Configurazione e richiesta di un server autonomo serie C in Intersight dopo la sostituzione della scheda madre

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Premesse](#)
[Problema: Il nuovo server RMA non è richiesto in Intersight e il server originale non funzionante è richiesto](#)
[Soluzione](#)
[Verifica di base per i problemi relativi alle attestazioni dei dispositivi](#)
[Requisiti generali di connettività di rete di Cisco Intersight](#)
[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare e richiedere un server serie C standalone in Cisco Intersight dopo la sostituzione della scheda madre.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Integrated Management Controller (CIMC)
- Cisco Intersight
- Cisco serie C Server

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Il presente documento può essere utilizzato anche per le seguenti versioni hardware e software:

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

> **Nota:** Per un elenco completo dei componenti hardware e software supportati, fare riferimento ai seguenti collegamenti: PID e sistemi supportati da Intersight supportati.

Premesse

- Il caso di utilizzo più comune per questo documento è quando una serie C è stata richiesta a Cisco Intersight e la scheda madre è stata sostituita da Return Material Authorization (RMA). Ogni volta che si verifica un'autorizzazione al reso (RMA), il server originale deve essere non richiesto e il nuovo server deve essere richiesto in Cisco Intersight.
- In questo documento si presume che il server serie C originale sia stato richiesto prima dell'autorizzazione al reso (RMA) della scheda madre e che non vi siano problemi di configurazione o di rete che potrebbero contribuire a un processo di richiesta non riuscito.
- Èpossibile annullare una richiesta di rimborso direttamente dal Cisco Intersight Portal o dal Device Connector dell'endpoint stesso. Si consiglia di annullare la richiesta di rimborso relativa agli oggetti dal Cisco Intersight Portal.
- Se un oggetto non viene richiesto direttamente dal connettore dei dispositivi e non dal portale Intersight, viene indicato come non richiesto all'interno di Cisco Intersight. Inoltre, l'endpoint deve essere annullato manualmente da Cisco Intersight.
- Èprobabile che lo stato del server originale serie C sia Non connesso in Cisco Intersight. Questa condizione può variare in base al motivo per cui la scheda madre deve essere sostituita.

Problema: Il nuovo server RMA non è richiesto in Intersight e il server originale non funzionante è richiesto

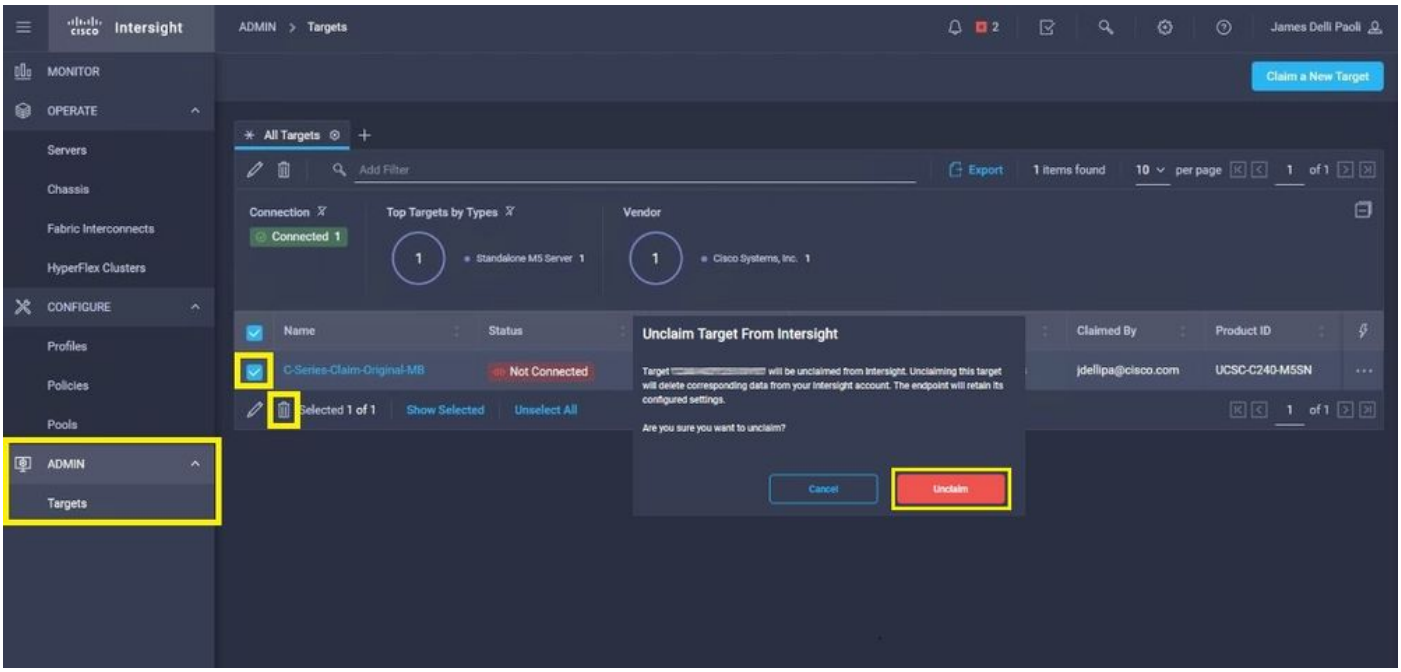
Se in Cisco Intersight è stato richiesto un server serie C standalone, il numero di serie del server (SN) viene associato a Cisco Intersight. Se il server richiesto richiede la sostituzione della scheda madre a causa di un guasto o per qualsiasi altra ragione, il server originale non deve essere richiesto e il nuovo server deve essere richiesto in Cisco Intersight. Il numero di serie C cambia con la scheda madre RMA.

Soluzione

Annullare la richiesta di sostituzione del server serie C di Cisco Intersight. Configurare i nuovi server CIMC e Device Connector, quindi richiedere il nuovo server a Cisco Intersight.

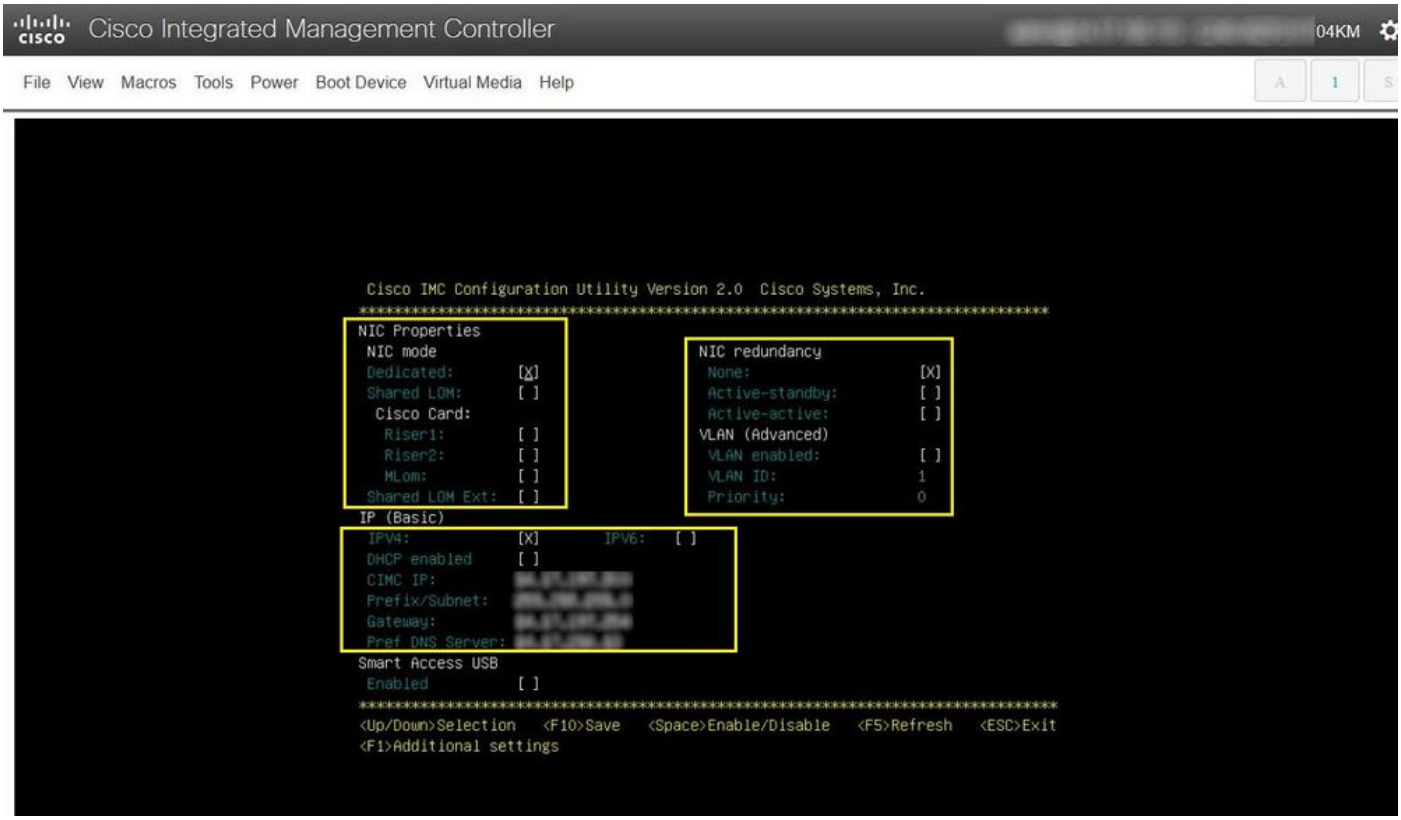
Passaggio 1. Avviare Cisco Intersight e fare clic su **Admin > Targets**. Selezionare la casella relativa alle destinazioni da sostituire e non richiedere e fare clic sul pulsante **Trash Can Icon > Unclaim** come

mostrato nell'immagine.



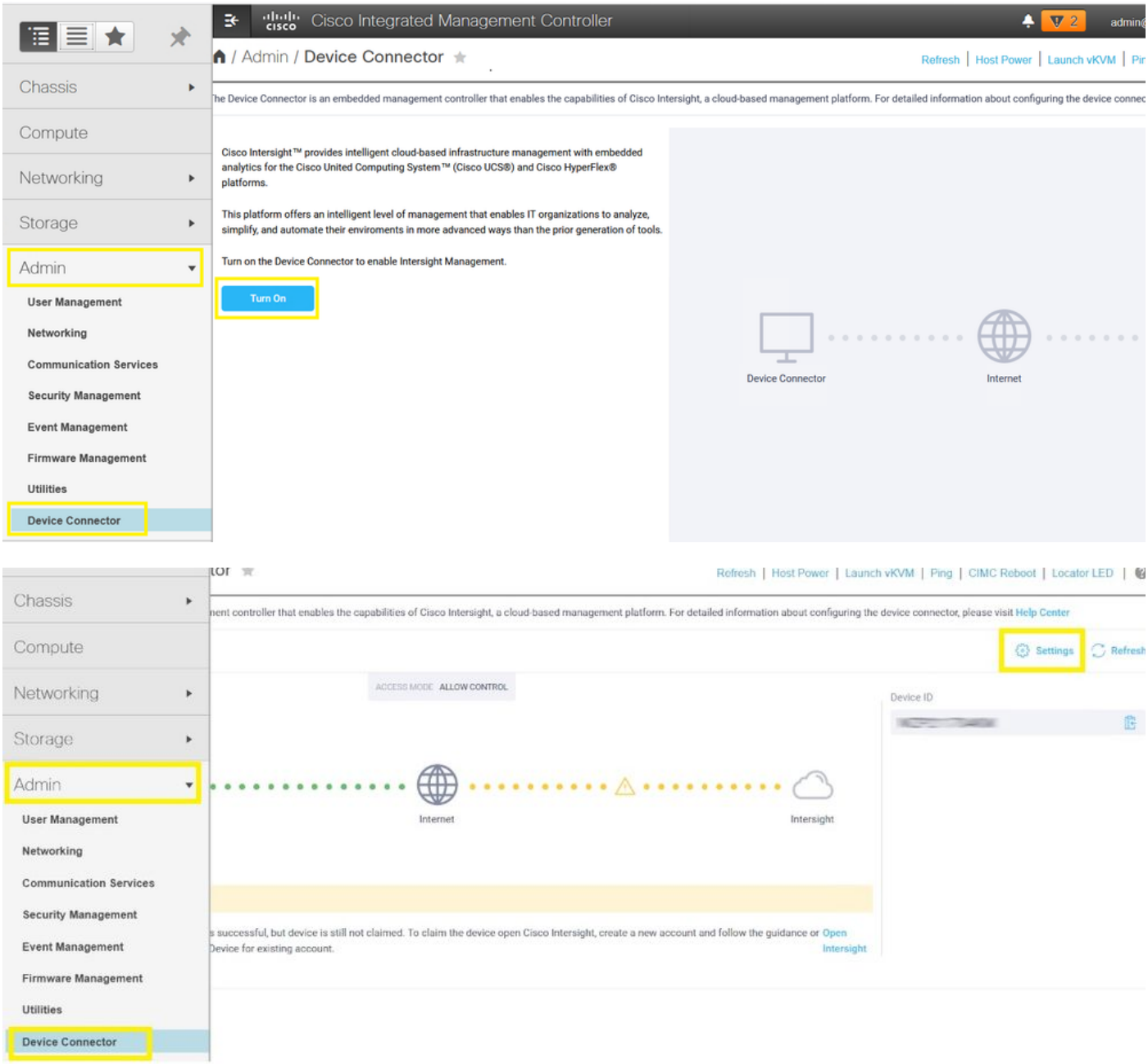
Passaggio 2. Collegare un KVM (Keyboard Video Monitor) al server appena sostituito (ignorare questo passaggio se CIMC è già stato configurato). Nella schermata iniziale di Cisco all'avvio, selezionare **F8** per configurare CIMC. Configurare il **Network Interface Card (NIC) Properties** per il vostro ambiente e premere **F10** a **Save**. Inserire i cavi fisici del server e del relativo dispositivo collegato in base al **NIC Properties** utilizzati per la gestione.

> **Nota:** Passaggio 2. illustra e descrive un'installazione locale del CIMC con un KVM collegato direttamente a un C240-M5. L'installazione iniziale del CIMC può essere eseguita anche in remoto con DHCP. Consultare la Guida all'installazione appropriata per il proprio modello di server e scegliere la configurazione CIMC iniziale più adatta alle proprie esigenze.

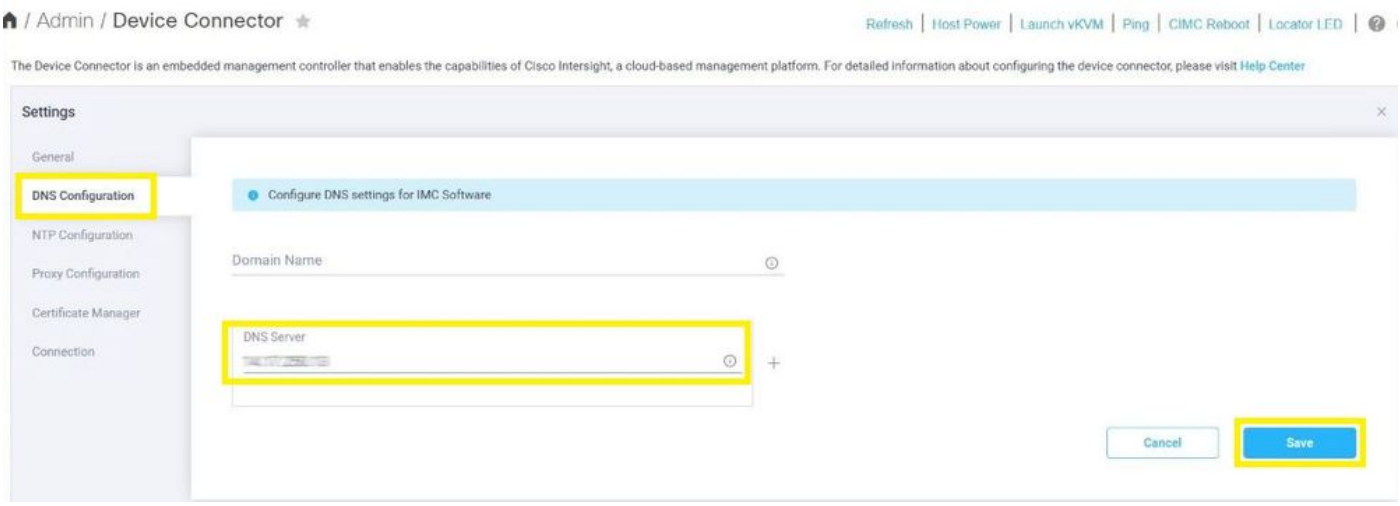


Passaggio 3. Avviare l'interfaccia grafica dell'utente (GUI) CIMC e passare a **Admin > Device Connector**. Se **Device Connector** è disattivato, scegliere **Turn On**. Una volta abilitato, selezionare **Settings**.

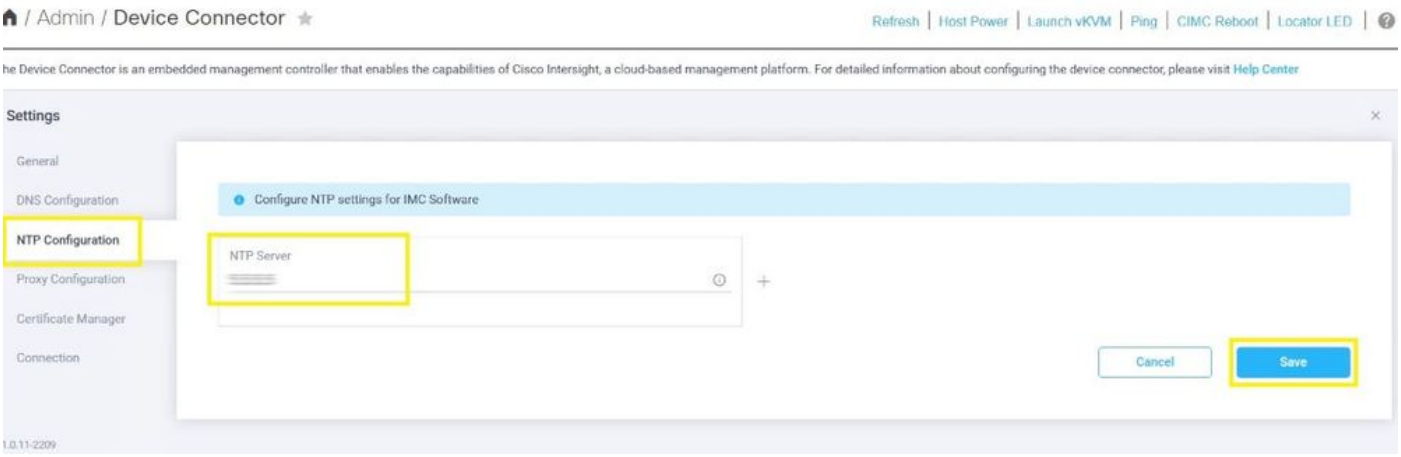
> **Suggerimento**: Nell'interfaccia utente di CIMC, selezionare **Chassis > Summary** e confronta **Firmware Version** per verificare che i requisiti minimi del firmware siano soddisfatti da Cisco Intersight. Utilizzare questo collegamento per verificare i requisiti minimi per il modello di server specifico: Sistemi supportati da Intersight. Se il firmware non soddisfa i requisiti minimi per la richiesta, eseguire una utility di aggiornamento dell'host (HUU) sul server, vedere qui: Processo di Cisco Host Upgrade Utility.



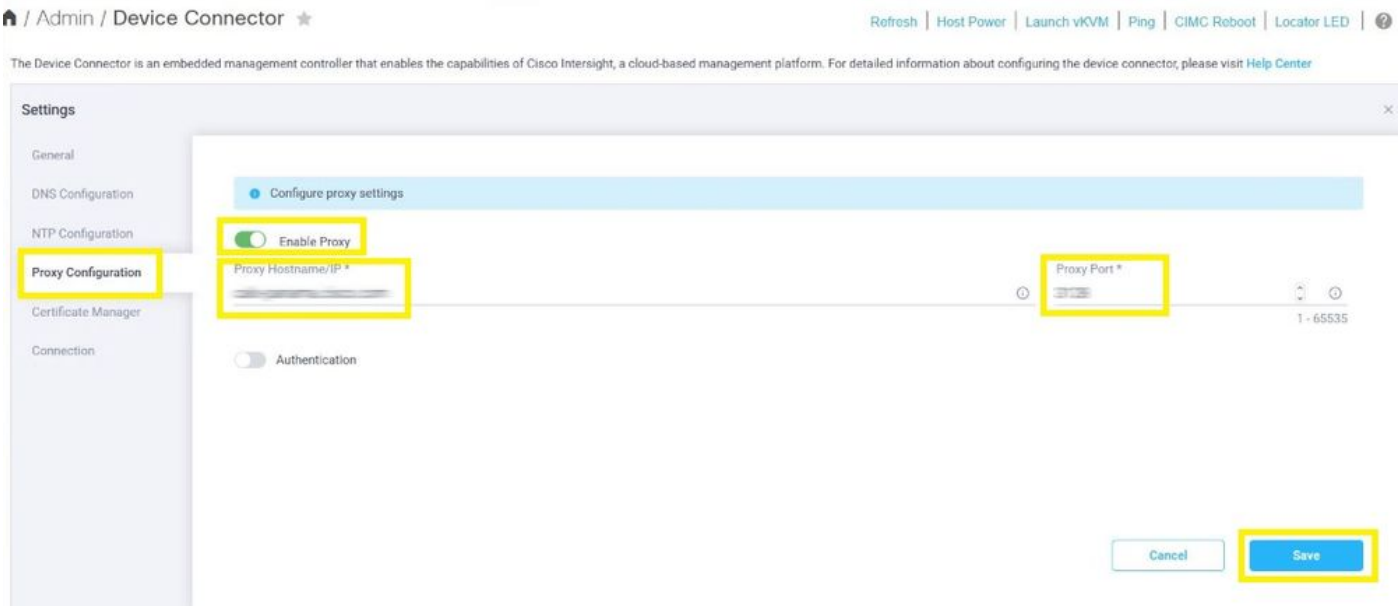
Passaggio 3.1. Passare a **Admin > Device Connector > Settings > DNS Configuration** e configurare il **DNS Server** e selezionare **Save** come mostrato nell'immagine.



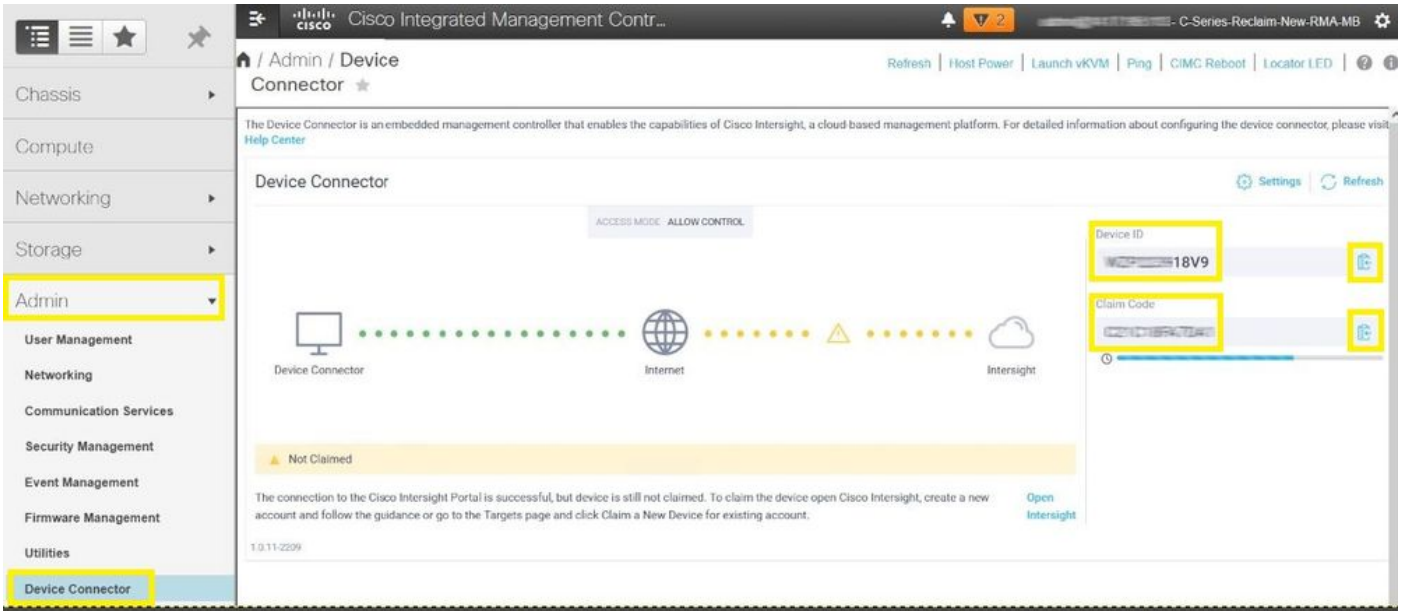
Passaggio 3.2. Passare a **Admin > Device Connector > Settings > NTP Configuration.** Configurare **NTP Server** in base all'ambiente e selezionare **Save** come mostrato nell'immagine.



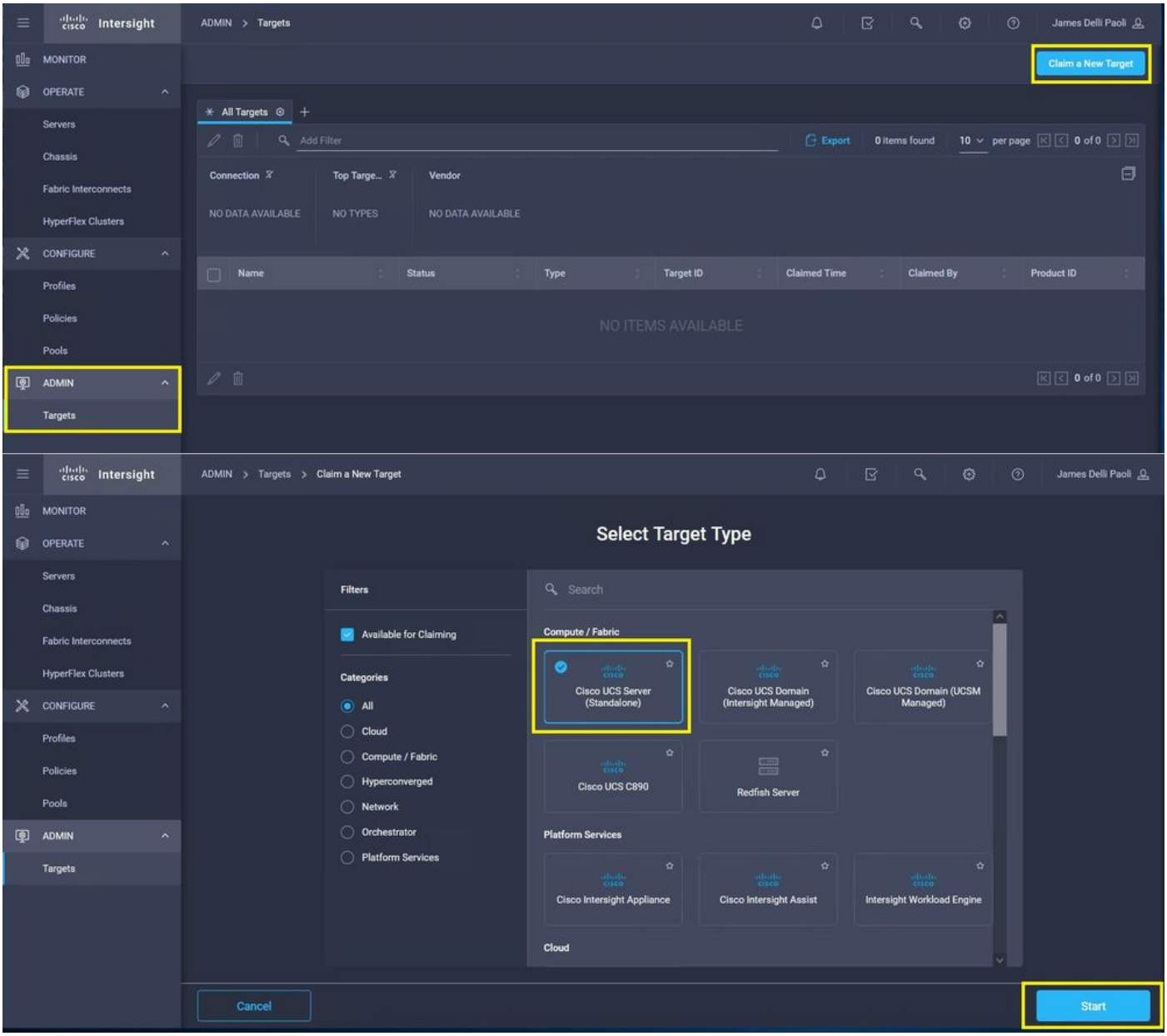
Passaggio 3.3. Facoltativamente, configurare un proxy se necessario per raggiungere Cisco Intersight. Passa a **Admin > Device Connector > Settings > Proxy Configuration > Enable Proxy.** Configurare **Proxy Hostname/IP** e **Proxy Port** e selezionare **Save.**

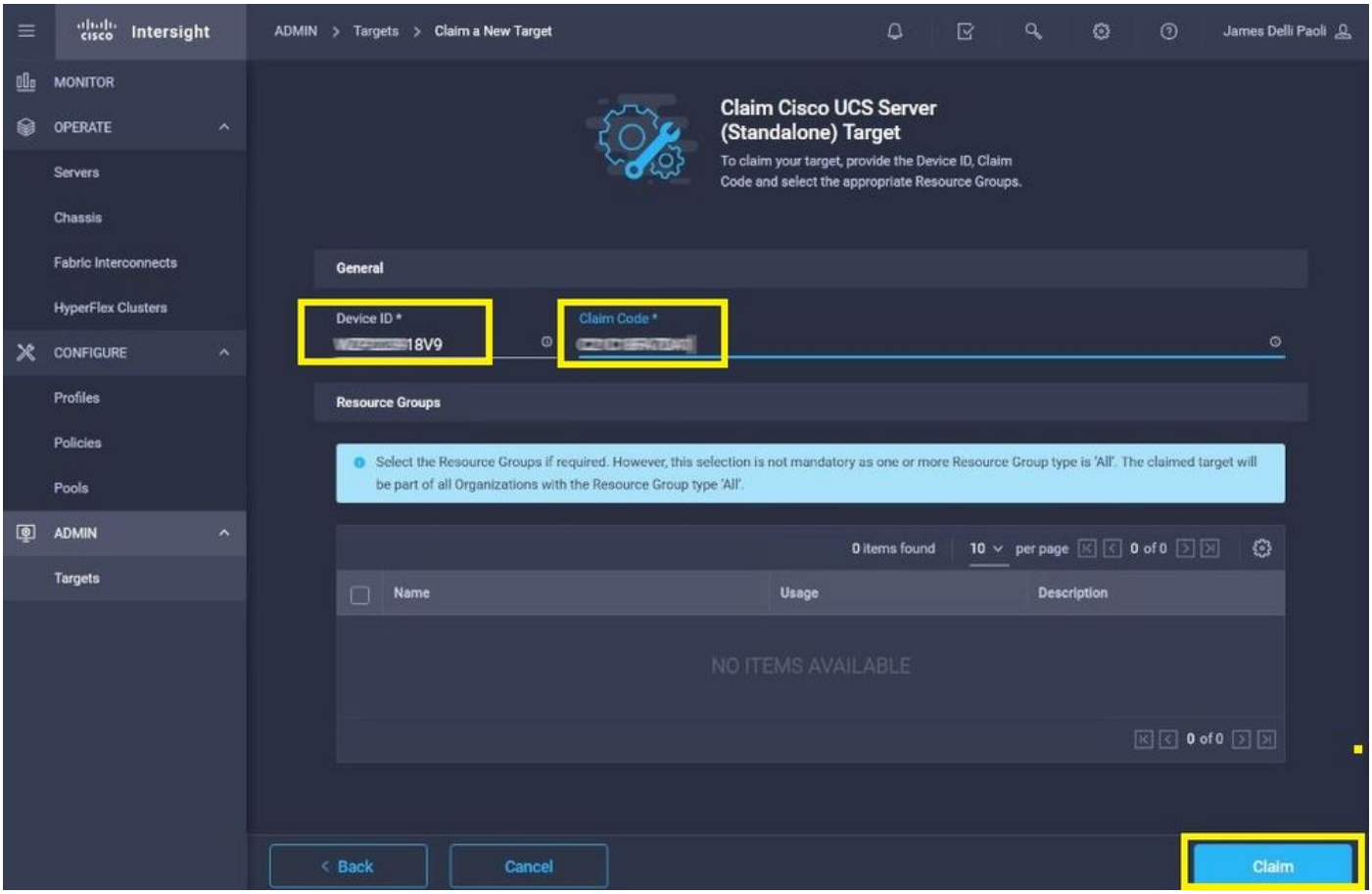


Passaggio 4. Selezione **Admin > Device Connector** e copiare **Device ID** e **Claim Code.** Copiare entrambi in un blocco note o in un file di testo per un utilizzo successivo.

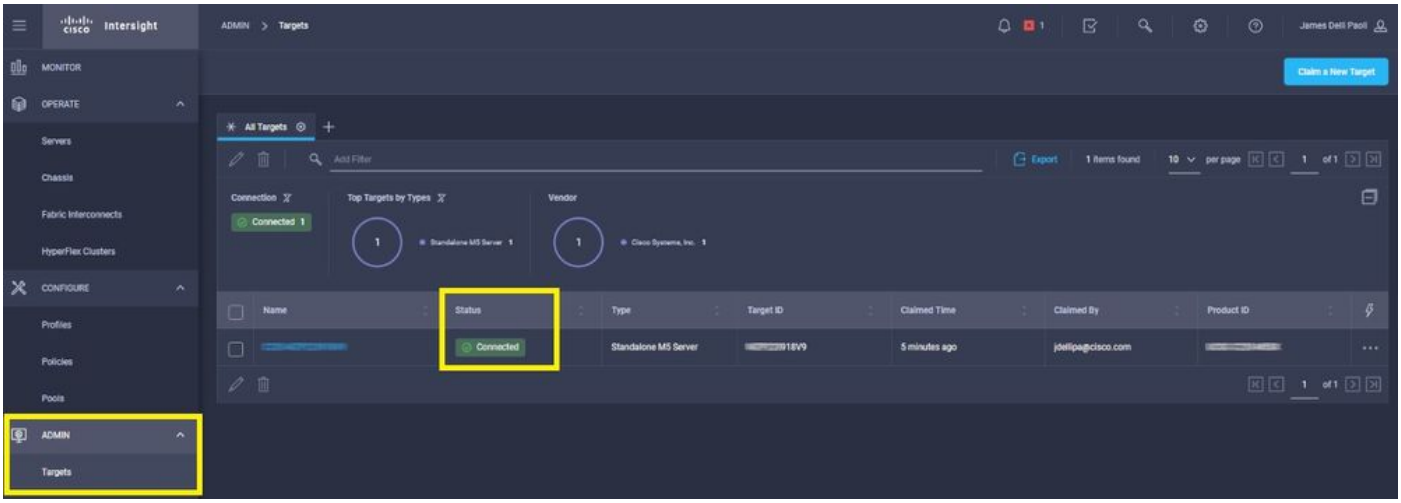


Passaggio 5. Avviare Cisco Intersight e passare a **Admin > Targets > Claim a New Target > Cisco UCS Server (Standalone) > Start.** Immettere il **Device ID** e **Claim Code** copiato dall'interfaccia grafica CIMC e selezionare **Claim.**





Passaggio 6. Passare a **Admin > Targets.** Una domanda accolta dimostra **Status > Connected,** come mostrato nell'immagine.



Verifica di base per i problemi relativi alle attestazioni dei dispositivi

Nota: Per un elenco completo delle condizioni di errore e delle azioni correttive, fare riferimento a questo collegamento: Condizioni di errore e azioni correttive di Device Connector.

Descrizioni dello stato della connessione a Device Connector	Spiegazioni sullo stato della connessione del connettore del dispositivo	Possibili rimedi

Richiesto	La connessione alla piattaforma Cisco Intersight è riuscita e la connessione è stata richiesta.	N/D
Non richiesto	La connessione alla piattaforma Cisco Intersight è riuscita, ma non è ancora possibile richiedere l'endpoint.	Èpossibile richiedere una connessione non richiesta tram Cisco Intersight.
Disattivato a livello amministrativo	Indica che Intersight Management/Device Connector è stato disabilitato sull'endpoint.	Abilitare Device Connector sull'endpoint.
Configurazione errata di DNS	Il DNS è stato configurato in modo errato in CIMC o non è stato configurato affatto.	Indica che nessuno dei server nomi DNS configurati nel siste raggiungibile. Verificare di aver immesso indirizzi IP validi per i server dei nomi DNS.
Errore di risoluzione DNS Intersight	Il DNS è configurato ma non è in grado di risolvere il nome DNS di Intersight.	Controllare questo collegamen verificare se Intersight è in manutenzione: Stato Intersight Intersight è operativo, è probab che il nome DNS del servizio Intersight non venga risolto.
Errore di rete della connessione UCS	Indica le configurazioni di rete non valide.	Verifica e conferma: L'MTU è corretta da end-to-end, le porte e 80 sono consentite, il firewall consente tutti gli IP fisici e virtu DNS e il NTP sono configurati sull'endpoint.
Errore di convalida del certificato	L'endpoint rifiuta di stabilire una connessione alla piattaforma Cisco Intersight perché il certificato presentato dalla piattaforma Cisco Intersight non è valido.	Certificato scaduto o non anco valido: Verificare che il protocol NTP sia configurato correttame che l'ora del dispositivo sia sincronizzata con l'ora UTC (Coordinated Universal Time). Verificare che DNS sia configu correttamente. Se è in uso un p Web trasparente, verificare che certificato non sia scaduto. Il nome del certificato presenta server Web non corrisponde al nome DNS del servizio Intersig Verificare che DNS sia configu correttamente. Contattare l'amministratore del proxy Web verificare che il proxy Web trasparente sia configurato correttamente. In particolare, il nome del certificato presentato proxy Web deve corrispondere nome DNS del servizio Intersig (svc.intersight.com). Il certificato è stato rilasciato da un'Autorità di certificazione (CA attendibile: Verificare che DNS

configurato correttamente. Contattare l'amministratore We infosec per verificare che il pro Web trasparente sia configurat correttamente. In particolare, il nome del certificato presentato proxy Web deve corrispondere nome DNS del servizio Intersig

Requisiti generali di connettività di rete di Cisco Intersight

- Una connessione di rete alla piattaforma Intersight viene stabilita dal connettore dispositivo nell'endpoint
- Verificare se tra la destinazione gestita e Intersight è stato introdotto un firewall o se le regole per un firewall corrente sono state modificate. Ciò potrebbe causare problemi di connessione end-to-end tra l'endpoint e Cisco Intersight. Se le regole vengono modificate, verificare che le regole modificate consentano il traffico attraverso il firewall.
- Se si utilizza un proxy HTTP per instradare il traffico fuori dalla sede e sono state apportate modifiche alla configurazione del server proxy HTTP, assicurarsi di modificare la configurazione del connettore del dispositivo per riflettere le modifiche. Questa operazione è necessaria perché Intersight non rileva automaticamente i server proxy HTTP.
- Configurare DNS e risolvere il nome DNS. Il connettore dispositivo deve essere in grado di inviare richieste DNS a un server DNS e di risolvere i record DNS. Device Connector deve essere in grado di risolvere svc.intersight.com in un indirizzo IP.
- Configurare NTP e verificare che l'ora del dispositivo sia sincronizzata correttamente con un server di riferimento orario.

Nota: Per un elenco completo dei requisiti di connettività di Intersight, fare riferimento ai requisiti di connettività di Intersight Network.

Informazioni correlate

- Destinazioni delle richieste di rimborso Getting Started di Cisco Intersight
- Sistemi supportati da Cisco Intersight SaaS
- PID supportati da Cisco Intersight SaaS
- Requisiti di connettività di rete di Cisco Intersight
- Video di formazione Cisco Intersight
- ID bug Cisco CSCvw76806 - Un server standalone serie C non può inviare correttamente la richiesta di assistenza in Cisco Intersight se la versione del connettore del dispositivo è inferiore a 1.0.9.
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).