Na vervanging van moederbord een standalone C-Series server in Intersight configureren en opeisen

Inhoud

Inleiding

Dit document beschrijft hoe u een standalone C-Series server kunt configureren en claimen in Cisco Intersight nadat het moederbord is vervangen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Integrated Management Controller (CIMC)
- Cisco-onderschepping
- Cisco C-Series servers

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco C240-M5 4.1(3d) switch
- Cisco Intersight-software als een service (SAAs)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Verwante producten

Dit document kan ook worden gebruikt voor de volgende hardware- en softwareversies:

- C-Series M4 3.0(4) en hoger
- C-Series M5 3.1 en hoger
- C-Series M6 4.2 en hoger
- S-Series M5-4.0(4e) en hoger

> **Opmerking:** Raadpleeg voor een uitgebreide lijst met ondersteunde hardware en software deze links: Door Intersight ondersteunde PID's en door Intersight ondersteunde systemen.

Achtergrondinformatie

- De meest voorkomende gebruikscase voor dit document is wanneer een C-Series is geclaimd bij Cisco Intersight en het moederbord wordt vervangen door Return Material Authorisation (RMA). Telkens wanneer een RMA optreedt, moet de oorspronkelijke server niet worden geclaimd en moet de nieuwe server worden geclaimd in Cisco Intersight.
- In dit document wordt ervan uitgegaan dat de oorspronkelijke C-Series-server succesvol is geclaimd voor het moederbord van RMA en dat er geen configuratie- of netwerkproblemen zijn die zouden bijdragen aan een mislukt claimproces.
- U kunt doelstellingen rechtstreeks van het Cisco Intersight Portal of van de Connector van het Apparaat van het eindpunt zelf ongedaan maken, wordt het aanbevolen om doelstellingen van Cisco Intersight Portal te annuleren.
- Als een doel direct niet wordt geclaimd via de Apparaatconnector en niet via de Intersight Portal, wordt het doel binnen Cisco Intersight niet geclaimd. Het eindpunt moet ook handmatig worden geclaimd via Cisco Intersight.
- De oorspronkelijke C-Series server geeft waarschijnlijk de status weer als Niet verbonden met Cisco Intersight. Dit kan variëren afhankelijk van de reden waarom het moederbord moet worden vervangen.

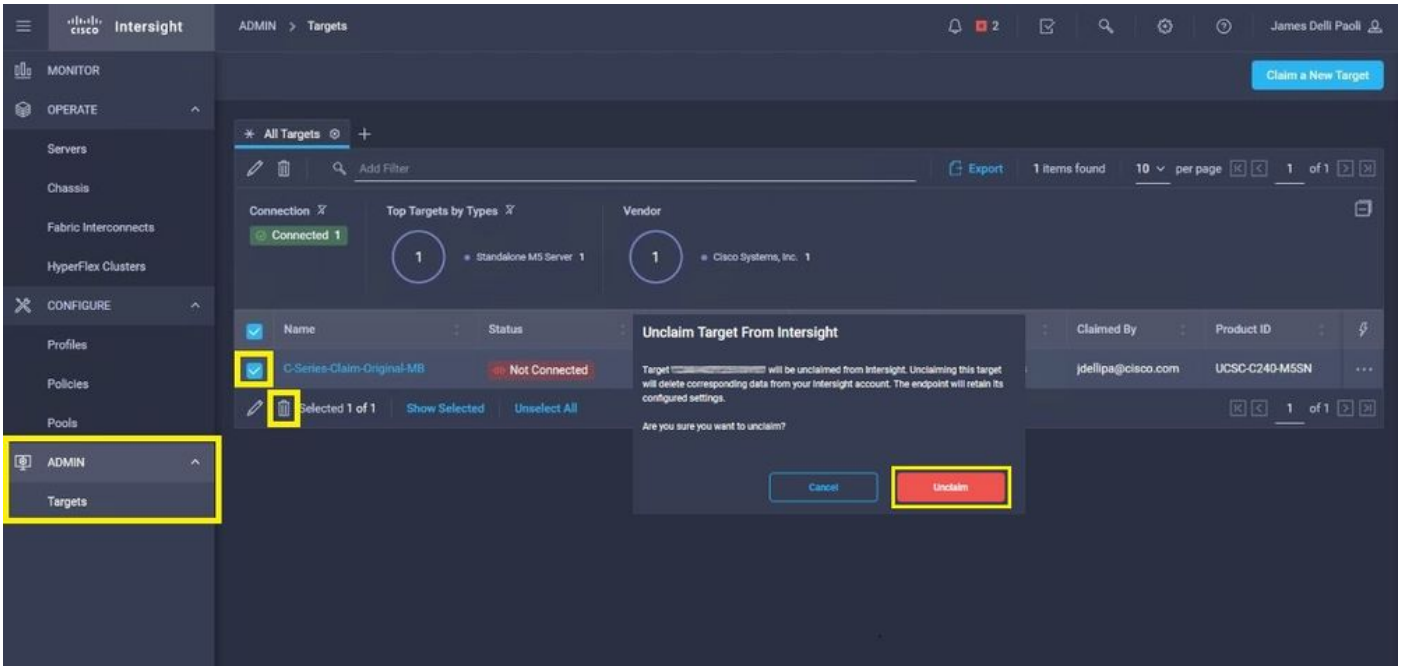
Probleem: Nieuwe RMA-server wordt niet geclaimd tijdens interviews en oorspronkelijke mislukte server wordt geclaimd

Als een standalone C-Series server is geclaimd in Cisco Intersight wordt het server Serial Number (SN) gekoppeld met Cisco Intersight. Als de geclaimde server om een storing of om een andere reden moet worden vervangen, moet de oorspronkelijke server niet worden geclaimd en moet de nieuwe server worden geclaimd in Cisco Intersight. De C-Series SN verandert met het moederbord RMA.

Oplossing

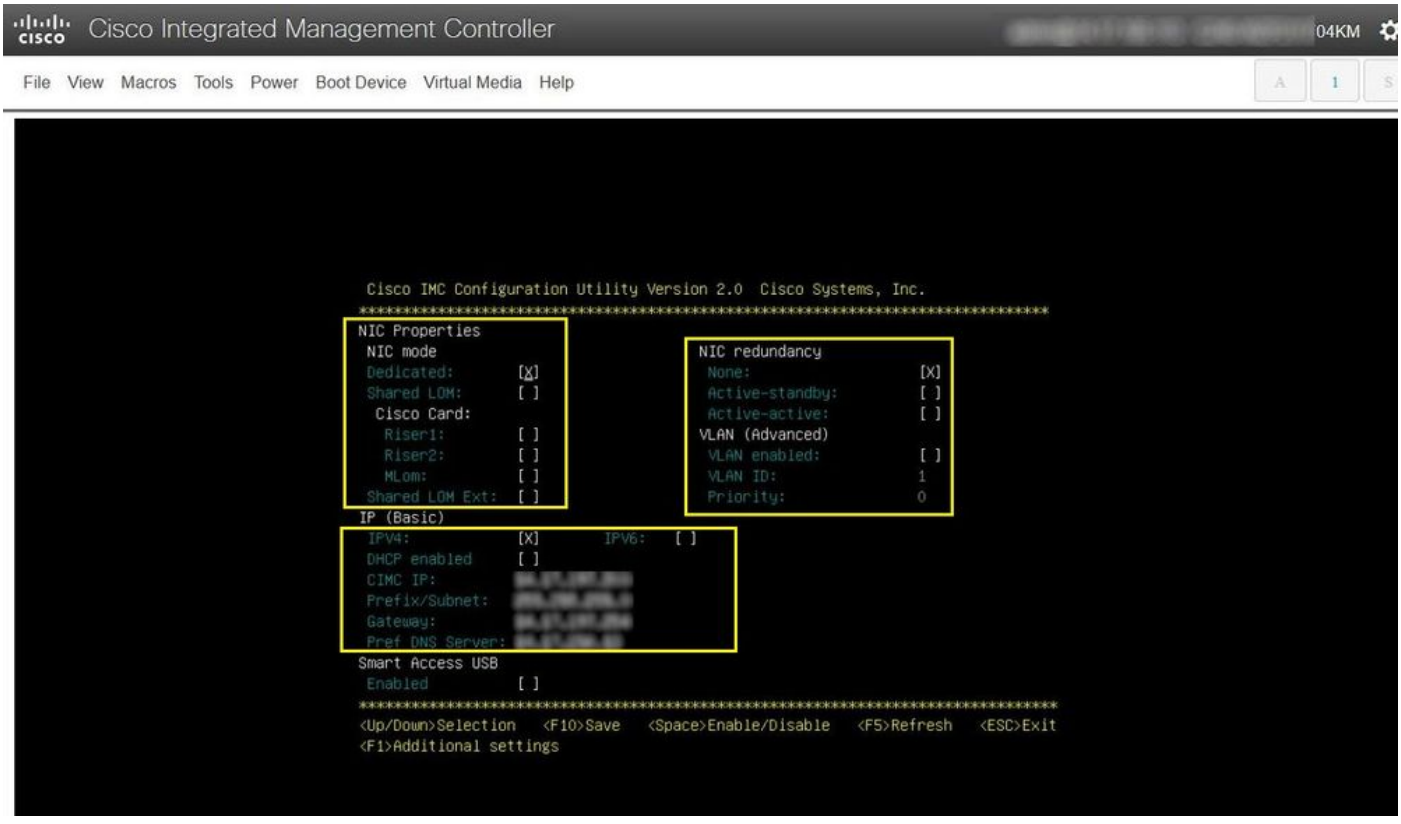
Annuleert de C-Series server van Cisco Intersight die moet worden vervangen. Configureer de nieuwe servers CIMC en Device Connector en claimt de nieuwe server naar Cisco Intersight.

Stap 1. Start Cisco Intersight en klik op **Admin > Targets**. Selecteer het vakje voor de te vervangen en niet-geclaimde doelgroep(en) en klik op de **Trash Can Icon > Unclaim** zoals in deze afbeelding.



Stap 2. Sluit een Keyboard Video Monitor (KVM) aan op de nieuwe vervangen server (sla deze stap over als CIMC al is geconfigureerd). Selecteer in het welkomstscherm van Cisco bij het opstarten **F8** om CIMC te configureren. Configureer de juiste instellingen **Network Interface Card (NIC) Properties** voor uw omgeving en druk op **F10** in **Save**. Plaats fysieke kabels in de server en het aangesloten apparaat op basis van de **NIC Properties** gebruikt voor het beheer.

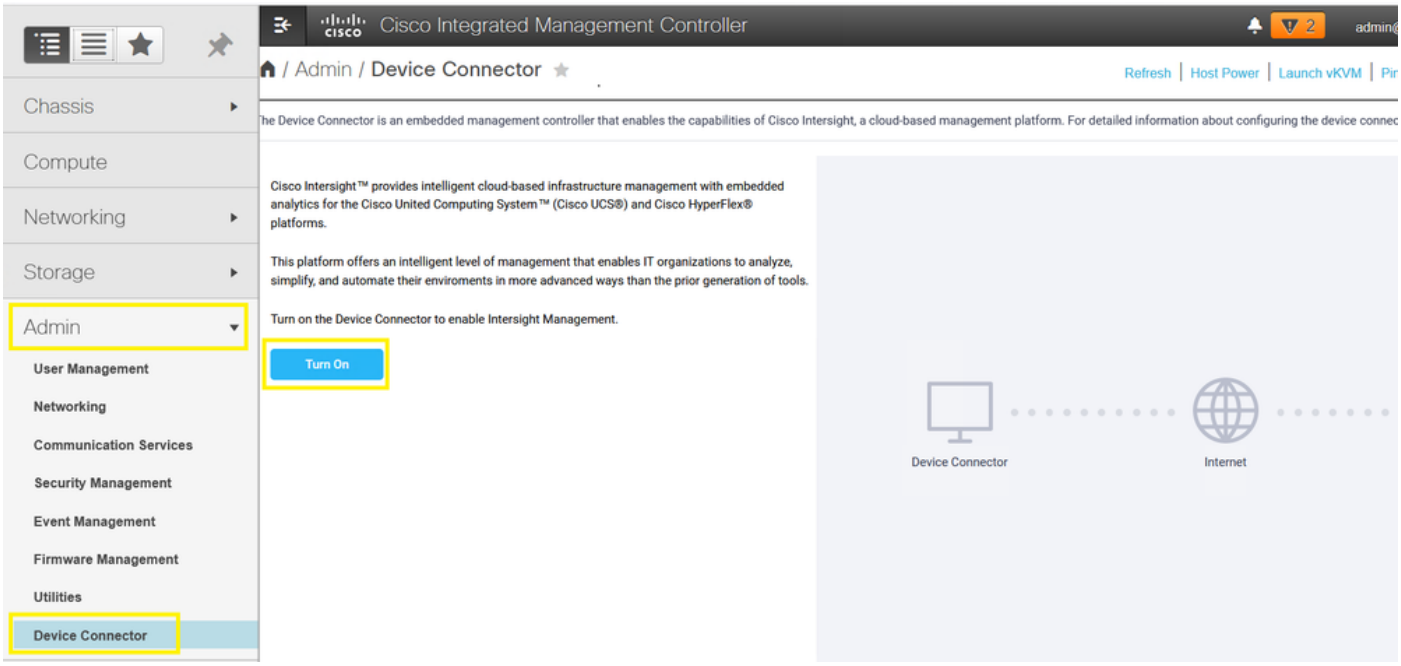
> **Opmerking:** Stap 2. illustreert en beschrijft een lokale installatie van de CIMC met een aangesloten KVM rechtstreeks op een C240-M5. De eerste CIMC-installatie kan ook op afstand met DHCP worden uitgevoerd. Raadpleeg de juiste installatiehandleiding voor uw servermodel en kies welke eerste CIMC-installatie het beste voor u is.

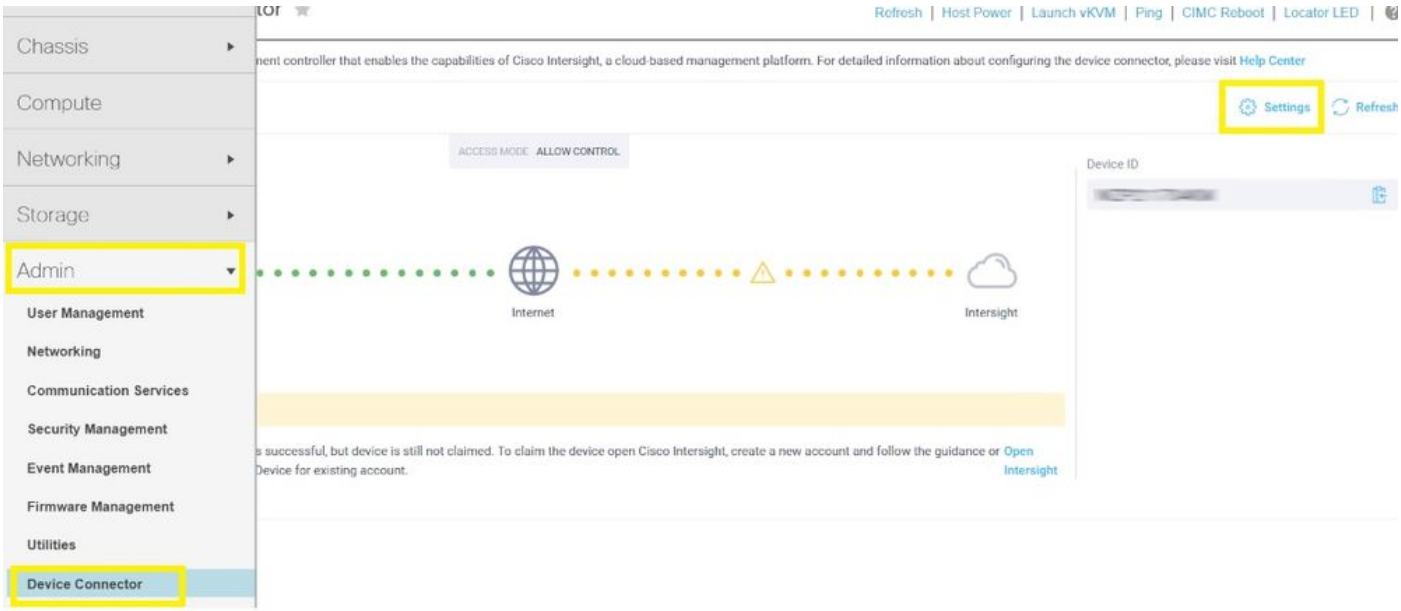


Stap 3. Start CIMC Graphical User Interface (GUI) en navigeer naar **Admin > Device Connector.** Indien

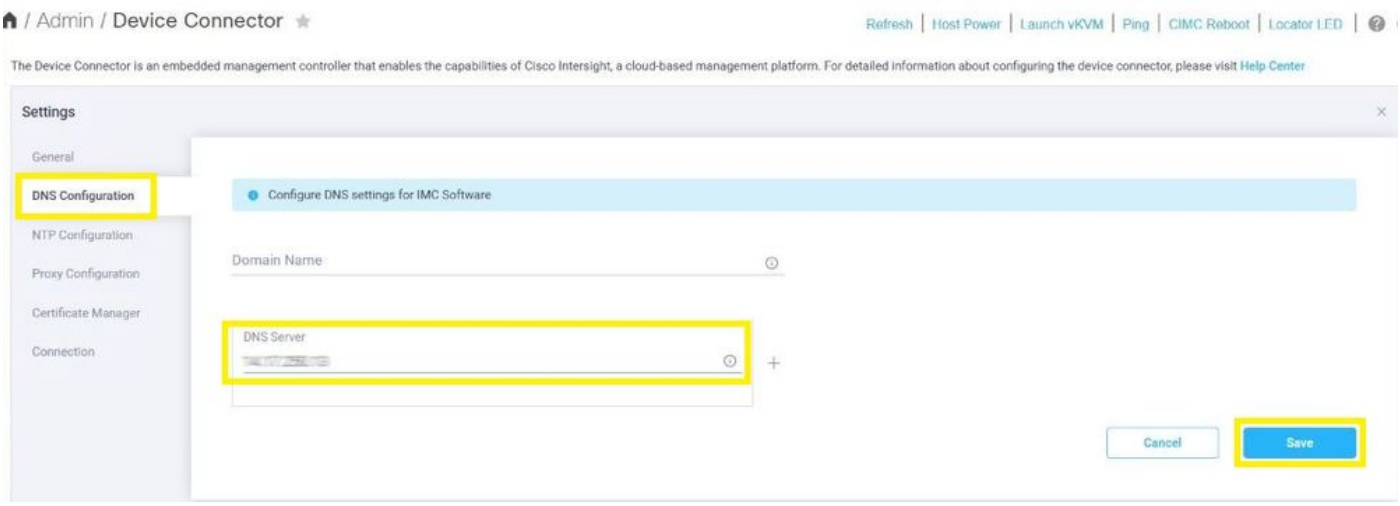
Device Connector is uitgeschakeld, kiest u **Turn On.** Zodra deze is ingeschakeld, selecteert u **Settings.**

> **Tip**: In de CIMC GUI navigeer naar **Chassis > Summary** en vergelijk de **Firmware Version** om te bevestigen dat aan de minimale vereisten voor de firmware is voldaan, dient Cisco Intersight te worden geclaimd. Gebruik deze link om de minimumvereisten voor uw specifieke servermodel te verifiëren: Intersight Ondersteunde Systems. Als de firmware niet voldoet aan de te claimen minimumeisen, voert u een Host Upgrade Utility (HUU) uit op de server. Zie hier: Cisco-proces voor upgrade op host.

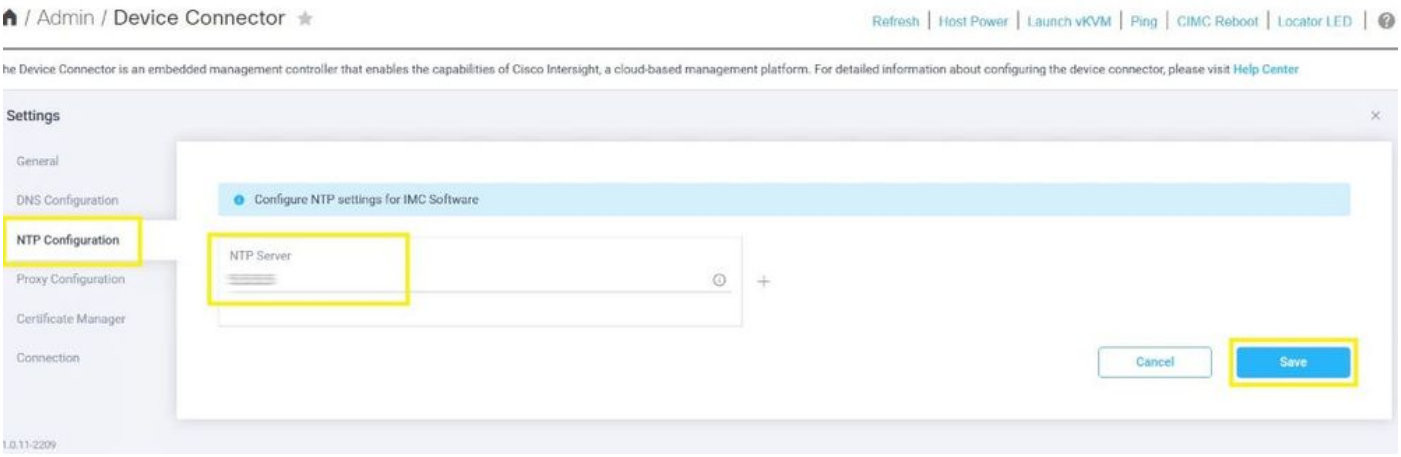




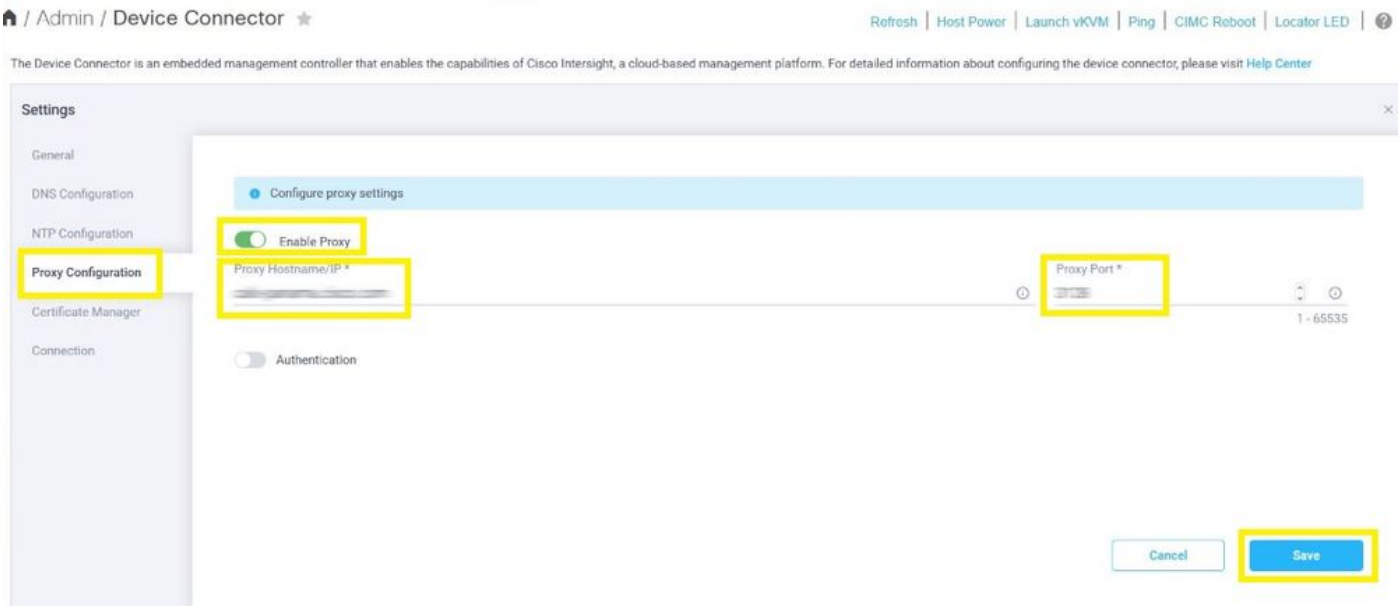
Stap 3.1. Navigeer naar **Admin > Device Connector > Settings > DNS Configuration** en de juiste instellingen te configureren **DNS Server** en selecteer **Save** zoals in deze afbeelding.



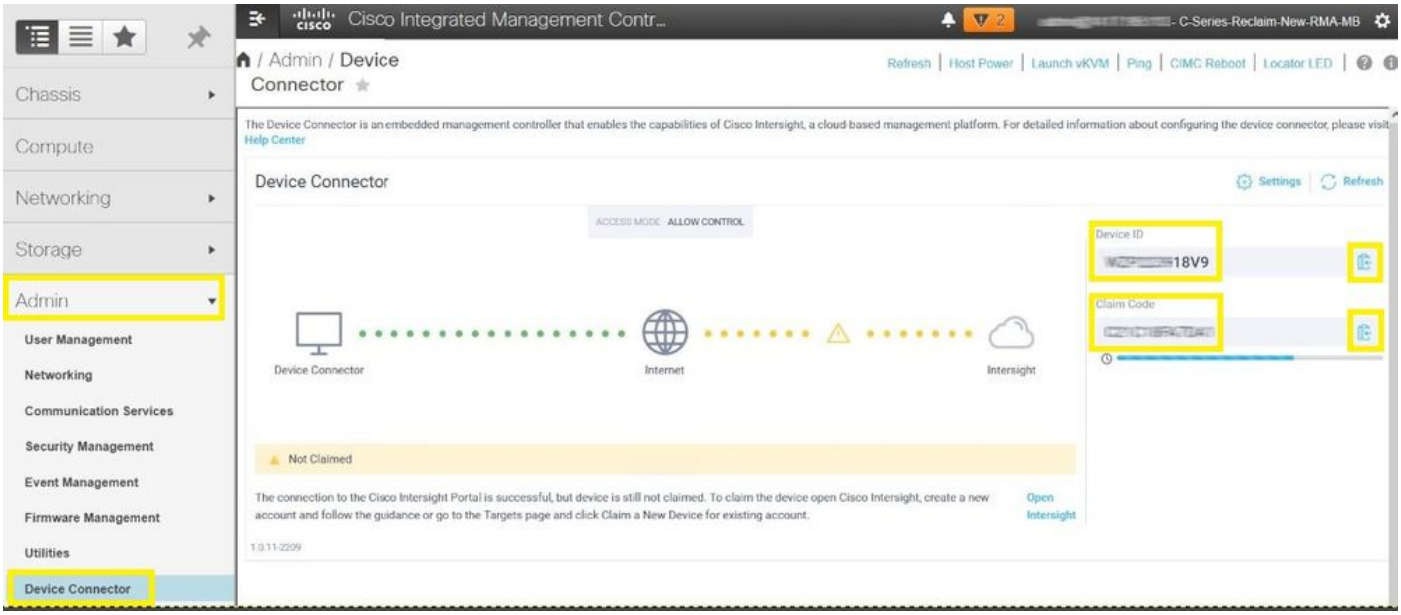
Stap 3.2. Navigeer naar **Admin > Device Connector > Settings > NTP Configuration.** Configureer de **NTP Server** richten per omgeving en selecteren **Save** zoals in deze afbeelding.



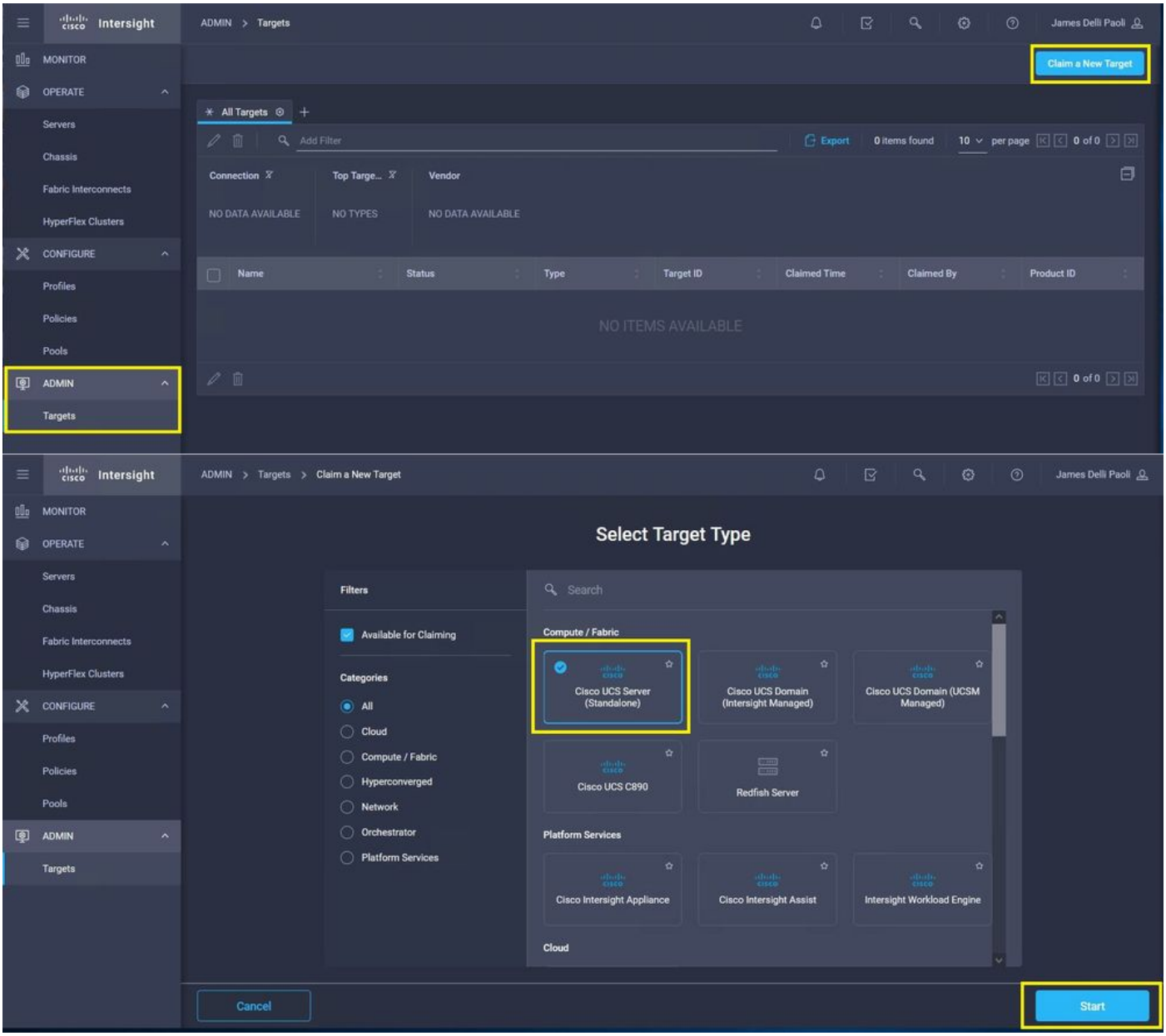
Stap 3.3. Configureer indien nodig een proxy om Cisco Intersight te bereiken. Navigeer naar **Admin > Device Connector > Settings > Proxy Configuration > Enable Proxy.** Configureer de **Proxy Hostname/IP** en de **Proxy Port** en selecteer **Save.**

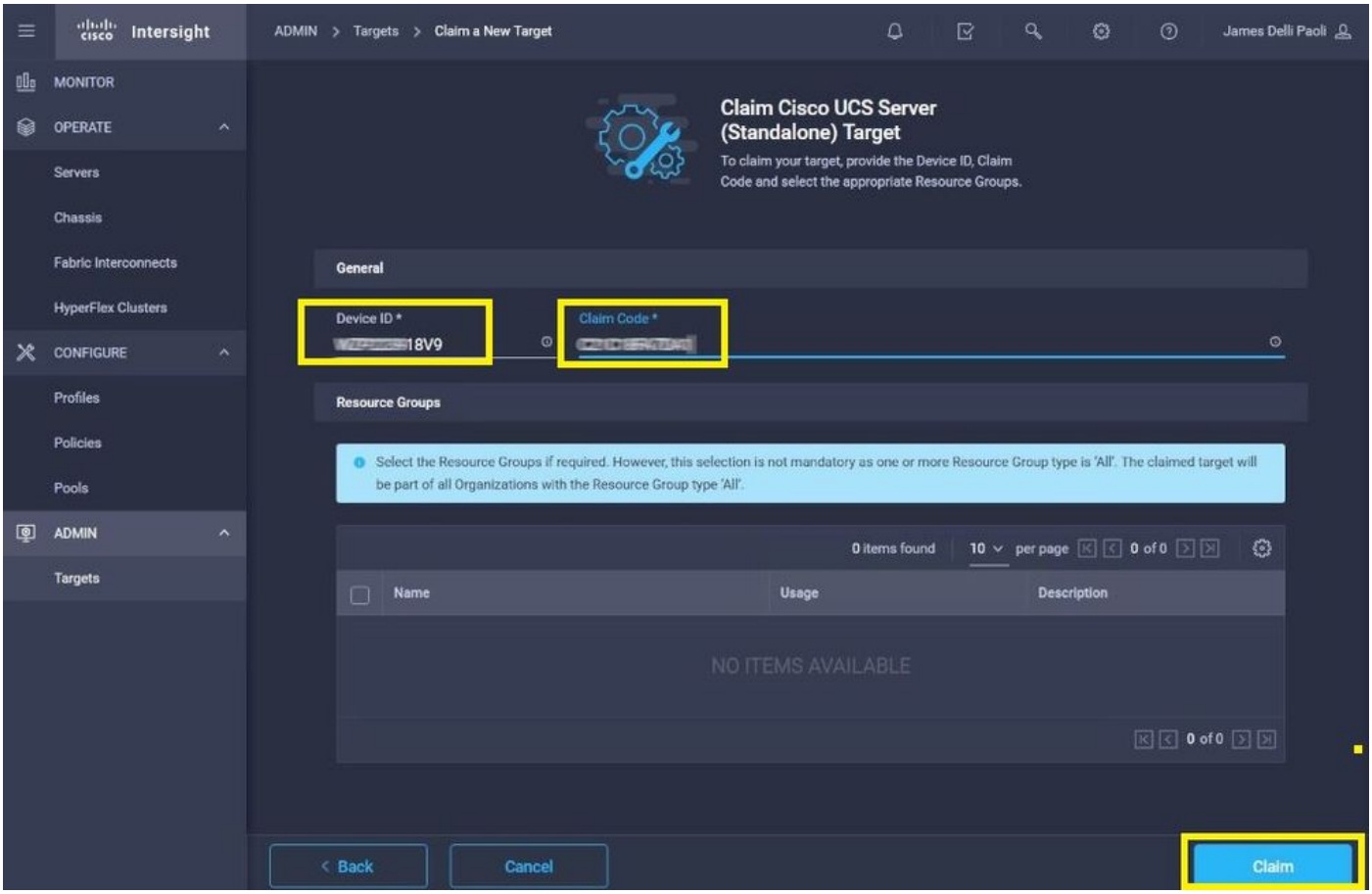


Stap 4. Selecteer **Admin > Device Connector** en kopieert de **Device ID** en **Claim Code.** Kopieer beide naar een blocnote of tekstbestand voor later gebruik.

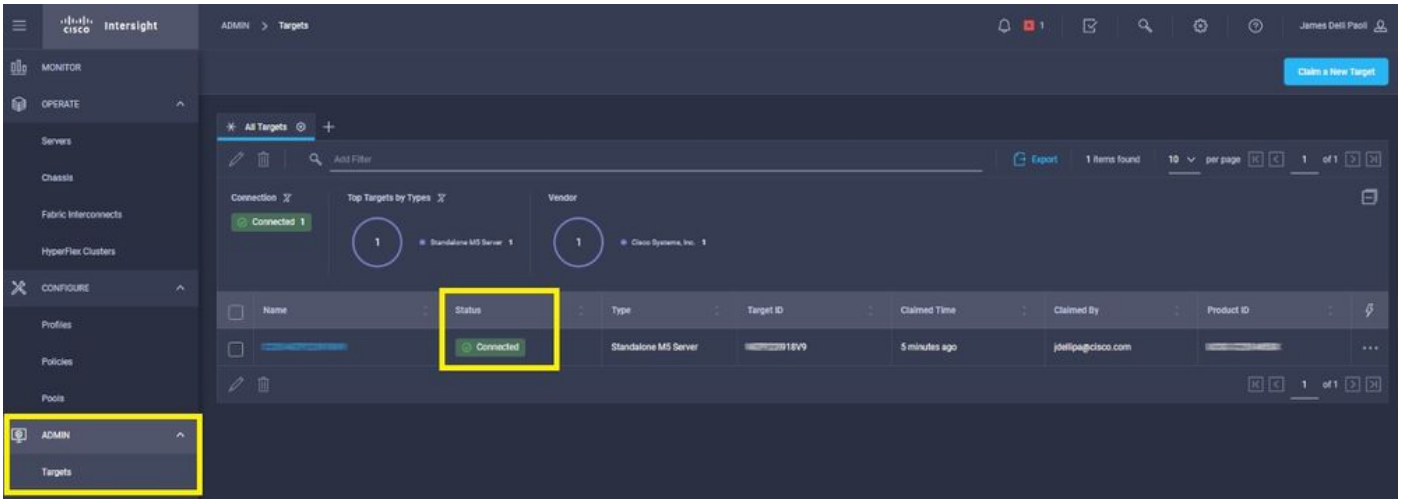


Stap 5. Start Cisco Intersight en navigeer naar **Admin > Targets > Claim a New Target > Cisco UCS Server (Standalone) > Start.** Voer het **Device ID** en **Claim Code** dat is gekopieerd van de CIMC GUI en selecteer **Claim.**





Stap 6. Navigeer naar **Admin > Targets.** Een succesvolle claim toont de **Status > Connected,** zoals in deze afbeelding.



Basisverificatie voor problemen met apparaatclaims

Opmerking: Zie voor een uitgebreide lijst van foutvoorwaarden en herstelstappen deze link: [Device Connector foutvoorwaarden en herstelstappen.]

Beschrijving van de verbindingsstatus van Apparaatconnector	Uitleg over de verbindingsstatus van de apparaatconnector	Mogelijke oplossingen
beweerd	De verbinding met het Cisco Intersight-platform is succesvol en u	N.v.t.

	hebt de verbinding geclaimd.	
Niet aangegeven	De verbinding met het Cisco Intersight-platform is succesvol, maar het eindpunt moet nog worden geclaimd.	U kunt een niet-opgeëiste verbinding claimen via Cisco Intersight.
Administratief uitgeschakeld	Geeft aan dat de Intersight Management/Device Connector is uitgeschakeld op het eindpunt.	Schakel de Apparaatconnector het eindpunt.
DNS niet correct geconfigureerd	DNS is in CIMC niet correct geconfigureerd of helemaal niet geconfigureerd.	Geeft aan dat geen van de DN naamservers die op het systee zijn geconfigureerd, bereikbaar Controleer of u geldige IP-adre voor de DNS-naamservers heb ingevoerd.
Intersight DNS Resolve-fout	DNS is ingesteld maar kan de DNS-naam van Intersight niet oplossen.	Controleer deze link om te zien Intersight onderhoud ondergaa Intersight Status. Als Intersight operationeel is, betekent dit waarschijnlijk dat de DNS-naar de Intersight-dienst niet is opge
UCS Connect-netwerkfout	Geeft de ongeldige netwerkconfiguraties aan.	Controleer en bevestig: MTU is correct van end-to-end, de poo 443 en 80 zijn toegestaan, de firewall staat alle fysieke en vir IP's toe, DNS en NTP zijn op h eindpunt geconfigureerd.
Fout bij certificaatvalidatie	Het eindpunt weigert een verbinding met het Cisco Intersight-platform te maken omdat het certificaat dat wordt aangeboden door het Cisco Intersight-platform ongeldig is.	Verlopen of nog niet geldig certificaat: Controleer of NTP g is geconfigureerd en of de apparaattijd is gesynchronisee met de gecoördineerde univers tijd. Controleer of DNS goed is geconfigureerd. Als een transparante webproxy in gebr verifieert u of het certificaat nie verlopen. De certificaatnaam die wordt weergegeven door de webserv komt niet overeen met de DNS naam van de Intersight-service Controleer of DNS goed is geconfigureerd. Neem contact met uw webproxy beheerder o controleren of de transparante webproxy correct is geconfigur Met name de naam van het certificaat dat wordt aangebod door de webproxy moet overeenkomen met de DNS-na van de Intersight-dienst (svc.intersight.com). Het certificaat is afgegeven do

een onbetrouwbare certificeringsinstantie (CA): Controleer of DNS goed is geconfigureerd. Neem contact met uw webbeheerder of infos te controleren of de transparan webproxy correct is geconfigur Met name de naam van het certificaat dat wordt aangebod door de webproxy moet overeenkomen met de DNS-na van de Intersight-dienst.

Vereisten voor Cisco Intersight General Network Connectivity

- Een netwerkverbinding met het Intersight-platform wordt tot stand gebracht via de Apparaatconnector in het eindpunt
- Controleer of een firewall is geïntroduceerd tussen het beheerde doel en Intersight of dat de regels voor een huidige firewall zijn gewijzigd. Dit kan end-to-end verbindingsproblemen tussen het eindpunt en Cisco Intersight veroorzaken. Als de regels worden gewijzigd, zorg er dan voor dat de gewijzigde regels verkeer via de firewall toestaan.
- Als u een HTTP proxy gebruikt om verkeer uit uw gebouw te routeren, en als u wijzigingen hebt aangebracht in de HTTP proxy server configuratie, zorg ervoor dat u de apparaat connector configuratie om de wijzigingen te weerspiegelen. Dit is nodig omdat Intersight niet automatisch HTTP proxy servers detecteert.
- Configureer DNS en los de DNS-naam op. De Device Connector moet DNS-verzoeken naar een DNS-server kunnen verzenden en DNS-records kunnen oplossen. De Apparaatconnector moet svc.intersight.com naar een IP-adres kunnen oplossen.
- Configureer NTP en bevestig dat de apparaattijd correct gesynchroniseerd is met een tijdserver.

Opmerking: Voor een uitgebreide lijst van de connectiviteitsvereisten van Intersight Connectiviteitsvereisten voor het Intersight-netwerk.

Gerelateerde informatie

- Cisco Intersight Get Started Claim-doelstellingen
- Door Cisco Intersight ASA ondersteunde systemen
- Door Cisco Intersight ASA ondersteunde PID's
- Vereisten voor Cisco Intersight Network Connectivity
- Cisco-trainingsvideo's voor interviews
- Cisco bug-id CSCvw76806 - Een standalone C-Series server kan niet met succes claimen in Cisco Intersight als de versie van de apparaatconnector minder is dan 1.0.9.
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.