Configuración y reclamación de un servidor independiente de la serie C en Intersight tras la sustitución de la placa base

Contenido

Introducción

Este documento describe cómo configurar y reclamar un servidor C-Series autónomo en Cisco Intersight después de que se haya reemplazado la placa base.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Integrated Management Controller (CIMC)
- Cisco Intersight
- Servidores Cisco C-Series

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco C240-M5 4.1(3d)
- Software como servicio (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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Productos Relacionados

Este documento también puede utilizarse con estas versiones de software y hardware:

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

Nota: Para obtener una lista completa de hardware y software compatibles, consulte estos enlaces: PID compatibles con Intersight y sistemas compatibles con Intersight.

Antecedentes

- El caso práctico más común de este documento es cuando se reclamó una serie C a Cisco Intersight y la placa madre se sustituyó por una autorización de devolución de mercancía (RMA). Cada vez que se produce una RMA, el servidor original debe ser reclamado y el nuevo servidor debe ser reclamado en Cisco Intersight.
- Este documento asume que el servidor C-Series original fue reclamado exitosamente antes de la RMA de la placa base, y no hay problemas de configuración o de red que contribuyan a un proceso de reclamación fallido.
- Puede anular la reclamación de los destinos directamente desde Cisco Intersight Portal o desde el conector de dispositivo del terminal en sí. Se recomienda anular la reclamación de los destinos desde Cisco Intersight Portal.
- Si un destino no se reclama directamente desde su conector de dispositivo y no desde el portal de intersight, muestra el destino dentro de Cisco Intersight como no reclamado. El terminal también debe dessolicitarse manualmente de Cisco Intersight.
- Es probable que el servidor original de la serie C muestre el estado como No conectado en Cisco Intersight. Esto puede variar en función de la razón por la que la placa base necesita ser reemplazada.

Problema: No se reclama el nuevo servidor RMA en el intervalo y se reclama el servidor original fallido

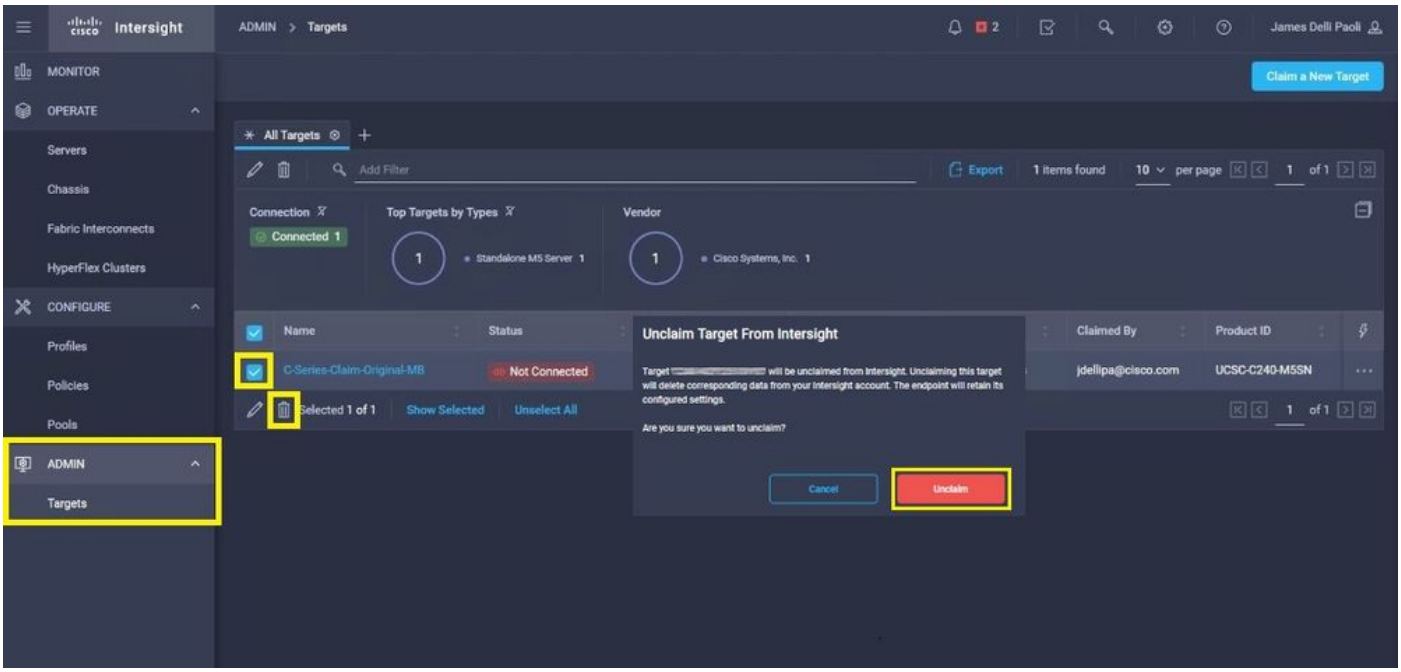
Si se ha solicitado un servidor C-Series independiente en Cisco Intersight, el número de serie (SN) del servidor se empareja con Cisco Intersight. Si el servidor reclamado requiere una sustitución de la placa base debido a un error o a cualquier otro motivo, el servidor original debe ser reclamado y el nuevo servidor debe ser reclamado en Cisco Intersight. El SN de la serie C cambia con la RMA de la placa base.

Solución

Quite la reclamación del servidor C-Series de Cisco Intersight que necesita ser sustituido. Configure los nuevos servidores CIMC y Device Connector y reclame el nuevo servidor a Cisco Intersight.

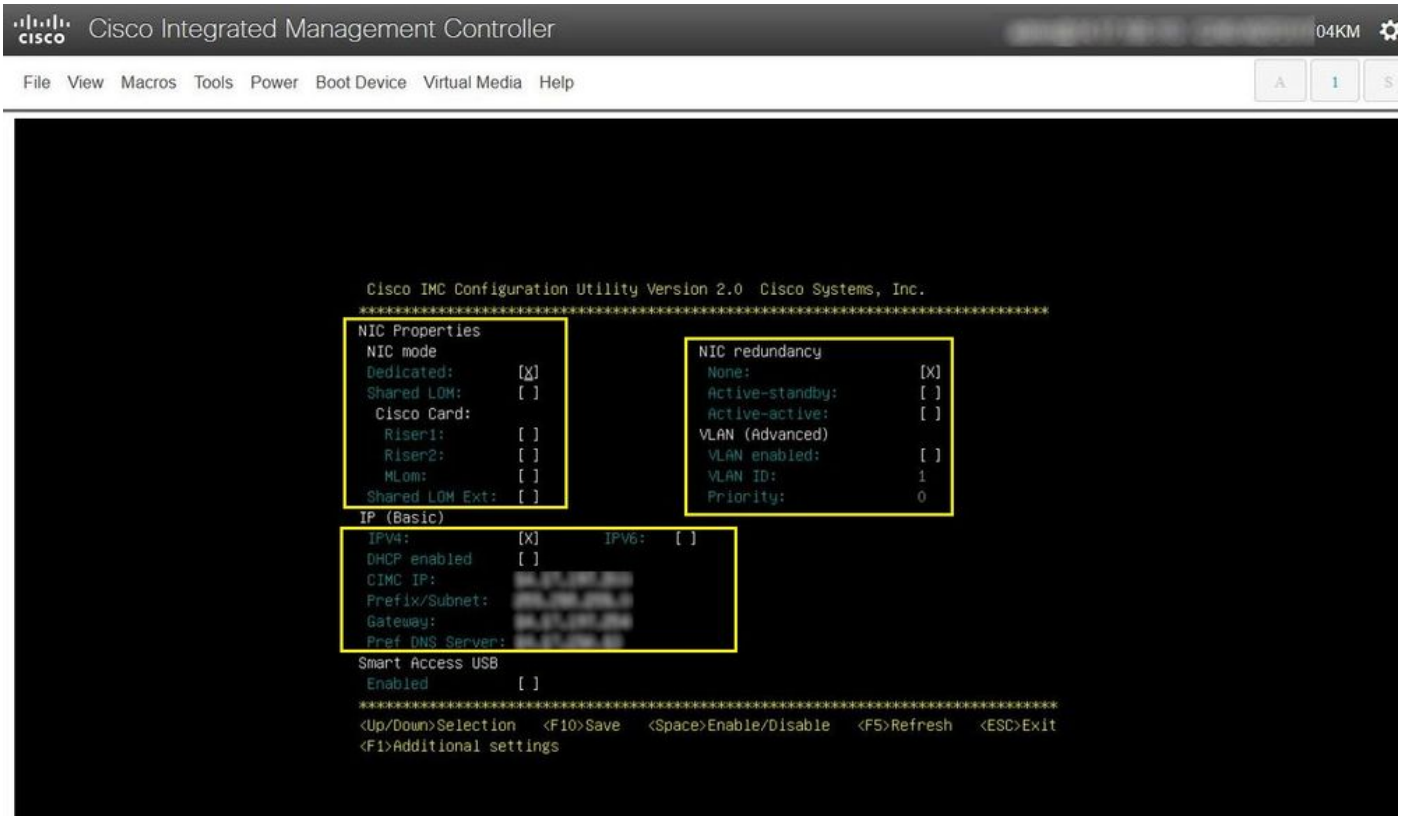
Paso 1. Inicie Cisco Intersight y haga clic en **Admin > Targets**. Seleccione la casilla de los destinos

que se van a sustituir y no reclamar y haga clic en el botón **Trash Can Icon > Unclaim** como se muestra en esta imagen.



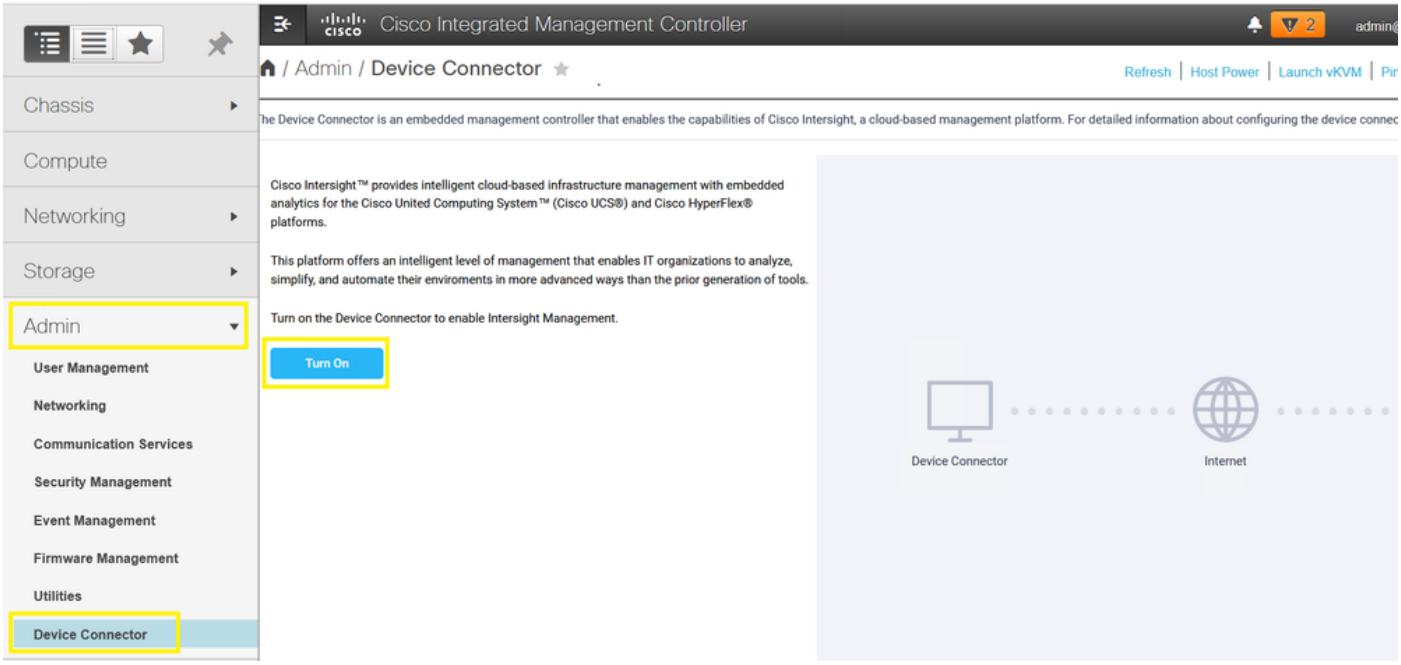
Paso 2. Conecte un monitor de vídeo de teclado (KVM) al servidor que acaba de sustituir (omita este paso si CIMC ya se ha configurado). En la pantalla de inicio de Cisco, seleccione **F8** para configurar CIMC. Configure el **Network Interface Card (NIC) Properties** para su entorno y pulse **F10** a **Save.** Inserte cables físicos en el servidor y su dispositivo conectado en función de la **NIC Properties** se utiliza para la gestión.

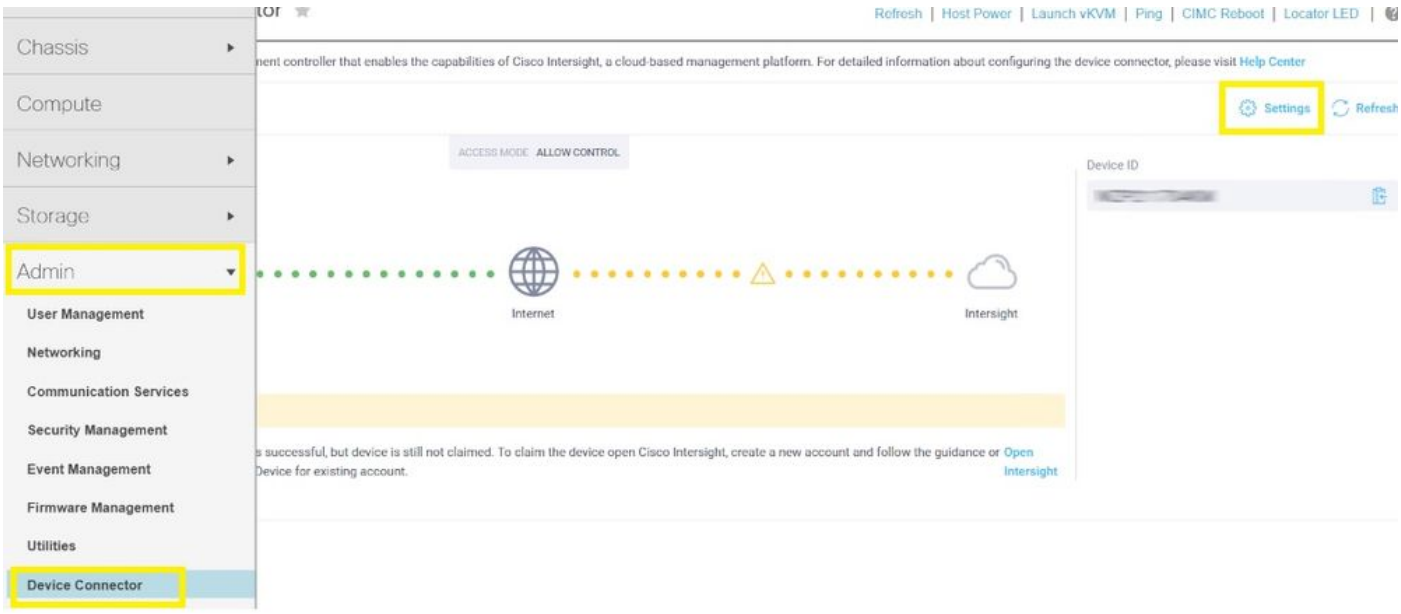
> **Nota:** Paso 2. ilustra y describe una configuración local del CIMC con un KVM conectado directamente a un C240-M5. La configuración inicial del CIMC también se puede realizar de forma remota con DHCP. Consulte la guía de instalación adecuada para el modelo de servidor y elija la configuración inicial de CIMC que más se ajuste a sus necesidades.



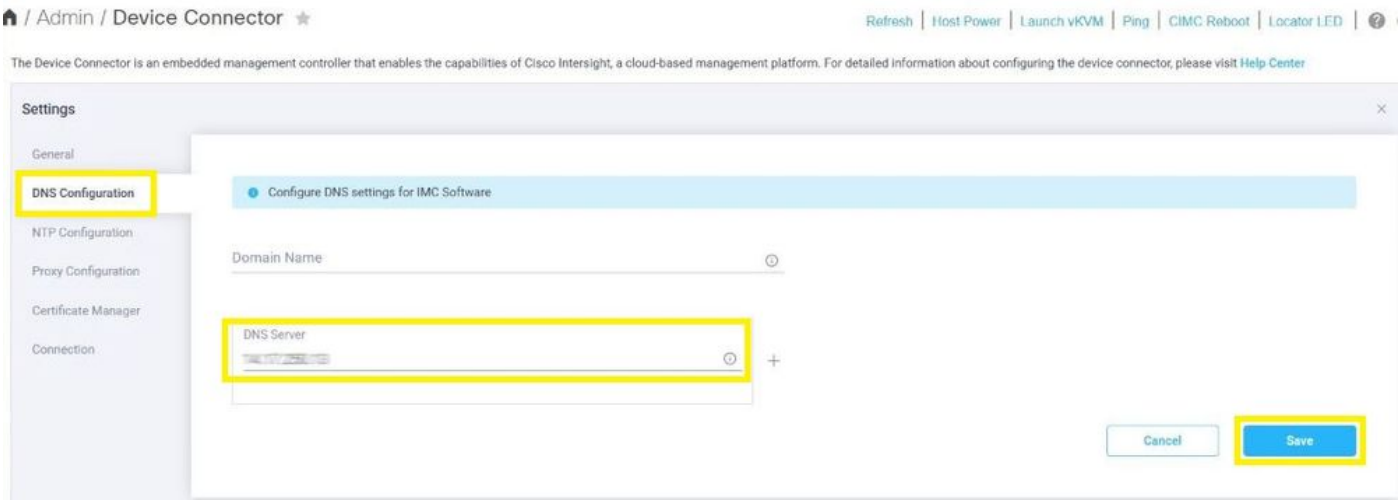
Paso 3. Inicie la interfaz gráfica de usuario (GUI) de CIMC y acceda a **Admin > Device Connector.** Si **Device Connector** está desactivado, seleccione **Turn On.** Una vez activada, seleccione **Settings.**

> **Consejo:** En la GUI de CIMC, vaya a **Chassis > Summary** y compare el **Firmware Version** para confirmar que se cumplen los requisitos mínimos de firmware y que Cisco Intersight puede solicitarlos. Utilice este enlace para verificar los requisitos mínimos para su modelo de servidor específico: Intersight Supported Systems. Si el firmware no cumple los requisitos mínimos que se deben reclamar, ejecute una utilidad de actualización de host (HUU) en el servidor, consulte la siguiente información: Proceso de la utilidad de actualización de host de Cisco.

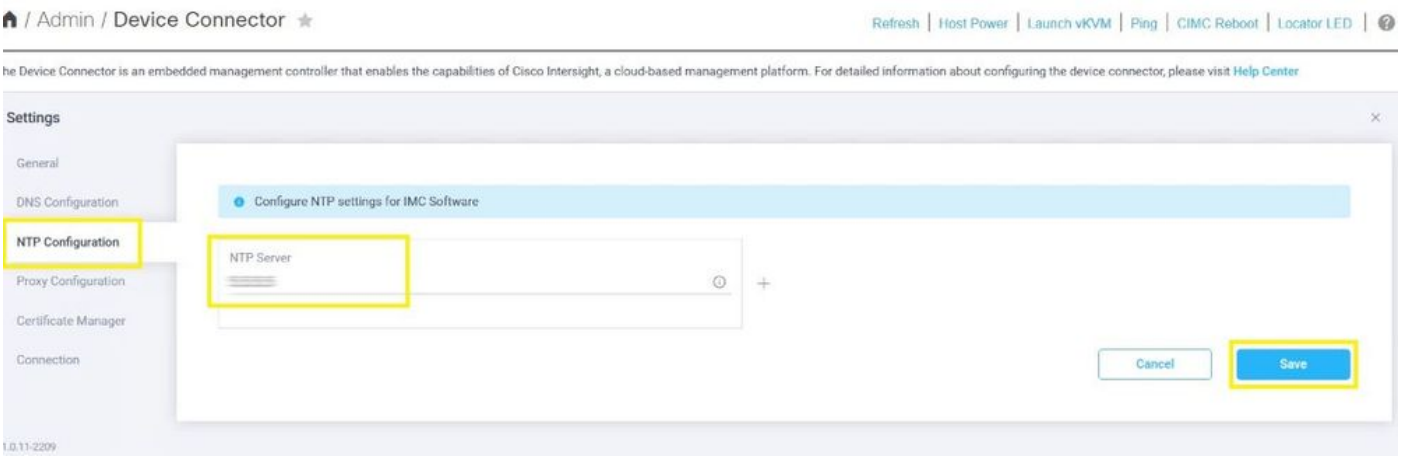




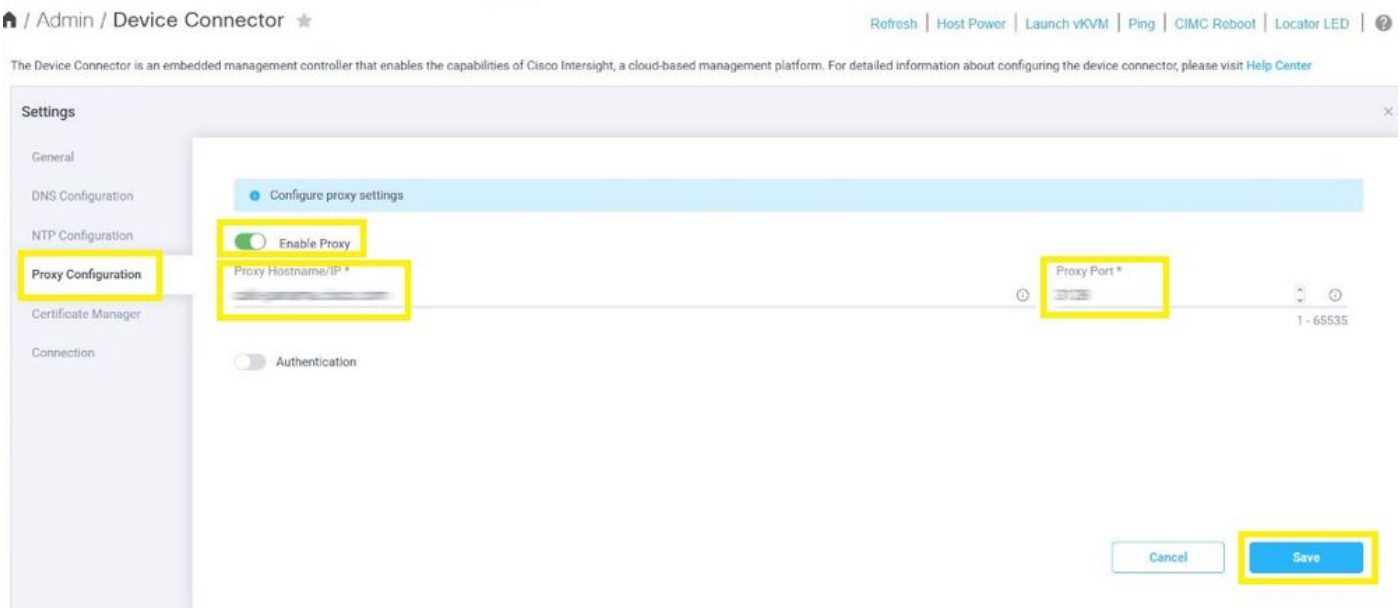
Paso 3.1. Acceda a **Admin > Device Connector > Settings > DNS Configuration** y configure el **DNS Server** y seleccione **Save** como se muestra en esta imagen.



Paso 3.2. Acceda a **Admin > Device Connector > Settings > NTP Configuration.** Configure el **NTP Server** por el entorno y seleccione **Save** como se muestra en esta imagen.

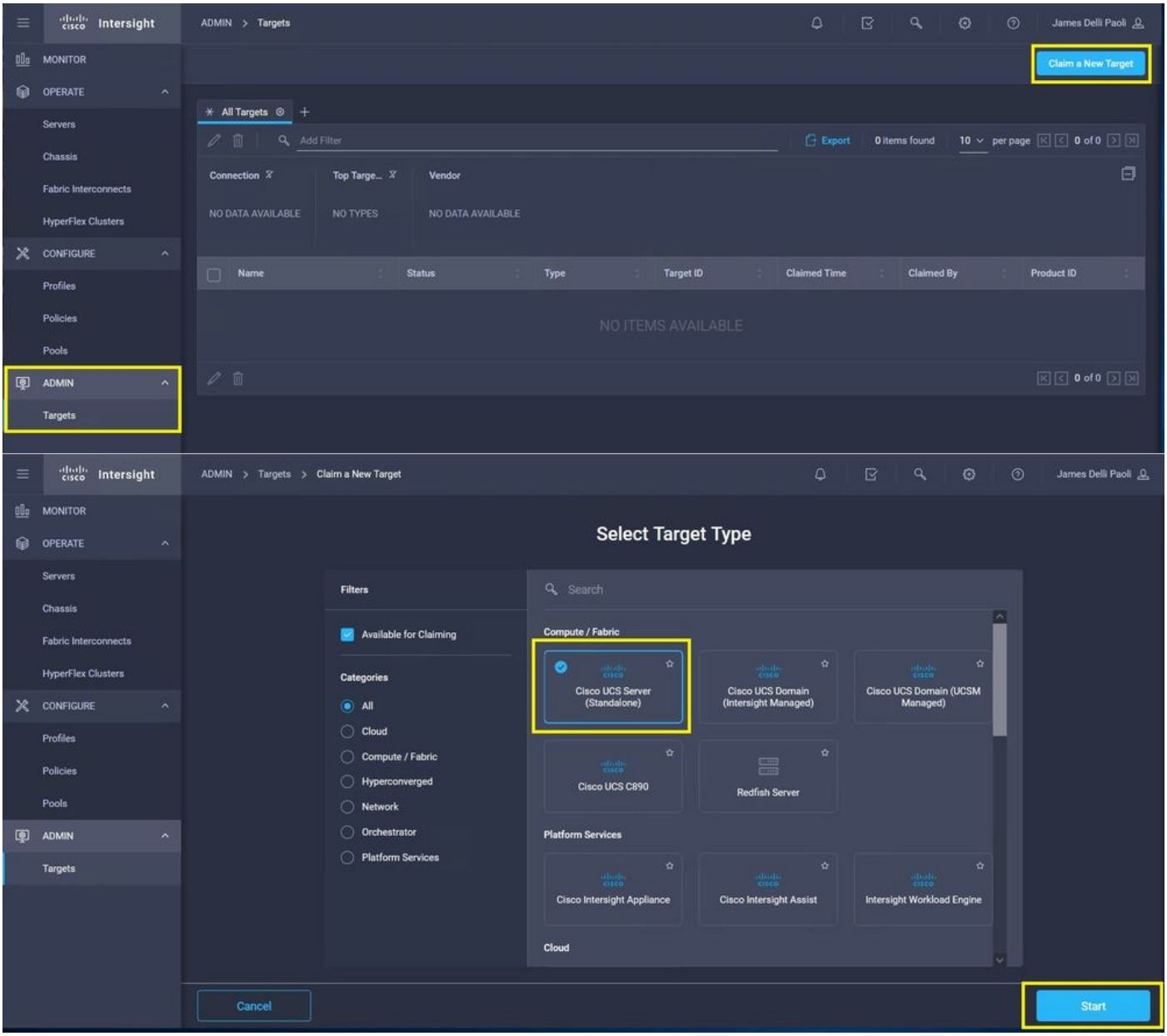


Paso 3.3. Configure opcionalmente un proxy si es necesario para alcanzar Cisco Intersight. Vaya a **Admin > Device Connector > Settings > Proxy Configuration > Enable Proxy.** Configure el **Proxy Hostname/IP** y el **Proxy Port** y seleccione **Save.**

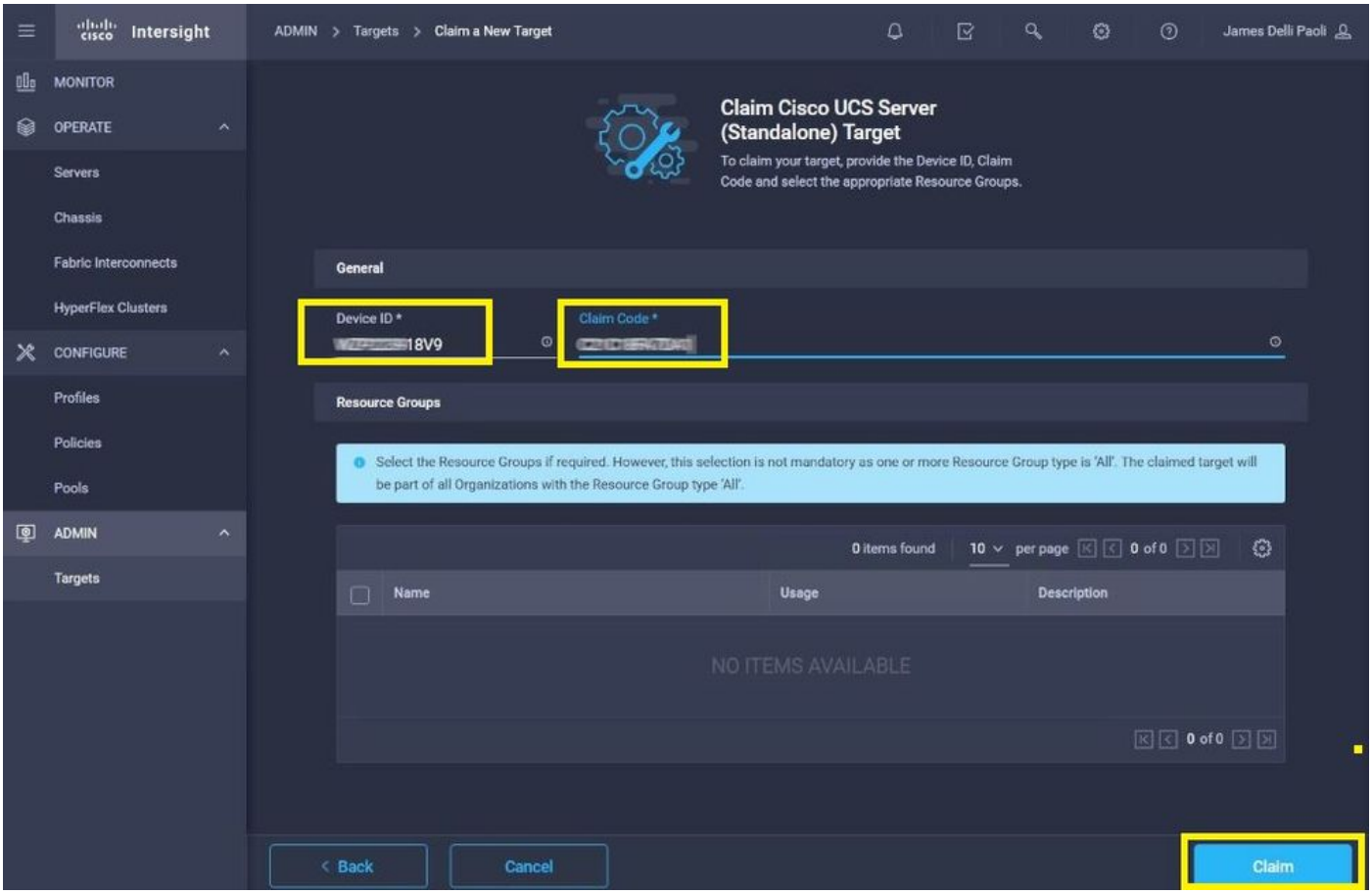


Paso 4. Seleccione **Admin > Device Connector** y copie el **Device ID** y **Claim Code**. Copie ambos a un bloc de notas o archivo de texto para su uso posterior.

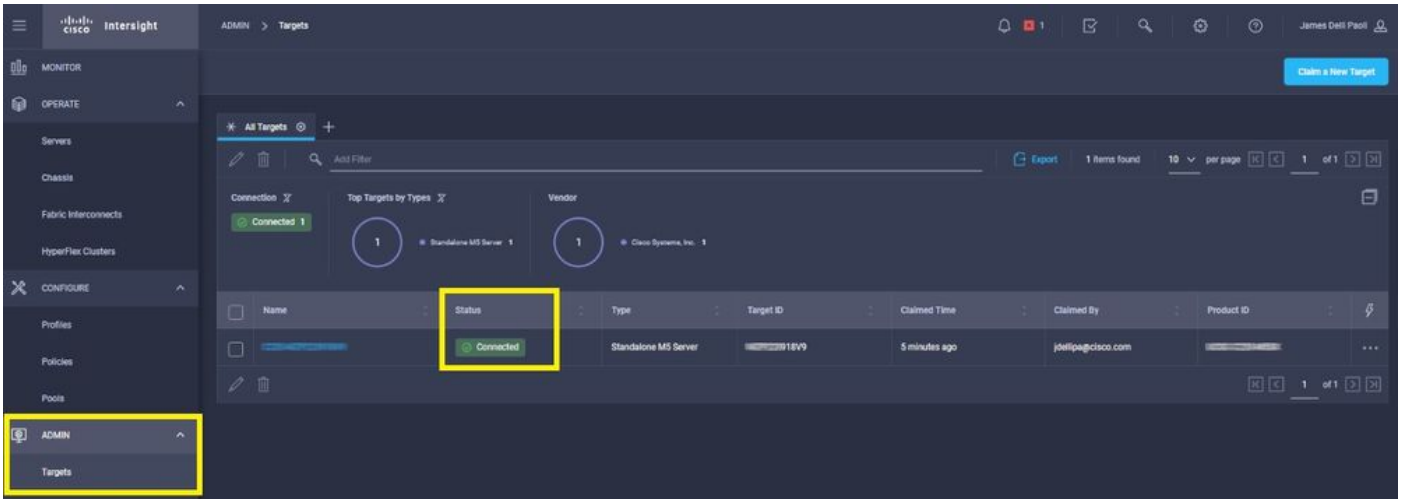
Paso 5. Inicie Cisco Intersight y navegue hasta **Admin > Targets > Claim a New Target > Cisco UCS Server (Standalone) > Start.** Escriba el **Device ID** y **Claim Code** que se copió de la GUI de CIMC y seleccione **Claim.**


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



Paso 6. Acceda a **Admin > Targets.** Una reclamación correcta muestra la **Status > Connected,** como se muestra en esta imagen.



Verificación básica para problemas de reclamación de dispositivos

Nota: Para obtener una lista completa de las condiciones de error y las remediaciones, consulte este enlace: [Condiciones de error del conector del dispositivo y pasos para remediar.]

Descripciones del estado de conexión del conector de dispositivo	Explicaciones del estado de conexión del conector de dispositivo	Posibles soluciones
Reclamado	La conexión a la plataforma Cisco	N/A

	Intersight se ha realizado correctamente y ha solicitado la conexión.	
No reclamado	La conexión a la plataforma Cisco Intersight se ha realizado correctamente, pero el terminal no se ha reclamado todavía.	Puede solicitar una conexión n reclamada a través de Cisco Intersight.
Administrativamente desactivado	Indica que el conector de dispositivo/administración de intersight se ha deshabilitado en el terminal.	Active el conector de dispositiv el terminal.
DNS mal configurado	DNS se ha configurado incorrectamente en CIMC o no se ha configurado en absoluto.	Indica que no se puede accede ninguno de los servidores de nombres DNS configurados en sistema. Compruebe que ha especificado direcciones IP vá para los servidores de nombre DNS.
Error de resolución de DNS de intersección	DNS está configurado pero no se puede resolver el nombre DNS de Intersight.	Consulte este enlace para ver Intersight está en mantenimien Estado de la entrevista. Si Inte está operativo, esto probablem indica que el nombre DNS del servicio Intersight no está resu
Error de red de conexión UCS	Indica las configuraciones de red no válidas.	Comprobar y confirmar: MTU e correcta de extremo a extremo permiten los puertos 443 y 80, firewall permite que todas las I físicas y virtuales, DNS y NTP configuren en el terminal.
Error de validación de certificado	El punto final rechaza establecer una conexión con la plataforma Cisco Intersight porque el certificado presentado por la plataforma Cisco Intersight no es válido.	Certificado caducado o aún no válido: Verifique que el NTP es configurado correctamente y q hora del dispositivo esté sincronizada con la hora unive coordinada. Verifique que DNS configurado correctamente. Si está utilizando un proxy web transparente, compruebe que certificado no ha caducado. El nombre de certificado prese por el servidor web no coincide el nombre DNS del servicio Intersight: Verifique que DNS e configurado correctamente. Póngase en contacto con el administrador del proxy web pa comprobar que el proxy web transparente está configurado correctamente. Específicamen nombre del certificado present por el proxy web debe coincidi el nombre DNS del servicio

	Intersight (svc.intersight.com). El certificado ha sido emitido p una entidad emisora de certific (CA) no fiable: Verifique que D esté configurado correctament Póngase en contacto con el administrador web o infosec pa comprobar que el proxy web transparente está configurado correctamente. Específicamen nombre del certificado present por el proxy web debe coincidi el nombre DNS del servicio Intersight.

Requisitos generales de conectividad de red de Cisco Intersight

- Se establece una conexión de red a la plataforma Intersight desde el conector de dispositivo del terminal
- Compruebe si se ha introducido un firewall entre el destino gestionado y Intersight o si han cambiado las reglas de un firewall actual. Esto podría causar problemas de conexión de extremo a extremo entre el terminal y Cisco Intersight. Si se cambian las reglas, asegúrese de que las reglas modificadas permiten el tráfico a través del firewall.
- Si utiliza un proxy HTTP para enrutar el tráfico fuera de las instalaciones y ha realizado cambios en la configuración del servidor proxy HTTP, asegúrese de cambiar la configuración del conector del dispositivo para reflejar los cambios. Esto es necesario porque Intersight no detecta automáticamente los servidores proxy HTTP.
- Configure DNS y resuelva el nombre DNS. El conector de dispositivo debe poder enviar solicitudes DNS a un servidor DNS y resolver registros DNS. El conector de dispositivo debe poder resolver svc.intersight.com en una dirección IP.
- Configure NTP y valide que la hora del dispositivo esté sincronizada correctamente con un servidor de hora.

Nota: Para obtener una lista completa de los requisitos de conectividad de la red Intersight, consulte los requisitos de conectividad de la red Intersight.

Información Relacionada

- Objetivos de la reclamación de Cisco Intersight Getting Started
- Sistemas compatibles con Cisco Intersight SaaS
- PID compatibles con Cisco Intersight SaaS
- Requisitos de conectividad de red de Cisco Intersight
- Vídeos de formación de Cisco Intersight
- Id. de error de Cisco CSCvw76806: un servidor independiente de la serie C puede no reclamarse correctamente en Cisco Intersight si su versión de conector de dispositivo es inferior a 1.0.9.
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).