Defaults (グローバルデフォルトを使用)]** をクリアして、カスタム値を入力します。
5. ルールの対象を選択します。対象とするコンピュータグループ(1つまたは複数)を設定します。各コンピュータグループについて、検疫方法に使用する設定済みNACを指定します。
6. **[Save (保存)]** をクリックします。
7. ルールは設定された頻度で実行されます。ルールのすべてを今すぐ実行するには、**[Run Now (今すぐ実行)]** をクリックします。

違反の表示と対処

ルールを実行した後、保存されたQestionの条件を満たすコンピュータのリストが返されます。すべての違反を表示するには、Network Quarantine**のOverview (概要)**ページの **[Issues (問題)]** セクションの **[Volations (違反)]** タブに移動します。

- 定義済みルールに違反しているデバイスの検疫を承認するには、そのエンドポイントを選択し、[**Approve (承認)**] をクリックします。
- エンドポイントの接続を維持するには、エンドポイントを選択して [**Deny (拒否)**] をクリックします。
- エンドポイントのCSVリストを生成するには、エンドポイントを選択して**[Export (エクスポート)]**をクリックします。

> 検疫の自動承認を設定する場合は、Taniumサポートに詳細をお問い合わせください。

グローバルルール設定を指定する

ルールはデフォルトで6時間ごとに評価され、1つのルールに対して100を超えるエンドポイントが返されるとイベントが生成されます。Network Quarantine **Overview (概要)**ページからグローバル設定を変更するには、Settings (設定) をクリックし、[**Automated Rules (自動ルール)**] タブをクリックします。

MACアドレスを個別に検疫する

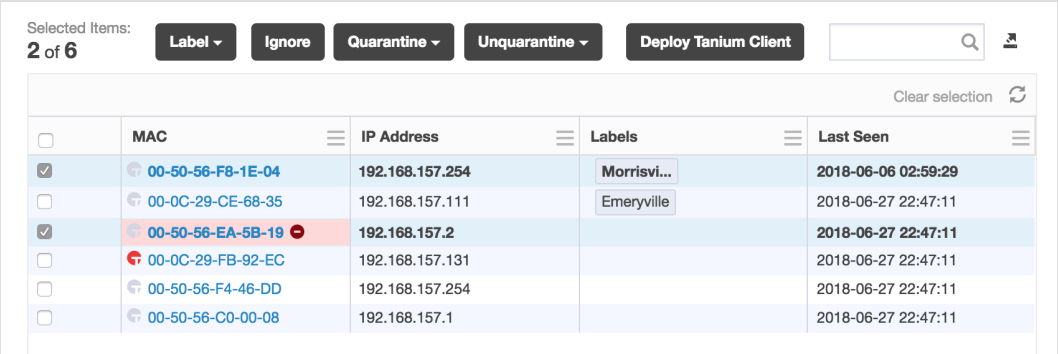
1. Network QuarantineのOverview (概要)ページの [**Issues (問題)**] セクションの [**Quarantine (隔離)**] タブで、[**Create Quarantine (検疫の作成)**] をクリックします。
2. 以下のような利用可能なオプションを使用してエンドポイントを隔離します。
    1. Cisco Identity Services Engine (ISE) pxGrid NACを使用してエンドポイントを検疫するには、検疫を適用するMACアドレスのリストを入力し、使用する検疫方法を選択します。適応型ネットワーク制御(ANC) ポリシーはISEで設定されています。
3. [**Save (保存)**] をクリックします。
4. 指定したMAC アドレスが、Network Quarantineの **Overview (概要)**ページの [**Quarantine (検疫)**] セクションに表示されます。エンドポイントの検疫を無効にするには、MACアドレスを選択して、[**Remove Quarantine (検疫の解除)**]をクリックします。

Discoverで検疫する

Tanium Discoverがインストールされている場合は、MACアドレスを個別に検疫したり、検疫を解除したりすることができます。**[Interfaces (インターフェイス)]**ページに移動して、隔離するエンドポイントに関連する行を選択し、**[Quarantine (隔離)]**をクリックして、エンドポイントを隔離するのに使用するNACを選択します。

検疫されたMACアドレスはBlocked (ブロック済み)のマークが付けられます。

詳細は、「Tanium Discoverユーザガイド」を参照してください。



通知の設定

Tanium Connectで接続を作成して、NACの開始と停止時、エンドポイントが隔離されたとき、ルールの一致がエンドポイントを返したとき、ルールが承認または否定されたとき、あるいはルールの一致違反が発生したときに通知を送信できます これらの通知は、電子メール、SIEM、Splunkなどの宛先に送信できます。

前提条件

- Connectをインストールしている必要があります。詳細については、Tanium Connectユーザーガイド：Tanium Connectのインストールを参照してください。
- 接続の作成には、**Connect User**ロールが必要です。また、通知の送信には、Network Quarantineサービスアカウントに**Connect User**ロールが必要です。ユーザロールの設定ついての詳細は、以下を参照してください。Tanium Core Platform ユーザガイド：ユーザにロールを割り当てる。

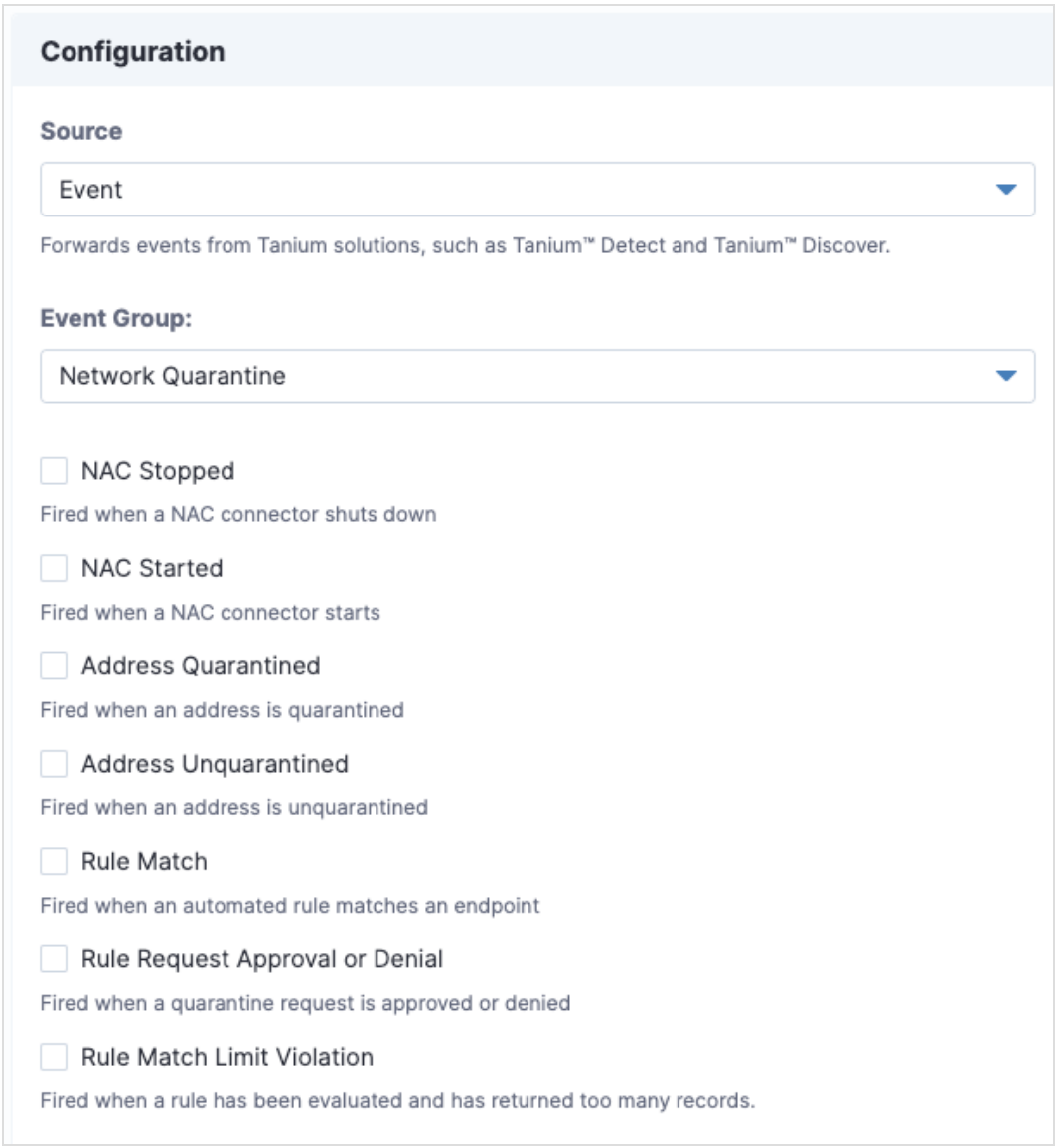
Connectで通知を設定する

1. 接続を作成します。
   a. メインメニューから **[Modules (モジュール)] > [Connect]** に移動してConnectの**Overview (概要)**ページを開きます。**[Create Connection (接続の作成)]** をクリックします。
   b. 接続の名前と説明を入力します。

2. データソースを設定します。

   a. [**Configuration (構成)**] セクションで、**Source (情報元)**として**Event (イベント)**を選択します。

   b. **Network Quarantine**イベントグループを選択し、通知を生成するイベントを選択します。



3. 接続先を設定します。
   [Select Destination (送信先を選択)]メニューにリスト表示された、いずれかの接続先を選択します。通知の一般的なオプションには、Email、SIEM、およびSplunkがあります。ただし、使用可能な送信先ならどれでも使用できます。詳細については、Tanium Connectユーザーガイドを参照してください。必要なフィールドに必要事項を入力して、**[Create Connection (接続の作成)]**をクリックします。

Network Quarantineのトラブルシューティング

トラブルシューティングのために情報を収集してTaniumに送信するには、ログなどの関連情報を収集します。

ログを収集する

情報は、ブラウザでダウンロードできる圧縮ZIPファイルとして保存されます。

1. Network Quarantineの**Overview (概要)**ページでHelp (ヘルプ) をクリックし、**[Troubleshooting (トラブルシューティング)]** タブをクリックします。
2. **[Troubleshooting ZIP File (ZIPファイルのトラブルシューティング)]** セクションで **[Download the File (ファイルをダウンロード)]** をクリックします。
   `networkquarantine-support.zip`ファイルがローカルのダウンロードディレクトリにダウンロードされます。
3. Taniumサポートに問い合わせて、ZIPファイルを送信する最適なオプションを決めてください。詳細は、Taniumサポートに問い合わせる(28ページ)を参照してください。

Tanium Network Quarantineは、ログ情報を以下のディレクトリにある`networkquarantine`*`NN`*`.log`ファイルで保持します：`\Program Files\Tanium\Tanium Module Server\services\networkquarantine-files`。ファイルサイズが1MBになるたびに新しいログファイルが作成されます。

ログレベルを設定する

1. Network Quarantineの**Overview (概要)**ページでHelp (ヘルプ) をクリックし、**[Troubleshooting (トラブルシューティング)]** タブをクリックします。
2. **[Logging Level (ロギングレベル)]**セクションで、有効にするログレベルを選択します。

監査ログを表示する

監査ログには、設定されたNACで発生するすべての隔離および隔離解除アクションが含まれます。

1. Network Quarantineメニューから、**[Audit log (監査ログ)]**をクリックします。
2. 特定のIPアドレスやMACアドレス、アクション、NAC名などでログをフィルタリングすることができます。
3. **[Export (エクスポート)]**をクリックして、監査ログの現在の状態をCSVファイルに保存します。

SASLError not-authorizedエラーを解決する

問題

クライアントが証明書を使用してISEに接続すると、ISEはその証明書を記憶し、証明書をクライアントに結び付けます。そのクライアントが別のクライアント証明書で接続を試みると、`SASL: not-authorized`エラーで接続は拒否されます。

ソリューション

1. ISE UIで、**[Administration (管理)] > [pxGrid Services (pxGridサービス)] > [All Clients (すべてのクライアント)]**に移動します。
2. ユーザーを選択し、セッションを削除します。
3. Network Quarantineで、NACを開始します。

Network Quarantineをアンインストールする

1. メインメニューから **[Administration (管理)] > [Configuration (構成)] > [Solutions (ソリューション)]** に移動します。
2. **[Content (コンテンツ)]** セクションで、**[Network Quarantine]** 行を選択します。
3. [Delete Selected (選択項目を削除)] をクリックし、**[アンインストール]** をクリックしてプロセスを実行します。

Taniumサポートに問い合わせる

Taniumサポートに問い合わせるには、https://support.tanium.comにサインインします。