マザーボード交換後のIntersightでのスタンドアロンCシリーズサーバの設定と要求

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[背景説明](#)
[問題：新しいRMAサーバがIntersightで要求されず、元の障害のあるサーバが要求される](#)
[解決方法](#)
[デバイス要求の問題の基本的な検証](#)
[Cisco Intersightの一般的なネットワーク接続要件](#)
[関連情報](#)

概要

このドキュメントでは、マザーボード交換後にCisco Intersightでスタンドアロンシリーズサーバを設定および要求する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco インテグレーテッド マネージメント コントローラ（CIMC）
- Cisco Intersight
- Cisco Cシリーズサーバ

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco C240-M5 4.1(3d)
- Cisco Intersight Software as a Service(SaaS)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

関連製品

このドキュメントは、次のバージョンのハードウェアとソフトウェアにも使用できます。

- CシリーズM4 3.0(4)以降
- CシリーズM5 3.1以降
- CシリーズM6 4.2以降
- SシリーズM5 4.0(4e)以降

注：サポートされているハードウェアとソフトウェアの一覧については、次のリンクを参照してください。IntersightがサポートするPIDおよびIntersightがサポートするシステム。

背景説明

- このドキュメントの最も一般的な使用例は、CシリーズがCisco Intersightに請求され、マザーボードがReturn Material Authorization(RMA)に交換された場合です。 RMAが発生するたびに、元のサーバの要求を解除し、新しいサーバをCisco Intersightで要求する必要があります。
- このドキュメントでは、マザーボードのRMAの前に元のCシリーズサーバが正常に請求され、請求プロセスの失敗の原因となる設定やネットワークの問題がないことを前提としています。
- Cisco Intersight Portalまたはエンドポイント自体のDevice Connectorから直接ターゲットの要求を解除できます。Cisco Intersight Portalからターゲットの要求を解除することをお勧めします。
- ターゲットがIntersight PortalではなくDevice Connectorから直接要求されていない場合、Cisco Intersight内のターゲットは要求されていないものとして表示されます。エンドポイントは、Cisco Intersightから手動で要求を解除する必要もあります。
- 元のCシリーズサーバのステータスは、Cisco IntersightではNot Connectedと表示されている可能性があります。これは、マザーボードの交換が必要な理由によって異なります。

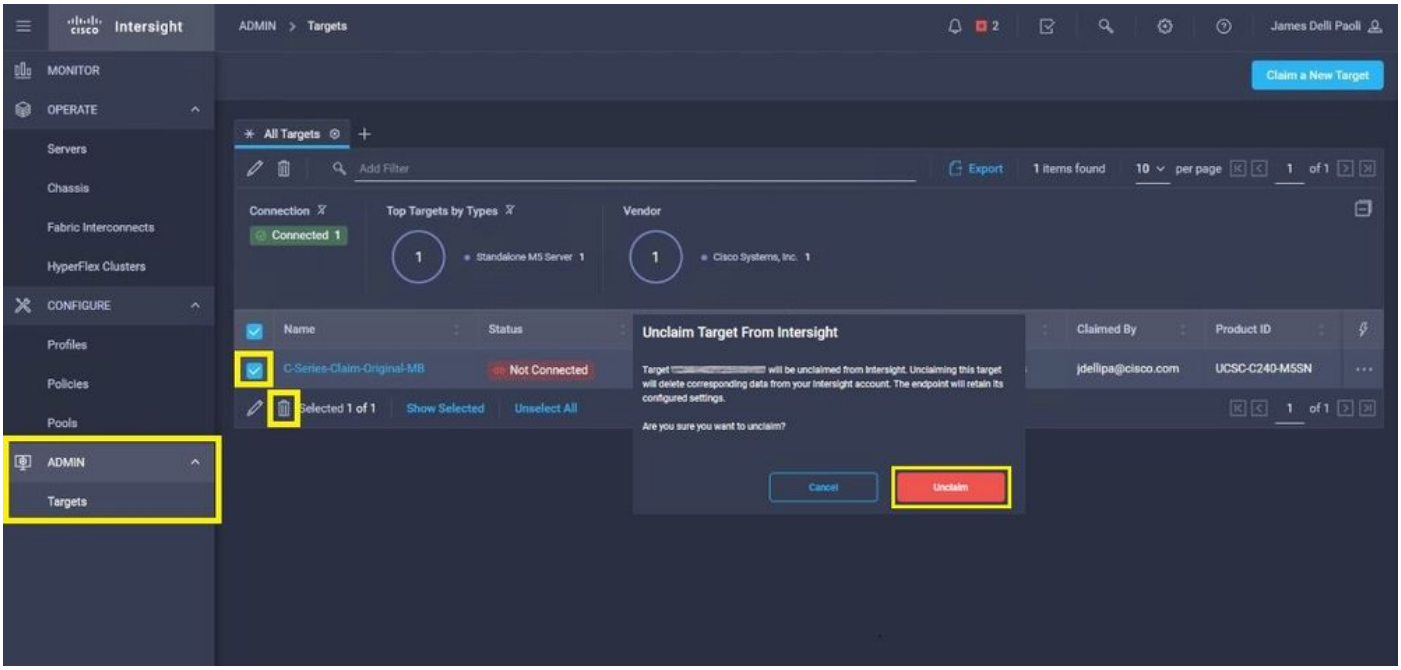
問題：新しいRMAサーバがIntersightで要求されず、元の障害のあるサーバが要求される

スタンドアロンCシリーズサーバがCisco Intersightで要求された場合、サーバのシリアル番号(SN)はCisco Intersightとペアになります。障害またはその他の理由により、請求されたサーバにマザーボードの交換が必要になった場合は、元のサーバを請求せずに、新しいサーバをCisco Intersightで請求する必要があります。CシリーズのSNはマザーボードのRMAで変更されます。

解決方法

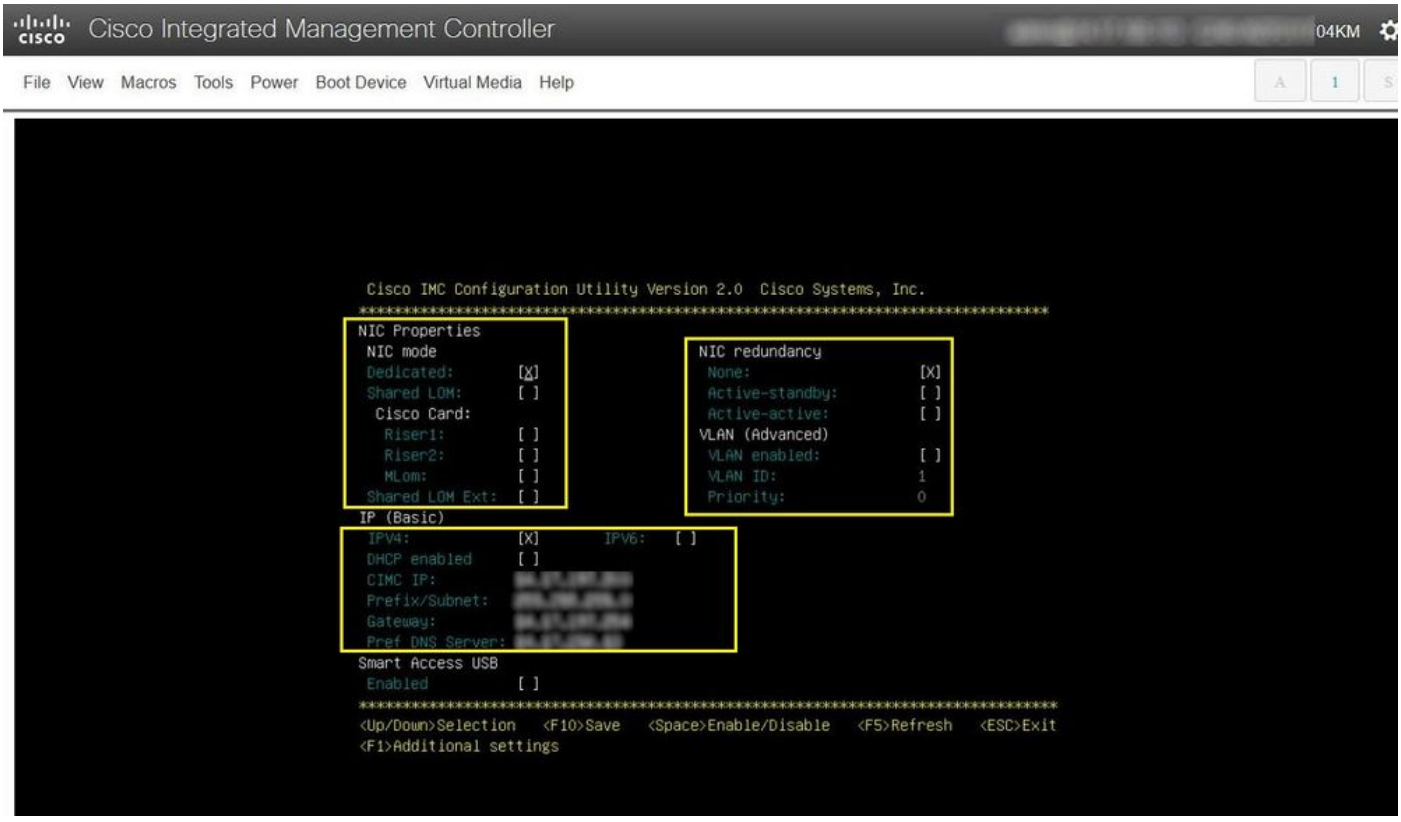
交換が必要なCシリーズサーバをCisco Intersightから取り外します。新しいサーバCIMCとデバイスコネクタを設定し、新しいサーバをCisco Intersightに要求します。

ステップ1:Cisco Intersightを起動し、 **Admin > Targets**. 置き換えるターゲットと請求しないターゲットのボックスを選択し、 **Trash Can Icon > Unclaim** 以下の図に、出力例を示します。



ステップ2：新しく交換したサーバにキーボードビデオモニタ(KVM)を接続します（CIMCがすでに設定されている場合は、このステップをスキップします）。 ブートアップ時のCiscoスプラッシュ画面で、 **F8** CIMCを設定します。適切な **Network Interface Card (NIC) Properties** を押してください **F10** から **Save.** 物理ケーブルをサーバおよび接続されているデバイスに接続します。 **NIC Properties** 管理に使用されます。

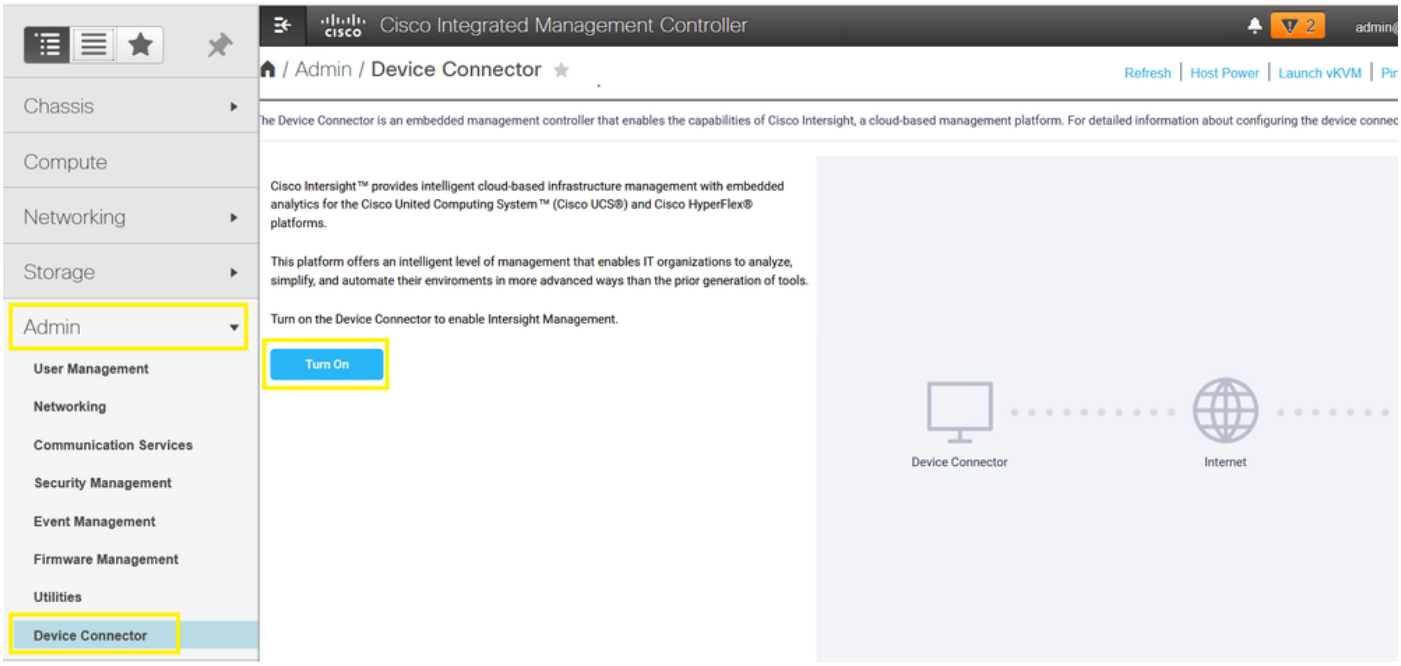
> **注**：手順2:C240-M5に直接接続されたKVMを使用したCIMCのローカルセットアップを示し、説明します。CIMCの初期セットアップは、DHCPを使用してリモートで行うこともできます。ご使用のサーバモデルに適したインストールガイドを参照し、最適な初期CIMCセットアップを選択してください。

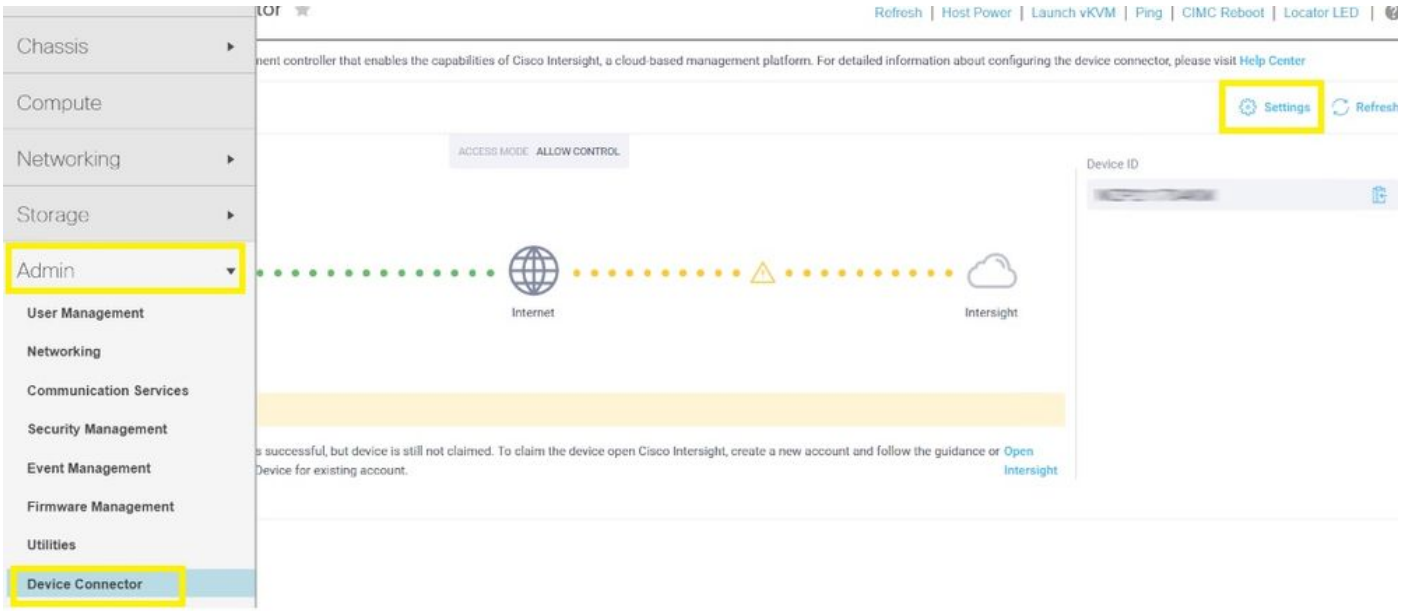


ステップ3:CIMCグラフィカルユーザインターフェイス(GUI)を起動し、 **Admin > Device Connector.** も

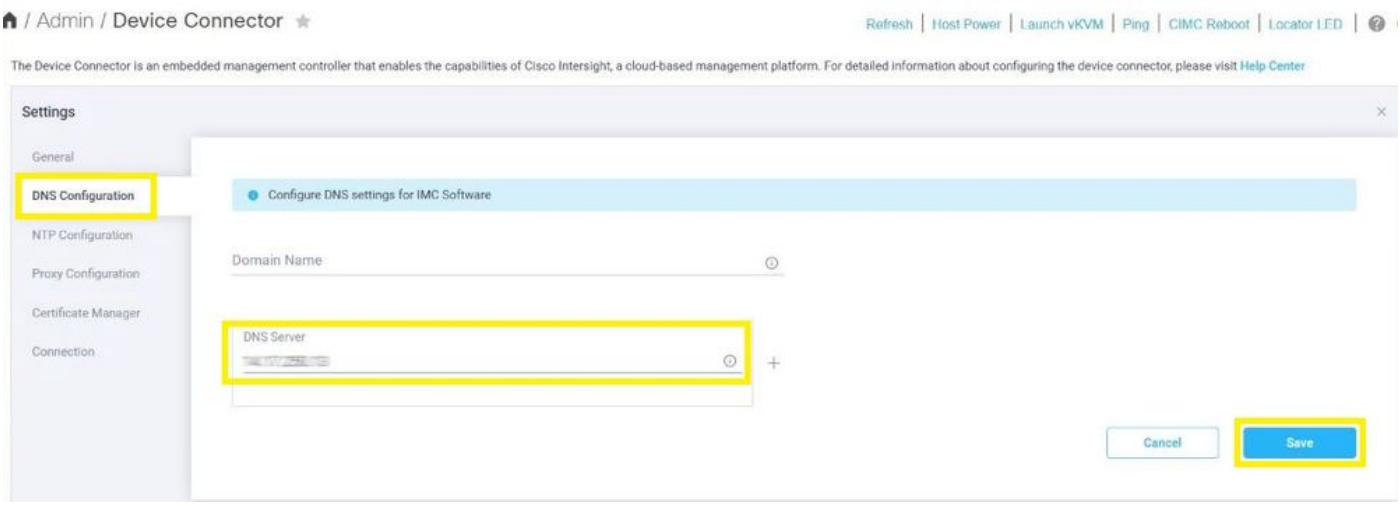
し **Device Connector** が無効な場合は、 **Turn On.** 有効になったら、次の項目を選択します。 **Settings.**

> **ヒント**：CIMC GUIで、 **Chassis > Summary** 比較して **Firmware Version** Cisco Intersightが要求する最小ファームウェア要件が満たされていることを確認します。特定のサーバモデルの最小要件を確認するには、次のリンクを使用します。Intersight Supported Systems。ファームウェアが要求される最小要件を満たしていない場合は、サーバでHost Upgrade Utility(HUU)を実行します。次を参照してください。Cisco Host Upgrade Utilityのプロセス』を参照してください。

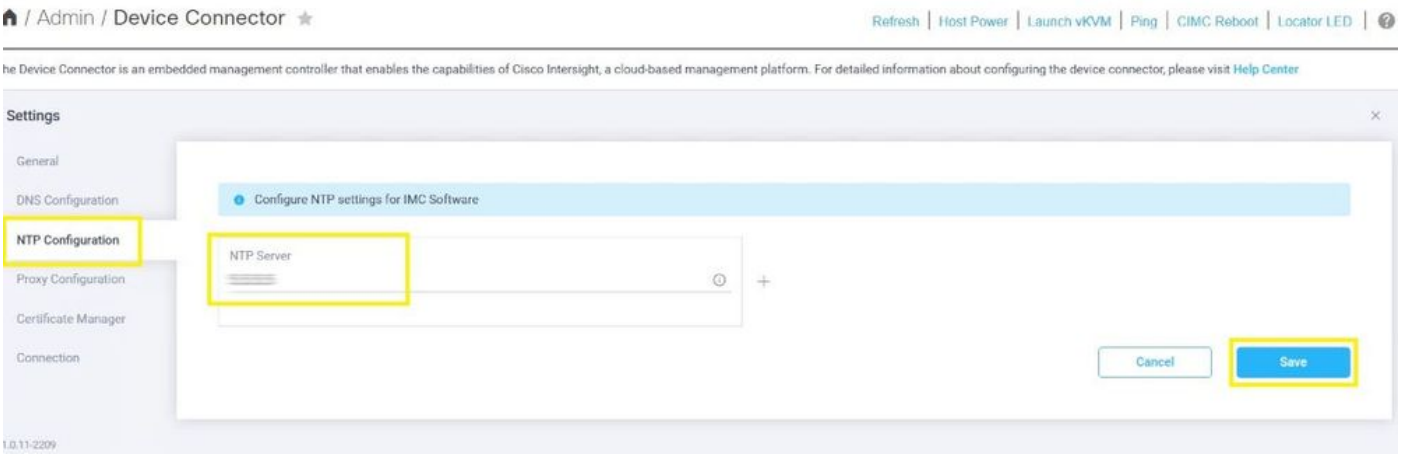




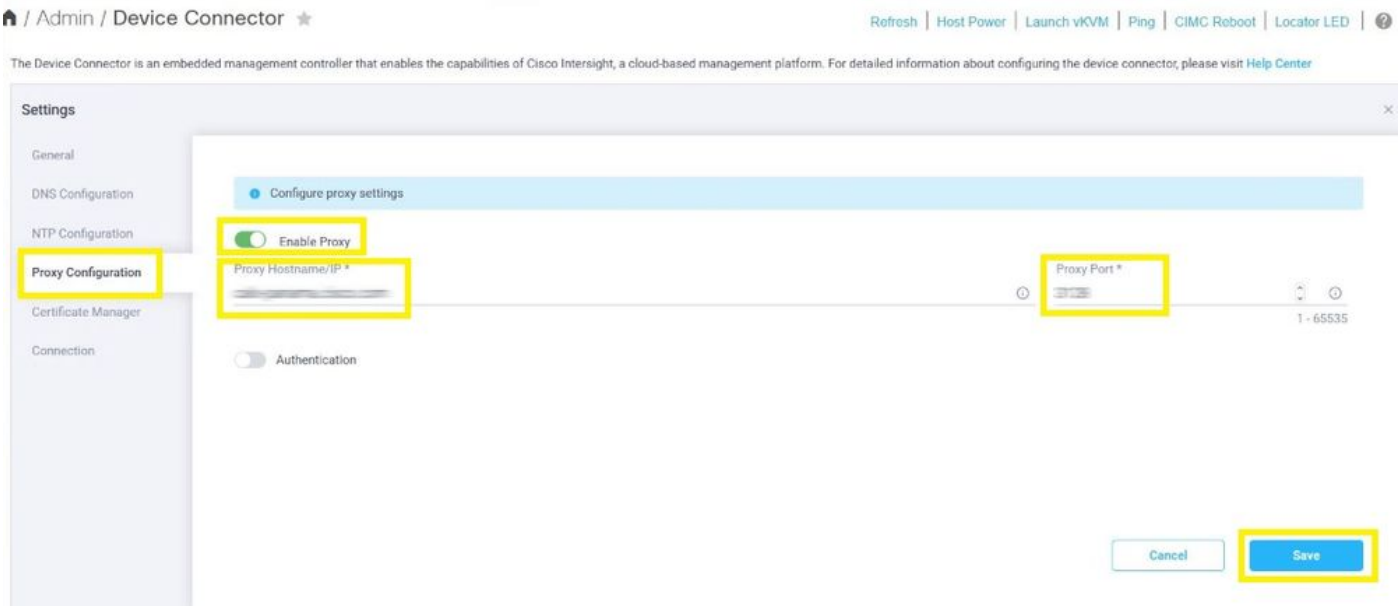
ステップ3.1.次に移動する **Admin > Device Connector > Settings > DNS Configuration** 適切な **DNS Server** 選択します **Save** 以下の図に、出力例を示します。



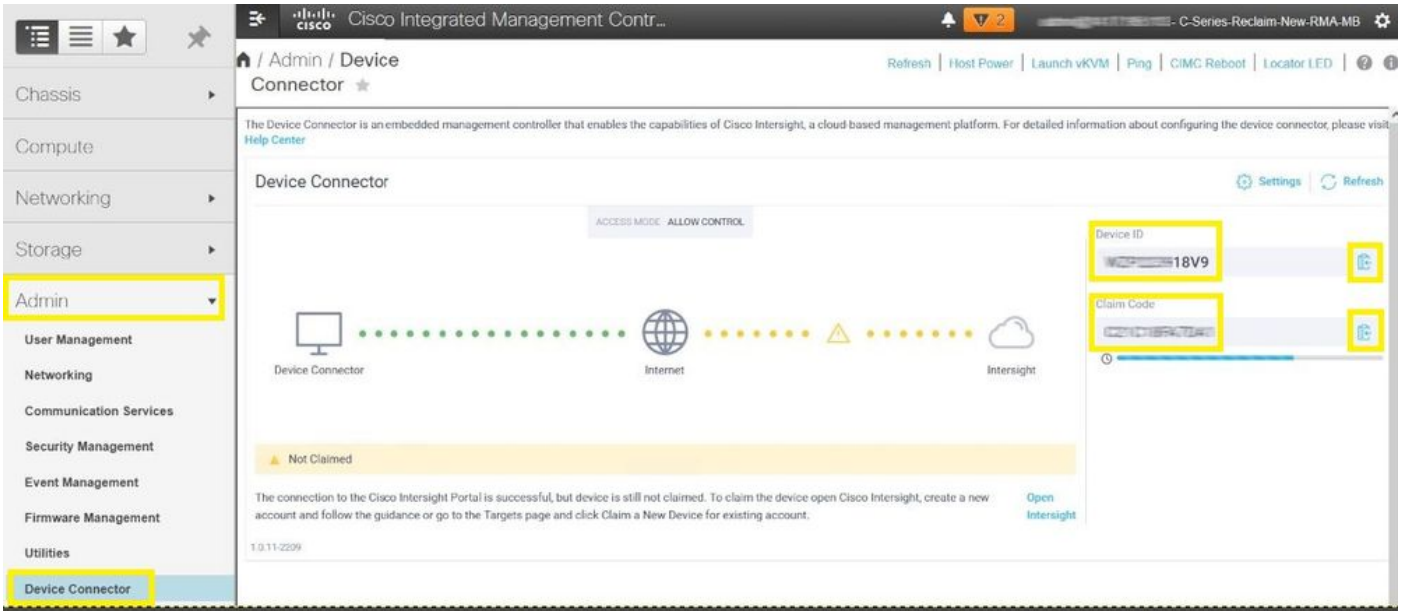
ステップ3.2.次のページに移動する **Admin > Device Connector > Settings > NTP Configuration.** Cisco IOSソフトウェアの **NTP Server** アドレスを指定し、 **Save** 以下の図に、出力例を示します。



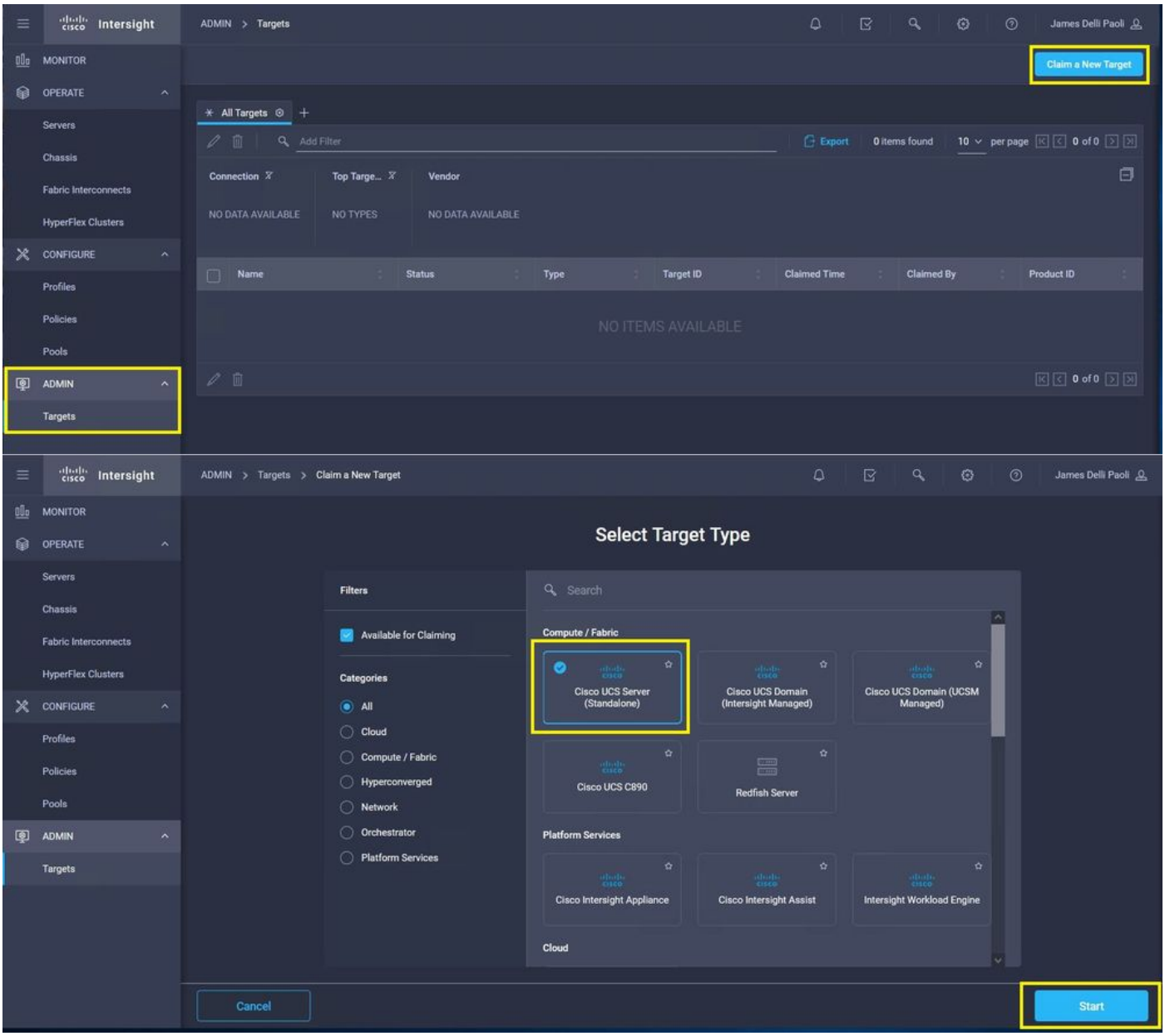
ステップ3.3:Cisco Intersightに到達するために必要に応じてプロキシを設定します。移動先 **Admin > Device Connector > Settings > Proxy Configuration > Enable Proxy.** Cisco IOSソフトウェアの **Proxy Hostname/IP** および **Proxy Port** 選択します **Save.**

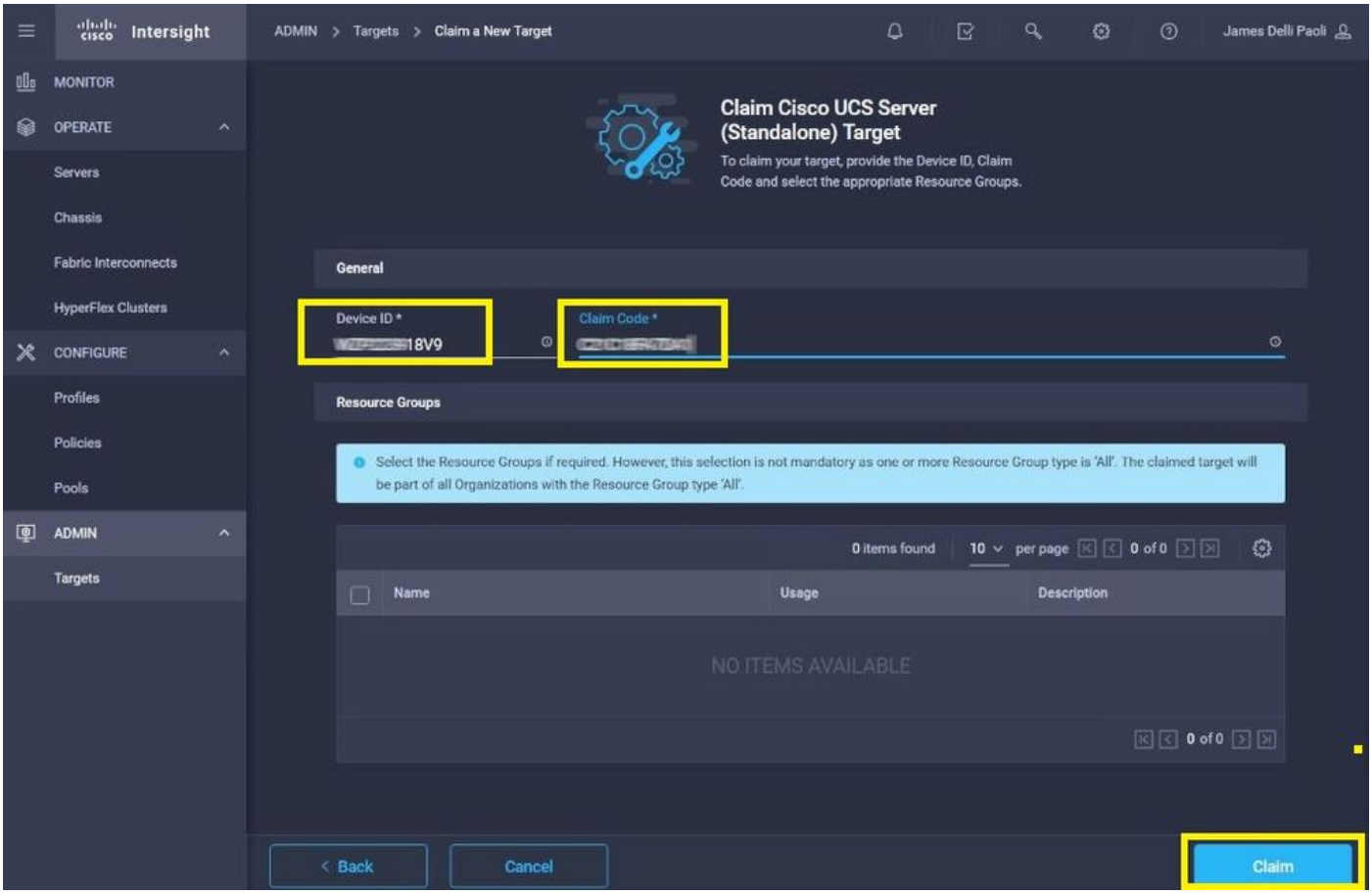


ステップ4：選択 **Admin > Device Connector** をコピーし、 **Device ID** と **Claim Code.** 後で使用するために、両方をメモ帳またはテキストファイルにコピーします。

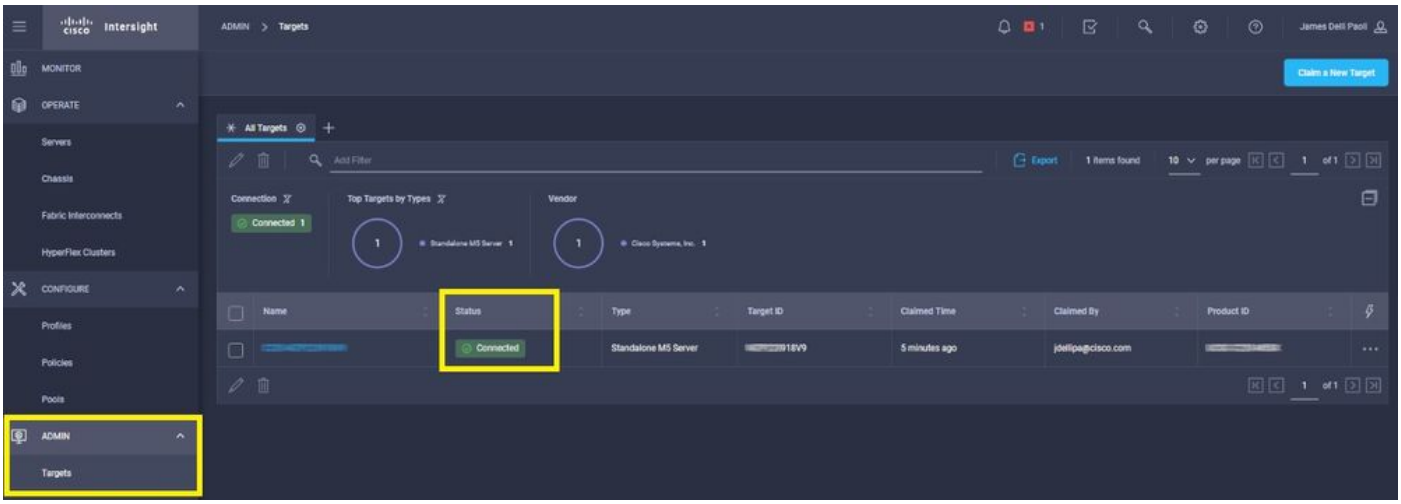


ステップ5:Cisco Intersightを起動し、 **Admin > Targets > Claim a New Target > Cisco UCS Server (Standalone) > Start.** 次を入力します。 **Device ID** と **Claim Code** CIMC GUIからコピーし、 **Claim.**





ステップ6：に移動します。 **Admin > Targets.** 成功した要求は、 **Status > Connected,** 以下の図に、出力例を示します。



デバイス要求の問題の基本的な検証

> **注**：エラー状態と修復の包括的なリストについては、「デバイスコネクタのエラー状態と修復手順」を参照してください。

デバイスコネクタの接続状態の説明	デバイスコネクタの接続状態の説明	可能な修復
請求	Cisco Intersightプラットフォームへの接続が成功し、接続が要求されました。	N/A
請求なし	Cisco Intersightプラットフォームへ	Cisco Intersightを通じて、要求

	の接続は成功しましたが、エンドポイントはまだ要求されていません。	ていない接続を要求できます。
管理上無効	Intersight Management/Device Connectorがエンドポイントで無効になっていることを示します。	エンドポイントでデバイスコネを有効にします。
DNSの設定ミス	CIMCでDNSが正しく設定されていないか、まったく設定されていません。	システムに設定されているDNムサーバのいずれにも到達できことを示します。DNSネームサーに有効なIPアドレスを入力しとを確認してください。
Intersight DNS解決エラー	DNSは設定されていますが、IntersightのDNS名を解決できません。	Intersightがメンテナンス中かどを確認するには、次のリンクをックします。Intersightステータ Intersightが動作している場合はIntersightサービスのDNS名が解されていないことを示している性があります。
UCS接続ネットワークエラー	無効なネットワーク構成を示します。	確認して確認します。MTUはエツーエンドで正しく、ポート443は許可され、ファイアウォーすべての物理および仮想IPを許、DNSとNTPはエンドポイント定されます。
証明書検証エラー	Cisco Intersightプラットフォームによって提示された証明書が無効であるため、エンドポイントはCisco Intersightプラットフォームへの接続の確立を拒否します。	期限切れまたは無効な証明書：NTPが正しく設定され、デバの時刻が協定世界時(UTC)と同ていることを確認します。DNしく設定されていることを確認す。透過Webプロキシが使用中合は、証明書が期限切れでないを確認します。 Webサーバから提示された証明がIntersightサービスのDNS名と致しません：DNSが正しく設定ていることを確認します。Webキシ管理者に連絡して、透過Wプロキシが正しく設定されているを確認します。具体的には、Wプロキシによって提示される証明名前が、Intersightサービス(svc.intersight.com)のDNS名とする必要があります。 信頼されていない認証局(CA)によて証明書が発行されました：DNS正しく設定されていることを確ます。Web管理者またはInfosec連絡して、透過Webプロキシが正く設定されていることを確認しださい。具体的には、Webプロによって提示される証明書の各IntersightサービスのDNS名とするする必要があります。

Cisco Intersightの一般的なネットワーク接続要件

- Intersightプラットフォームへのネットワーク接続は、エンドポイントのデバイスコネクタから確立されます
- 管理対象ターゲットとIntersightの間にファイアウォールが導入されているかどうか、または現在のファイアウォールのルールが変更されているかどうかを確認します。これにより、エンドポイントとCisco Intersight間のエンドツーエンド接続の問題が発生する可能性があります。ルールが変更された場合は、変更されたルールがファイアウォールを通過するトラフィックを許可していることを確認します。
- HTTPプロキシを使用して施設外にトラフィックをルーティングする場合、およびHTTPプロキシサーバの設定を変更した場合は、必ず変更が反映されるようにデバイスコネクタの設定を変更してください。IntersightはHTTPプロキシサーバを自動的には検出しないため、これが必要です。
- DNSを設定し、DNS名を解決します。デバイスコネクタは、DNSサーバにDNS要求を送信し、DNSレコードを解決できる必要があります。デバイスコネクタは、svc.intersight.comをIPアドレスに解決できる必要があります。
- NTPを設定し、デバイスの時刻がタイムサーバと正しく同期されていることを確認します。

注：Intersightの接続要件の包括的なリストについては、『Intersightネットワークの接続要件』を参照してください。

関連情報

- Cisco Intersight Getting Started Claim Targets
- Cisco Intersight SaaS対応システム
- Cisco Intersight SaaSでサポートされるPID
- Cisco Intersightネットワーク接続要件
- Cisco Intersightトレーニングビデオ
- Cisco Bug ID CSCvw76806：スタンドアロンCシリーズサーバのデバイスコネクタのバージョンが1.0.9未満の場合、Cisco Intersightでの要求が失敗する可能性があります。
- テクニカル サポートとドキュメント – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。