Tanium™ Direct Connect ユーザガイド

バージョン 1.4.3

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

Direct Connectの概要

Direct Connectは、他のTaniumTMモジュールに通信チャネルを提供すると共に、モジュールにまたがってエンドポイントとの直接接続を設定および管理するための一元的な場所を提供します。

Direct Connectを使用すると、エンドポイントとの直接接続を確立するためにTaniumモジュールが共有する接続を設定できます。Direct Connectでは相互認証方式が採用されているため、IPアドレスと自己署名証明書の両方がサポートされています。

製品の統合

Tanium™ Performance

Direct ConnectとPerformanceを組み合わせると、単一のエンドポイントからプロセスレベルの履歴データを表示して、分析とトラブルシューティングに利用できます。詳細については、Performanceユーザガイド：エンドポイントとの直接接続を参照してください。

Tanium™ Protect

Protectの暗号化管理ポリシーはDirect Connectを使用して、エンドポイントから暗号化キーを安全に取得します。詳細については、Protectユーザガイド：暗号化管理を参照してください。

Tanium™ Reveal

RevealはDirect Connectを使用して、設定されたルールとパターンに一致するエンドポイント上のファイルを表示します。詳細については、Revealユーザガイド：一致ルールの調査および、Revealユーザガイド：一致パターンの検証を参照してください。

アクティブなエンドポイントセッション

Taniumモジュール間の開いているエンドポイントセッションと保留中のエンドポイントセッションを確認できます。アクティブなエンドポイント接続を使用すると、サーバ上のアクティブな接続を確認できます。

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。

はじめに

1. Direct Connectをインストールおよび設定する詳細については、15ページのDirect Connectのインストールを参照してください。
2. エンドポイントに接続するための設定をします。詳細については、15ページのDirect Connectのインストールを参照してください。

Direct Connectの要件

Direct Connectをインストールおよび使用するにあたっては、要件を確認してください。

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	• 7.2.314.2831以降 • 7.3.314.3668以降 • 7.4.1.1939以降
Tanium™ Appliance	(任意)Zone ServerにTanium Applianceを使用する場合は、Taniumオペレーティングシステム(TanOS)1.5.2以降を使用する必要があります。 • TanOS 1.5.2～1.5.4にDirect Connect Zone Proxyをインストールするには、TanOSシェルを使用する必要があります。 • TanOS 1.5.5またはそれ以降のZone Serverアプライアンスの場合は、Tanium Operationsメニューから Direct Connect Zone Proxyをインストールできます。詳細については、Applianceデプロイガイド：Direct Connect Zone Proxyをインストールするを参照してください。
Tanium™ Client	• 7.2.314.3211以降 • 7.4.1.1955以降
Tanium™ の製品	次のモジュールは任意ですが、Performanceと併用するには、指定された最小バージョン要件を満たす必要があります。 • **Tanium Protect**: Direct Connect 1.3.xまたはそれ以降をインストールして、Protectと併用する場合は、Protect 2.1.1以降を使用する必要があります。
	TaniumTM Client Recorder Extensionを使用する次のいずれかのTaniumTMモジュールを使用する場合は、以下のバージョンを使用する必要があります。 • TaniumTM Integrity Monitor 1.7.0.0035以降 • TaniumTM Map 1.1.1.0006以降 • TaniumTM Threat Response 1.2.0.0037以降 • TaniumTM Trace 2.9.0.0035以降

Tanium Module Server

Direct Connectがインストールされると、Module Server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

サポートされているオペレーティングシステム

Direct Connectは、以下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。

- Windows
- Linux
- macOS

オペレーティングシステムの具体的なバージョンについては、Tanium Clientユーザガイドをご覧ください。ホストシステム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

Direct Connectを実行するには、特定のポートが必要です。

ポート

Direct Connectとの通信には、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	17475	インバウンド	エンドポイントと直接接続するためのModule Serverとの接続。

コンポーネント	ポート	方向	目的
Zone Server[1]	17486	インバウンド	Zone Serverがエンドポイントとの接続に使用するバインドポート。 デフォルトのポート番号は17486です。Zone Proxyの設定時に、必要に応じて別のポート番号を指定できます。
	17487	インバウンド (Module Server から Zone Server)	Zone Serverがモジュールサーバとの接続に使用するバインドポート。 デフォルトのポート番号は17487です。Zone Proxyの設定時に、必要に応じて別のポート番号を指定できます。
	17488	インバウンド (Module Server から Zone Server)	Direct Connect Zone Proxyインストーラは、Zone Server上のポート17488を自動的に開くことで、Zone ServerとModule Serverとの間で通信を行えるようにします。

[1] これらのポートは、Zone Serverを使用する場合にのみ必要です。

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：Direct Connectのセキュリティ除外

対象デバイス	プロセス
Windowsエンドポイント	<*Tanium Client*>\TaniumClientExtensions.dll
	<*Tanium Client*>\TaniumClientExtensions.dll.sig
	<*Tanium Client*>\extensions\TaniumDEC.dll
	<*Tanium Client*>\extensions\TaniumDEC.dll.sig

対象デバイス	プロセス
macOSエンドポイント	<*Tanium Client*>/libTaniumClientExtensions.dylib
	<*Tanium Client*>/libTaniumClientExtensions.dylib.sig
	<*Tanium Client*>/extensions/libTaniumDEC.dylib
	<*Tanium Client*>/extensions/libTaniumDEC.dylib.sig
Linuxエンドポイント	<*Tanium Client*>/libTaniumClientExtensions.so
	<*Tanium Client*>/libTaniumClientExtensions.so.sig
	<*Tanium Client*>/extensions/libTaniumDEC.so
	<*Tanium Client*>/extensions/libTaniumDEC.so.sig

ゾーンプロキシサーバの要件

Direct Connectを使用して、Zone Server経由でモジュールサーバにルーティングされるエンドポイントに接続する場合は、そのZone ServerにDirect Connect Zone Proxyをインストールおよび設定する必要があります。詳細については、ゾーンプロキシを設定を参照してください。

> **重要：** 最良の結果を得るには、Zone Serverの手前でロードバランサを使用しないでください。ロードバランサを使用する必要がある場合は、バランサを持続TCP接続に設定し、Direct Connect Zone Proxyで設定する**エンドポイントのインバウンドポート**のポートはロードバランサ上で開いておく必要があります。デフォルトでは、このポートは`17486`です。

ユーザロールの要件

表2：Tanium Direct Connectユーザロール権限

アクセス許可	Direct Connect管理者	Direct Connect読み取り専用ユーザ	Direct Connectサービスアカウント	Direct Connectユーザ
Direct Connectの表示 ユーザにDirect Connectワークベンチへのアクセスを許可します				
Direct Connectセッションの読み取り ユーザにエンドポイント接続の表示を許可します				
Direct Connectセッションの書き込み ユーザにエンドポイント接続の作成と管理を許可します				
Direct Connect設定の読み取り ユーザにDirect Connect設定の表示を許可します				
Direct Connect設定の書き込み ユーザにDirect Connect設定の修正を許可します				
Direct Connectログの読み取り ユーザにDirect Connectログの表示を許可します				
Direct Connect Cronの実行 サービスアカウントの操作を許可します				

表 3：Tanium 7.1.314.3071以降用の拡張ユーザロールアクセス許可

アクセス許可	アクセス許可用コンテンツセット	Direct Connect管理者	Direct Connect読み取り専用ユーザ	Direct Connectサービスアカウント	Direct Connectユーザ
Read Sensor (センサーの読み取り)	予約				
Read Sensor (センサーの読み取り)	ベース				
Read Sensor (センサーの読み取り)	Direct Connect				
Read Action (アクションの読み取り)	Direct Connect				
Read Own Action (自身のアクションの読み取り)	Direct Connect	1	1	1	1
Write Action (アクションの書き込み)	Direct Connect				
Show Preview (プレビューの表示)	Direct Connect	1		1	1
Read Plugin (プラグインの読み取り)	Direct Connect	1	1	1	1
Execute Plugin (プラグインの実行)	Direct Connect				
Read Package (パッケージの読み取り)	Direct Connect	1		1	1
Write Package (パッケージの書き込み)	Direct Connect				
Read Saved Question (保存されたQuestionの読み取り)	予約				
Read Saved Question (保存されたQuestionの読み取り)	Direct Connect				

[1] 提供された許可を示します。

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。

Direct Connect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、Direct Connectをインストールし、自動または手動設定を選択します。

- **デフォルト設定での自動設定** (Tanium Core Platform 7.4.2以降のみ): Direct Connectは、必要なすべての依存関係およびその他の選択された製品と共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。Direct Connectの自動設定についての詳細は、15ページのデフォルト設定でDirect Connectをインポートおよび設定するを参照してください。
- **カスタム設定を使用した手動構成**: Direct Connectのインストール後に、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、推奨されるデフォルト設定とは異なる設定をDirect Connectが必要とする場合にのみ選択します。詳細は、16ページのカスタム設定でDirect Connectをインポートおよび設定する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。
- 8ページのDirect Connectの要件を確認してください。
- 旧バージョンからアップグレードする場合は、Direct Connectをアップグレードするを参照してください。

デフォルト設定でDirect Connectをインポートおよび設定する

自動設定でDirect Connectをインポートすると、次のデフォルト設定が適用されます。

- Direct Connectサービスアカウントは、モジュールのインポートに使用したアカウントに設定されます。
- Direct Connectアクショングループは、`[All Computers (すべてのコンピュータ)]`コンピュータグループに設定されます。

Direct Connectをインポートして、デフォルト設定を適用するには、必ず、Tanium Consoleユーザガイドの手順の実行時に**[Apply Tanium recommended configurations (Tanium推奨設定を適用)]**チェックボックスを選択してください。Taniumモジュールの管理を参照してください。インポート後に、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。22ページのDirect Connectのバージョンを確認するを参照してください。

カスタム設定でDirect Connectをインポートおよび設定する

デフォルト設定を自動的に適用することなくDirect Connectをインポートするには、必ず、Tanium Consoleユーザガイドの手順の実行時に**[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。Taniumモジュールの管理を参照してください。インポート後に、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。22ページのDirect Connectのバージョンを確認するを参照してください。

Direct Connectアクショングループを設定する

アクショングループでは、Direct Connectパッケージをデプロイするエンドポイントのセットを定義します。デフォルトでは、Direct Connectアクショングループの**[Computer Group Targets (コンピュータグループのターゲット)]** は、**[No Computers (コンピュータなし)]**に設定されます。アクショングループを、**[All Computers (すべてのコンピュータ)]**または定義した任意のコンピュータグループに設定できます。

1. Direct Connectの**ホーム**ページの**[Configure (設定)]** セクションで**[Configure Action Group (アクショングループを設定する)]**ステップをクリックし、**[Configure Action Group (アクショングループを設定する)]**をクリックします。
2. Direct Connectに使用するエンドポイントグループのコンピュータグループを選択します。**[Save (保存)]**をクリックします。

サービスアカウントを設定する

Direct Connectサービスアカウントは、Direct Connectサービスのバックグラウンド処理を実行します。入力した資格情報は、Direct Connectをアップグレードするたびに再設定する必要があります。Direct Connectサービスアカウントには、**Direct Connectサービスアカウント**ロールが必要です。

1. Direct Connectの**ホーム**ページの**[Configure (設定)]** セクションで**[Configure Service Account (サービスアカウントを設定する)]**ステップをクリックし、**[Configure Service Account (サービスアカウントを設定する)]**をクリックします。
2. Taniumの資格情報を入力し、**[Save (保存)]**をクリックします。

> **注意：** Direct Connectの設定からサービスアカウントを設定または更新することもできます。設定 をクリックして、**[Service Account (サービスアカウント)]**タブのサービスアカウント設定を更新します。**[Save (保存)]**をクリックします。

エンドポイントとの接続設定をする

エンドポイントとの接続設定では、Tanium Module Serverとの接続に使用するドメイン名と、Tanium Module Serverおよびエンドポイントとの接続認証のための証明書、接続に使用するポートを指定します。

1. Direct Connectの**ホーム**ページの[Configuration (設定)]セクションで、**[Configure Endpoint Connection (エンドポイントとの接続設定をする)]**ステップをクリックし、**[Configure Endpoint Connection (エンドポイントとの接続設定をする)]**をクリックします。
2. **[完全修飾ドメイン名]**セクションで、Tanium Module Serverとの接続に使用するドメイン名を指定します。入力するドメイン名は、エンドポイントとのあらゆる直接接続においてすべてのエンドポイントからTanium Module Serverに解決される必要があります。Direct Connectは、入力された名前の形式が妥当であることを確認します。入力さたドメイン名が正しいことを確認します。
3. デフォルトでは、**ポート**は17475に設定され、変更できません。このポートへの着信接続が、該当するファイアウォール構成によって許可されていることを確認します。
4. **[Action Lock (アクションロック)]** セクションでは、エンドポイントでアクションロックが有効な場合のDirect Connectの動作を指定します。
   - **すべての直接接続アクションをブロック**
   - **新規接続を許可**
   - **新規接続と設定の変更を許可**

   > **注意：** 詳細については、Tanium Consoleユーザガイド：アクションロックの管理を参照してください。
5. **[Save (保存)]**をクリックします。

完全修飾ドメイン名の検証に成功すると、成功メッセージが表示されます。
エンドポイント接続設定が正常に保存されました。
コンテンツの作成が進行中です。接続設定が完了すると、エンドポイントにデプロイされます。

エラーが発生した場合は、完全修飾ドメイン名を修正し、再度保存します。情報が検証され、保存に成功すると、サポート対象の各オペレーティングシステムのパッケージが、直接接続の使用に必要な設定情報とともに作成されます。それらパッケージは、スケジュール済みアクションを使用してTanium Direct Connectアクショングループに配布されます。

証明書を設定する

Tanium Module Serverおよびエンドポイントとの接続認証のための証明書を設定します。

1. Direct Connectの**ホーム**ページから、設定 をクリックします。**[Certificates (証明書)]**タブをクリックします。
2. デフォルトでは、**[Server Certificate (サーバ証明書)]**セクションでは、**[Install a new certificate (新規証明書をインストールする]**オプションが選択されており、初期設定中は変更できません。エンドポイントが接続を開始すると、サーバ認証のための証明書が生成およびインストールされます。
   証明書がサーバにインストールされると、証明書の有効期限日が表示されます。証明書がインストールされている場合は、**[Renew (更新)]**を選択することで証明書を更新できます。
3. デフォルトでは、**[Client Certificate (クライアント証明書)]**セクションでは、**[Install a new certificate (新規証明書をインストールする)]** オプションが選択されており、初期設定中は変更できません。エンドポイントがサーバへの接続権限を持つTanium Clientであることを認証するための証明書が生成およびインストールされ、エンドポイントにデプロイされます。
   証明書がインストールされると、証明書の有効期限日が表示されます。証明書がインストールされている場合は、**[Renew (更新)]**を選択することで証明書を更新できます。
4. **[Save (保存)]**をクリックします。

ゾーンプロキシを設定する

必要に応じてゾーンプロキシを設定することで、TaniumTM Zone Server経由でのエンドポイント接続を有効にできます。Zone Server経由でModule Serverに接続するエンドポイントがある場合、Direct Connectを使用するにはこの設定が必須です。

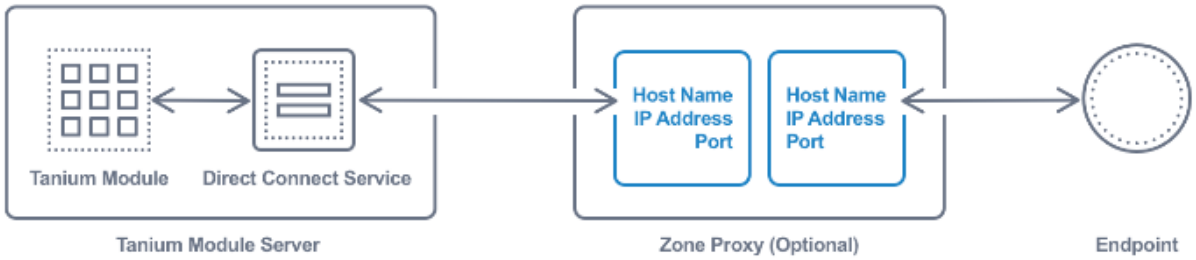


図1：Zone Proxy Serverの概要

重要：最良の結果を得るには、Zone Serverの手前でロードバランサを使用しないでください。ロードバランサを使用する必要がある場合は、バランサを持続TCP接続に設定し、Direct Connect Zone Proxyで設定する**エンドポイントのインバウンドポート**のポートはロードバランサ上で開いておく必要があります。デフォルトでは、このポートは`17486`です。

使用を開始する前に

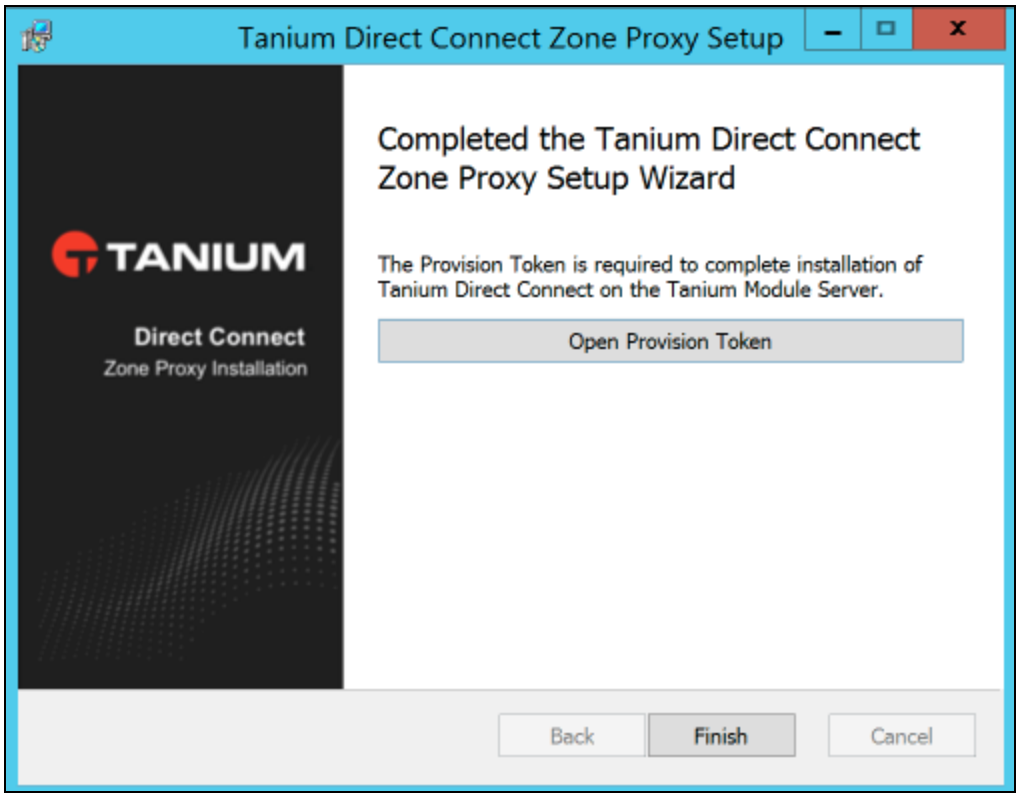
テクニカルアカウントマネージャに連絡して、ご使用のZone Serverオペレーティングシステム用のDirect Connect Zone Proxy Installerファイルを入手してください。

DIRECT CONNECT ZONE PROXYをインストールおよび設定する

1. Direct Connect Zone Proxy InstallerをZone Serverにコピーします。
2. Zone ServerでDirect Connect Zone Proxy Installerを実行して、Direct Connect Zone Proxyをインストールします。

   注意：
   - TanOS 1.5.2～1.5.4にDirect Connect Zone Proxyをインストールするには、TanOSシェルを使用する必要があります。
   - TanOS 1.5.5またはそれ以降のZone Serverアプライアンスの場合は、Tanium OperationsメニューからDirect Connect Zone Proxyをインストールできます。詳細については、Applianceデプロイガイド：Direct Connect Zone Proxyをインストールするを参照してください。

   インストールプロセスでは、プロビジョニングシークレットと証明書(**プロビジョニングペイロード**と呼ばれる)が生成されます。
   プロビジョニングペイロードは`provision.txt`に保存されます。このファイルは次のディレクトリにあります。
   - **TanOS**：*`<Tanium Install Directory>`*`/TaniumDirectConnectZoneProxy/settings/PROVISION.txt`
     TanOSへのインストールプロセス中、インストールを実行しているコンソールには、プロビジョニングシークレットと証明書も表示されます。プロビジョニングシークレットおよび証明書は、コンソールまたは`PROVISION.txt`ファイルのどちらからもコピーできます。
   - Windows：*`<Tanium Install Directory>`*`\\Tanium Direct Connect Zone Proxy\\settings\\PROVISION.txt`
     Windowsへのインストールの最後に、**[Open Provision Token (プロビジョニングトークンを開く)]**をクリックして`PROVISION.txt`を開きます。このファイルから、プロビジョニングシークレットおよび証明書をコピーできます。



以降の設定手順で使用するこれらのテキストは、インストール中にコピーするか、または`provision.txt`から取得します。例：

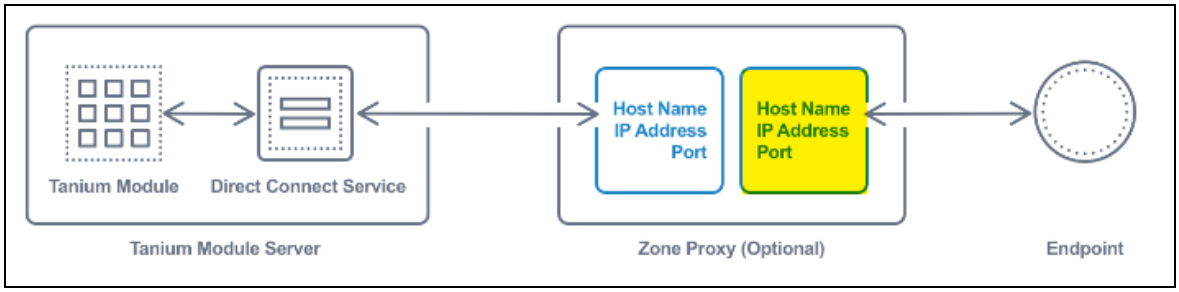
```
-----BEGIN PROVISION SECRET-----
 +EPQlEuU1oBizbexjtshLuoxhNHA0JuMeOAEwFq/OKpEk6+jUJbFPx8Do1+vL22F
 geNrd4/+wbsZwTgL3EUsqg==
 -----END PROVISION SECRET-----
 -----BEGIN CERTIFICATE-----
 MIIC7TCCAdWgAwIBAgIgAwi2sO+h6dq/XIroZ1vK96/sHqxcMRWvkLXFrZrb5pAw
 r3AxeSY2NpzDmVcQFNlYUhyR8QOr5hRE7AF9gGKDei6A
 -----END CERTIFICATE-----
```

必要に応じて、インストーラを再実行して新しいプロビジョニングペイロードを生成できます。

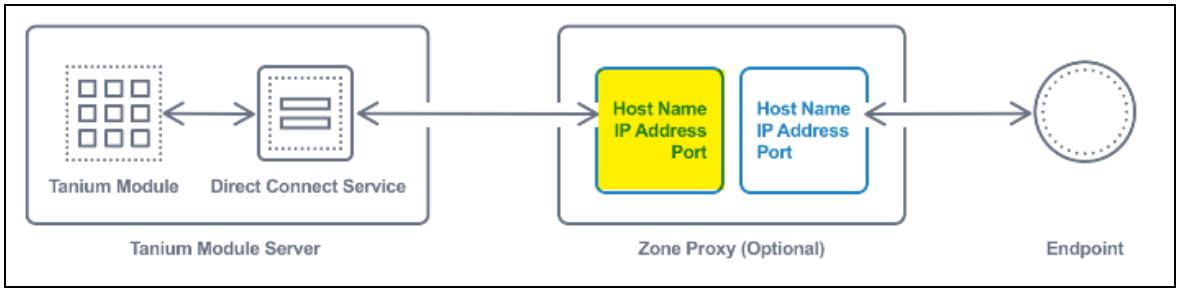
インストールが完了し、プロビジョニングペイロード(プロビジョニングシークレットと証明書)を保存したら、Direct Connectに戻ります。

3. Direct Connectのメニューで**[Zone Proxies (ゾーンプロキシ)]**をクリックします。
4. **[Add Zone Proxy (ゾーンプロキシを追加)]**をクリックします。

5. ゾーンプロキシの**名前**を指定します。
6. インストール中に保存したプロビジョニングシークレットおよび証明書を**[Provision Payload (プロビジョニングペイロード)]**フィールドに貼り付けます。
7. **Zone Serverとのエンドポイント接続を設定**します。



   a. **エンドポイントターゲットホスト名**を指定します。
   この値は、Zone Serverに接続するためにエンドポイントが使用するホスト名か完全修飾ドメイン名、またはIPアドレスです。
   b. **エンドポイントのインバウンドIPアドレス**を指定します。
   この値は、Zone Serverがエンドポイントとの接続に使用するバインドIPアドレスです。この値を使用して、マルチホームサーバー上のエンドポイント接続でバインドするZone Server上のIPv4インタフェースを指定できます。
   c. **[Endpoint Inbound Port (エンドポイントのインバウンドポート)]**を指定します。
   この値は、Zone Serverがエンドポイントとの接続に使用するバインドポートです。デフォルト値は`17486`です。
8. **[Tanium Module Server Connection to the Zone Server (Zone ServerとのTanium Module Server接続)]**を設定します。



   a. **[Module Server Target Hostname (Module Serverターゲットホスト名)]**を指定します。
   この値は、Zone Serverに接続するためにModule Serverが使用するホスト名か完全修飾ドメイン名、またはIPアドレスです。
   b. **[Module Server Inbound IP Address (Module Serverのインバウンド IPアドレス)]**を指定します。

この値は、Zone Serverがモジュールサーバ接続に使用するバインドIPアドレスです。この値を使用して、マルチホームサーバ上のモジュールサーバ接続でバインドするZone Server上のIPv4インタフェースを指定できます。

> **注意：** ほとんどの環境では、この値はModule ServerのIPアドレスと同じではありません。

c. **[Module Server Inbound Port (Module Serverのインバウンドポート)]**を指定します。
この値は、Zone Serverがモジュールサーバ接続に使用するバインドポートです。デフォルト値は`17487`です。

9. **[Save (保存)]**をクリックします。

[Status (ステータス)]列にゾーンプロキシのステータスが表示されます。設定が完了すると、ステータスが**[Connected (接続)]**になります。

プロビジョニングプロセスのため、既存のゾーンプロキシ設定を変更することはできません。必要に応じて、設定を削除して、別の値で再作成できます。設定を削除するには、その設定の上にカーソルを置いて、**[Delete (削除)]**をクリックします。

このページから、既存のゾーンプロキシのステータスとアクティビティを確認することもできます。

Direct Connectをアップグレードする

Direct Connectをアップグレードする手順は、Tanium Consoleユーザガイド:をご覧ください。Taniumモジュールの管理を参照してください。アップグレード後に、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。22ページのDirect Connectのバージョンを確認するを参照してください。

Direct Connectのバージョンを確認する

Direct Connectをインポートまたはアップグレード後は、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. メインメニューで**[Direct Connect]**をクリックして、Direct Connectの**ホーム**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

Direct Connectの使用については、7ページのはじめにを参照してください。

アクティブなエンドポイントセッションの確認

Direct Connectを使用すると、エンドポイントとTanium Module Serverとの間のすべての接続を可視化できます。Direct Connectに表示される接続は、直接接続機能を使用しているTaniumモジュールによって作成されます。

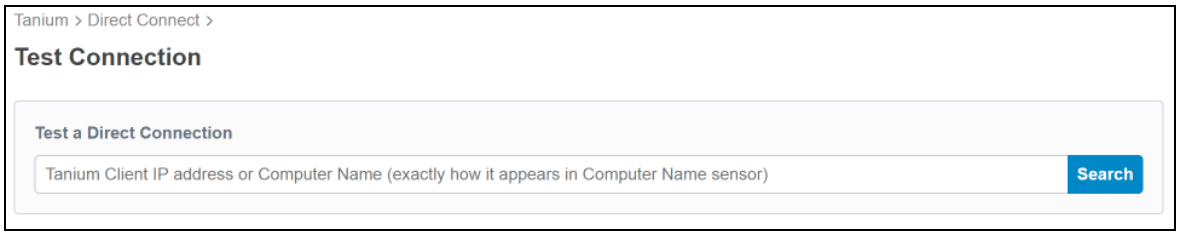
1. [Direct Connect] メニューから、**[Active Endpoint Sessions (アクティブなエンドポイントセッション)]** を選択します。Taniumモジュール全体の現在のすべてのセッションが結果グリッドに表示されます。
2. 結果グリッドには、アクティブな各セッションに関する次の詳細が表示されます。
   - **ホスト名**: エンドポイントのコンピュータ名。
   - **Tanium Client ID**: 接続に使用されているエンドポイントID。
   - **IPアドレス**: エンドポイントのIPアドレス。
   - **アクションステータス**: [Open Session (セッションを開く)] アクションの現在のステータス。ステータス値は、[Creating (作成中)]、[Downloading (ダウンロード中)]、[Running (実行中)]、[Error (エラー)]、[Succeeded (成功)]、[Not Succeeded (不成功)]、[Complete (完了)]、[Closed (終了)] のいずれかです。
   - **セッションステータス**: セッションの現在のステータス。
   - **Duration (期間)**: そのエンドポイントで初めて接続が確立されてからの経過時間。
   - **前回のメッセージ**: エンドポイントから最後にメッセージを受信してからの経過時間。

エンドポイントとの直接接続のテスト

Direct Connectを使用すると、公式に接続を作成することなくエンドポイントとの接続をテストできます。接続のテストは、Taniumモジュールのユーザがエンドポイントに接続できることを確認したり、接続で問題が発生した場合にトラブルシューティングするための有用なツールです。

エンドポイントとの直接接続をテストする

1. Direct Connectのメインメニューで**[Test Connection (接続のテスト)]**をクリックします。
2. 接続をテストするエンドポイントのIPアドレスまたはコンピュータ名 (コンピュータ名 センサーに表示されている名前)を入力します。**[Search (検索)]**をクリックします。



テスト接続に失敗した場合は、25ページの直接接続のトラブルシューティングを参照します。

直接接続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。

サポートパッケージを生成する

トラブルシューティングに使用するDirect Connectサービスの現在の状態に関する情報を収集します。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. Direct Connectの**ホーム**ページでヘルプ をクリックして、**[Troubleshooting (トラブルシューティング)]**タブをクリックします。
2. **[Generate Support Package (サポートパッケージの生成)]**をクリックします。
3. パッケージが生成されると、**[Download Support Package (サポートパッケージのダウンロード)]**ボタンが表示されます。このボタンをクリックして、ローカルのダウンロードディレクトリにZIPファイルをダウンロードします。
4. 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。

ログレベルを変更する

より詳細なログが必要な場合は、ログレベルを変更できます。

1. Direct Connectの**ホーム**ページでヘルプ をクリックして、**[Troubleshooting (トラブルシューティング)]**タブをクリックします。
2. 必要に応じて**ログレベル**を調整します。
   ログレベル値は、**trace**、**debug**、**info**(デフォルト)、**warn**、**error**、**fatal**のいずれかです。

> **注意：**この更新により、以降のログ記録のログレベルが変更されます。これは、サポートパッケージにある以前にログされたイベントに関するデータには影響しません。

エンドポイント接続の問題をトラブルシューティングする

エンドポイント接続を確立できない場合は、**[Action History (アクション履歴)]**ページから`[Deploy Direct Connect (Direct Connectのデプロイ)] - [Open Session (セッションを開く)] - [Operating System (オペレーティングシステム)] - [Session ID (セッションID)]`アクションのステータスを確認します。

アクションは実行されたが、成功しなかった場合は、エンドポイント上の*<Tanium Client>*/Logs/extensions0.txtログを確認します。エンドポイントが、**[Endpoint Connection (エンドポイント接続)]**タブのDirect Connect設定で設定した**完全修飾ドメイン名とポート**を使用してModule Serverに接続できることを確認します。

エンドポイントに対してアクションが実行されなかった場合は、エンドポイントがDirect Connectアクショングループのメンバーであり、かつ最新のツールがインストールされていることを確認します。

[Deploy Direct Connect (Direct Connectのデプロイ)] - [Tools (ツール)]および**[Deploy Direct Connect (Direct Connectのデプロイ)] - [Configure Extension (エクステンションの設定)]**で保存されたアクションのステータスも、トラブルシューティングに役立つことがあります。

Direct Connectをアンインストールする

Direct Connectをアンインストールする必要がある場合は、まずエンドポイントでDirect Connectの痕跡をクリーンアップして、サーバからDirect Connectをアンインストールします。

> **注意：**Direct Connectは、複数のTaniumソリューションで使用される共有サービスです。Direct Connectが別のTaniumソリューションで使用されている場合、Direct Connectをアンインストールするか、エンドポイントからツールを削除すると、予期しない結果が生じることがあります。テクニカルアカウントマネージャに相談して、ご使用の環境でDirect Connectのアンインストールが推奨されるかどうかを確認してください。

エンドポイントからDirect Connectのコンテンツとツールを削除する

各オペレーティングシステムには、専用の削除アクションがあります。このため、クリーンアップ時は、オペレーティングシステムが同じエンドポイントのグループを選択する必要があります。

1. メインメニューで **[Interact]** をクリックします。
2. 質問で、削除するDirect Connectのコンテンツとツールがあるエンドポイントを絞り込みます。たとえば、`Get Direct Connect - Tools Version from all machines`などです。
3. Direct Connectツールを削除するエンドポイントの行を選択します(**Windows Package Installed**、**Mac Package Installed**、または**Linux Package Installed**のいずれか)。
4. **[Deploy Action (アクションをデプロイ)]**をクリックします。
5. **[Deploy Action (アクションのデプロイ)]**ページで、**[Enter package name here (ここにパッケージ名を入力)]**フィールドに`Direct Connect - Remove`と入力します。

6. **[Direct Connect - Remove Tools [*Operating system*]]**アクションを選択します。ここで、*オペレーティングシステム*は、*選択したエンドポイントのオペレーティングシステム*のことです。
7. **[Show Preview to Continue (プレビューを表示して続行)]**をクリックします。
8. 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。

Tanium Module ServerからDirect Connectソリューションを削除する

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 Content (Taniumコンテンツ)]**セクションで**[Direct Connect]**行を選択します。
3. **[Uninstall Solution (ソリューションのアンインストール)]**をクリックします。**[Uninstall (アンインストール)]**をクリックしてプロセスを完了します。