Konfiguration und Beantragung eines eigenständigen Servers der C-Serie in Intersight nach dem Austausch des Motherboards

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie in Cisco Intersight einen Standalone-Server der C-Serie konfigurieren und beanspruchen, nachdem die Hauptplatine ausgetauscht wurde.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Integrated Management Controller (CIMC)
- Cisco Interview
- Cisco Server der C-Serie

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Verwandte Produkte

Dieses Dokument kann auch mit folgenden Hardware- und Softwareversionen verwendet werden:

- C-Serie M4 3.0(4) und höher
- C-Serie M5 3.1 und höher
- C-Serie M6 4.2 und höher
- S-Serie M5 4.0(4e) und höher

> **Anmerkung:** Eine umfassende Liste der unterstützten Hardware und Software finden Sie unter den folgenden Links: Von Intersight unterstützte PIDs und von Intersight unterstützte Systeme.

Hintergrundinformationen

- Der häufigste Anwendungsfall für dieses Dokument ist, wenn eine C-Serie bei Cisco Intersight angemeldet wurde und das Motherboard durch eine Retourengenehmigung (Return Material Authorization, RMA) ersetzt wird. Bei jeder RMA muss der ursprüngliche Server zurückgezogen werden, und der neue Server muss in Cisco Intersight angemeldet werden.
- In diesem Dokument wird davon ausgegangen, dass der ursprüngliche Server der C-Serie vor der RMA für das Motherboard erfolgreich angefordert wurde und dass es keine Konfigurations- oder Netzwerkprobleme gibt, die zu einem fehlgeschlagenen Anfrageprozess führen würden.
- Sie können Ziele direkt über das Cisco Intersight-Portal oder den Device Connector des Endpunkts selbst freigeben. Es wird empfohlen, Ziele über das Cisco Intersight-Portal freizugeben.
- Wenn ein Ziel direkt aus dem Device Connector und nicht aus dem Intersight-Portal entfernt wird, wird es in Cisco Intersight als nicht beansprucht angezeigt. Außerdem muss das Endgerät manuell aus Cisco Intersight entfernt werden.
- Der ursprüngliche Server der C-Serie zeigt in Cisco Intersight wahrscheinlich den Status Not Connected (Nicht verbunden) an. Dies kann je nach dem Grund, warum das Motherboard ausgetauscht werden muss, variieren.

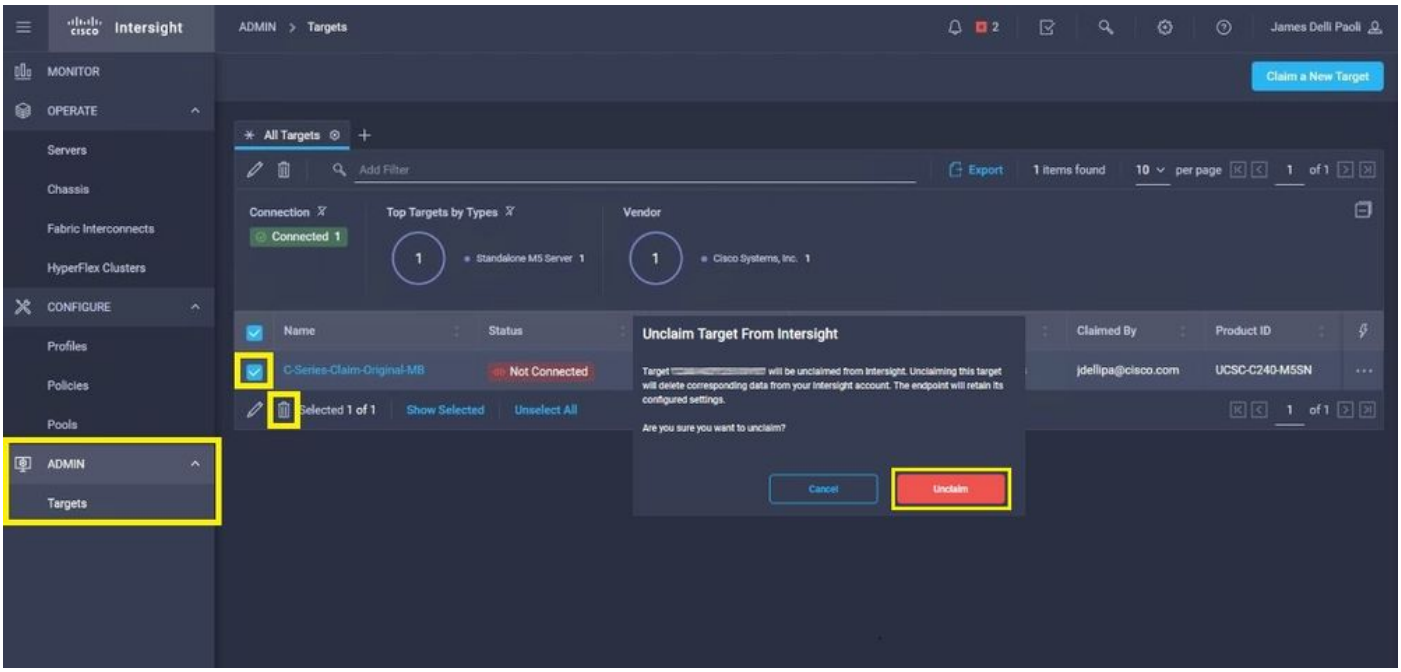
Problem: Neuer RMA-Server wird in Intersight nicht beansprucht, und der ursprüngliche ausgefallene Server wird beansprucht

Wurde in Cisco Intersight ein Standalone-Server der C-Serie angefordert, wird die Seriennummer (SN) des Servers mit Cisco Intersight gepaart. Wenn der beanspruchte Server aufgrund eines Fehlers oder aus einem anderen Grund einen Austausch der Hauptplatine erfordert, muss der Anspruch für den ursprünglichen Server aufgehoben und der neue Server in Cisco Intersight eingefordert werden. Die SN der C-Serie ändert sich mit der RMA des Motherboards.

Lösung

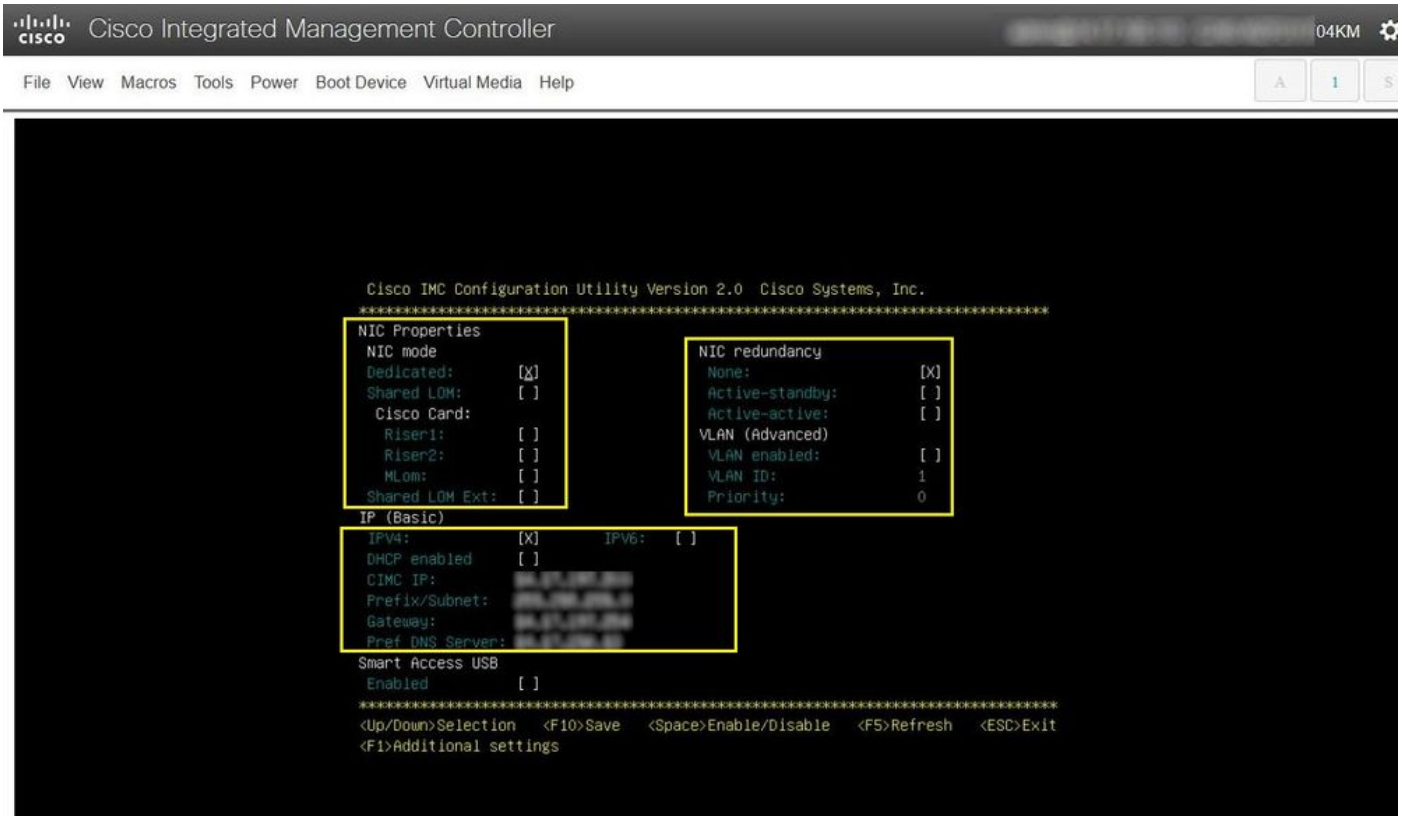
Heben Sie die Rücknahme des Servers der C-Serie von Cisco Intersight auf, der ersetzt werden muss. Konfigurieren Sie die neuen Server CIMC und Device Connector, und fordern Sie den neuen Server bei Cisco Intersight an.

Schritt 1: Starten Sie Cisco Intersight, und klicken Sie auf **Admin > Targets**. Wählen Sie das Kästchen für die Zielgeräte aus, die ersetzt und nicht beansprucht werden sollen, und klicken Sie auf **Trash Can Icon > Unclaim** wie in diesem Bild dargestellt.



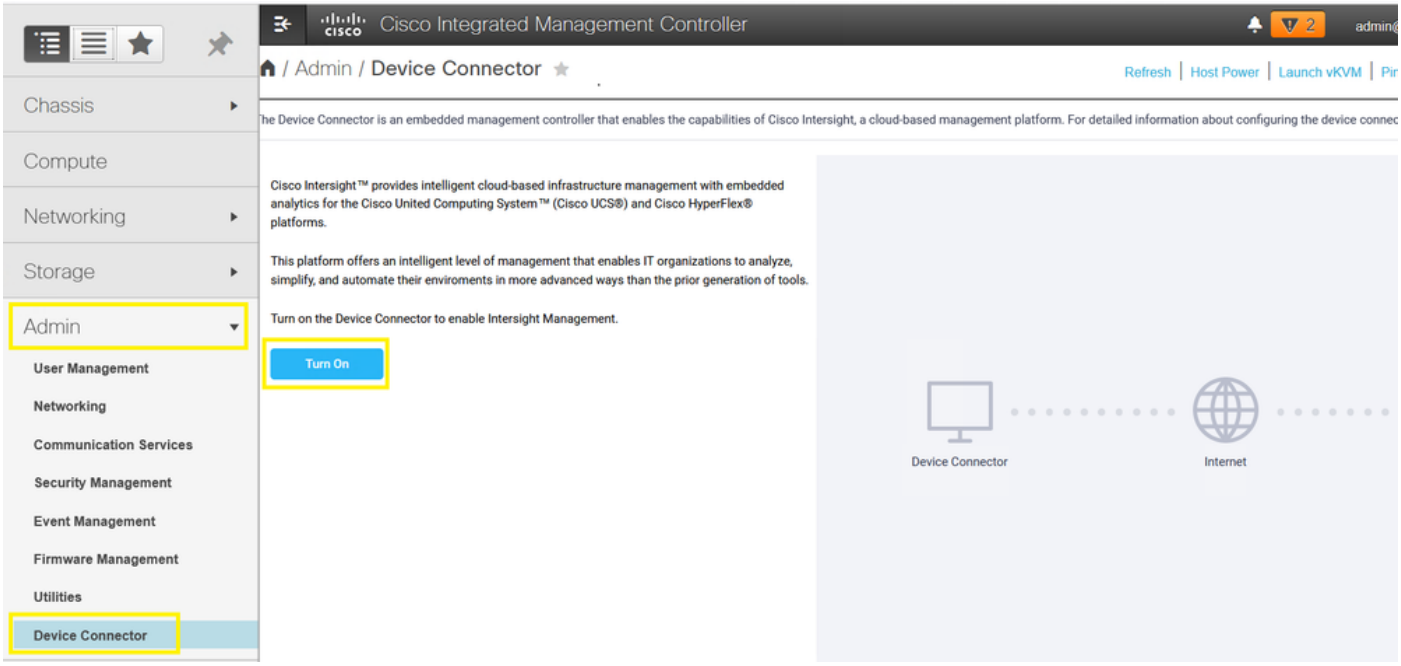
Schritt 2: Schließen Sie einen Keyboard Video Monitor (KVM) an den neu ausgetauschten Server an (überspringen Sie diesen Schritt, wenn CIMC bereits konfiguriert wurde). Wählen Sie im Cisco Begrüßungsbildschirm beim Start **F8** um CIMC zu konfigurieren. Konfigurieren Sie die entsprechenden **Network Interface Card (NIC) Properties** für Ihre Umgebung und drücken Sie **F10** zu **Save.** Verlegen Sie physische Kabel zum Server und zum angeschlossenen Gerät auf Basis des **NIC Properties** zur Verwaltung verwendet.

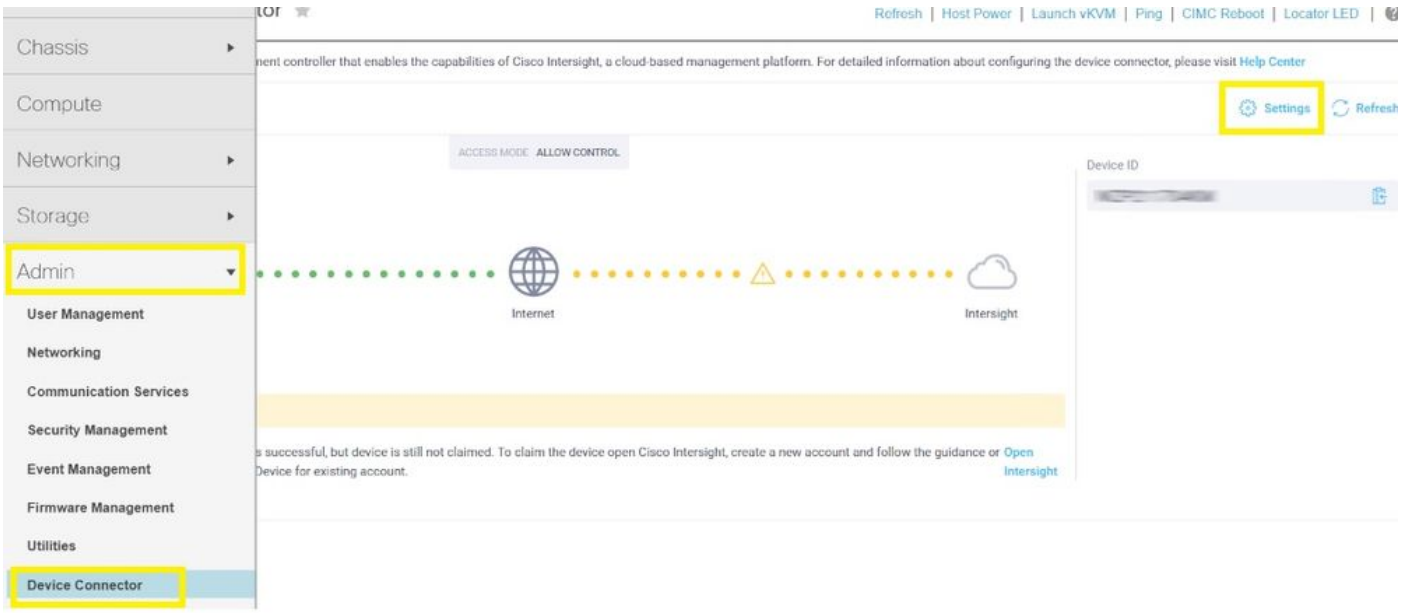
> **Anmerkung:** Schritt 2. zeigt und beschreibt eine lokale Einrichtung des CIMC mit einem angeschlossenen KVM direkt an einen C240-M5. Die erste CIMC-Einrichtung kann auch remote über DHCP durchgeführt werden. Bitte beachten Sie die Installationsanleitung für Ihr Servermodell, und wählen Sie die für Sie optimale CIMC-Ersteinrichtung aus.



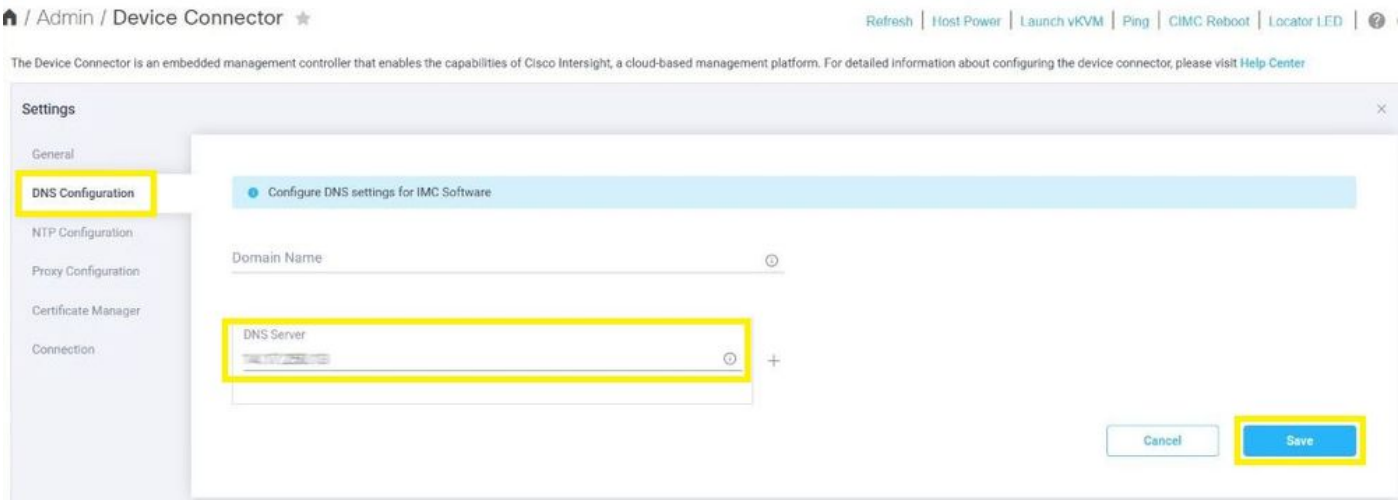
Schritt 3: Starten Sie die grafische Benutzeroberfläche (GUI) von CIMC, und navigieren Sie zur **Admin > Device Connector.** Wenn **Device Connector** ist deaktiviert. Wählen Sie **Turn On.** Nach der Aktivierung wählen Sie **Settings.**

> **Tipp:** Navigieren Sie in der CIMC-GUI zu **Chassis > Summary** und vergleichen Sie **Firmware Version** um zu bestätigen, dass die Firmware-Mindestanforderungen erfüllt sind und von Cisco Intersight angefordert werden. Verwenden Sie diesen Link, um die Mindestanforderungen für Ihr spezifisches Servermodell zu überprüfen: Intersight Supported Systems (Intersight-unterstützte Systeme). Wenn die Firmware nicht die erforderlichen Mindestanforderungen erfüllt, führen Sie ein Host Upgrade Utility (HUU) auf dem Server aus. Weitere Informationen finden Sie hier: Cisco Host Upgrade Utility-Prozess.

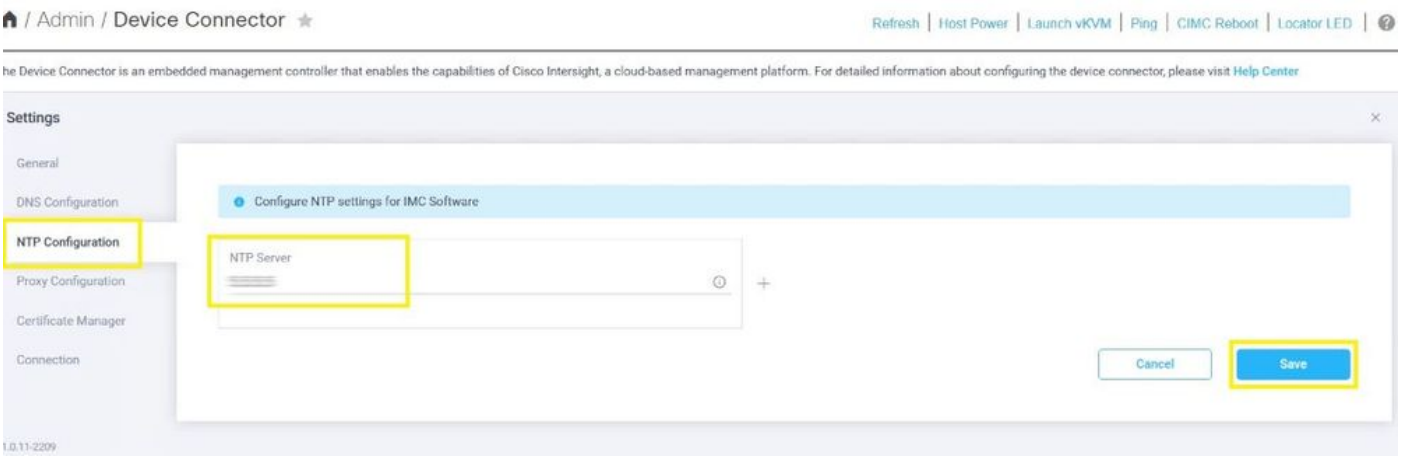




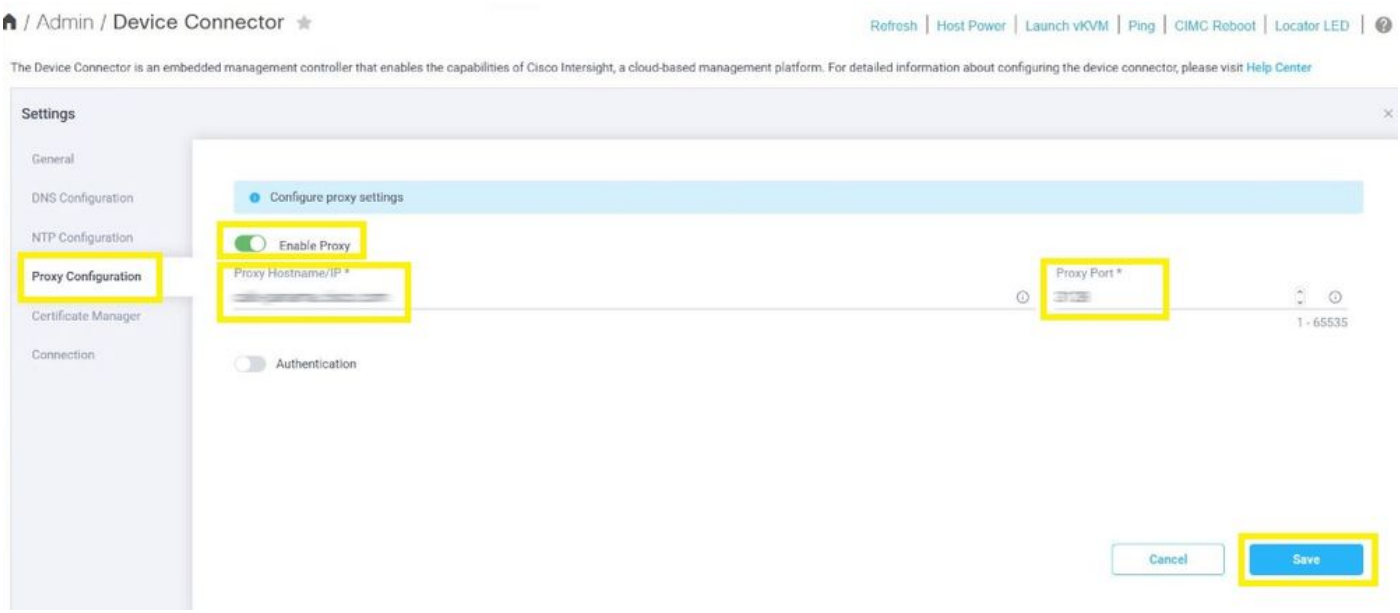
Schritt 3.1. Navigieren Sie zu **Admin > Device Connector > Settings > DNS Configuration** und die entsprechenden **DNS Server** und **Save** wie in diesem Bild dargestellt.



Schritt 3.2. Navigieren Sie zu **Admin > Device Connector > Settings > NTP Configuration.** Konfigurieren Sie **NTP Server** für die jeweilige Umgebung zu adressieren und **Save** wie in diesem Bild dargestellt.

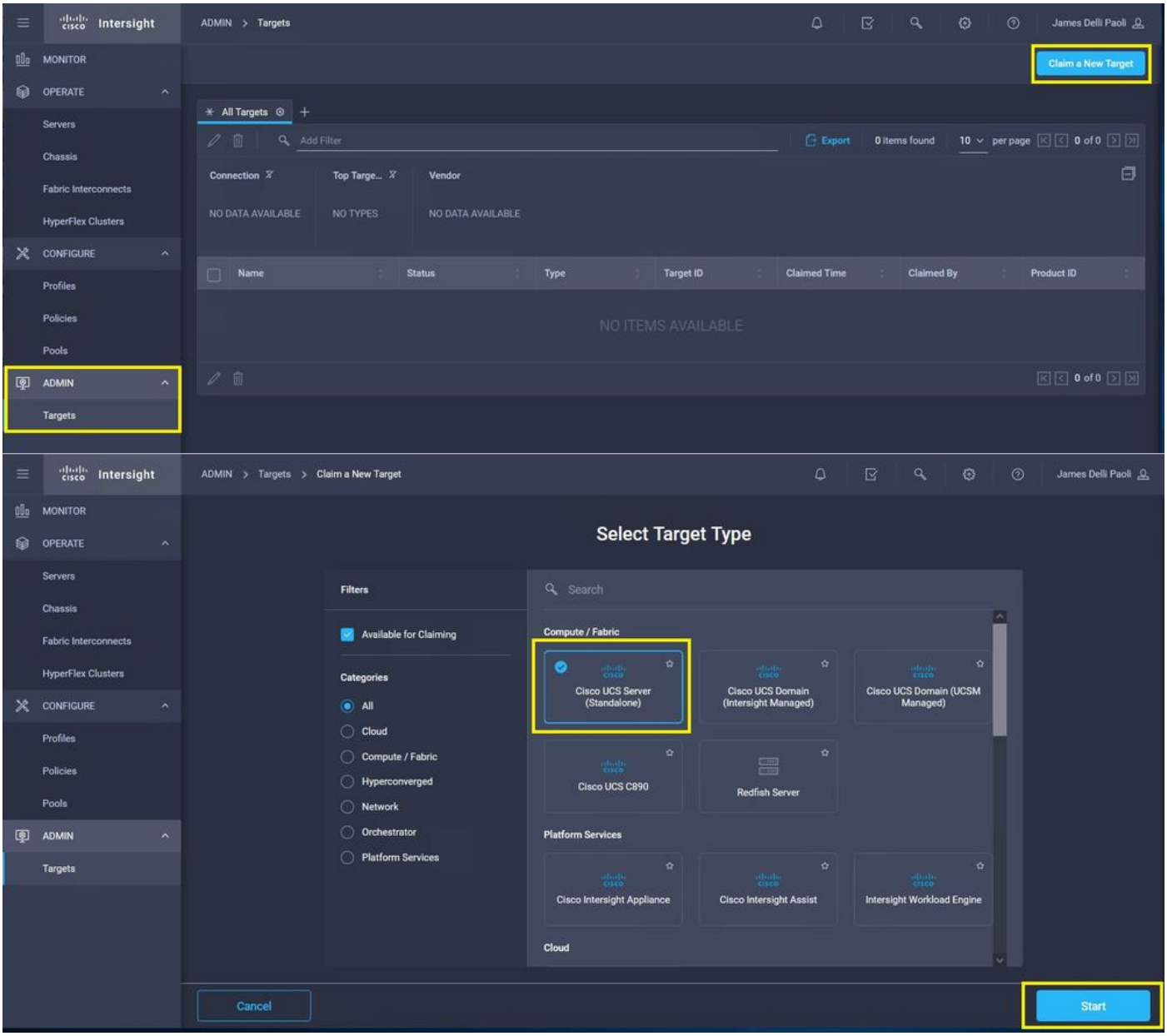


Schritt 3.3. Konfigurieren Sie bei Bedarf optional einen Proxy, um Cisco Intersight zu erreichen. Navigieren Sie zu **Admin > Device Connector > Settings > Proxy Configuration > Enable Proxy.** Konfigurieren Sie **Proxy Hostname/IP** und **Proxy Port** und **Save.**

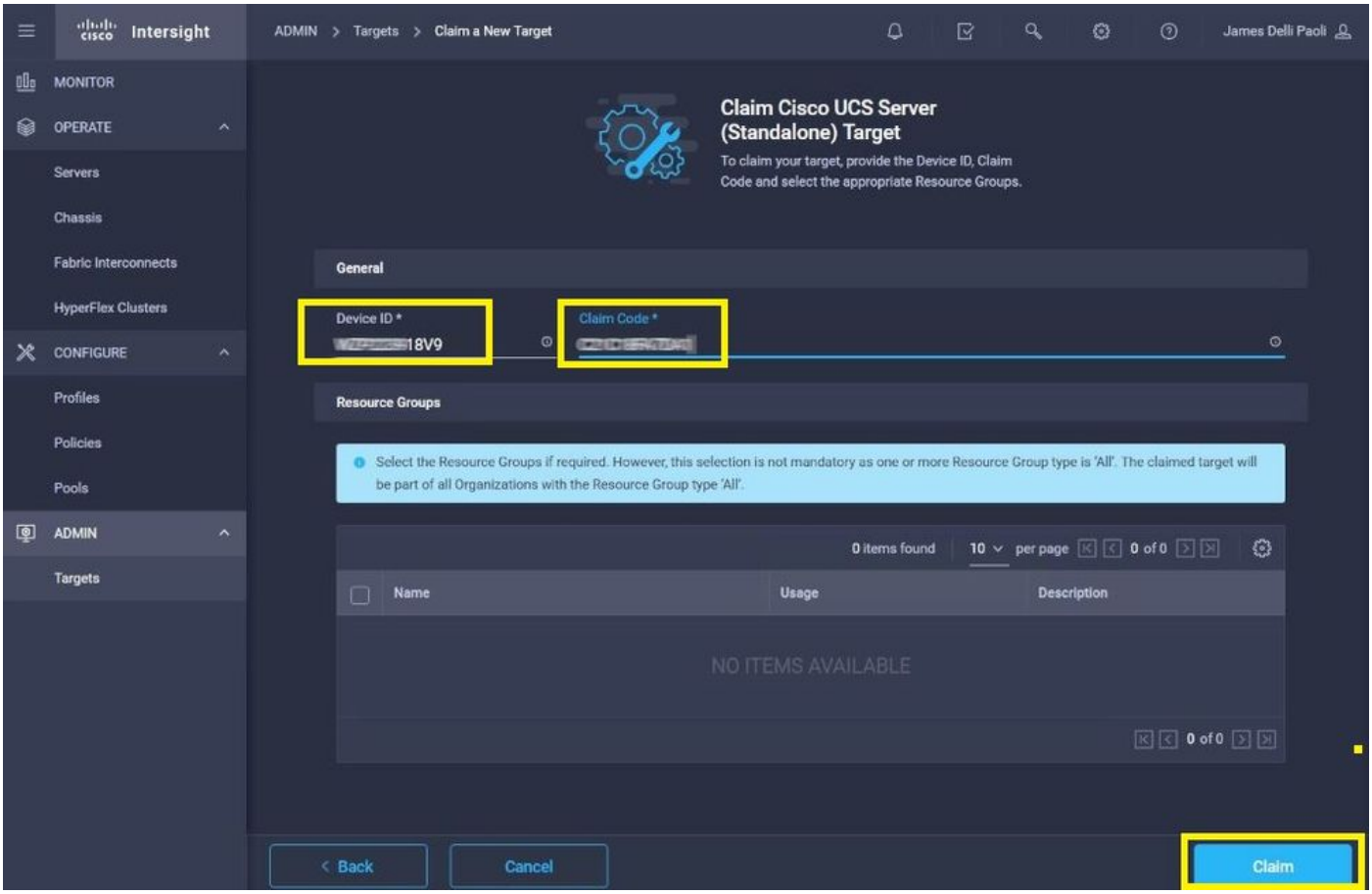


Schritt 4: Wählen **Admin > Device Connector** und kopieren Sie **Device ID** und **Claim Code.** Kopieren Sie beide in einen Notizblock oder eine Textdatei zur späteren Verwendung.

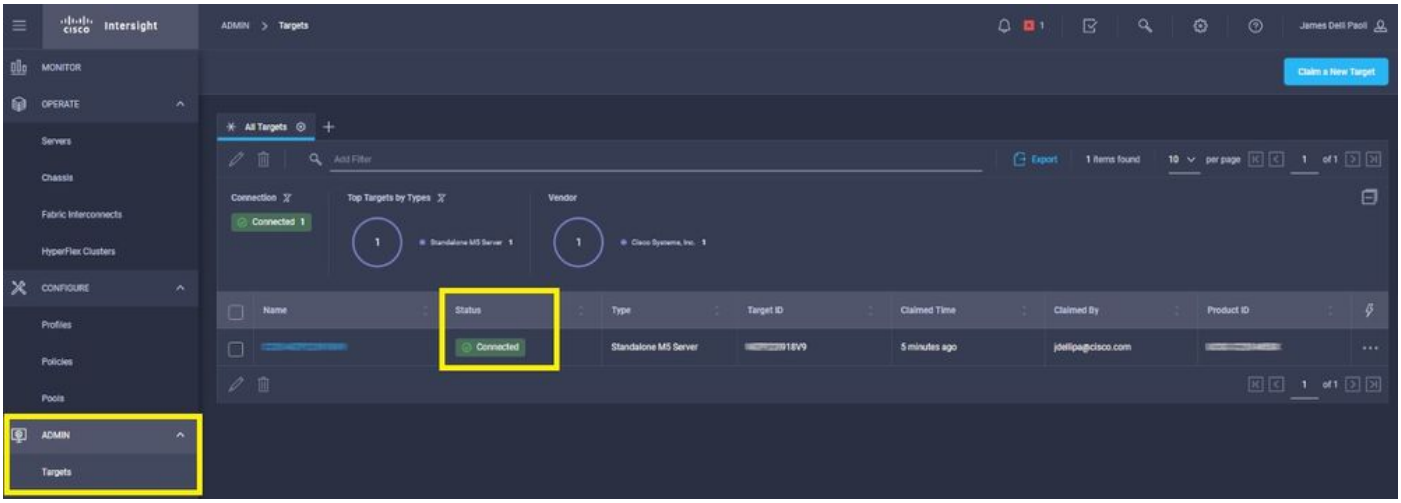
Schritt 5: Starten Sie Cisco Intersight, und navigieren Sie zu **Admin > Targets > Claim a New Target > Cisco UCS Server (Standalone) > Start.** Geben Sie **Device ID** und **Claim Code** der aus der CIMC-GUI kopiert wurde, und wählen Sie **Claim.**


Intersight
ADMIN > Targets
James Delli Paoli
MONITOR
OPERATE
Servers
Chassis
Fabric Interconnects
HyperFlex Clusters
CONFIGURE
Profiles
Policies
Pools
ADMIN
Targets
Claim a New Target
All Targets
Add Filter
Export
0 items found
10 per page
0 of 0
Connection
Top Targe...
Vendor
NO DATA AVAILABLE
NO TYPES
NO DATA AVAILABLE
Name
Status
Type
Target ID
Claimed Time
Claimed By
Product ID
NO ITEMS AVAILABLE
0 of 0

Intersight
ADMIN > Targets > Claim a New Target
James Delli Paoli
MONITOR
OPERATE
Servers
Chassis
Fabric Interconnects
HyperFlex Clusters
CONFIGURE
Profiles
Policies
Pools
ADMIN
Targets
Select Target Type
Filters
Available for Claiming
Categories
All
Cloud
Compute / Fabric
Hyperconverged
Network
Orchestrator
Platform Services
Search
Compute / Fabric
Cisco UCS Server (Standalone)
Cisco UCS Domain (Intersight Managed)
Cisco UCS Domain (UCSM Managed)
Cisco UCS C890
Redfish Server
Platform Services
Cisco Intersight Appliance
Cisco Intersight Assist
Intersight Workload Engine
Cloud
Cancel
Start



Schritt 6: Navigieren Sie zu **Admin > Targets.** Ein erfolgreicher Anspruch zeigt die **Status > Connected,** wie in diesem Bild dargestellt.



Grundlegende Überprüfung bei Problemen mit Geräteansprüchen

Anmerkung: Eine umfassende Liste der Fehlerbedingungen und Problembehebungen finden Sie unter: [Device Connector Error Conditions and Remediation Steps.]

Statusbeschreibungen der Geräteanschlussverbindungen	Statuserklärungen für Geräteanschluss-Verbindungen	Mögliche Problembehebung
Gefordert	Die Verbindung zur Cisco Intersight-Plattform wurde erfolgreich	–

	hergestellt, und Sie haben die Verbindung angefordert.	
Nicht beansprucht	Die Verbindung zur Cisco Intersight-Plattform ist erfolgreich, der Anspruch auf das Endgerät steht jedoch noch aus.	Sie können über Cisco Intersig eine noch nicht beanspruchte Verbindung anfordern.
Administrator deaktiviert	Zeigt an, dass der Intersight-Management-/Geräteanschluss auf dem Endpunkt deaktiviert wurde.	Aktivieren Sie den Geräteansc am Endpunkt.
DNS falsch konfiguriert	DNS wurde im CIMC falsch oder überhaupt nicht konfiguriert.	Zeigt an, dass keiner der auf d System konfigurierten DNS-Namenserver erreichbar ist. Überprüfen Sie, ob Sie gültige Adressen für die DNS-Namens eingegeben haben.
Intersight-DNS-Auflösungsfehler	DNS ist konfiguriert, kann jedoch den DNS-Namen von Intersight nicht auflösen.	Über diesen Link können Sie feststellen, ob Intersight derzei gewartet wird: Status des Interviews. Wenn Intersight betriebsbereit ist, weist dies wahrscheinlich darauf hin, das DNS-Name des Intersight-Dien nicht aufgelöst wurde.
UCS Connect-Netzwerkfehler	Zeigt die ungültigen Netzwerkkonfigurationen an.	Prüfen und bestätigen: MTU is End-to-End korrekt, Port 443 u sind zulässig, die Firewall lässt physischen und virtuellen IPs z DNS und NTP werden auf dem Endpunkt konfiguriert.
Fehler bei der Zertifikatsüberprüfung	Das Endgerät weigert sich, eine Verbindung zur Cisco Intersight-Plattform herzustellen, da das von der Cisco Intersight-Plattform vorgelegte Zertifikat ungültig ist.	Abgelaufenes oder noch ungül Zertifikat: Überprüfen der ordnungsgemäßen Konfigurati des NTP und der Synchronisie der Gerätezeit mit der koordini Weltzeit Überprüfen der ordnungsgemäßen Konfigurati des DNS Wenn ein transparen Webproxy verwendet wird, stel Sie sicher, dass das Zertifikat n abgelaufen ist. Der vom Webserver angegebe Zertifikatname stimmt nicht mit DNS-Namen des Intersight-Die überein: Überprüfen der ordnungsgemäßen Konfigurati des DNS Wenden Sie sich an Webproxy-Administrator, um zu überprüfen, ob der transparent Webproxy richtig konfiguriert is Insbesondere muss der Name vom Webproxy bereitgestellter Zertifikats mit dem DNS-Name Intersight-Dienstes

(svc.intersight.com) übereinstimmen.
Das Zertifikat wurde von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt
Überprüfen der ordnungsgemä
Konfiguration des DNS Wende
sich an Ihren Webadministrato
an infosec, um zu überprüfen,
der transparente Webproxy ric
konfiguriert ist. Insbesondere n
der Name des vom Webproxy
bereitgestellten Zertifikats mit d
DNS-Namen des Intersight-Die
übereinstimmen.

Allgemeine Anforderungen an die Netzwerkkonnektivität von Cisco Intersight

- Eine Netzwerkverbindung zur Intersight-Plattform wird über den Device Connector im Endpunkt hergestellt.
- Überprüfen Sie, ob zwischen dem verwalteten Ziel und Intersight eine Firewall implementiert ist oder ob sich die Regeln für eine aktuelle Firewall geändert haben. Dies kann zu End-to-End-Verbindungsproblemen zwischen dem Endgerät und Cisco Intersight führen. Wenn die Regeln geändert werden, stellen Sie sicher, dass die geänderten Regeln den Datenverkehr durch die Firewall zulassen.
- Wenn Sie einen HTTP-Proxy verwenden, um den Datenverkehr von Ihrem Standort aus weiterzuleiten, und wenn Sie Änderungen an der Konfiguration des HTTP-Proxyservers vorgenommen haben, stellen Sie sicher, dass Sie die Konfiguration des Gerätekonnektors entsprechend den Änderungen ändern. Dies ist erforderlich, da Intersight HTTP-Proxyserver nicht automatisch erkennt.
- Konfigurieren Sie DNS, und lösen Sie den DNS-Namen auf. Der Geräte-Connector muss DNS-Anfragen an einen DNS-Server senden und DNS-Einträge auflösen können. Der Geräteanschluss muss in der Lage sein, svc.intersight.com in eine IP-Adresse aufzulösen.
- Konfigurieren Sie das NTP, und überprüfen Sie, ob die Gerätezeit ordnungsgemäß mit einem Zeitserver synchronisiert wurde.

Anmerkung: Eine umfassende Liste der Verbindungsanforderungen für Intersight finden Sie in Intersight Network Connectivity Requirements.

Zugehörige Informationen

- Cisco Intersight: Erste Schritte - Forderungsziele
- SaaS-unterstützte Systeme von Cisco Intersight
- Von Cisco Intersight SaaS unterstützte PIDs
- Cisco Intersight-Netzwerkanbindungsanforderungen
- Cisco Interview-Schulungsvideos
- Cisco Bug-ID CSCvw76806 - Ein eigenständiger Server der C-Serie kann in Cisco Intersight nicht erfolgreich behaupten, wenn die Geräteanschlussversion kleiner als 1.0.9 ist.
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.