Tanium™ Health Check ユーザガイド

バージョン 1.11.26

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

Health Checkの概要

Health Checkを使うことで、Taniumプラットフォームアナライザー(TPAN)レポートの収集を構成可能なスケジュールで自動化できます。TPANレポートにより、問題、リスク、Tanium環境のパフォーマンスの包括的なビューを得ることができます。ローカルでレポートをダウンロードし、Taniumと共有することもできます。これらのレポートを定期的に収集および共有することにより、Taniumは最善のサポートを提供することができます。

TPANレポートの自動収集を有効にすると、収集スケジュールを設定することもできます。Health Checkは、HTTPSプロトコルと共有キー認証を使用して、サニタイズ版TPANレポートをTaniumに送信します。Taniumでのサニタイズ版TPANレポートの自動共有設定が有効な場合、Health Checkは、プッシュベースのメカニズムを使用します。すなわち、TaniumにHTTPSアクセスし、そのサーバ展開とアカウントに固有の書き込み専用ファイルの接続先への有効期限付きURLを受信して、その接続先にサニタイズ版ペイロードを送信します。サニタイズ版ペイロードの内容についての詳細は、以下を参照してください。関連情報：サニタイズ版のレポート例(13ページ)。

Health Checkの基本手順

手順1: Health Checkをインストールおよび設定する

Tanium Health Checkをインストールおよび設定します。

詳細は、「Health Checkのインストール(9ページ)」を参照してください。

手順2: レポートを生成およびダウンロードする

レポートを生成およびダウンロードします。

詳細は、「レポートの生成(13ページ)」を参照してください。

Health Checkの要件

Health Check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

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	7.2以降。
ライセンス	ライセンスについての詳細は、Taniumサポートに問い合わせる(16ページ)。

Tanium™ Module Server

Health Checkは、Module Server上のサービスとしてインストールされ、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

Health Checkはエンドポイントにパッケージを展開しません。Tanium Clientのオペレーティングシステムのサポートについては、以下を参照してください。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。

ホストとネットワークセキュリティの要件

Health Check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

Health Check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)	17242	TCP	内部使用、外部からアクセスできません
Module Server	Tanium Server	445	TCP	Tanium Serverのホスト情報の収集
Module Server	Zone Server	445	TCP	Zone Serverのホスト情報の収集

アプリケーションIDベースのルールではなく、TCPベースのルールを使用してTaniumトラフィックのポートを開くようにファイアウォールポリシーを設定します。たとえば、Palo Alto Networksのファイアウォールであれば、アプリケーションオブジェクトやアプリケーショングループではなく、サービスオブジェクトやサービスグループを使用してルールを設定します。

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。

Health Checkのセキュリティ除外

対象デバイス	注	プロセス
Module Server		*<Module Server>*\services\comply-service\node.exe
		<Module Server>\services\health-service\twsm.exe

ユーザロールの要件

Health Checkのすべてのタスクに、**Administrator**予約ロールが必要です。

WindowsでTanium Serverを実行している場合は、Tanium Health Checkサービスの実行に使用するアカウントを**LOCAL SYSTEM**からTanium ServerとZone Serverへのアクセス権を持つアカウントに変更する必要があります。これ以外の場合、生成されたレポートには、Tanium ServerとZone Serverに関するサーバ情報は含まれません。

Health Check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、Health Checkをインストールし、自動または手動構成のいずれかを選択します。

- **Automatic Configuration with default settings (デフォルト設定を使用した自動構成)**](Tanium Core Platform 7.4.2以降のみ): Health Checkは、必要な依存関係とその他の選択された製品ととも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。Health Checkの自動構成についての詳細は、「Health Checkのインポートおよび構成でデフォルト設定を使用する(9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構成**: Health Check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、Health Check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。詳細は、Health Checkのインポートおよび構成でカスタム設定を使用する(9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。
- Health Checkの要件(7ページ)を確認してください。
- 旧バージョンからのアップグレードの場合は、「Health Checkをアップグレードする(12ページ)」を参照してください。

Health Checkのインポートおよび構成でデフォルト設定を使用する

Health Checkのインポートで自動構成を使用すると、次のデフォルト設定が適用されます。

- Health Checkサービスアカウントには、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。
- 週1回の収集スケジュールが有効になり、設定されます。
- 有効なライセンスの場合、自動データ共有が有効になります。
- ログの詳細レベルやHealth Checkチューニングパラメータなどのその他設定が適用されます。

Health Checkをインポートして、デフォルト設定を適用するには、**[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(「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。インポートしたら、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。「Health Checkのバージョンを確認する(12ページ)」を参照してください。

Health Checkのインポートおよび構成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Health Checkのインポートだけ行うには、手順の実行で必ず **[Apply Tanium recommended configurations (Tanium推奨設定を適用)]** 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。インポートしたら、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。Health Checkのバージョンを確認する(12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、Health Check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**Administrator**予約ロールが必要です。

Health Check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)] > [Health Check] に移動**して、Health Checkの **[Overview (概要)]** ページを開きます。
2. [Settings (設定)] をクリックし、必要に応じて **[Service Account (サービスアカウント)]** をクリックします。
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。

> WindowsでTanium Serverを実行している場合は、Tanium Health Checkサービスの実行に使用するアカウントを**LOCAL SYSTEM**からTanium ServerとZone Serverへのアクセス権を持つアカウントに変更する必要があります。これ以外の場合、生成されたレポートには、Tanium ServerとZone Serverに関するサーバ情報は含まれません。

収集スケジュールを設定する

TPANレポートの自動コレクションを設定できます。エンドポイントのほとんどがオンラインである場合、毎週レポートを1つ以上実行します。

1. Health Checkの**[Overview (概要)]** ページで、[Settings (設定)] をクリックし、必要に応じて **[Collection Schedule (収集スケジュール)]** をクリックします。
2. **[Enable (有効)]** を選択し、少なくとも1日を選択して、時間を選択します。

   > **[Disable (無効)]** を選択すると、レポートを手動で実行することができます。詳細については、TPANレポートを手動で生成する(13ページ)を参照してください。

3. **[Save (保存)]** をクリックします。

共有設定を設定する

有効なライセンスがあると、Taniumを使用してサニタイズ版レポートを自動的に共有設定することができます。ライセンスが更新されていない場合、自動的にレポートを共有設定しない場合は、レポートをローカルにダウンロードして他の方法で共有することができます。

1. Health Checkの **[Overview (概要)]** ページで、[Settings (設定)] をクリックし、必要に応じて **[Sharing (共有)]** をクリックします。
2. レポートの自動共有設定を無効にするには、**[Do not automatically share (自動的に共有設定しない)]** を選択し、**[Save (保存)]** をクリックします。

3. レポートの自動共有設定を無効にするには、**Do not automatically share (自動的に共有設定しない)**を選択し、**[Save (保存)]** をクリックします。

> 有効なライセンスがない場合、**Automatically share with Tanium (Taniumで自動的に共有する)**を選択することはできません。Health Checkでのレポートの共有設定の設定方法についての詳細は、Taniumサポートに問い合わせる(16ページ)。

その他の設定を設定する

ログバーボ傾向や、パラメータのHealth Check調整などの他の設定を構成することができます。

1. Health Checkの **[Overview (概要)]** ページで、[Settings (設定)] をクリックし、必要に応じて **[Other Settings (その他の設定)]** をクリックします。
2. 以下の設定を構成します。

   ログレベル
   Tanium Health Checkのログディテールのレベル

   Number of reports to keep on disk (ディスクに保存するレポートの数)
   ディスクに保存するTPANレポートのローリング番号

   情報ページ収集スケジュール
   バックグラウンドで情報ページを収集する頻度

   指標収集スケジュール
   バックグラウンドで指標ページを収集する頻度

   VDI in use (使用中のVDI)
   サーバの**[Tuning (チューニング)]**レポートで使用

   Active-Active 50/50? (アクティブ-アクティブ50/50？)
   Tanium Serverの高可用性(HA)デプロイがある場合は、**[Yes (はい)]**を選択します

   Bandwidth Sensitive (Tanium Server 7.2) (帯域幅感度 (Tanium Server 7.2))
   サーバの **[Tuning (チューニング)]**レポートで使用

   Bandwidth Limit (Tanium Server 7.3 or later) (帯域幅制限(Tanium Server 7.3以降))
   サーバの**[Tuning (チューニング)]**レポートで使用

3. **[Save (保存)]** をクリックします。

Taniumソリューションの依存関係を管理する

初めてHealth Checkワークベンチを起動すると、Tanium Consoleは、Health Check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。Health Check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)] > Health Check** に移動してHealth Checkの**[Overview (概要)]**ページを開きます。

Health Checkをアップグレードする

Health Checkをアップグレードする手順については、Tanium Consoleユーザガイドを参照してください。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。「Health Checkのバージョンを確認する(12ページ)」を参照してください。

Health Checkのバージョンを確認する

Health Check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)] > [Health Check]** に移動して、Health Check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。

レポートの生成

通常のスケジュールでTPANレポートを自動的に生成、またはTPANレポートを手動で生成するようにHealth Checkを構成できます。ディスクに保存されている各レポートについて、HTMLまたは圧縮ZIPファイルをダウンロードできます。

TPANレポートを手動で生成する

TPANレポートを手動で作成するには、Health Checkの**Overview (概要)**ページの [**Manual Report Generation (レポートの手動生成)**] セクションで [**Run TPAN Report Now (今すぐTPANレポートを実行)**] をクリックします。

TPANレポートを自動的に生成する

TPANレポートを自動的に生成するには収集スケジュールを設定する(10ページ)します。スケジュールを変更するには、Health Checkの [Settings (設定)] で [**Collection Schedule (収集スケジュール)**] をクリックします。

TPANレポートをダウンロードする

ディスクに保存されるレポートには、必ずサニタイズ版と完全版の両方があります。サニタイズ版には、パスワードやコンピュータ名、IPアドレスなどのセンシティブ、すなわち機密情報は含まれません。Health Checkは、設定された数のレポートのみをディスクに保持することで、使用されるディスク容量を最小にします。

サニタイズ版では、圧縮形式のZIPファイルをダウンロードできます。Health Checkの [**Overview (概要)**] ページの [**Reports (レポート)**] セクションでサニタイズ版レポートの横にある**Zip**をクリックすると、TPANレポートをダウンロードすることができます。

完全版では、HTMLまたはZIP形式のファイルをダウンロードすることができます。Health Checkの [**Overview (概要)**] ページの [**Reports (レポート)**] セクションで完全版レポートの横にある**HTML**または**Zip**をクリックすると、TPANレポートをダウンロードすることができます。

サニタイズ版TPANレポートを共有する

特定のTPANレポートのサニタイズ版を手動で共有設定することができます。Health Checkの [**Overview (概要)**] ページの [**Reports (レポート)**] セクションでサニタイズ版レポートの横にある**Share (共有)**をクリックすると、TPANレポートを共有設定することができます。

TPANレポートの生成のたびにサニタイズ版TPANレポートを自動的に共有設定するには、レポートの自動共有を有効にします。詳細は、「共有設定を設定する(10ページ)」を参照してください。

関連情報：サニタイズ版のレポート例

サニタイズ版レポートのデータは、お客様が管理する環境に関するデータではなく、Taniumインスタンスに関するデータに限定されます。Taniumでの共有設定をする前にレポートをダウンロードするか、レポートの自動共有設定を有効にすることで、サニタイズ版レポートに含まれるデータを正確に表示することでできます。

サニタイズ版TPANレポートには、以下のファイルが含まれます。

SanitizedPlatform.json

このファイルは、お客様が管理する環境に関するデータではなく、Taniumの展開に関するサニタイズ版データを含むマシン読み取り可能な形式のファイルです。そうしたデータには、アクティブクライアント数とトレンディングクライアント数、Questionとアクションの発行量のサマリ、Tanium Serverホストシステムの健全性を判定するための情報、インストールされている各ソリューションのバージョン、グローバルチューニングパラメータなどあります。

SanitizedPlatform.txt

このファイルは、Tanium展開の状態に関する基本情報の詳細を含み人間が読み取り可能な形式のファイルです。これには、最新のTPAN日とバージョン、Tanium Platformのバージョン、上位クライアント数、リーダの割合、文字列形式の情報、SAMLやTLSなどのセキュリティモードの有効/無効、インストールされているモジュールとそのバージョン、最新のTPANの調査結果が含まれます。

SanitizedTotesEvents.json

このファイルには、Tanium展開内のコンテンツの使用に関する匿名化されたデータが含まれます。Taniumが公開していないか、Taniumの署名のないセンサー名は、`__SANITIZED_UNSIGNED_SENSOR__`にサニタイズされ、お客様作成のカスタムセンサーの名前が含まれないようになっています。このデータは、各種コンテンツの展開先や、それらコンテンツの用途をTaniumが把握するのに役立ち、コンテンツパックで重要な問題が発見された場合にお客様に注意を喚起する目的に利用することができます。

TANIUMセンサーのエントリ例


```
{
  "datetime": 2020-06-08T15:40:04",
  "hash": 1744818157,
  "qid": 63,
  "sensor": "Tanium Client Subnet",
  "signed_status": "Tanium Signed",
  "soln_category": "Core",
  "soln_id": "01-001-0001",
  "soln_name": "Initial Content - Base",
  "soln_version": "7.1.14.0000",
  "type": "ad-hoc",
  "user": 1
},
```


お客様のセンサーのエントリ例


```
{
  "datetime": 2020-06-04T20:49:43",
  "hash": 965165056,
  "qid": 55,
  "sensor": "__SANITIZED_UNSIGNED_SENSOR__",
  "signed_status": "Likely Unsigned",
  "soln_category": null,
  "soln_id": null,
```

```
  "soln_name": null,
  "soln_version": null,
  "type": "automatic",
  "user": 1
},
```

Health Check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

トラブルシューティングパッケージをリクエストする場合ログファイルは、ブラウザでダウンロードできるZIPファイルとして提供されます。

1. Health Check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. **[Download Package (ダウンロードパッケージ)]**をクリックします。`health-troubleshooting.zip`ローカルダウンロードディレクトリへのファイルダウンロード。
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(16ページ)」を参照してください。

Tanium Health Checkは、`health-service.log`ファイルを`\Program Files\Tanium\Tanium Module Server\services\health-service`ディレクトリにログ情報を保存します。

サニタイズ版レポートの自動共有設定を有効にできない

Taniumでのサニタイズ版レポートの共有設定は、有効なライセンスを持つお客様にのみ提供されます。Health Check 1.2または、それ以降が必要です。

Health Check [Settings (設定)] の **[Sharing (共有設定)]** タブで**[Automatically share with Tanium (Taniumでの自動共有)]** を選択できない場合は、Taniumサポートに問い合わせる(16ページ)有効なライセンスを入手する必要があります。

Health Check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、**[Health Check]** 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。