Tanium™ Map ユーザガイド

バージョン 3.4.26

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

Mapの概要

Mapがあれば、アプリケーションとサービスのコンポーネントを特定し、それらが実行されているエンドポイントとアプリケーション間の関係を表示できます。この関係を知ることによって、メンテナンスのためにエンドポイントを停止する前にその影響を知ることができます。

アプリケーションサービスのマップ

Mapでは、アプリケーションは、ソフトウェアとデバイス、ネットワークトラフィックの論理的なグループです。アプリケーションサービスマップを作成すると、これらのコンポーネント間の過去24時間の依存関係を視覚的に表示することができます。

たとえば、データベースサーバとウェブサービス、データベースで構成される3つの階層のウェブアプリケーションがあるとします。一連のクライアントはネットワーク経由でこのアプリケーションにアクセスします。Mapを使用すると、アプリケーションコンポーネント、コンポーネントをホストしているサーバ、およびウェブアプリケーションにアクセスするクライアントを視覚化することができます。

詳細は、「アプリケーションサービスのマッピング(28ページ)」を参照してください。

エンドポイントのマップ

エンドポイントマップでは、特定のIPアドレスにあるプロセスと依存関係のマップを作成することができます。特定のエンドポイントで実行中のプロセスを確認して、そのプロセスが行っている接続を把握し、そのエンドポイントに依存しているアプリケーションサービスを確認することができます。

詳細は、「エンドポイントのマッピング(32ページ)」を参照してください。

アプリケーションの回復力

アプリケーションの依存関係とエンドポイント、インフラストラクチャ、アーキテクチャを分かることによって、単一障害点や容量計画の問題、ITの非効率使用をより良い形で特定できるようになります。

たとえば、特定のエンドポイントの保守が必要な場合、その停止の影響を受けるすべてのアプリケーションを把握できます。

他のTanium製品との統合

Mapは、関連データの追加レポート作成のため、Tanium™ Trendsと統合しています。

Trends

MapはMapコンセプトのデータ視覚化を提供するトレンドボードを備えています。

[Map] パネルには、Mapがインストールされているエンドポイントの数、アプリケーションにマッピングされているサーバの数、およびMapツールがインストールの有無に関する情報が表示されます。**Map**ボードには、以下のパネルがあります。

- Map Coverage Status (Mapのカバー率ステータス)
- アプリケーションへのサーバのマッピング
- Tools Installations (Mapツールのインストール状況)

Mapにより提供されているトレンドボードのインポート方法の詳細については、Tanium Trendsユーザガイド：初期ギャラリーをインポートするを参照してください。

Mapでの成功

以下のベストプラクティスに従うことで、Tanium Mapの価値を最大化し、成功を収めてください。これらの手順は、主要ベンチマーク指標の「カバー率の増加」および「アプリケーションにマッピングされているサーバ」に沿っています。

手順1: 組織的効果を達成する

Mapの価値を最大化する主要組織ガバナンス手順を実行します。各タスクについての詳細は、組織的効果の達成(11ページ)を参照してください。

☐ 専用の変更管理プロセスを開発する。

☐ RACIチャートで役割と責任を明確に定義する。

☐ 部署横断的な組織連携を検証する。

☐ 運用指標を追跡する。

手順2: エンドポイントの検出設定をする

デフォルトでは、Mapは各種Windows ServerおよびLinuxシステムをはじめとするサーバのオペレーティングシステムを対象にします。

Windowsエンドポイント

☐ Taniumイベントレコーダ用ドライバがインストールされていることを確認します。Question「`Get Tanium Driver Status from all machines with Windows OS Type contains Windows Serve`」を実行して、[**Search** (検索)] をクリックします。詳細は、以下を参照してください。Windows系システム(23ページ) Windows系システム(23ページ) 。

Linuxエンドポイント

☐ 監査デーモンauditdの最新の安定バージョンとaudisp-pluginsパッケージがインストールされていることを確認します。次のQuestionを実行をします: `Get Installed Application Exists[audit] from all machines with Is Linux containing "true"`. 詳細は、「auditdがないLinuxエンドポイントを特定する (34ページ)」を参照してください。

☐ **Recorder - Disable Raw Logging (Rawパッケージを無効)[Linux]**パッケージをLinuxエンドポイントに展開して、Rawログを無効にします。このパッケージによって、`auditd.conf`ファイルが編集されて、適切な設定が適用されます。

☐ Tanium以外のツールを使用して、監査デーモンが変更されているかどうかを確認します。

☐ SELinuxを無効にします。`/etc/sysconfig/selinux`ファイルで`SELINUX=disabled`を設定します。

手順3: Taniumのモジュールをインストールする

☐ Tanium Mapをインストールします。「Map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(24ページ)」を参照してください。

☐ Tanium Trendsをインストールします。以下を参照してください。Tanium Trendsユーザガイド：Trendsのインストールを参照してください。

☐ Tanium Endpoint Configurationを提供するTanium Client Managementをインストールする。Tanium Client Managementユーザガイド：Client Managementのインストールを参照してください。

手順4: Mapを設定してエンドポイント初期化する

☐ サービスアカウントを設定します。「サービスアカウントを構成する(25ページ)」を参照してください。

☐ デフォルトでは、Mapのツールは、各種Windows ServerおよびLinuxシステムをはじめとするサーバオペレーティングシステムにのみインストールされます。Mapアクショングループは、必要に応じて変更することができます。アクショングループの対象設定を変更すると、15分間隔でエンドポイントに更新が配布されます。「Mapアクショングループを設定する(25ページ)」を参照してください。Mapアクショングループを設定する(25ページ)をご覧ください。

☐ Mapの**Overview (概要)**ページの **[Health (健全性)]** セクションでエンドポイントの初期化の進行状況を確認します。**Tools Needed (ツールが必要)**値は、Mapツールがインストールされていないシステムの数です。ステータスの詳細を表示するには、チャートの **[Tools Needed (ツールが必要)]** バーをクリックし、**[View Current Results filtered by Tools Needed (現在の結果をツールが必要でフィルタ)]** をクリックします。

Mapのインポートで自動設定を使用すると、次のデフォルト設定が適用されます。

- Mapサービスアカウントには、そのモジュールのインポートに使用したアカウントが設定されます。
- Mapアクション グループには、`All Windows Severs`と`All Linux`コンピュータグループが設定されます。
- Mapのツールがエンドポイントに展開されて、設定後にネットワークイベントの記録が開始されます。

☐ マップデータを保持する時間範囲を設定します。Mapデータベースとすべてのマップ両方のデータを保存しておく時間数を設定することができます。デフォルトでは、Mapのエンドポイントデータベース、エンドポイントマップ、およびアプリケーションマップには、24時間分のデータが含まれます。これらの値を変更するには、Mapの **Overview (概要)**ページに移動し、[Settings (設定)] をクリックして、**[Time Range (時間範囲)]** タブをクリックします。これらの値は、Mapのすべてのマップとエンドポイントデータベースに適用されます。

> 開始するには、時間範囲の両方の値を168時間(1週間)に設定します。データベースのサイズと使用率を監視し、必要に応じて設定を調整することができます。

手順5: アプリケーションサービスを検出およびマッピングする

☐ Mapの**Overview (概要)**ページの **[Application Discovery (アプリケーションの検出)]** セクションに表示されているアプリケーションのエントリポイントを調べて、Apacheなどの目的のシステムを探します。

☐ エントリポイントを選択し、検出を開始します。

☐ アプリケーションマップを保存します。

詳細は、「アプリケーションサービスのマッピング(28ページ)」を参照してください。

手順6: Mapの指標を監視する

☐ Trendsでメニューに移動して **[Boards (ボード)]** をクリックし、**[IT Operations Metrics (IT運用指標)]** をクリックして、**[Map Coverage (カバー率)]** と **[Servers Mapped to an A@pplication (アプリケーションにマッピングされているサーバ)]** パネルを表示されます。

☐ Mapのカバー率を監視およびトラブルシューティングする(35ページ)。

☐ アプリケーションにマッピングされたサーバを監視およびトラブルシューティングする(36ページ)。

組織的効果の達成

Mapが提供する価値を最大化するの4つの重要な組織ガバナンス ステップは次のとおりです。

- 専用の変更管理プロセスを開発する。変更管理(11ページ)を参照してください。
- 役割と責任を明確に定義する。RACIチャート(11ページ)を参照してください。
- 運用の達成度を追跡する。運用指標(13ページ)を参照してください。
- 部署横断の連携を検証する。組織的連携(13ページ)を参照してください。

変更管理

アプリケーションサービスのアクティビティに対するTanium固有の一元的な変更管理プロセスを統合することができます。

- すべてのアプリケーションサービスについてサービスレベル合意事項(SLA) を更新したTanium固有の変更管理プロセスを作成する。
- サーバ依存データを利用する組織の主要リソースを特定して、アップタイムと可用性を最大化する。
- ITセキュリティ、IT運用、ITリスク/コンプライアンスにまたがるアプリケーションサービスのアクティビティについて、主要リソースに合わせてアクティビティを調整する。
- サーバの依存関係を特定し、変更またはメンテナンス時期のアップタイムを最大化する。
- Tanium運営グループ(TSG) を創設し、サーバマッピングアクティビティのSLAに沿ったプロセスの審査と承認を滞りなく進められるようにする。

RACIチャート

RACIチャートでは、「**Responsible (担当責任者)**」「**Accountable (説明責任者)**」「**Consulted (問い合わせ先)**」「**Informed (情報所有者)**」となるチームまたはリソースを特定し、ITセキュリティ、IT運用、ITリスク/コンプライアンスにまたがる主要業務を表す指針の働きをします。組織の1つ1つに具体的なビジネスプロセスとIT組織の要求があります。次の表は、Taniumから見たアプリケーションサービスに対する組織の職務別リソースのあり方を表しています。ベースラインの一例としてご利用ください。

タスク	ITセキュリティ	IT運用	ITリスク/コンプライアンス	経営陣	根拠
アプリケーションサービスインフラストラクチャのトラブルシューティング	C	A/R	C	-	IT運用チームは、アプリケーションサービスの可用性について義務と責任を負います。アプリケーションに問題がある場合、IT運用チームは、アプリケーションのコンポーネントとそれらホスト場所を把握する必要があります。パッチを適用するかどうか、脅威があるかどうかについて、ITセキュリティおよびITリスク/コンプライアンスチームと協議します。
サーバ変更管理	I	A/R	I	-	IT運用チームは、サーバの役割と依存関係を理解し、サーバの変更と再起動、アップタイムの確保について義務と責任を負います。セキュリティとコンプライアンスチームの両方にダウンタイムの可能性を通知します。
サーバのコンプライアンス違反または脆弱性緩和計画	C	A/R	C	I	IT運用チームは、アプリケーションサービスの可用性およびサービス回復計画について義務と責任を負います。サーバにパッチ適用または処置が必要な場合は、ITセキュリティおよびITリスク/コンプライアンスの両方と協議します。広範囲に及ぶサービス停止とサービスの回復について経営陣に通知します。

タスク	ITセキュリティ	IT運用	ITリスク/コンプライアンス	経営陣	根拠
データセンタの移行	C	A/R	C	C	データセンタ間のアプリケーションサービスの移行は、ITのすべての分野が対象になります。IT運用チームは、ダウンタイムを最小限に抑え、移行前の体制を回復する義務と責任があります。移行したサービスのコンプライアンスとリスク回避を確実にするために、ITセキュリティおおびITリスク/コンプライアンスチームの両方と協議します。基幹業務のアプリケーションのダウンタイムと可用性把握できるよう、このプロセス全体を通じて経営陣と協議します。

アプリケーションのパフォーマンスのトラブルシューティングワークフロー

データセンタの移行ワークフロー

サーバのコンプライアンス違反/脆弱性のワークフロー

組織的連携

成功している組織は、縦割りの部署を超える共通のプラットフォームとしてTaniumを活用することで、高品質のエンドポイントデータと一元的なエンドポイント管理を実現しています。Taniumは、セキュリティと運用、リスク/コンプライアンス担当チームが、統一された1つのプラットフォームが提供する一連の共通の事実に基づいて業務を行うことを可能にする共通のデータスキーマを提供します。

部署横断の連携がなく、部署が縦割り化していると、アプリケーションサービスのアクティビティを改善する意思決定にではなく、データ品質の調査に時間と労力が費やされます。

運用指標

Mapの達成度

アプリケーションおよびサービスのデータの活用の成功には、テクノロジの運用実現と主要ベンチマーク指標を使用した測定の成功が必要です。Tanium Map プログラムの運用達成度を測定し、指針とするための4つの主要なプロセスは次のとおりです。

プロセス	説明
使用法	組織でのTanium Mapの利用状況と利用のタイミング - Tanium Mapは唯一のツールであるか、または他のレガシーツールの補助ツールか
自動化	エンドポイントにまたがるTanium Mapの自動化方法
機能的統合	ITセキュリティ、IT運用、ITリスク/コンプライアンスにまたがるTanium Mapの統合方法
レポート作成	Tanium Mapの自動化状況とマップの報告対象者

ベンチマーク指標

主要なアプリケーションサービスプロセスに加え、Tanium Mapプログラムの運用達成度に連携して価値を最大化し成功を収めるための2つの主要ベンチマーク指標は次のとおりです。

経営陣の指標	Mapのカバー率	アプリケーションへのサーバのマッピング
説明	Tanium Mapがインストールされて実行されているエンドポイントの割合。	アプリケーションにマッピングされているサーバの割合。
インストルメンテーション	Mapツールが存在するサーバの数 / 環境内のサーバ数 (サポートされているサーバグループ)	アプリケーション関連サーバ数 / サーバ数
この指標が重要な理由	サポートされているすべてのサーバにMapツールをインストールすることで、アプリケーションサービスを最大限可視化し、最高度の認識を実現することができます。	正式なアプリケーションに含まれていないサーバが存在する場合は、追加の精査が保証されます。スタンドアロンサーバは、不承認アプリケーション、移行の失敗、またはデバイスの遺棄の兆候である場合があります。スタンドアロンサーバの目的を明らかにすることは、コストの再利用や、サービスの整理統合の機会になります。

次表を使用して、Tanium Mapに関する組織の達成度を判断してみてください。

		レベル1 (要改善)	レベル2 (平均以下)	レベル3 (平均)	レベル4 (平均以上)	レベル5 (最適)
プロセス	使用法	Mapを設定済み	検出されたエントリーポイントを確認	重要なアプリケーションサービスのマッピングと保存	重要なアプリケーションサービスのマッピングと変更、保存	重要なアプリケーションサービスのマッピングと変更、保存
	自動化	Mapでデフォルトのポートを使用するエントリポイントを自動的に検出	Mapでデフォルトのポートを使用するエントリポイントを自動的に検出	Mapでデフォルトとカスタムポートを使用するエントリポイントを自動的に検出	Mapでデフォルトとカスタムポートを使用するエントリポイントを自動的に検出	Mapでデフォルトとカスタムポートを使用するエントリポイントを自動的に検出
	機能的統合	部署が縦割り化	アドホックタスクについてIT運用チームが縦割り化	アプリケーションの依存関係の可視化についてIT運用チームが縦割り化	IT運用チームとセキュリティチームの間でMapデータを共有することで、アプリケーションコンポーネントを表示	IT運用チームとセキュリティチームの間でMapデータを共有することで、他のTaniumモジュールで使用されるアプリケーションコンポーネントとアプリケーション定義に基づいてコンピュータグループを表示し、状況に応じて関連情報を提供
	レポート作成	アドホック	アドホック - 検出されたエントリポイントをMapワークベンチに一覧表示	恒常的 - アプリケーションマップをMapワークベンチに表示	Mapデータを使用して、以前にマッピングされたアプリケーション構成システムの新規追加または消失の経時変化を判断	Mapデータを使用して、アプリケーションの構成システムの変更に基づいてアラートを生成
指標	Mapのカバー率	0～59%	60～74%	75～85%	86～96%	97～100%
	アプリケーションへのサーバのマッピング	0～49%	50～64%	65～79%	80～94%	95～100%

Mapの要件

Mapをインストールし、利用するには次の要件を満たす必要があります。

Taniumの依存関係

Map製品モジュールのライセンスに加えて、ご使用の環境が以下の要件を満たしていることを確認してください。

コンポーネント	要件
Tanium™ Core Platform	• 7.3.314.4250以降 • 7.4.1.1939以降
Tanium™ Client	特定のTanium Clientのバージョンについての詳細は、Tanium Clientデプロイガイド：クライアントホストシステムの要件を参照してください。 OSごとに、以下の7.2 Tanium Clientバージョンのいずれかが必須です。 • サポートされている任意のTanium Clientバージョン(Linux、MacOS*、Windows) • 7.2.314.3608以降(MacOS10.15.x以降) * = 10.15.x Catalinaより前のMacOS 各OSでサポートされているTanium Clientのバージョンについては、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。 リストされていないクライアントバージョンを使用する場合、特定の製品機能は利用できない可能性があります。または、リストされたクライアントバージョンのいずれかにアップグレードすることによってのみ解決できる安定性の問題が発生する可能性があります。
Taniumの製品	Mapのインストールで[**Install with Recommended Configurations (推奨構成でインストール)**]が選択された場合、Tanium Serverはライセンス契約のあるすべてのモジュールを自動的に一括インストールします。これ以外の場合は、Mapが機能するために必要な各モジュールを手動でインストールする必要があります(Tanium Consoleユーザガイドを参照)。Taniumモジュールの管理を参照してください。 以下の最小バージョンのモジュールが必要です。 • Tanium™ Endpoint Configuration 1.2以降(Tanium Client Management 1.5以降に含まれる) 次のモジュールは任意ですが、併用するには、Mapが次の最小バージョンが必要です。 • Tanium Trends 3.6.310以降

Tanium™ Module Server

Map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。使用状況によりますが、Module Serverへの影響はごくわずかです。

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

Mapは、次のエンドポイントオペレーティングシステムに対応しています。MapはTaniumTM Client Recorder Extensionを使用してエンドポイントからデータを収集します。

オペレーティングシステム	バージョン	注
Windows	• Windows 7 SP1以降 • Windows Server 2008 R2 SP1以降	Windows 7エンドポイントの場合は、可能な限りWindows 7 SP2以降にアップグレードしてください。Windows 7 SP1にはMicrosoft Windows Update KB2758857が必要です。
macOS	Tanium Clientサポートと同じです。Tanium Clientユーザガイド：ホストシステム要件を参照してください。	

オペレーティングシステム	バージョン	注
Linux	• Red Hat Enterprise Linux 5.4以降 • CentOS 5.4以降 対応しているその他のLinuxバージョンについては、以下を参照してください。Tanium Clientユーザガイド：ホストシステム要件を参照してください。	Client Recorder Extensionは、CentOSおよびRed Hat Enterprise Linuxバージョン5.3以前に対応していません。エンドポイントには、バージョン5.4またはそれ以降のCentOSまたはRed Hat Enterprise Linuxが必要です。 Client Recorder Extensionは、以下の配布物およびバージョンにSELinuxポリシーを実装します。 • Oracle Linux 5.x、6.x、7.x、8.x SELinuxが有効な場合に、プロセス情報のみが返される。これは既知の問題であり、Mapの今後のバージョンで対処される予定です。 • Red Hat Enterprise Linux (RHEL) 5.4以降、6.x、7.x、8.x • CentOS 5.4以降、6.x、7.x、8.x • Amazon Linux 2 LTS (2017.12) 現時点では、SELinuxは他のLinuxディストリビューションではサポートされていません。 Linuxエンドポイント： • 最新の安定版の監査デーモンとaudispdプラグインをインストールします。監査デーモン設定の非推奨パラメータについては、「Tanium Clientのレコーダ拡張ユーザガイド」を参照してください。手順については、特定のオペレーティングシステムのマニュアルを参照してください。 • 不変の「-e 2」モードを使用する場合、レコーダは不変フラグの前にTanium監査ルールを追加することに注意してください。Linuxで-e 2フラグを使用する場合は、レコーダを有効にした後でエンドポイントを再起動する必要があります。 • 障害「-f 2」モードを使用する場合、監査メッセージが失われた場合にLinuxカーネルパニックが発生することに注意してください。設定が検出されると、レコーダは監査ルールを追加しません。 SELinuxを無効にします。`/etc/sysconfig/selinux`ファイルで`SELINUX=disabled`を設定します。

必要なディスク容量

各エンドポイントのMapデータベースには、過去24時間のTCP接続の記録が含まれます。このデータベースのサイズは、TCP接続の本数によって異なります。ほとんどの場合、データベースの最大サイズは200 MBです。

CPUおよびメモリ要件

エンドポイントでのCPU要求は平均1%未満です。エンドポイント1つあたり少なくとも最低2つのCPUコアが必要です。Tanium Client Recorder Extensionは、CPUコア数が2つ未満では動作できません。

各エンドポイントデバイスには、最低4GBのRAMが必要です。

ホストとネットワークセキュリティの要件

Mapの実行には、いくつかのプロセスが必要です。

セキュリティの除外

未知のホストシステムプロセスを監視およびブロックするために環境でセキュリティソフトウェアが使用されている場合、セキュリティ管理者はTaniumプロセスが問題なく実行できるよう除外を作成する必要があります。Taniumで定義するすべてのセキュリティ除外のリストについては、Tanium Core Platformデプロイリファレンスガイドを参照してください。ホストシステムセキュリティの除外を参照してください。

マップセキュリティの除外

対象デバイス	注	プロセス
Module Server		*<Module Server>*\services\map-service\node.exe
		<Module Server>\services\endpoint-configuration-service\TaniumEndpointConfigService.exe
Windowsエンドポイント	7.2.*x*クライアント	*<Tanium Client>*\Python27\TPython.exe
	7.4.*x*クライアント	*<Tanium Client>*\Python38\TPython.exe
	7.4.*x*クライアント	*<Tanium Client>*\Python38*.dll
		<Tanium Client>\TaniumCX.exe
Linuxエンドポイント	7.2.*x*クライアント	*<Tanium Client>*/python27/bin/pybin
	7.4.*x*クライアント	*<Tanium Client>*/python38/python
		<Tanium Client>/TaniumCX
macOSエンドポイント		*<Tanium Client>*/TaniumCX

ユーザロールの要件

Mapユーザロールのアクセス権限

特権	Map Administrator[1、2]	Map Operator[1、2]	Map Read Only User[1]	Map Service Account[1、2、3]	Map Endpoint Configuration Approver[1、2]
Mapの表示 Mapマップワークベンチへのアクセス					
Mapアプリケーション定義読み取り Mapのアプリケーション定義読み取り					
Mapアプリケーション定義書き込み Mapのアプリケーション定義編集					
アプリケーション構成サービスのマッピング Mapのエンドポイント構成アイテムの登録、使用、書き込み					
Map Operator設定読み取り 大部分のマップ設定の読み取り					
Map Operator設定書き込み 大部分のマップ設定の編集					

Mapユーザロールのアクセス権限 (続き)

特権	Map Administrator[1、2]	Map Operator[1、2]	Map Read Only User[1]	Map Service Account[1、2、3]	Map Endpoint Configuration Approver[1、2]
Map設定読み取り すべてのMap設定の読み取り					
Map Settings Write (Map設定の書き込み) すべてのMap設定の編集					
Mapのエンドポイント構成承認 Mapのエンドポイント構成アイテムの承認					

[1] このロールは、Tanium Trendsに対するモジュールアクセス権限を提供します。このロールに付与されているTrendsアクセス権限はTanium Consoleで確認できます。詳細は、以下を参照してください。Tanium Trendsユーザガイド: ユーザロール要件を参照してください。

[2] このロールは、Tanium Endpoint Configurationに対するモジュールアクセス権限を提供します。このロールに付与されているEndpoint Configurationアクセス権限はTanium Consoleで確認できます。詳細は、以下を参照してください。Tanium Endpoint Configurationユーザガイド: ユーザロール要件を参照してください。

[3]Tanium Client Managementをインストールした後でEndpoint Configurationをインストールする場合、デフォルトでは、モジュールサービスアカウントが開始する構成変更(ツールのデプロイなど)には承認が必要です。**[Endpoint Configuration Bypass Approval (エンドポイント設定のバイパス承認)]**アクセス権限をこのロールに適用し、関連するコンテンツセットを追加すると、モジュール生成の構成変更に対する承認をバイパスできます。詳細は、Tanium Endpoint Configurationユーザガイド: ユーザロールの要件を参照してください。

Mapマイクロ管理者と拡張ユーザーロールのアクセス許可を提供

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	Map Administrator (Reputation管理者)	Map Operator	Map User	Map Read Only User (読み取り専用ユーザー)	Map Service Account	Map Endpoint Configuration Approver
[Read Action Group (アクショングループの読み取り)]	Micro Admin							

Mapマイクロ管理者と拡張ユーザーロールのアクセス許可を提供 (続き)

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	Map Administrator (Reputation管理者)	Map Operator	Map User	Map Read Only User (読み取り専用ユーザー)	Map Service Account	Map Endpoint Configuration Approver
Execute Plugin (プラグインの実行)	詳細	予約						
Execute Plugin (プラグインの実行)	詳細	Map						
Execute Plugin (プラグインの実行)	詳細	Trends						
Execute Plugin (プラグインの実行)	詳細	Endpoint Configuration						
Read Plugin (プラグインの読み取り)	詳細							

Map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、Map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。

- **デフォルト設定での自動設定**(Tanium Core Platform 7.4.2以降のみ): Map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。Mapの自動設定についての詳細は、「Map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(24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**: Mapをインストールした後、必要な設定を手動で行う必要があります。このオプションは、Map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、Mapのインポートおよび設定でカスタム設定を使用する(25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。
- Mapの要件(16ページ)を確認してください。

エンドポイントの準備をする

Windows系システム

> WindowsサーバにTaniumイベントレコーダ用ドライバをインストールしてください。Mapの展開範囲を拡張して他のWindowsデバイスを含める場合は、必ず、それらの追加デバイスにTaniumイベントレコーダ用ドライバをインストールします。

1. TaniumのHome (ホーム)ページからQuestion「`Get Tanium Driver Status from all machines with Windows OS Type contains Windows Server`」を実行し、**[Search (検索)]** を実行します。
2. **[Install Recommended (インストールを推奨)]**を選択します。
3. デプロイアクションページから、**[Install Tanium Driver (Taniumドライバのインストール)]**を選択します。
4. パッケージインストールの終了時に実行する検証クエリを確認することで、インストールがうまくいったことを確認します。
5. Live Responseを使用して検証クエリに失敗したすべてのエンドポイントからアクションログを収集します。
6. Tanium Event Recorderドライバサービスステータスで SERVICE_RUNNING以外を返したエンドポイントでは、**[Remove Tanium Driver (Taniumドライバの削除)]**アクションを実行します。

Linux系システム

> Linuxシステムでは、監査デーモンをインストールして有効にし、rawログを無効にしてください。

1. 安定バージョンの監査デーモンとaudisp-pluginsがインストールされていることを確認します。TaniumのHome (ホーム)ページからQuestion `Get Running Processes contains auditd from all machines with Is Linux contains true`。詳細は、「auditdがないLinuxエンドポイントを特定する (34ページ)」を参照してください。
2. rawログが無効になっていることを確認します。
   a. 次のQuestionを実行をします: `Get Client Extensions - Status from all machines with Is Linux contains true`。rawログが有効な場合は、health_checkステータスが返されます。

      > **Client Extensions - Status (Client Extensions - ステータス)**センサーがない場合は、Tanium Client Managementをインストールすることで Tanium CXコンテンツを取得することができます。『Tanium Client Managementユーザガイド』を参照してください。

   b. **Recorder - Disable Raw Logging[Linux]**パッケージをLinuxエンドポイントに展開して、Rawログを無効にします。このパッケージによって、`auditd.conf`ファイルが編集されて、適切な設定が適用されます。
3. Tanium以外のツールを使用して、監査デーモンが変更されているかどうかを確認します。
4. SELinuxを無効にします。`/etc/sysconfig/selinux`ファイルで`SELINUX=disabled`を設定します。

レガシーのClient Recorder Extensionを削除する

対象のエンドポイントにClient Recorder Extensionバージョン1.xが存在する場合は、Client Recorder Extensionバージョン2.xツールをインストールする前に削除する必要があります。Client Recorder Extensionバージョン1.xが存在するエンドポイントを対象にするには、次のQuestionを使用します。`Legacy - Recorder Installed`。[Supported Endpoints (サポートされているエンドポイント)]列に**No (いいえ)**と表示された場合は、エンドポイントにClient Recorder Extension 2.xツールをインストールする前に、Client Recorder Extensionバージョン1.xを削除する必要があります。Client Recorder Extensionバージョン1.xを削除するには、対象のエンドポイントに**Recorder - Remove Legacy Recorder *[オペレーティングシステム]***パッケージをデプロイします。

Map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

Mapのインポートで自動設定を使用すると、次のデフォルト設定が適用されます。

- Mapサービスアカウントには、そのモジュールのインポートに使用したアカウントが設定されます。
- Mapアクション グループには、`All Windows Severs`と`All Linux`コンピュータグループが設定されます。
- Mapのツールがエンドポイントに展開されて、設定後にネットワークイベントの記録が開始されます。

Mapをインポートして、デフォルト設定を適用するには、インポートの手順で必ず **[Apply Tanium recommended configurations (Tanium推奨構成を適用)]** チェックボックスを選択します。手順の詳細は、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。Mapのバージョンを確認する(27ページ)を参照してください。

(Tanium Core Platform 7.4.5以降のみ)自動構成でMapをインポートする手順には、Mapアクショングループが**No Computers**フィルタグループを対象にするように設定するためのオプションの手順が含まれています。このオプションを選択すると、Mapがエンドポイントに自動的に「tools」をデプロイしなくなります。たとえば、すべてのエンドポイントにtoolsをデプロイする前に、一部エンドポイントでテストしたいとしましょう。この場合、その一部のみを対象とするtoolsアクショングループを手動でデプロイできます。

Mapのインポートおよび設定でカスタム設定を使用する

デフォルトの設定を自動的に適用することなくMapのインポートだけ行うには、インポートの手順で必ず **[Apply Tanium recommended configurations (Tanium推奨構成を適用)]** チェックボックスをオフにします。手順の詳細は、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。Mapのバージョンを確認する(27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、Map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。

- **Tanium Administrator**ロール。
- Tanium Client Managementをインストールした後でEndpoint Configurationをインストールする場合、デフォルトでは、モジュールサービスアカウントが開始する構成変更(ツールのデプロイなど)には承認が必要です。**[Endpoint Configuration Bypass Approval (エンドポイント設定のバイパス承認)]**アクセス権限をこのロールに適用し、関連するコンテンツセットを追加すると、モジュール生成の構成変更に対する承認をバイパスできます。詳細は、Tanium Endpoint Configurationユーザガイド：ユーザロールの要件を参照してください。

Mapのアクセス権限についての詳細は、「ユーザロールの要件(20ページ)」を参照してください。

1. メインメニューから **[Modules (モジュール)] > [Map]** に移動します。
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、**[Save (保存)]**をクリックします。

Mapアクショングループを設定する

デフォルトでは、Mapアクション グループには、`All Windows`と`All Linux`コンピュータグループが設定されます。このアクショングループは必要に応じて更新できます。アクショングループを設定すると、選択したエンドポイントにMapのツールが自動的に展開されます。

アクショングループをデフォルトから更新する場合は、Taniumイベントレコーダ用ドライバがコンピュータグループのすべてのエンドポイントにインストールされていることを確認します。「エンドポイントの準備をする(23ページ)」を参照してください。

1. メインメニューから **[Administration (管理)] > [Actions (アクション)] > [Scheduled Actions (スケジュール済みアクション)]** に移動します。
2. アクショングループのリストで**Tanium Map**をクリックします。
3. **[Edit (編集)]**をクリックし、アクショングループに含めるコンピュータグループを選択して、**[Save (保存)]**をクリックします。

> 初めてツールを展開した後、エンドポイントから結果が返されるまでに最大20分ほど時間がかかることがあります。返された結果は、アプリケーション検出やエンドポイントのマップで表示することができます。

Tanium Endpoint Configurationでソリューションの構成を管理する

Taniumエンドポイント設定は、Taniumソリューションの構成情報と必要なツールをエンドポイントに提供します。エンドポイント設定は、従来Taniumの追加機能に付随していた設定アクションを統合し、ソリューションの構成を実施してから、その構成がエンドポイントに到達するまでの間にタイミングエラーが発生する可能性を排除します。このように設定を管理することで、Tanium機能のインストール、設定、および使用する時間が大幅に短縮されるとともに、エンドポイントのグループをより柔軟に特定の設定の対象にすることができます。

> エンドポイント設定は、Tanium Client Managementの一部としてインストールされます。詳細は、以下を参照してください。Tanium Client Managementユーザガイド：Client Managementのインストール

また、エンドポイント設定を使用して、設定の承認を管理することもできます。たとえば、エンドポイント設定で承認権限を持つユーザが構成の変更を承認するまで構成変更がデプロイされないようにできます。Mapの設定変更の承認に必要なロールと権限についての詳細は、「ユーザロールの要件 (20ページ)」を参照してください。

エンドポイント設定を使用して承認を管理するには、構成の承認を有効にする必要があります。

1. メインメニューから、**[Administration (管理)] > [Shared Services (共有サービス)] > [Endpoint Configuration (エンドポイント設定)]** に移動して、エンドポイント設定の **[Overview (概要)]** ページを開きます。
2. [Settings (設定)] をクリックし、**[Global (グローバル)]** タブをクリックします。
3. **[Enable configuration approvals (構成の承認を有効化)]** を選択し、**[Save (保存)]** をクリックします。

エンドポイント設定についての詳細は、Tanium エンドポイント設定ユーザガイドを参照してください。

Taniumソリューションの依存関係を管理する

初めてMapワークベンチを起動すると、Tanium Consoleは、Mapに必要なすべての依存関係の必要なバージョンがインストールされているか確認します。Mapワークベンチを読み込むには、必要なTanium依存関係のすべてがインストールされている必要があります。環境にインストールされていないTanium依存関係があると、バナーが表示されます。Tanium Consoleは、必要なTanium依存関係と必要なバージョンを一覧表示します。

1. Tanium Consoleが依存関係として挙げたモジュールおよび共有サービスをインストールします。詳しくは、『Tanium Console ユーザガイド』の「特定のソリューションをインポート/再インポート/更新する」を参照してください。
2. メインメニューから**[Modules (モジュール)] > Map** に移動してMapの**[Overview (概要)]**ページを開きます。

Mapをアップグレードする

Map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。アップグレードを終えたら、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。「Mapのバージョンを確認する(27ページ)」を参照してください。

Mapのバージョンを確認する

Map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 **[Modules (モジュール)]> Map** に移動して Map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。

アプリケーションサービスのマッピング

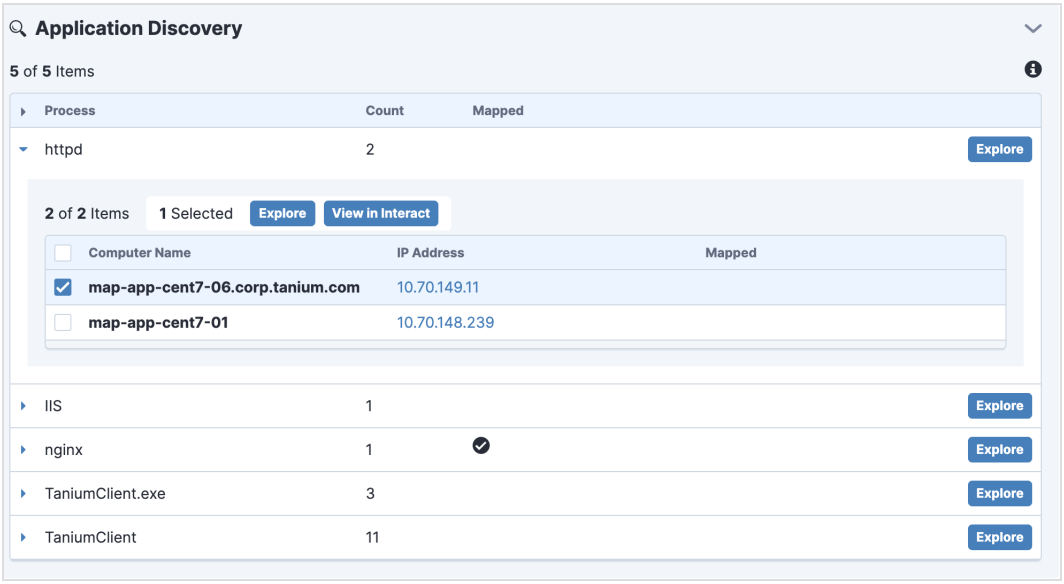
1つのプロセスを起点する接続を探索することで、アプリケーションサービスのマップを作成することができます。

デフォルトでは、Mapのエンドポイントデータベース、エンドポイントマップ、およびアプリケーションマップには、24時間分のデータが含まれます。これらの値を変更するには、Mapの **Overview (概要)**ページに移動し、[Settings (設定)] をクリックして、**[Time Range (時間範囲)]** タブをクリックします。これらの値は、Mapのすべてのマップとエンドポイントデータベースに適用されます。

プロセスを探索する

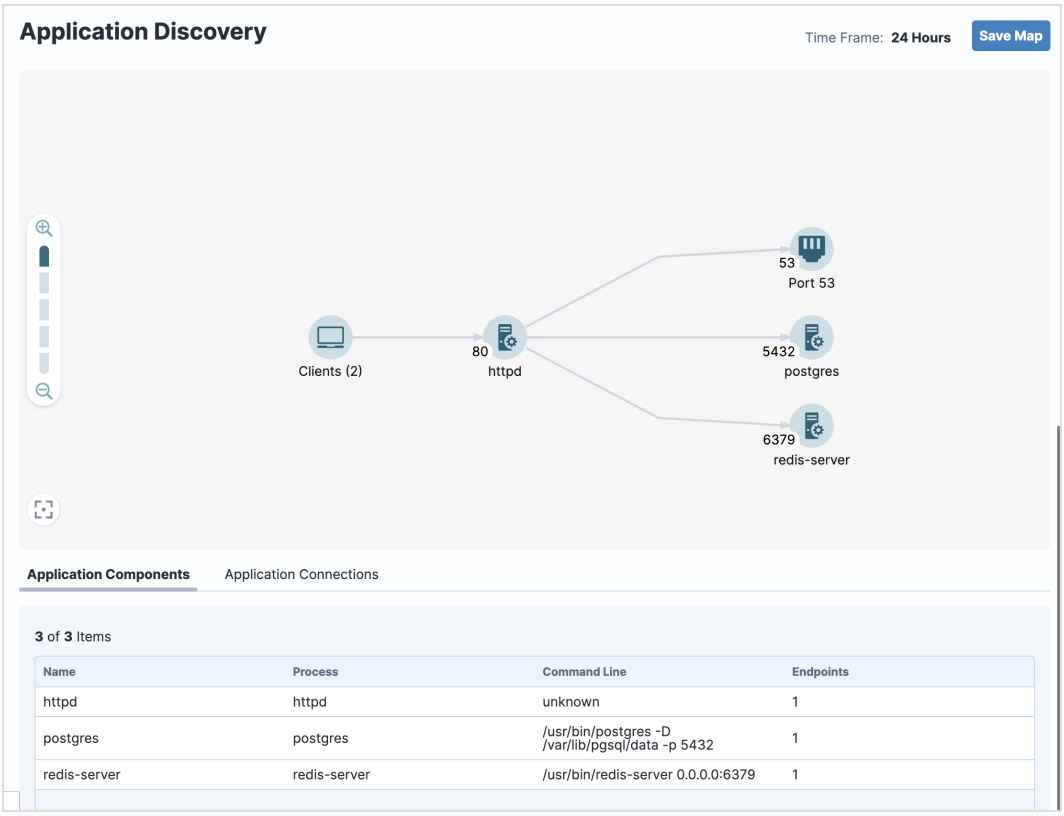
アプリケーションサービスは、サーバでプロセスとして実行される、1つまたは複数のアプリケーションコンポーネントで構成されます。Mapをエンドポイントにインストールして設定すると、アプリケーションの検出が自動的に行われて、アプリケーションサービスへのエントリポイントのリストが特定されます。デフォルトでは、このリストには、TCPポート80、443、17272、または17473への接続があったことが記録されたすべてのプロセスが含まれます。ポートへのアプリケーション検出の追加については、「アプリケーション検出ポートを更新する(31ページ)」を参照してください。

1. Mapの**Overview (概要)**ページで、**[Application Discovery (アプリケーションの検出)]** セクションに移動します。
2. 目的のプロセスを特定します。



そのプロセスを実行しているエンドポイントを表示するには、セクションを展開します。このプロセスから他のアプリケーションコンポーネントへの接続を表示するには、**[Explore (探索)]** をクリックします。

3. 探索したプロセスを視覚化したマップが表示されます。



このプロセスと他のアプリケーションコンポーネントとの接続を表示することができます。一般に、マップはアプリケーションレイヤにあり、左から右に流れます。たとえば、Webアプリケーションであれば、左側にアプリケーションクライアントが表示され、続いてWebサーバ、アプリケーションサーバ、バックエンドのデータベースサーバが表示されます。

4. (任意) マップを中央に表示し直すには、中央寄せをクリックします。

コンポーネントの詳細を表示する

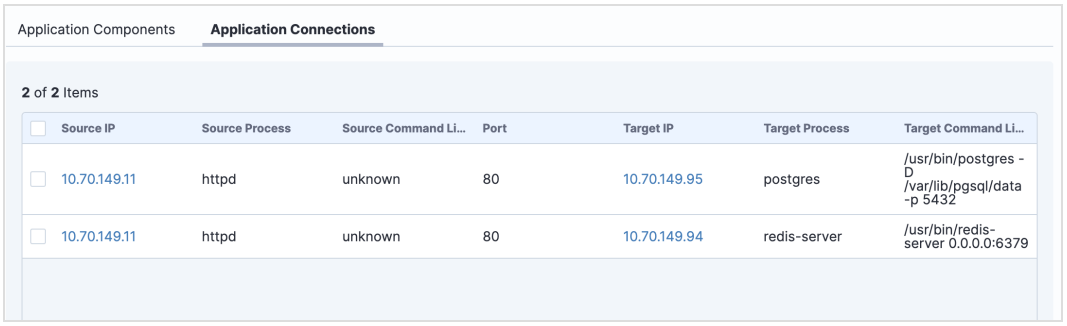
[Application Discovery (アプリケーションの検出)] ページでコンポーネントのリストを表示するには、**[Application Components (アプリケーションのコンポーネント)]** タブをクリックします。このタブには、各アプリケーションコンポーネントの名前とプロセス、コマンドライン、プロセスが実行されているエンドポイント数が表示されます。

コンポーネントの詳細を表示するには、マップでそのコンポーネントをクリックします。コンポーネントの詳細としては、種類とプロセス名、ポート、プロセスの実行に使用されたコマンドライン、コンポーネントを実行しているエンドポイントのリストなどが表示されます。

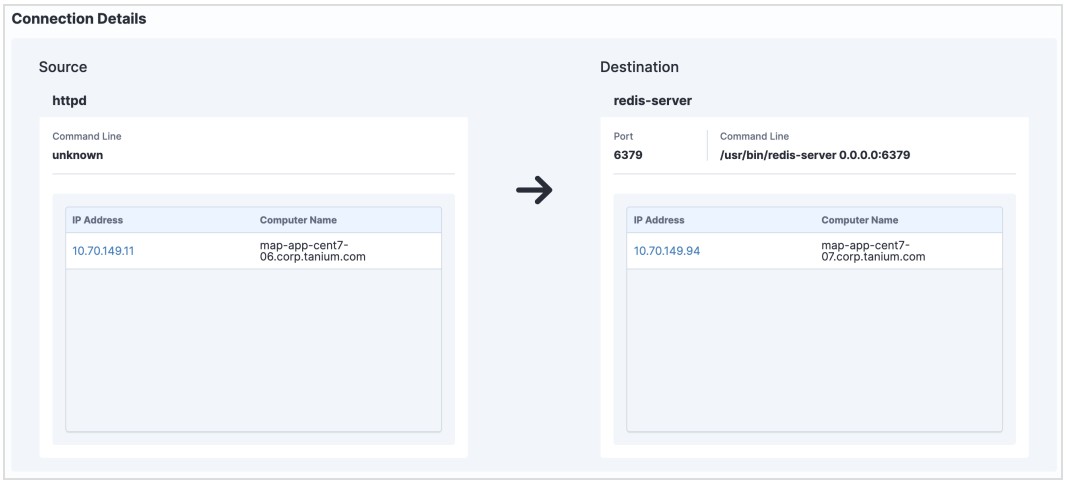
コンポーネントのラベルをカスタマイズするには、マップを保存または編集します。

接続の詳細を表示する

アプリケーションのコンポーネント間の接続のリストを表示するには、[**Application Connections (アプリケーションの接続)**] タブをクリックします。この表には、情報元と接続先のIP、コマンド、プロセス、通信に使用されているポートのリストが表示されます。

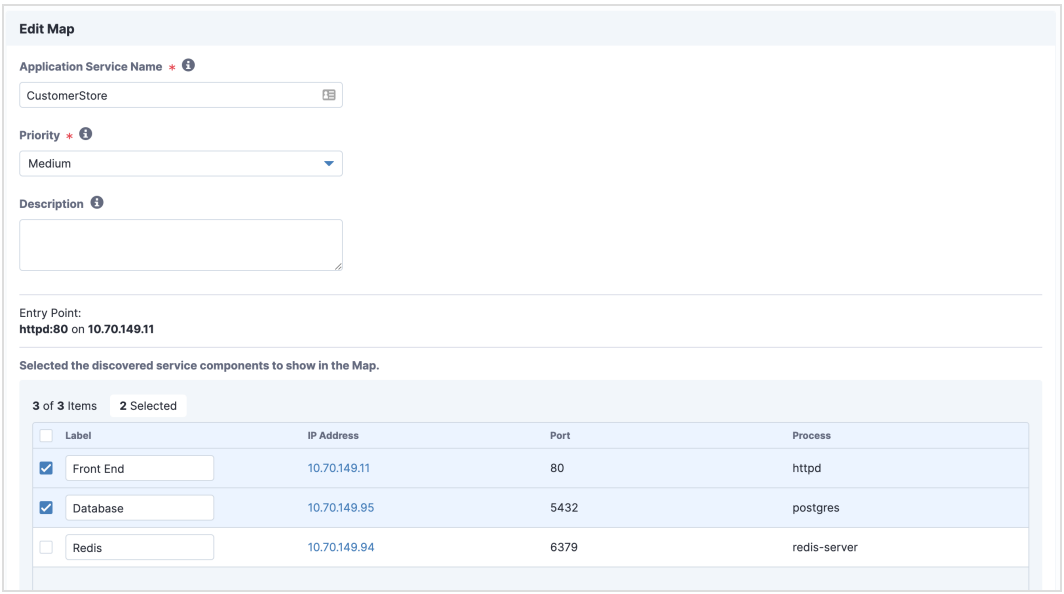


個々の接続の詳細までドリルダウンするには、マップ内のコンポーネントとコンポーネントの間のエッジをクリックします。



マップを保存する

1. [**Save Map (マップの保存)**] をクリックします。
2. アプリケーションサービス名、優先順位、説明など、マップの詳細を入力します。**Priority (優先順位)**は、作成されている他のマップとの関連でユーザが割り当てた値です。
3. マップに表示するアプリケーションのコンポーネントを選択します。コンポーネントを削除するには、ラベルの横のチェックボックスをオフにします。コンポーネントのラベルをカスタマイズすることができ、`myapp front end`などの分かりやすい名前を付けることができます。



[Save (保存)]をクリックします。

アプリケーション検出ポートを更新する

デフォルトでは、アプリケーション検出ではTCPポート80、443、17272、または17473での接続があったことが記録されたプロセスが探されます。このリストを更新するには、設定 に移動し、**[Application Discovery (アプリケーションの検出)]** タブをクリックします。ポートを追加するには、リストでポート番号を入力し、Enterキーを押します。ポートを削除するには、削除 をクリックします。

エンドポイントのマッピング

エンドポイントのマップでは、IPアドレスに関連付けられている接続とアプリケーション、rawプロセスが返されます。エンドポイントをオフラインにし、影響を受ける可能性があるアプリケーションを正確に確認したい場合は、エンドポイントマップを作成します。

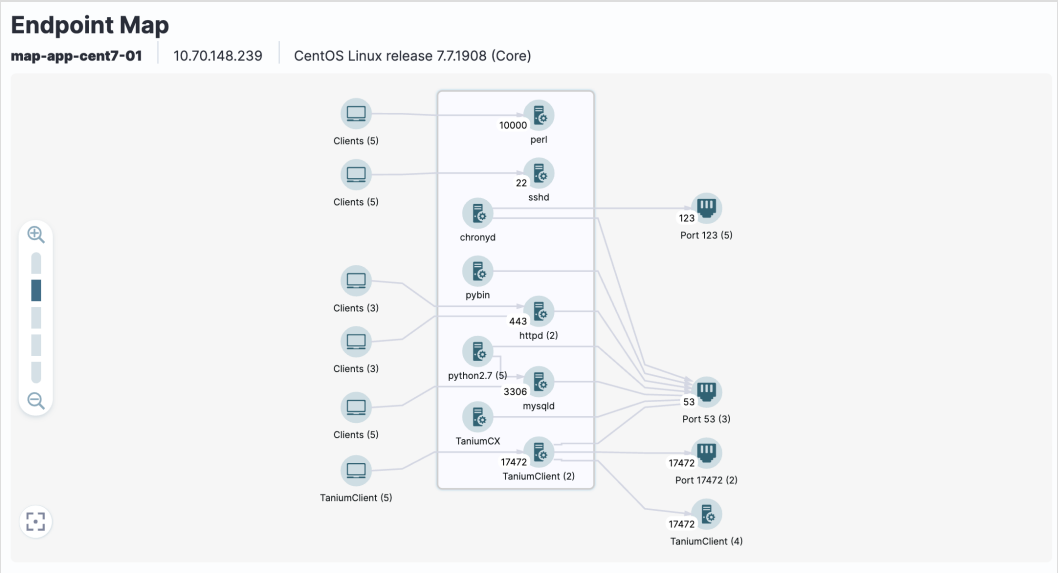
IPアドレスは動的であることがあるため、エンドポイントマップは頻繁な更新が必要になることがあります。エンドポイントマップは、環境を一時的に視覚化するためのものです。

エンドポイントマップを作成するには、マップの対象とするIPアドレスを把握しておく必要があります。最良の結果を得るには、エンドポイントにMapツールがインストールされている必要があります。エンドポイントにインストールされたMapツールを取得するには、エンドポイントがMapアクショングループになければなりません。「Mapアクショングループを設定する(25ページ)」「」を参照してください。

デフォルトでは、Mapのエンドポイントデータベース、エンドポイントマップ、およびアプリケーションマップには、24時間分のデータが含まれます。これらの値を変更するには、Mapの **Overview (概要)**ページに移動し、[Settings (設定)] をクリックして、**[Time Range (時間範囲)]** タブをクリックします。これらの値は、Mapのすべてのマップとエンドポイントデータベースに適用されます。

エンドポイントマップを表示する

1. Mapの**Overview (概要)**ページから **[Maps (マップ)]** セクションに移動し、**[Endpoints (エンドポイント)]** タブをクリックします。マップを作成するIPアドレスを入力します。
2. 生成されるマップには、ホストのIPアドレスと、そのホストで実行中のすべてのプロセスが表示されます。



ホストへの矢印とホストからの矢印は、この通信が行われているポートを含めて、他のプロセスへのインバウンドおよびアウトバウンド接続を示しています。

3. (任意) マップを中央に表示し直すには、中央寄せ をクリックします。

コンポーネントを表示する

エンドポイントで実行されているアプリケーションのコンポーネントを表示するには、[**Components (コンポーネント)**] タブをクリックします。このタブには、各アプリケーションコンポーネントの実行されているプロセスと、そのプロセスのコマンドライン、ポートが表示されます。

エンドポイントマップにアプリケーションを表示する

このエンドポイントを含むアプリケーションサービスを表示するには、[**Active Applications (アクティブなアプリケーション)**] タブをクリックします。このリストには、アプリケーションと、エンドポイントで実行されているアプリケーションコンポーネントが表示されます。

接続の詳細を表示する

接続の詳細を表示するには、プロセスまたはポート間のコネクタをクリックします。

Map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

Mapトラブルシューティングパッケージは、圧縮ZIPファイルとして保存できます。

1. Mapの**Overview (概要)**ページから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. **[Create Package (パッケージの作成)]**をクリックします。
3. ステータスが完了と表示されている場合は、**[Download Package (パッケージをダウンロード)]** をクリックします。ローカルのダウンロードディレクトリに`health-troubleshooting.zip`ファイルがダウンロードされます。
4. 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(38ページ)を参照してください。

Tanium Mapは、`<Module Server>/services/Map`ディレクトリの`Map.log`ファイルにログ情報を保持します。

auditdがないLinuxエンドポイントを特定する

Linuxエンドポイントイベントが記録されていない場合、監査デーモンとaudispdサービスが欠落している可能性があります。Mapモジュールをインストールする前に、auditdデーモンをインストール、および設定しておくことが望ましいですが、エンドポイントを後からオンラインにすることも可能です。

1. (任意) auditdパッケージを作成します。
   一般的なインストールパッケージを作成してロジックをスクリプトに入れるか、単純なスクリプトを作成してロジックをTaniumクエリに入れることができます。「Tanium Core Platformユーザガイド：パッケージの作成と管理」を参照してください。
2. 次のQuestionを実行をします：`Get Installed Application Exists [audit] from all machines with Is Linux containing "true"`
3. 適切なauditdパッケージを識別されたエンドポイントにデプロイします。

   > パッケージを多数のエンドポイントに配布する必要がある場合は、ネットワークへの悪影響を避けるために、変更に要する時間を長い期間に延長してください。

Mapのコンポーネントの健全性を表示する

Mapの**Overview (概要)**ページで **[Health (健全性)]** セクションに移動します。エンドポイントに存在する問題と、Mapツールのステータスを確認することがきます。

インストールされているレガシー Client Recorder Extensionの問題を解決する

`Get Endpoint Configuration - Tools Status`という質問が実行されて、レガシーバージョンのClient Recorder Extensionがインストールされているエンドポイントを検知した場合、Tanium エンドポイント設定は、結果グリッドのレコーダ列でそのエンドポイントを**Unsupported (未対応)**と報告します。対象のエンドポイントにClient Recorder Extensionバージョン1.xが存在する場合は、Client Recorder Extensionバージョン2.xツールをインストールする前に削除する必要があります。Client Recorder Extensionバージョン1.xが存在するエンドポイントを対象にするには、次のQuestionを使用します。`Legacy - Recorder Installed`。[Supported Endpoints (サポートされているエンドポイント)]列に**No (いいえ)**と表示された場合は、エンドポイントにClient Recorder Extension 2.xツールをインストールする前に、Client Recorder Extensionバージョン1.xを削除する必要があります。Client Recorder Extensionバージョン1.xを削除するには、対象のエンドポイントに**Recorder - Remove Legacy Recorder *[オペレーティングシステム]***パッケージをデプロイします。

Oracle Linuxサーバでファイルやネットワーク、セキュリティ事象が表示されない

レコーダの結果にファイル、ネットワーク、またはセキュリティ事象が表示されない場合は、SELinuxを無効にすることができます。Oracle LinuxでSELinuxが有効、auditdフォールバックが無効の場合、プロセス情報のみが返されます。あるいは、Client Recorder Extensionの構成パラメータが次のように設定されていることを確認してください。

- **CX.recorder.AuditdStopAuditdService**が0に設定されている。
- **CX.recorder.AuditdEnableAudispdFallback**が1に設定されている。

詳細については、Client Recorder Extensionユーザガイド：記録されたイベントの設定を参照してください。

Mapのカバー率を監視およびトラブルシューティングする

次の表は、**Mapのカバー率ステータス**指標が期待値に満たない場合の要因と、実施可能な是正措置をまとめています。

理由	是正措置
デプロイされていないツール	• Tanium Clientが最新でサポートされていることを確認します。Mapでサポートされ ているTanium Clientのバージョンについては、「Mapの要件 (16ページ)」のリストを参照してください。 • 目的のターゲットが適切なマップアクション グループに含まれていることを確認します。「Mapアクショングループを設定する(25ページ)」を参照してください。
レコーダの健全性	• Windowsシステムの場合は、Taniumドライバが使用中であることを確認します。「Windows系システム(23ページ)」「」を参照してください。 • auditdがログを記録しないように設定されていることを確認します。「Linux系システム(24ページ)」「」を参照してください。 • 十分なドライブ容量があることを確認します。Mapのデータベースには最大200MBの空きディスク容量が必要です。 • **Client Extensions - Status (ステータス)**センサーの結果で、対処する必要がある健全性チェックの調査結果があるか確認します。

理由	是正措置
CXの健全性	• **Client Extensions - Status (ステータス)**センサーの結果で、重点的に処置すべき範囲を判断します。 • エンドポイントがアプリケーション検出の要件を満たしていることを確認します。「手順2: エンドポイントの検出設定をする(8ページ)」を参照してください。

アプリケーションにマッピングされたサーバを監視およびトラブルシューティングする

次の表は、**Servers Mapped to an Application (アプリケーションにマッピングされているサーバ)**指標が期待値に満たない場合の要因と、実施可能な是正措置をまとめています。

理由	是正措置
スタンバイ状態	フェイルオーバーテストの実施頻度を増やし、関係するすべてのマシンにライブトラフィックを発生させてみてください。
デコミッショニングされてはいるが、実際には退役されていない	エンドポイントマップを使用して、正当なトラフィックが発生していないか確認し、その結果に従ってトラフィックをリダイレクトしてください。「エンドポイントのマッピング(32ページ)」を参照してください。
適切な承認なしにオンライン化	システムアクティビティログで現在のユーザと管理者を確認してください。
縮退状態	Taniumを使用して、システムをトリアージして診断し、ベストとなる一連の措置を決定してください。

エンドポイントからMapツールを削除する

エンドポイントまたはコンピュータグループからMapツールを削除するアクションをデプロイすることができます。使用できるアクションは、Windowsエンドポイントと Windows以外のエンドポイントとで分かれています。

1. Interactで、ツールを削除するコンピュータを対象にします。たとえば、特定のオペレーティングシステムを対象とするQuestionを実行するとしましょう。
   `Get Endpoint Configuration - Tools Status from all machines with Is <OS> equals True`。例:
   `Get Endpoint Configuration - Tools Status from all machines with Is Windows equals True`
2. 結果で、**Map**の行を選択し、必要に応じてドリルダウンして、Mapツールを削除する対象を選択します。詳細は、『Tanium Interactユーザガイド』を参照してください。Questionの結果の管理を参照してください。
3. **[Deploy Action (アクションをデプロイ)]** をクリックします。
4. **[Deploy Action (アクションをデプロイ)]** ページで `[Enter package name here (ここにパッケージ名を入力)]` ボックスに **Endpoint Configuration - Uninstall**を入力し、対象にするエンドポイントに従って **[Endpoint Configuration - Uninstall Tool (ツールのアンインストール) [Windows]]** または **[Endpoint Configuration - Uninstall Tool (ツールのアンインストール)[Non-Windows]]** を選択します。
5. **[Tool Name (ツール名)]** で**Map**を選択します。

6. (任意) デフォルトでは、削除したツールを再インストールすることはできません。ツールを自動的に再インストールできるようにするには、**[Block reinstallation (再インストールをブロック)]** を選択解除します。ほぼすぐに再インストールが行われます。

   > エンドポイントに対する再インストールがブロックされている場合、モニターのデプロイ時には、対象のエンドポイントに従って、**[Endpoint Configuration - Unblock Tool (ツールのブロック解除)[Windows]]** または **[Endpoint Configuration - Unblock Tool (ツールのブロック解除)[Non-Windows]]** パッケージをデプロイする必要があります。

7. (任意) エンドポイントからすべてのMapデータベースとログを削除するには、**[Soft uninstall (ソフトアンインストール)]** を選択解除します。
8. (任意) Mapのツールと依存関係があったすべてのツール(RecorderやIndexなど)あるいは他のモジュールのツールと依存関係がないすべてのツールも削除するには、**[Remove unreferenced dependencies (参照されていない依存関係の削除)]** を選択します。
9. **[Show Preview to Continue (プレビューを表示して続行)]**をクリックします。
10. ページ下部に結果グリッドが現れて、アクション対象のエンドポイントが表示されます。結果に問題がなければ**[Deploy Action (アクションのデプロイ)]**をクリックします。

> エンドポイント設定を有効にしている場合、ツールがエンドポイントから削除されるには、エンドポイント設定でツールの削除が承認されている必要があります。

Mapをアンインストールする

1. Taniumの**Home (ホーム)**ページから **[Administration (運用管理)] > [Configuration (構成)] > [Solutions (ソリューション)]** に移動します。
2. Mapで、**[Uninstall (アンインストール)]**をクリックします。**[Proceed with Uninstall (アンインストールに進む)]**をクリックしてプロセスを完了します。
3. アクショングループを[コンピュータなし]に設定して、スケジュールされたアクションのマップを無効にします。
   a. メインメニューから、**[Actions (アクション)] > [Scheduled Actions (予定済みアクション)]**の順にクリックします。
   b. **Tanium Map**アクショングループをクリックします。**[Edit (編集)]** をクリックします。
   c. **[Computer Groups (コンピュータグループ)]** セクションで、選択されているコンピュータグループのチェックボックスをオフにし、**No computers**コンピュータグループを選択します。
   d. **[Save (保存)]** をクリックします。
4. エンドポイントからMapツールを削除します。「エンドポイントからMapツールを削除するを参照してください。
5. アンインストールプロセスの一環として、Module Serverにバックアップ用の `map-files/<unix_timestamp>`フォルダが作成されます。このフォルダは保持または削除できます。その他のMap痕跡物がModule Serverに残る場合は、Taniumサポートにお問い合わせください。

6. Mapの保存済みQuestionを削除します。以下の条件をすべて満たす保存されたQuestionは削除できます。
    1. Map用に設定したサービスアカウントが所有する保存済みQuestion
    2. 名前が`Map`で始まる保存済みQuestion
    3. `Map`コンテンツセットに含まれている保存済みQuestion
7. Mapアクショングループが削除されていない場合は、削除します。`Tanium Map`アクショングループが空でない場合、削除することはできません。

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。