Tanium™セキュリティ推奨事項 Guide

バージョン: すべて

2021年12月30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

Taniumのセキュリティ推奨事項

Taniumは、カスタマーがTanium Core Platformのアーキテクチャや構成を安全に実装できるよう、強化されたアプライアンスや文書など、さまざまなリソースを提供します。この文書ではこれらのリソースおよび推奨事項の概要を解説します。

インフラストラクチャオプション

Tanium Core Platformでのデプロイには主に2つのインフラストラクチャオプションがあります。

1. 強化した物理的、または仮想のTaniumアプライアンス。
2. カスタマーが提供するハードウェアへのWindowsインストール。

Taniumは、可能な限り、物理的または仮想的なアプライアンスのデプロイを推奨します。アプライアンスのアップデートはTaniumが提供します。アプライアンスが実践的ではない場合、Tanium Core Platformのソフトウェアを、カスタマーが提供するハードウェア、またはWindows仮想マシンでクラウドインフラストラクチャにインストールできます。クラウドインフラストラクチャまたはカスタマー提供のハードウェアのデプロイは、選択してインフラストラクチャをカスタマーが維持、アップデートする必要があります。

一般セキュリティ推奨事項

Taniumのデプロイ方法に関わらず、Taniumではセキュリティベストプラクティスに従うことを推奨します。

Tanium Consoleへの安全なアクセス

Taniumでは、Tanium Consoleへのネットワークアクセスを特定の管理ネットワークや特定のデバイスに制限するよう推奨します。また、ユーザアクセスには多要素認証(MFA)を使用する必要があります。Taniumは、ADIUS、TACACS+、X.509に基づくCACとSAMLを使用した証明書認証による多要素認証に対応しています。

関連リンク

- Tanium Core Platform展開リファレンスガイド：スマートカード認証
- Tanium Core Platformユーザガイド：SAMLの利用

有効なTLS証明書をインストールする

Tanium Consoleへのユーザ接続はTLSにより暗号化されます。自己署名証明書がインストールプロセス中に生成されます。ただし、Taniumはカスタマーが有効なTLS証明書を取得しインストールすることを推奨します。

関連リンク

- Tanium Core Platform展開リファレンスガイド：SSL証明書
- TaniumサポートKB：Tanium SSL/TLS証明書とキー(ログインが必要)

Tanium秘密キーへ強化したセキュリティを設定する

Taniumはキーマテリアルを高いレベルで保護するためにハードウェアセキュリティモジュール(HSM)の使用を推奨します。HSMを使用する場合、キーはTanium ServerではなくHSMに保管され、HSMから取得することはできません。Tanium Serverは、Taniumの要求に対し有効な署名をするHSMとやり取りをします。

関連リンク

- Tanium Consoleユーザガイド：Taniumキーの管理
- TaniumサポートKB：HSMを使用した暗号キーの保管(ログインが必要)

アクションにTPI (Two-Person Integrity)を使用する

可能な場合は、アクションの承認機能を有効にして使用することを推奨します。アクションの承認が有効な場合、ユーザがデプロイしたアクションはどれも、最初に2人目の従業員に承認されなければなりません。アクションの承認により、有害な可能性のあるアクションをオペレータが誤って発行するリスクを大幅に軽減します。

関連リンク

- Tanium Core Platformユーザガイド：アクション承認の利用

Taniumのログの有効化と転送

Taniumは監査ログを有効化し、ログを一元管理ソリューションへ転送することを推奨します。Taniumでは、APIトークン、コンピュータグループ、コンテンツセット、ダッシュボード、キー、グローバル設定、パッケージ、プラグインスケジュール、権限、保存済みQuestion、スケジュール済みアクション、ロール、センサー、ユーザ、ユーザグループ、ホワイトリストURLに関連する、ユーザによる変更を含むTaniumユーザが実行したすべてのアクションをログ記録することができます。

関連リンク

- TaniumサポートKB：Taniumユーザ監査ログ(ログインが必要)

ロールベースのアクセス制御(RBAC)

Taniumはきめ細いRBACに対応するため、組織は最少特権の原則を実現できます。Taniumは各製品できめ細かいロールを多種提供し、また、カスタム特権による追加のロール作成にも対応します。RBACのほか、コンピュータグループを使用してエンポイントセットへの許可の範囲を制限できます。Taniumはこれらの機能を活用し、既存のユーザに適切やロールを付与すること、また、新規ユーザへ、付与されるユーザ特定のジョブ要件に基づきの機能を制限することを推奨します。

関連リンク

- Tanium Core Platformユーザガイド：RBACの概要

インフラストラクチャ固有のセキュリティ推薦事項

一般的な推奨事項のほか、Taniumは、インフラストラクチャの各種類それぞれのセキュリティに関する考慮事項に従うことを推奨します。

Tanium仮想アプライアンスのセキュリティ確保

Taniumは、Tanium仮想アプライアンスのゲストへのアクセスを制限して、仮想ホストの安全性確保を推奨します。これには、適切な強化ガイドの適用や、可能な場合、ホストへのアクセスに多要素認証を求めることが含まれます。

クラウドインフラストラクチャのデプロイのセキュリティ確保

Taniumは、Tanium Core Platformサーバをホストするクラウド環境へのアクセスを厳格に制御し、既知の、限られたユーザグループのみ、Taniumのデプロイで使用するクラウドリソースへのアクセスまたは変更を許可することを推奨します。Taniumはクラウドプロバイダのアクセスコントロール機能を活用し、Tanium Core Platformサーバを他の内部または本番システムから隔離することを推奨します。

- Amazon Web Services (AWS)のインフラストラクチャでは、組織を使用しTanium固有のAWSアカウントでデプロイします。
- Google Cloud Platform (GCP)のインフラストラクチャでは、Tanium固有のプロジェクトでTaniumをデプロイします。
- Microsoft Azureのインフラストラクチャでは、Tanium固有のリソースグループでTaniumをデプロイします。

さらに、クラウドプロバイダおよび業界標準の利用可能なセキュリティのベストプラクティスに従い、仮想ネットワークとのネットワーク通信の制限し、クラウドユーザの多要素認証の有効化、クラウドのAPIアクティビティ監視などを行います。

カスタマーが提供するWindowsインフラストラクチャのデプロイのセキュリティ確保

TaniumをWindows Serverにインストールするときは、カスタマーはTaniumの強化ガイドに従うことを推奨します。ガイドは国防情報システム局(DISA)の協力のもと開発され、Windows環境におけるTanium Serverの安全を確保するための推奨事項を提供します。

TaniumはさらにTanium Windowsのインストールのセキュリティに影響を与えるドメイン認証情報の侵害リスクを低減するため、お客様が厳格なアクセス制御を導入することを推奨します。最低限、以下を含めてください。

- ハードウェアまたはソフトウェアベースのファイアウォールを使用するWindows管理プロトコルへの、インバウンドのアクセスの制御。特に多要素認証で保護されていない場合。アクセスは、ドメインからWindows Serverを削除することで制限することもできます。
- サービスアカウントの数とサービスアカウントへの許可を、必要なアカウントおよび許可のみに制限します。