ターゲットの要求

デバイス コネクタの要件

組み込みデバイス コネクタを介してデバイスを Cisco Intersight 仮想アプライアンス で要求できます。ターゲットを要求する前に、デバイスコネクタの要件が満たされていることを確認します。次の表に、Intersight 仮想アプライアンスのソフトウェア互換性とサポートされているデバイス コネクタを示します。

表 *1*: デバイス コネクタの要件

コンポーネント	接続済み仮想アプライアンスの最小ソフトウェア バージョン	プライベート仮想アプライアンスの最小ソフトウェア バージョン	サポートされているデバイスコネクタのバージョン	サポートされているデバイスコネクタを含む最小サポートバージョン
Cisco UCS Manager	3.2(1)	4.0(2a)	1.0.9-2290	4.0(2a)
Cisco IMC ソフトウェア	M5 サーバの場合：3.1(3a) M4 サーバの場合：3.0(4)	4.0(2d)	1.0.9-335	4.0(2d)
HyperFlex Connect およびデータ プラットフォーム	2.6	3.5(2a)	1.0.9-1335	3.5(2a)
Cisco UCS Director	6.7.2.0	6.7.2.0	1.0.9: 911	6.7.2.0

デバイス コネクタのアップグレード

エンドポイント上のデバイス コネクタのバージョンに互換性がない場合は、次の方法でアップグレードできます。

- サポートされているデバイス コネクタが搭載されているバージョンにファームウェアの完全アップグレードを実行します。このプロセスには、構成設定の更新が含まれていることがあります。
- デバイス コネクタを手動でアップグレードします。このオプションは、Cisco UCS Manager のみでサポートされています。詳細については、「デバイス コネクタの手動アップグレード（Cisco UCS ファブリック インターコネクトにのみ適用）」を参照してください。
- Cisco Intersight 仮想アプライアンス クラウドからのデバイス コネクタのアップグレードをサポートしています。ターゲットの要求プロセスで、エンドポイントのデバイスコネクタのバージョンに互換性がないことが検出されると、Intersight Cloud からのデバイスコネクタのアップグレードがトリガーされます。このアップグレードを容易にするには、ポート 80 をアプライアンスとエンドポイントターゲット間で開く必要があります。ポート 80 で実行されている HTTPS プロキシは、ファイアウォールの設定でポート 80 を介して通信できる必要があります。

  Intersight クラウドからのデバイス コネクタのアップグレードはオプションです。クラウドからのアップグレード時に、アプライアンスからの一部のターゲット データ（サーバ インベントリ）が施設から離れます。このオプションを選択すると、次のデータが施設から離れます。

  - エンドポイント ターゲット タイプ：Cisco UCS ファブリック インターコネクト、Integrated Management Controller、Cisco HyperFlex System、Cisco UCS Director
  - エンドポイントのファームウェア バージョン
  - エンドポイント ターゲットのシリアル番号
  - エンドポイントターゲットの IP アドレス
  - エンドポイントターゲットのホスト名
  - エンドポイント デバイス コネクタのバージョンと公開キー

注目 ターゲット コネクタがアプライアンスをサポートしていない古いバージョンであり、初期セットアップ時にデータ収集オプションを無効にした場合は、デバイスの要求が失敗することがあります。1 回限りのアップグレードが機能するように施設から離れる必要があるエンドポイントの詳細によってこの障害が引き起こされます。ターゲットの要求が失敗しないようにするには、[データ 収集の有効化（Enable Data Collection）] オプションを一時的に選択するか、または前述の他の方法でデバイス コネクタをアップグレードします。

デバイス コネクタの手動アップグレード（Cisco UCS ファブリック インターコネクトにのみ適用）

ターゲットコネクタの自動アップグレードの一環としてデバイスデータを共有しない場合は、Cisco UCS ファブリック インターコネクトのデバイス コネクタを手動でアップグレードすることができます。デバイス コネクタをアップグレードするには、次の手順を実行します。

```
Log in to your UCS Fabric Interconnect as an admin user and run the following command:
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# copy scp://username@10.100.100.100/filepath/filename.bin workspace:/
UCS-A(local-mgmt)# update-device-connector workspace:/filename.bin
Update Started
Updating Device Connector on local Fabric interconnect
Successfully updated device connector on local Fabric interconnect
UCS-A(local-mgmt)#
```

Intersight 仮想アプライアンスから収集されたデータ

Cisco Intersight 仮装アプライアンスは接続モードで動作し、ホストされている Intersight サービスへの接続が必要です。Intersight にアプライアンスを登録し、UCS または HyperFlex のインフラストラクチャを管理する必要があります。

追加情報の収集を許可するオプションを有効にすると、**収集された最小データ**の表に一覧表示されているものを超えて、Intersight は管理対象システムに関するその他の詳細情報を収集することができます。データ収集オプションが有効になっている場合、Cisco は、診断および予防的なトラブルシューティングの目的で、より多くのデータを収集する権利を保有します。

次の表に、Intersight で収集されたデータの詳細を示します。

表 *2*：収集された最小データ

コンポーネント	収集したデータの詳細
Intersight 仮想アプライアンスから	• アプライアンス ID（シリアル番号） • アプライアンスの IP アドレス • アプライアンスのホスト名 • アプライアンス上のデバイス コネクタのバージョンと公開キー
アプライアンス ソフトウェアの自動アップグレード	ソフトウェア コンポーネントまたはアプライアンス上で実行しているサービスのバージョン

コンポーネント	収集したデータの詳細
アプライアンスの健全性	• CPU 使用率 • メモリ使用率 • ディスク使用量 • サービスの統計情報
ライセンス	サーバ カウント
エンドポイントターゲットに関する情報	• シリアル番号と PID（接続されている TAC に対応するため） • UCS ドメイン ID • プラットフォームタイプ

表 *3:* ワンタイム デバイス コネクタのアップグレード中に収集されたデータ

コンポーネント	収集したデータの詳細
エンドポイント ターゲットから（1 回限りのデバイス コネクタのアップグレードを使用する場合のみ）	• エンドポイント ターゲット タイプ：Cisco UCS ファブリック インターコネクト、Integrated Management Controller、Cisco HyperFlex System • エンドポイントのファームウェア バージョン • エンドポイント ターゲットのシリアル番号 • エンドポイント ターゲットの IP アドレス • エンドポイント ターゲットのホスト名 • エンドポイント デバイス コネクタのバージョンと公開キー

テクニカル サポート診断ファイルの収集 (TAC ケースを開く)

Cisco TAC でケースをオープンすると、Intersight はテクニカル サポートの診断ファイルを収集して、オープン サポート ケースを支援します。収集されたデータには、ハードウェア テレメトリ、システム設定、および TAC ケースのアクティブなトラブルシューティングに役立つその他の詳細情報が含まれることがあります。指定したデータ収集オプションに関係なく、テクニカル サポートの収集が実行されます。ただし、この情報は任意で収集されるわけではありま

せんが、システムに対してケースをオープンする場合に限り、システム サポートの支援が必要になります。

Intersight 仮想アプライアンスでのターゲットの要求

アカウント管理者の権限を持つユーザとしてアプライアンスにログインします。Cisco Intersight 仮想アプライアンスでターゲットを要求するには、次の手順を使用します。

始める前に

- Cisco Intersight 仮想アプライアンス OVA インストールを完了し、アプライアンスをセットアップしたことを確認します。
- 要求するターゲット上に管理者権限があるアカウントがあります。
- 1 つまたは複数のターゲットを一括して要求できます。

ステップ 1 **[管理（Admin）]** > **[ターゲット（Targets）]** > **[新しいターゲットの要求（Claim a New Target）]** に移動

ウィザードを使用して設定を行うか、ファイルを使用して設定を行うことができます。

ステップ 2 ウィザードを使用して設定を行うには、**[ウィザードを使用して設定する（Use Wizard to Set the Configuration）]** タブを選択し、**[スタート（Start）]** をクリックします。

a) **[請求可能（Available for Claiming）]** を選択します。
b) ターゲット タイプを選択します。
c) 要求するターゲットの IP/ホスト名、ターゲットのユーザー名、およびユーザのパスワードを入力します。このユーザには管理権限が必要です。
d) **[要求 (Claim)]** をクリックして、ターゲットの要求プロセスを開始します。

ステップ 3 ファイルを使用して設定を行うには、**[ファイルを使用して設定する（Use a File to Set the Configuration）]** タブを選択し、**[スタート（Start）]** をクリックします。

a) **[参照（Browse）]** をクリックして、ターゲットの詳細を含む .csv ファイルを選択します。

ターゲットごとに、ターゲット タイプ、ホスト名または IP アドレス、ユーザ名、およびパスワード含む行を.csvファイルに追加します。IP 範囲を指定するには、CIDR 表記を使用します。これらの詳細情報を含む行を .csv ファイルに追加できます。次の例は、ターゲットの詳細を .csv ファイルに追加するための形式を示しています。

```
UCSFI,10.1.1.3,user-1,password1
IMC,10.1.1.5/26,user-2,password2
HX,10.1.2.1/30,user-3,password3
UCSD,1.1.1.1,user-4,password4
```

b) **[次へ（Next）]** をクリックします。
c) [概要（Summary）] ページで詳細を確認し、**[要求（Claim）]**をクリックします。

重要 ターゲットの要求プロセスには数分かかる場合があります。必要に応じて、デバイス コネクタがこのプロセスの一環として自動的にアップグレードされます。

[ターゲット（Targets）] > **[テーブル ビュー（Table view）]** からターゲットを選択し、**[削除（Delete）]**（ごみ箱アイコン）をクリックして、ターゲットの要求を解除できます。ターゲットを要求する前述の手順を使用すると、必要に応じてターゲットを後で再要求することができます。

ターゲット証明書の更新

エンドポイントのターゲット証明書の有効期限が切れている場合、[ターゲットテーブルビュー（Target Table View）] ページにステータスが **[未接続（Not Connected）]** と表示され、このエンドポイントのバッジにターゲット証明書の有効期限が切れたことが示されます。

ステップ 1 **[管理（Admin）]** > **[ターゲット（Targets）]** の順に移動し、**[未接続（Not Connected）]** ステータスのターゲットを見つけます。

ステップ 2 対象の証明書の有効期限が切れているかどうかを確認するには、バッジにカーソルを合わせます。

ステップ 3 このターゲットの **[アクション（Actions）]** メニューをクリックし、**[証明書の更新（Renew Certificate）]** を選択します。。

（注） **[証明書の更新（Renew Certificate）]** オプションは、選択したエンドポイントの証明書を更新する必要がある場合にのみ使用できます。

ステップ 4 **[証明書の更新（Renew Certificate）]** ポップアップ ウィンドウで、ユーザ名とパスワードを入力し、**[更新（Renew）]** をクリックします。

証明書の更新プロセスが完了すると、エンドポイントのステータスは **[接続済み（Connected）]** と表示されます。