Configure e reivindique um servidor independente C-Series na Intersight após a substituição da placa-mãe

Contents

Introduction

Este documento descreve como configurar e reivindicar um servidor C-Series independente no Cisco Intersight após a substituição da placa-mãe.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Controlador de gerenciamento integrado da Cisco (CIMC)
- Entrevista da Cisco
- Servidores Cisco C-Series

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco C240-M5 4.1(3d)
- Software como serviço (SaaS) Cisco Intersight

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Produtos Relacionados

Este documento também pode ser usado com as seguintes versões de hardware e software:

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

> **Note**: Para obter uma lista abrangente de hardware e software compatíveis, consulte estes links: PIDs com suporte da Intersight e sistemas com suporte da Intersight.

Informações de Apoio

- O caso de uso mais comum para este documento é quando uma C-Series foi solicitada à Cisco Intersight e a placa-mãe é substituída pela RMA (Return Material Authorization, Autorização para material de devolução). Sempre que ocorre uma RMA, o servidor original precisa ser cancelado e o novo servidor precisa ser cancelado no Cisco Intersight.
- Este documento supõe que o servidor C-Series original foi reivindicado com êxito antes da RMA da placa-mãe e que não há problemas de configuração ou de rede que contribuam para um processo de reivindicação com falha.
- Você pode cancelar a reivindicação de alvos diretamente do Cisco Intersight Portal ou do Device Connector do próprio endpoint. Recomenda-se cancelar a reivindicação de alvos do Cisco Intersight Portal.
- Se um destino não for reivindicado diretamente do conector do dispositivo e não do portal Intersight, ele mostrará o destino dentro do Cisco Intersight como não reivindicado. O endpoint também precisa ser manualmente cancelado da Cisco Intersight.
- O servidor C-Series original provavelmente exibe o status como Não conectado no Cisco Intersight. Isso pode variar dependendo do motivo pelo qual a placa-mãe precisa ser substituída.

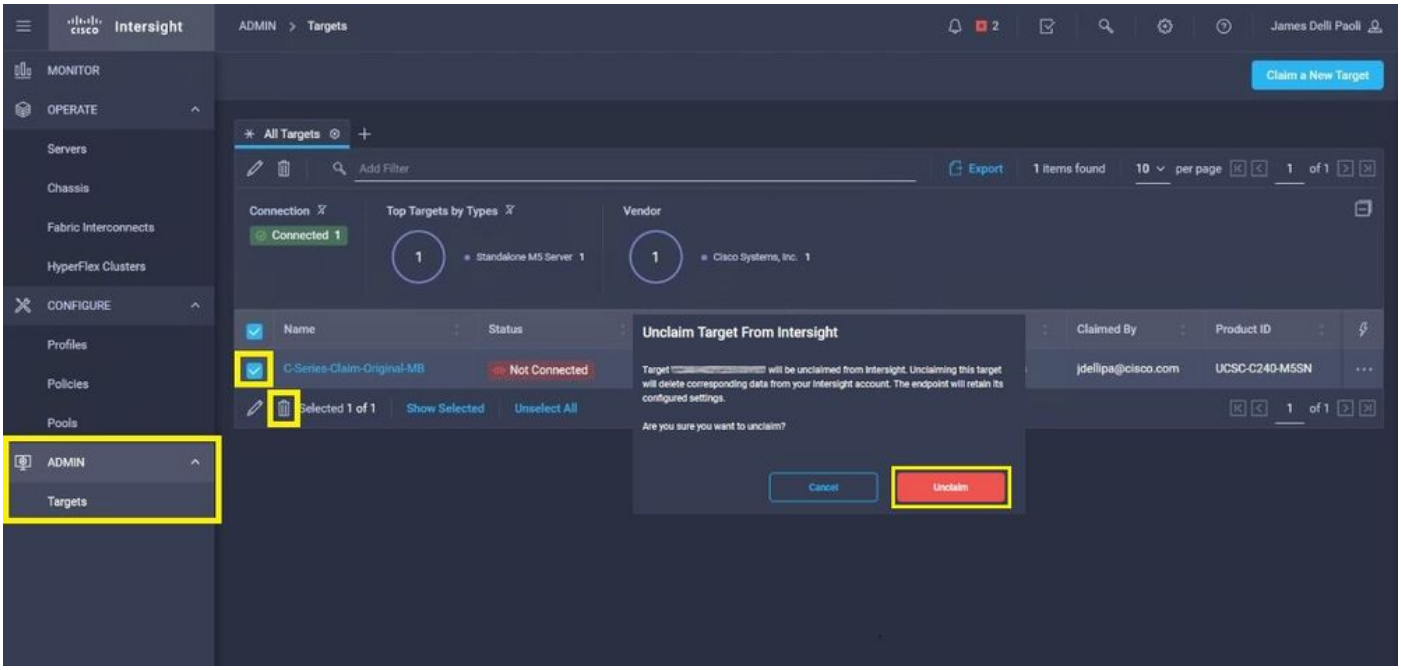
Problema: O novo servidor de RMA não é reivindicado na Intersight e o servidor com falha original é reivindicado

Se um servidor C-Series autônomo foi reivindicado no Cisco Intersight, o número de série do servidor (SN) torna-se emparelhado com o Cisco Intersight. Se o servidor solicitado precisar de uma substituição de placa-mãe devido a uma falha ou por qualquer outro motivo, o servidor original precisa ser cancelado e o novo servidor precisa ser solicitado no Cisco Intersight. O SN C-Series muda com a RMA da placa-mãe.

Solução

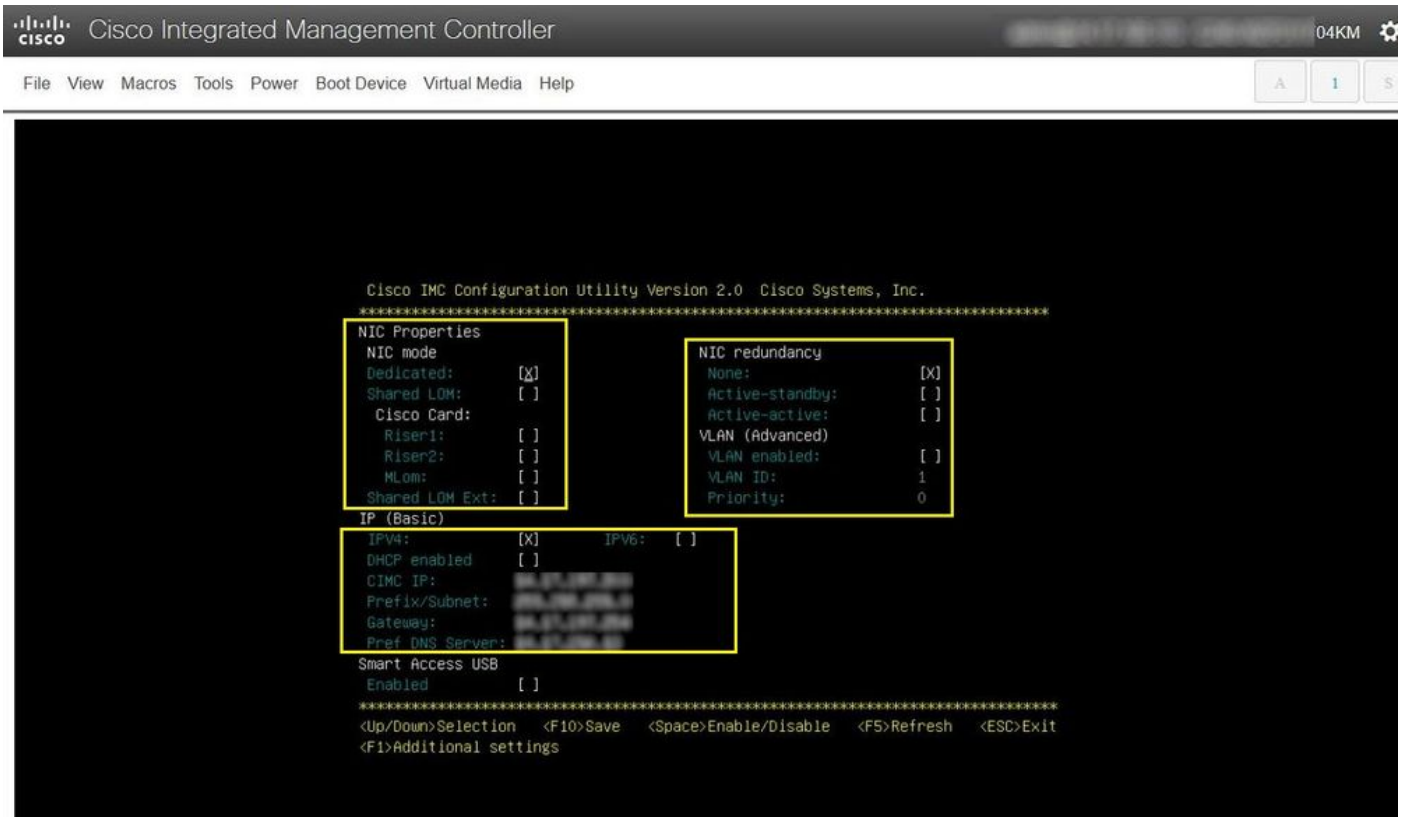
Não solicite a substituição do servidor C-Series da Cisco Intersight. Configure os novos servidores CIMC e Device Connector e solicite o novo servidor para a Cisco Intersight.

Etapa 1. Inicie o Cisco Intersight e clique em **Admin > Targets**. Selecione a caixa para o(s) destino(s) que deve(m) ser substituído(s) e não reivindicado(s) e clique no botão **Trash Can Icon > Unclaim** como mostrado nesta imagem.



Etapa 2. Conectar um KVM (Keyboard Video Monitor, Monitor de vídeo do teclado) ao servidor recém-substituído (ignore esta etapa se o CIMC já tiver sido configurado). Na tela inicial da Cisco na inicialização, selecione **F8** para configurar o CIMC. Configure o **Network Interface Card (NIC) Properties** para o seu ambiente e pressione **F10** para **Save**. Insira cabos físicos ao servidor e ao dispositivo conectado com base no **NIC Properties** usado para gerenciamento.

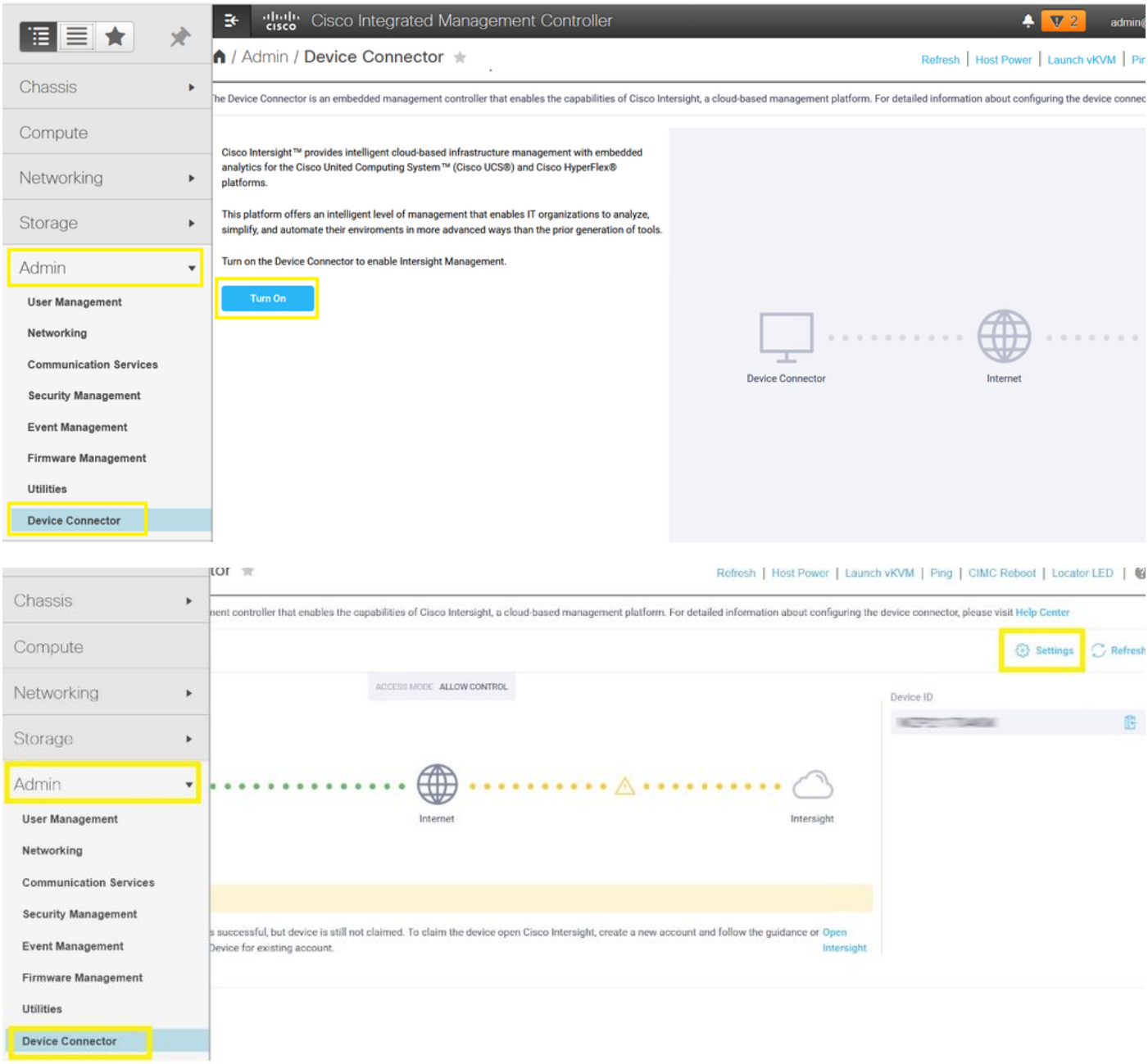
> **Note**: Etapa 2. ilustra e descreve uma configuração local do CIMC com um KVM conectado diretamente a um C240-M5. A configuração inicial do CIMC também pode ser feita remotamente com DHCP. Consulte o Guia de instalação adequado ao seu modelo de servidor e escolha qual configuração inicial do CIMC é melhor para você.



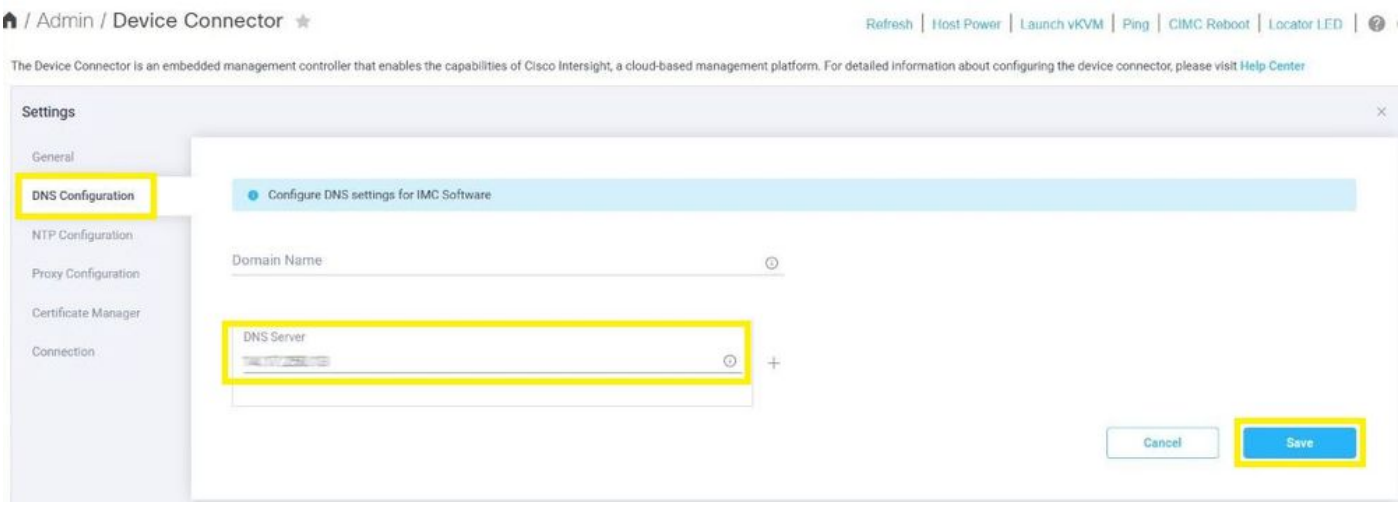
Etapa 3. Inicie a interface gráfica do usuário (GUI) do CIMC e navegue até **Admin > Device Connector.**

Se **Device Connector** estiver desativado, escolha **Turn On.** Depois de habilitado, selecione **Settings.**

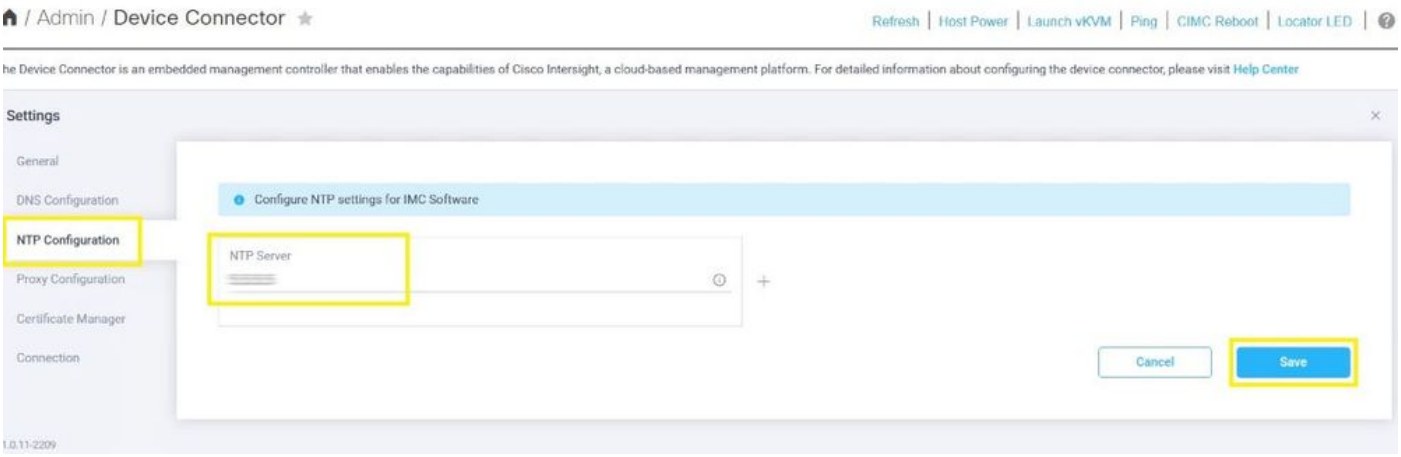
> **Tip**: Na GUI do CIMC, navegue até **Chassis > Summary** e comparar o **Firmware Version** para confirmar se os requisitos mínimos de firmware foram atendidos e serão solicitados pela Cisco Intersight. Utilize esse link para verificar os requisitos mínimos para seu modelo de servidor específico: Sistemas suportados pela Intersight. Se o firmware não atender aos requisitos mínimos a serem solicitados, execute um Host Upgrade Utility (HUU) no servidor, consulte aqui: Processo do utilitário de atualização de host da Cisco.



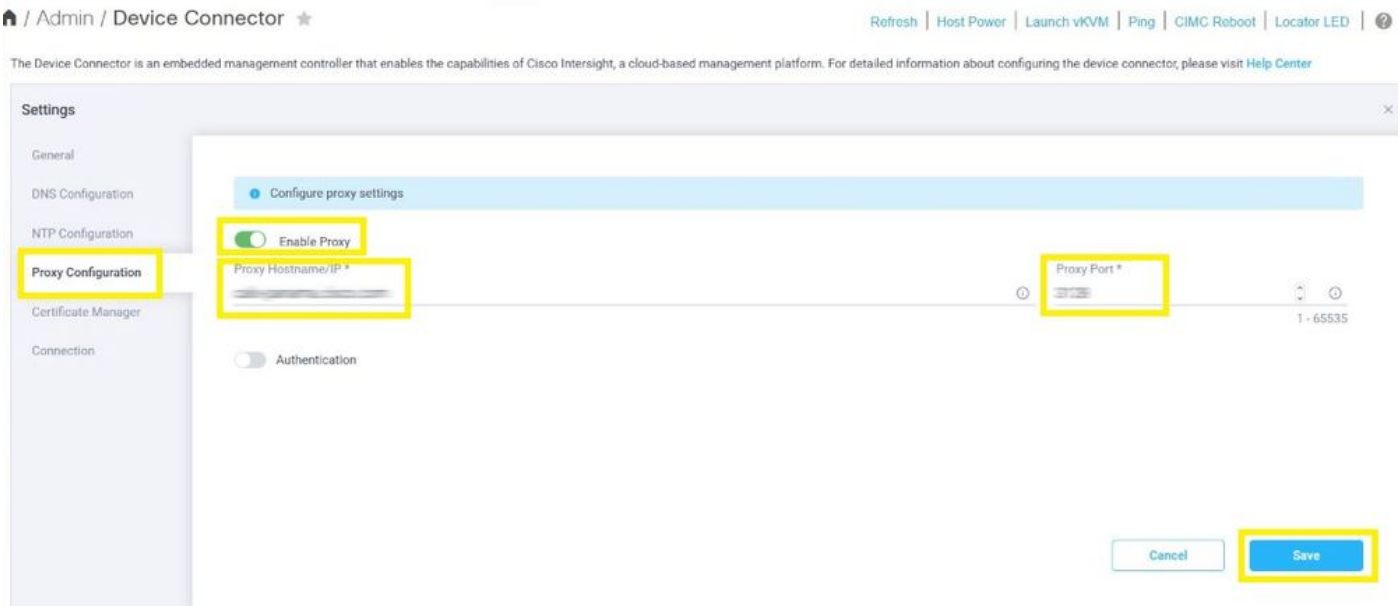
Etapa 3.1. Navegue até **Admin > Device Connector > Settings > DNS Configuration** e configurar o **DNS Server** e selecione **Save** como mostrado nesta imagem.



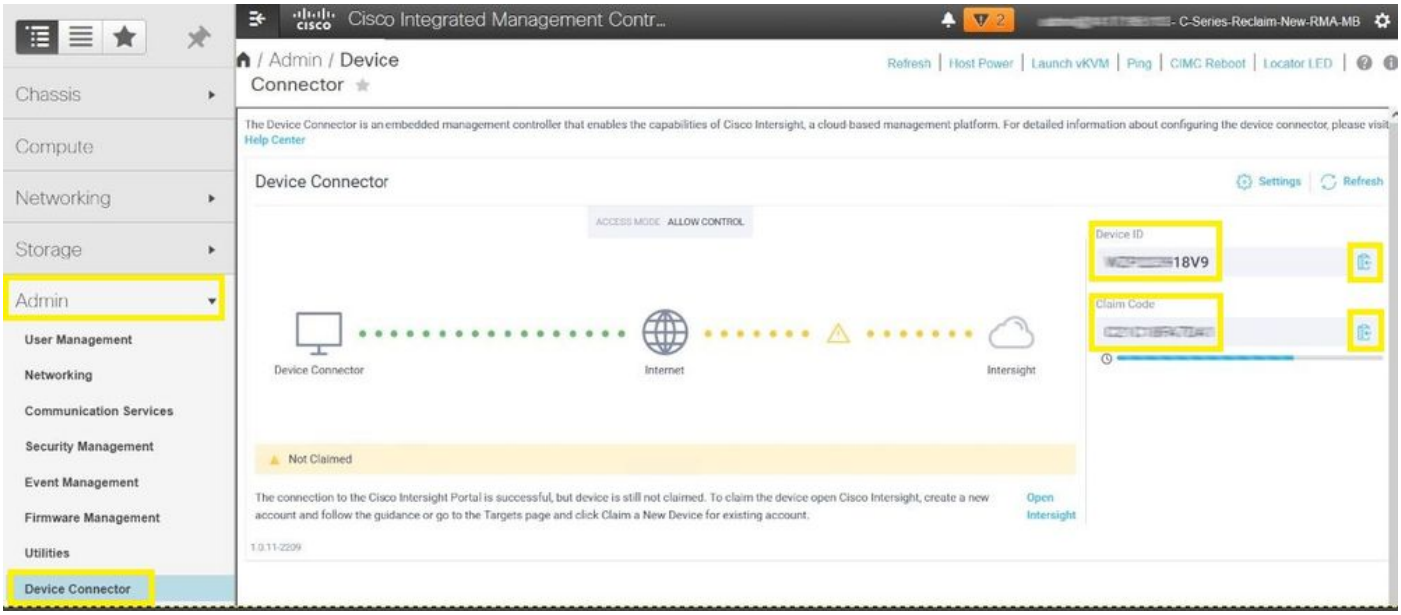
Etapa 3.2. Navegue até **Admin > Device Connector > Settings > NTP Configuration.** Configurar o **NTP Server** por ambiente e selecione **Save** como mostrado nesta imagem.



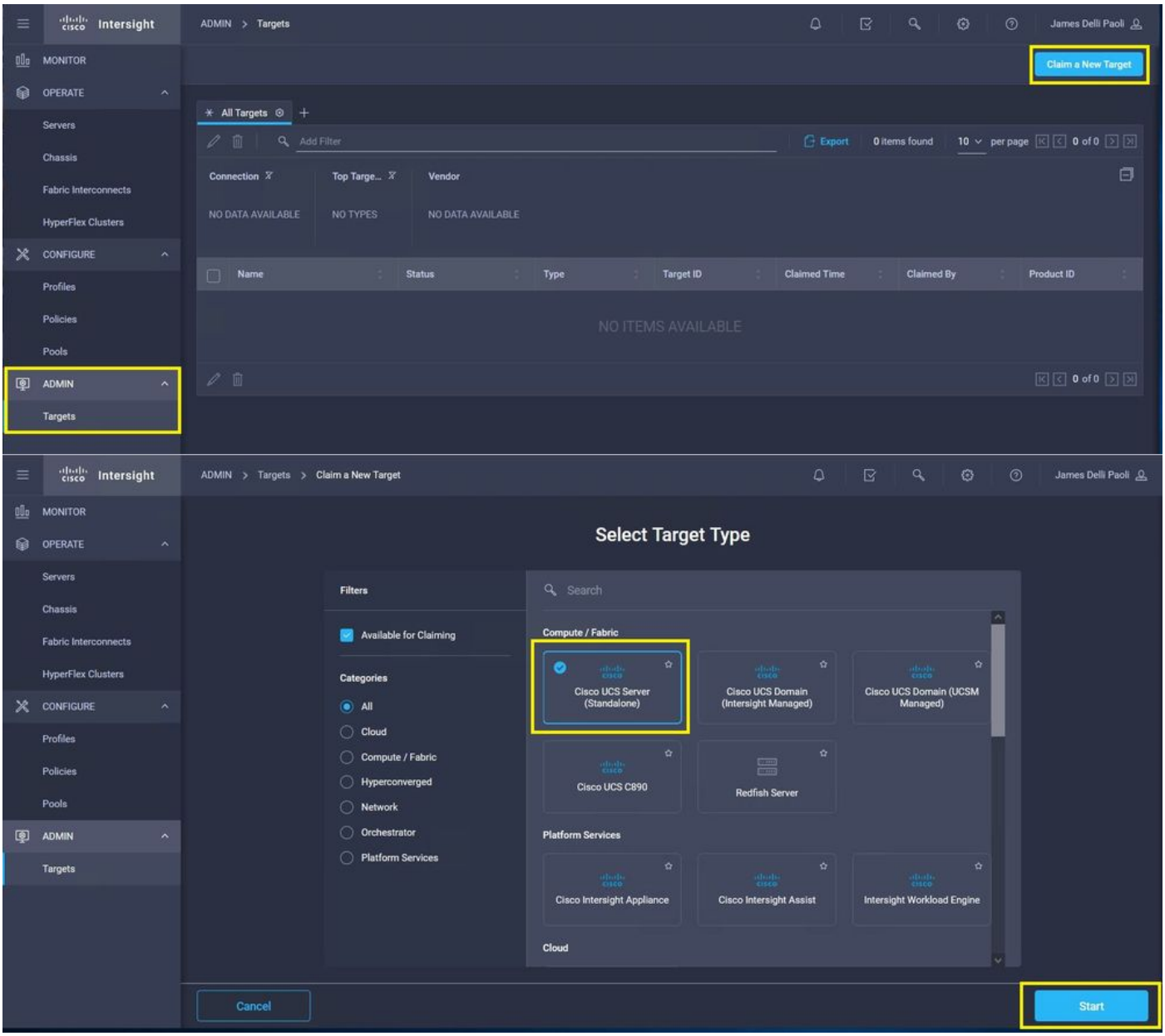
Etapa 3.3. Configure opcionalmente um proxy, se necessário, para acessar a Cisco Intersight. Navegue até **Admin > Device Connector > Settings > Proxy Configuration > Enable Proxy.** Configurar o **Proxy Hostname/IP** e o **Proxy Port** e selecione **Save.**

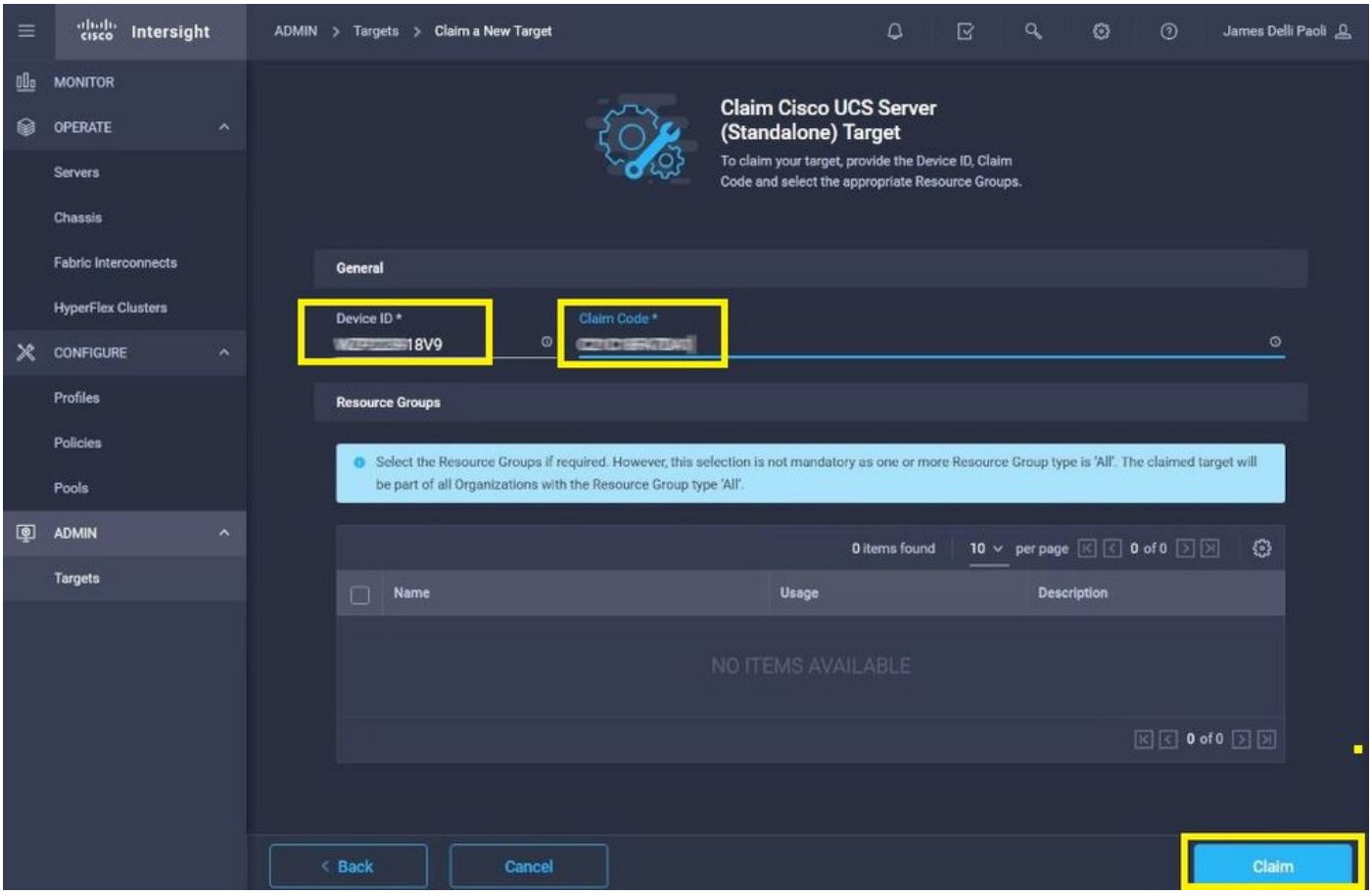


Etapa 4. Selecione **Admin > Device Connector** e copiar o **Device ID** e **Claim Code.** Copie ambos em um bloco de notas ou arquivo de texto para uso posterior.

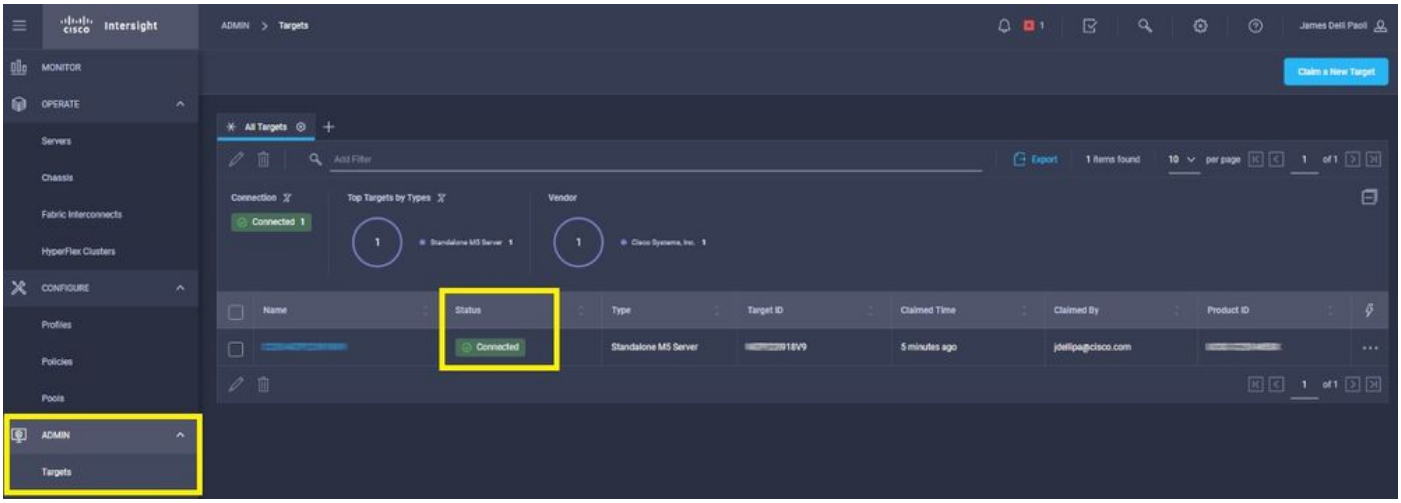


Etapa 5. Inicie o Cisco Intersight e navegue até **Admin > Targets > Claim a New Target > Cisco UCS Server (Standalone) > Start.** Digite o **Device ID** e **Claim Code** que foi copiado da GUI do CIMC e selecione **Claim.**





Etapa 6. Navegue até **Admin > Targets.** Uma reivindicação bem-sucedida mostra o **Status > Connected,** como mostrado nesta imagem.



Verificação básica para problemas de declaração do dispositivo

Note: Para obter uma lista abrangente de Condições de erro e correções, consulte este link: [Condições de erro do conector do dispositivo e Etapas de correção.]

Descrições de Status de Conexão do Conector de Dispositivo	Explicações de Status de Conexão do Conector de Dispositivo	Possíveis correções
Reivindicado	A conexão com a plataforma Cisco Intersight foi bem-sucedida e você solicitou a conexão.	N/A

Não reivindicado	A conexão com a plataforma Cisco Intersight foi bem-sucedida, mas o endpoint ainda não foi reivindicado.	Você pode solicitar uma conex não solicitada pela Cisco Inters
Administrativamente desabilitado	Indica que o Gerenciamento de Intersight/Conector do Dispositivo foi desabilitado no ponto de extremidade.	Ative o conector do dispositivo endpoint.
DNS configurado incorretamente	O DNS foi configurado incorretamente no CIMC ou não foi configurado.	Indica que nenhum dos servido de nome DNS configurados no sistema está acessível. Verifiq você inseriu endereços IP válid para os servidores de nome DI
Erro de Resolução DNS de Intersight	O DNS está configurado, mas não é possível resolver o nome DNS da Intersight.	Verifique este link para ver se a Intersight está passando por manutenção: Status de Intersig Se a Intersight estiver operacio isso provavelmente indica que nome DNS do serviço de Inters não foi resolvido.
Erro de rede do UCS Connect	Indica as configurações de rede inválidas.	Verifique e confirme: O MTU e correto de ponta a ponta, as po 443 e 80 são permitidas, o Fire permite que todos os IPs físico virtuais, DNS e NTP sejam configurados no endpoint.
Erro de validação de certificado	O endpoint se recusa a estabelecer uma conexão com a plataforma Cisco Intersight porque o certificado apresentado pela plataforma Cisco Intersight é inválido.	Certificado expirado ou ainda n válido: Verifique se o NTP está configurado corretamente e se hora do dispositivo está sincronizada com o Tempo Universal Coordenado. Verifiqu o DNS está configurado corretamente. Se um proxy da transparente estiver em uso, verifique se o certificado não expirou. O nome do certificado apresen pelo servidor Web não corresp ao nome DNS do serviço de Intersight: Verifique se o DNS configurado corretamente. Ent contato com o administrador d proxy da Web para verificar se proxy da Web transparente est configurado corretamente. Especificamente, o nome do certificado apresentado pelo pr da Web deve corresponder ao nome DNS do serviço Intersigh (svc.intersight.com). O certificado foi emitido por um Autoridade de Certificação (CA confiável: Verifique se o DNS e

configurado corretamente. Ent
contato com o administrador d
Web ou o infosec para verifica
proxy da Web transparente est
configurado corretamente.
Especificamente, o nome do
certificado apresentado pelo pr
da Web deve corresponder ao
nome DNS do serviço de Inters

Requisitos gerais de conectividade de rede da Cisco Intersight

- Uma conexão de rede com a plataforma Intersight é estabelecida a partir do conector do dispositivo no endpoint
- Verifique se um firewall foi introduzido entre o destino gerenciado e a Intersight ou se as regras de um firewall atual foram alteradas. Isso pode causar problemas de conexão fim-a-fim entre o endpoint e a Cisco Intersight. Se as regras forem alteradas, verifique se as regras alteradas permitem o tráfego pelo firewall.
- Se você usar um proxy HTTP para rotear o tráfego para fora das suas instalações e tiver feito alterações na configuração do servidor proxy HTTP, certifique-se de alterar a configuração do conector de dispositivo para refletir as alterações. Isso é necessário porque o Intersight não detecta automaticamente servidores proxy HTTP.
- Configure DNS e resolva o nome DNS. O Conector do Dispositivo deve ser capaz de enviar solicitações DNS a um servidor DNS e resolver registros DNS. O Conector do Dispositivo deve ser capaz de resolver svc.intersight.com para um endereço IP.
- Configure o NTP e valide se a hora do dispositivo está sincronizada corretamente com um servidor de hora.

Note: Para obter uma lista abrangente de Requisitos de Conectividade da Intersight, consulte Requisitos de Conectividade de Rede da Intersight.

Informações Relacionadas

- Metas da reivindicação do Cisco Intersight Getting Started
- Sistemas Cisco Intersight SaaS suportados
- PIDs compatíveis com Cisco Intersight SaaS
- Requisitos de conectividade da Cisco Intersight Network
- Vídeos de treinamento do Cisco Intersight
- ID de bug da Cisco CSCvw76806 - Um servidor autônomo C-Series pode falhar ao solicitar com êxito no Cisco Intersight se a versão do seu conector de dispositivo for inferior a 1.0.9.
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.