Tanium™ Enforce ユーザガイド

バージョン 0.1.0

2020年 11月 20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。

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

Enforceの概要

Enforceを使用すると、...

主要コンセプト1

詳細については、<link to related page>を参照してください。

主要コンセプト2

詳細については、<link to related page>を参照してください。

主要コンセプト3

詳細については、<link to related page>を参照してください。

はじめに

1. Tanium Enforceをインストールします。詳細については、<cross reference to install>を参照してください。
2. オブジェクトを構成します。詳細については、<cross reference>を参照してください。

Enforceの要件

Enforce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

Enforce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
プラットフォーム	7.2以降。
Console Web UI バージョン	
Tanium™ Client	
TaniumTM [other modules]	(必須) または(省略可)、バージョンをリスト

Tanium™ Server

Tanium™ Module Server

Enforceがインストールされると、Module Serverホストコンピュータ上で1つ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への影響は小さいです。

エンドポイント

サードパーティのソフトウェア

ホストとネットワークセキュリティの要件

Enforce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

Enforceの通信には、以下のポートが必要です。

コンポーネント	ポート	方向	目的
Module Server		アウトバウンド	
		インバウンド	

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セキュリティソフトウェアが環境内で使用されている場合、セキュリティ管理者はTaniumプロセスを干渉なく実行できるように除外を作成する必要があります。

表1：Enforceのセキュリティ除外

対象デバイス	プロセス
Module Server	"*<Tanium Module Server>*\services\Enforce\node.exe" service.js
	<Tanium Module Server>\services\twsm-v1\twsm.exe
エンドポイント	*<Tanium Client>*\Enforce\tanium-enforce.min.vbs
	<Tanium Client>\\Enforce\\scans\\wsusscn2.cab

[1] = ここでの*nnn*はアクションIDに対応します。

[2] = Volexity Surgeをメモリ収集に使用する場合は例外が必要です。

インターネットのURL

不明なURLを監視してブロックするため、セキュリティソフトウェアが適用されている環境では、セキュリティ管理者は以下のURLをホワイトリストに追加しなければならない場合があります。

- ここにリストする

ユーザロールの要件

表 2：Enforceユーザロールアクセス権限

アクセス許可	Enforce管理者	Enforceユーザ	Enforce読み取り専用ユーザ
Enforceの表示[1] Enforceワークベンチの表示	2	2	2
Enforceモジュールの読み取り Enforceモジュールへの読み取りアクセス	2	2	
Enforceモジュールの書き込み Enforceモジュールへの書き込みアクセス			
Enforce設定の書き込み Enforceモジュールでのグローバル設定への書き込みアクセス			

[1] Enforceをインストールするには、管理者の予約ロールが必要です。

[2] 提供された許可を示します。

表 3：Enforceのユーザロールが高度の場合のアクセス権限

アクセス許可	アクセス許可用コンテンツセット	Enforce管理者	Enforceユーザ	Enforce読み取り専用ユーザ
Read Sensor (センサーの読み取り)	予約			

アクセス許可	アクセス許可用コンテンツセット	Enforce管理者	Enforceユーザ	Enforce読み取り専用ユーザ
Read Sensor (センサーの読み取り)	デフォルト			
Write Package (パッケージの書き込み)	Enforce			

表4：Enforceのユーザロールがマイクロ管理者と高度の場合のアクセス権限

アクセス許可	ロールタイプ	アクセス許可用コンテンツセット	Enforce管理者	Enforceユーザ	Enforce読み取り専用ユーザ
Read User Group (ユーザグループの読み取り)	Micro Admin				
Read Sensor (センサーの読み取り)	高度	デフォルト			
Write Package (パッケージの書き込み)	高度	Enforce			

表5：Enforceのオプションのロール

ロール	許可されるアクション
Enforceユーザ	作成、編集、または削除...
Tanium Administrator (Tanium管理者)	予定済みアクションを作成...

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。

Enforceのインストール

Enforceは、**[Tanium Solutions (Taniumソリューション)]** ページからインストールできます。

使用を開始する前に

- リリースノートをお読みください。
- 7ページのEnforceの要件を確認してください。
- 以前のバージョンからアップグレードする場合は、Tanium Enforceのアップグレードを参照してください。

Enforceをインポートする

[Tanium Solutions (Taniumソリューション)] ページからEnforceをインポートします。

1. メインメニュー☰から**[Tanium Solutions (Taniumソリューション)]**をクリックします。
2. **[Tanium Enforce]**で**[Import (インポート)]**をクリックします。

   > **注意：** Enforceはライセンスされたソリューションです。Enforceが**[Tanium Solutions (Taniumソリューション)]** ページにない場合は、テクニカルアカウントマネージャ(TAM)にご連絡ください。

3. **[Content Import Preview (コンテンツインポートのプレビュー)]**ウィンドウでパッケージを展開して、インストールされるTaniumコンテンツを確認することができます。**[Proceed with Import (インポートを続行)]**をクリックします。
4. インストール処理が完了したら、ブラウザをリフレッシュします。
5. メインメニューから**[Enforce]**をクリックします。Enforceの**ホーム**ページが表示されます。

インストールを確認する

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、Enforce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を設定する必要があります。

- **Tanium Administrator (Tanium管理者)**または**Enforce Service Account (Enforceサービスアカウント)**ロール。
- (任意)**Connect User (Connectユーザ)**ロール - Tanium Connectにデータを送信します。

Enforceの**ホーム**ページからサービスアカウントを更新するには、設定 をクリックし、**[Service Account (サービスアカウント)]**タブを開きます。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。

Enforceの権限についての詳細については、7ページのEnforceの要件を参照してください。

Enforceをセットアップする

Enforce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ZIPファイルとして保存されます。

1. Enforceのホームページでヘルプ 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. **[Collect (収集)]**をクリックします。`Enforce-support.[timestamp].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サポートケースフォームにzipファイルを添付するか、担当のテクニカルアカウントマネージャに送信してください。

Tanium Enforceのログ情報は、次の場所に記録されます:`Enforce.log`ファイル `\Program Files\Tanium\Tanium Module Server\services\Enforce` ディレクトリ。

トラブルシューティングタスク1

Enforceをアンインストールする