Configuration et demande d'un serveur C autonome dans Intersight après le remplacement de la carte mère

Table des matières

Introduction

Ce document décrit comment configurer et revendiquer un serveur C-Series autonome dans Cisco Intersight après le remplacement de la carte mère.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Contrôleur de gestion intégré Cisco (CIMC)
- Cisco Intersight
- Serveurs Cisco série C

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Produits connexes

Ce document peut également être utilisé avec les versions de matériel et de logiciel suivantes :

- Série C M4 3.0(4) et versions ultérieures
- Série C M5 3.1 et versions ultérieures
- Série C M6 4.2 et versions ultérieures
- Série S M5 4.0(4e) et versions ultérieures

Remarque : pour obtenir une liste complète du matériel et des logiciels pris en charge, reportez-vous aux liens suivants : PID pris en charge par Intersight et Systèmes pris en charge par Intersight.

Informations générales

- L'exemple d'utilisation le plus courant de ce document est lorsqu'une série C a été réclamée à Cisco Intersight et que la carte mère est remplacée par une autorisation de retour de matériel (RMA). Chaque fois qu'une RMA se produit, le serveur d'origine doit être annulé et le nouveau serveur doit être réclamé dans Cisco Intersight.
- Ce document suppose que le serveur C-Series d'origine a été revendiqué avec succès avant la RMA de la carte mère, et qu'il n'y a aucun problème de configuration ou de réseau qui pourrait contribuer à un processus de revendication défaillant.
- Vous pouvez annuler la revendication de cibles directement à partir du portail Cisco Intersight ou du connecteur de périphérique du point d'extrémité lui-même. Il est recommandé d'annuler la revendication de cibles à partir du portail Cisco Intersight.
- Si une cible n'est pas réclamée directement à partir de son connecteur de périphérique et non du portail Intersight, elle est affichée comme non réclamée dans Cisco Intersight. Le point de terminaison doit également être retiré manuellement de Cisco Intersight.
- Le serveur C-Series d'origine affiche probablement l'état Non connecté dans Cisco Intersight. Cela peut varier en fonction de la raison pour laquelle la carte mère doit être remplacée.

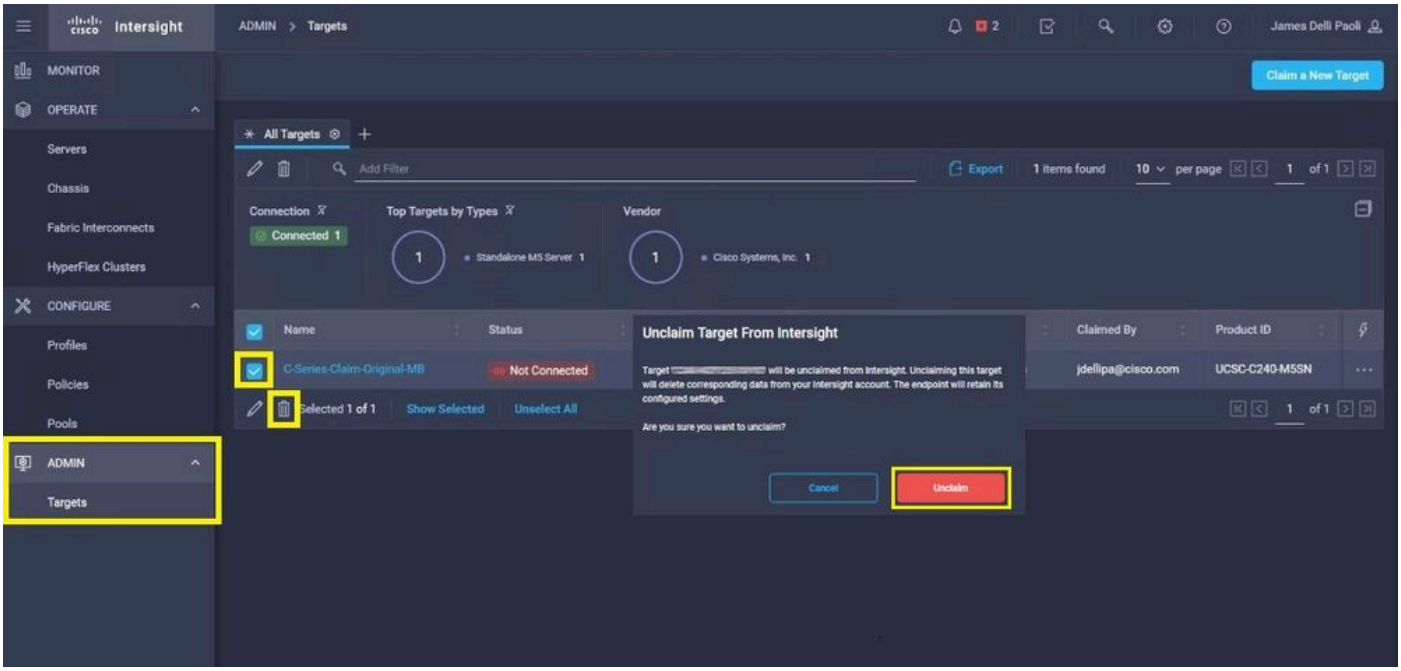
Problème : le nouveau serveur RMA n'est pas réclamé dans Intersight et le serveur défaillant d'origine est réclamé

Si un serveur C autonome a été revendiqué dans Cisco Intersight, le numéro de série du serveur (SN) est associé à Cisco Intersight. Si le serveur revendiqué nécessite un remplacement de carte mère en raison d'une défaillance ou pour toute autre raison, le serveur d'origine doit être annulé et le nouveau serveur doit être réclamé dans Cisco Intersight. Le numéro de série C change en fonction de la carte mère RMA.

Solution

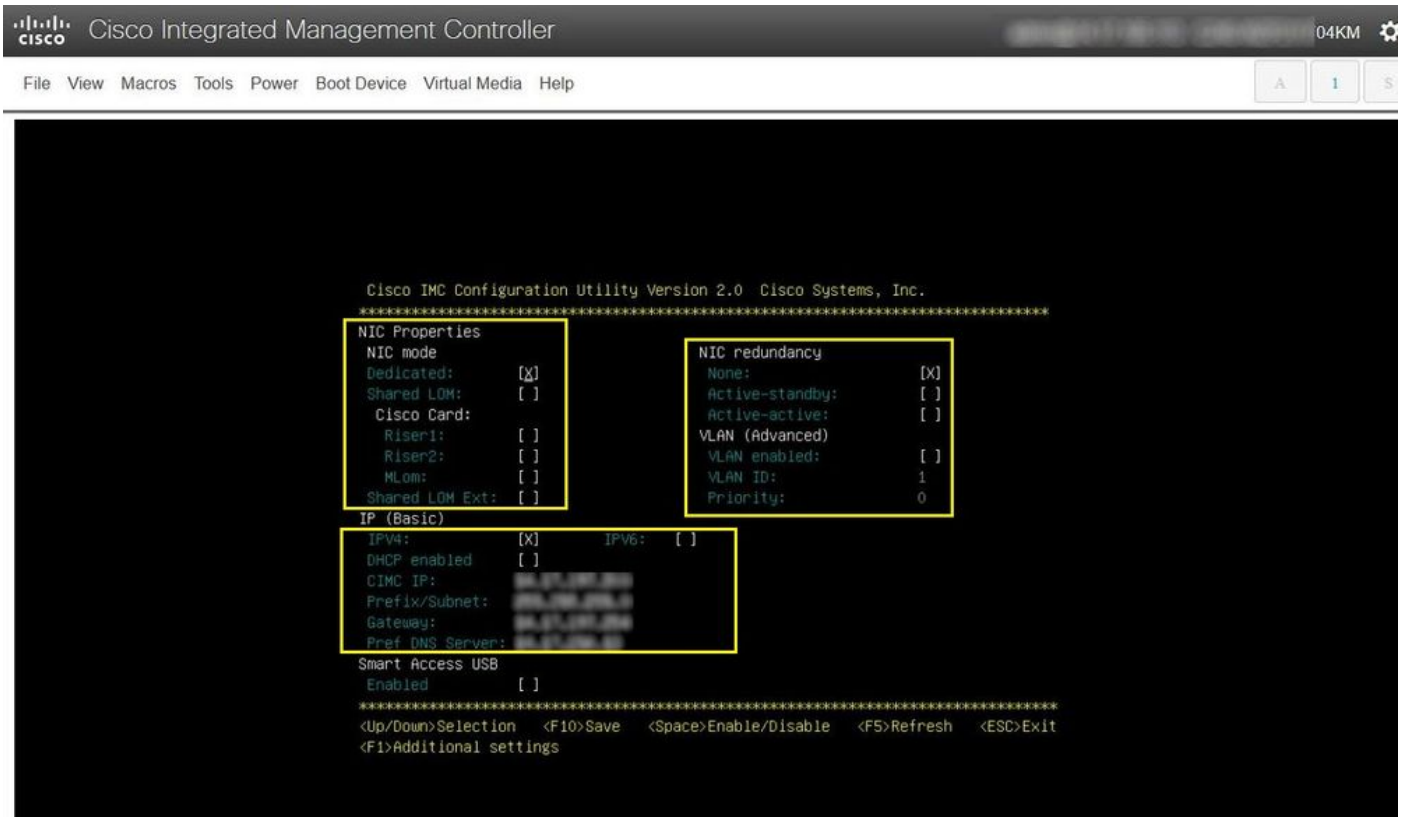
Ne réclamez pas le serveur de la gamme C de Cisco Intersight qui doit être remplacé. Configurez les nouveaux serveurs CIMC et Connecteur de périphérique, et Demandez le nouveau serveur à Cisco Intersight.

Étape 1. Lancez Cisco Intersight et cliquez sur **Admin** > **Targets**. Sélectionnez la case correspondant aux cibles à remplacer et à ne pas réclamer, puis cliquez sur le bouton, **Trash Can Icon** > **Unclaim** comme illustré dans cette image.



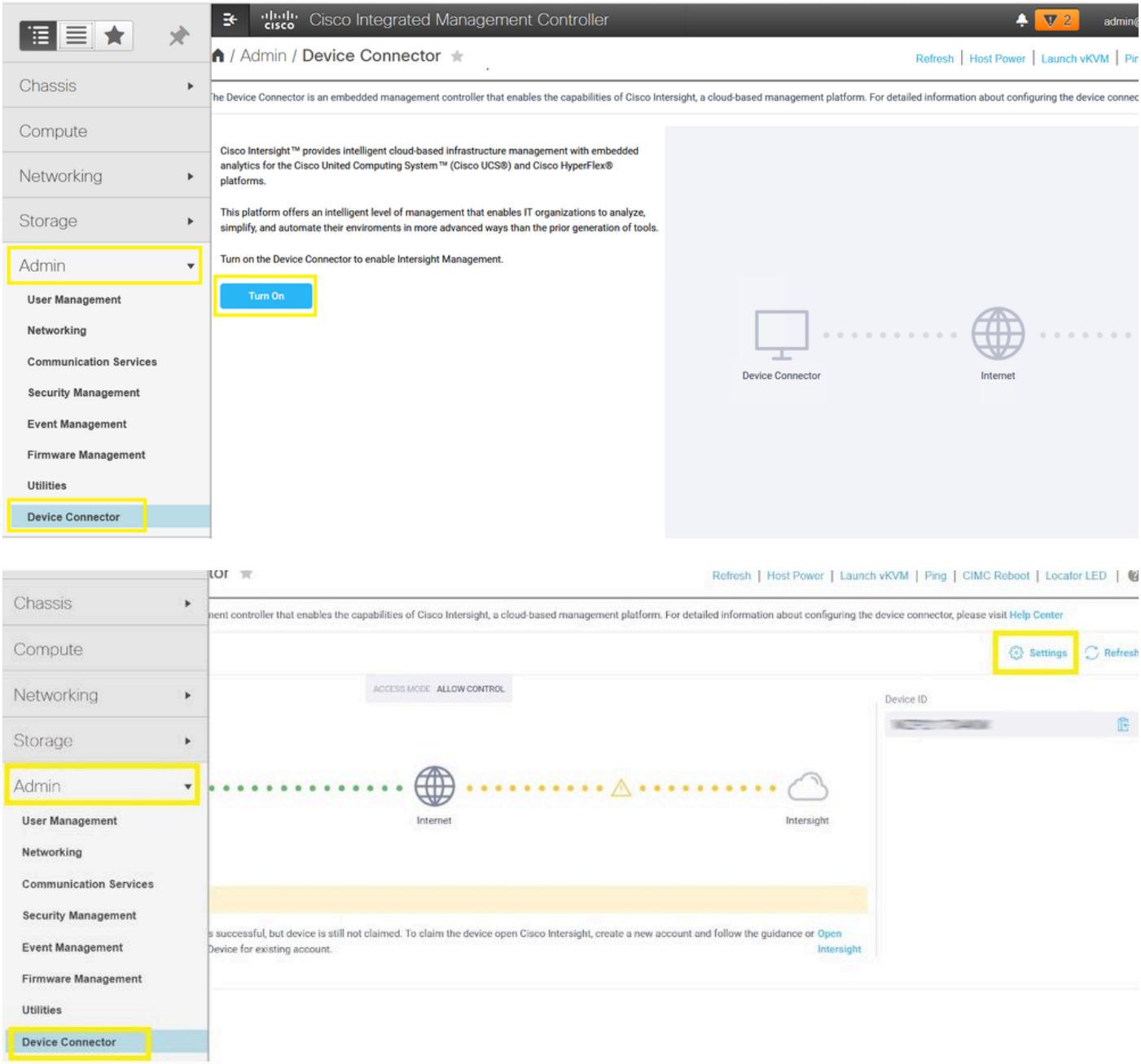
Étape 2. Connectez un moniteur KVM (Keyboard Video Monitor) au nouveau serveur remplacé (ignorez cette étape si CIMC a déjà été configuré). Dans l'écran d'accueil de Cisco au démarrage, sélectionnez **F8** pour configurer CIMC. Configurez le approprié **Network Interface Card (NIC) Properties** à votre environnement et appuyez sur **F10** pour **Save**. Insérer des câbles physiques au serveur et à son périphérique connecté en fonction de la configuration **NIC Properties** utilisée pour la gestion.

Remarque : l'étape 2 illustre et décrit une configuration locale du CIMC avec un KVM connecté directement à un C240-M5. La configuration CIMC initiale peut également être effectuée à distance avec DHCP. Référez-vous au guide d'installation approprié à votre modèle de serveur et choisissez la configuration CIMC initiale qui vous convient le mieux.

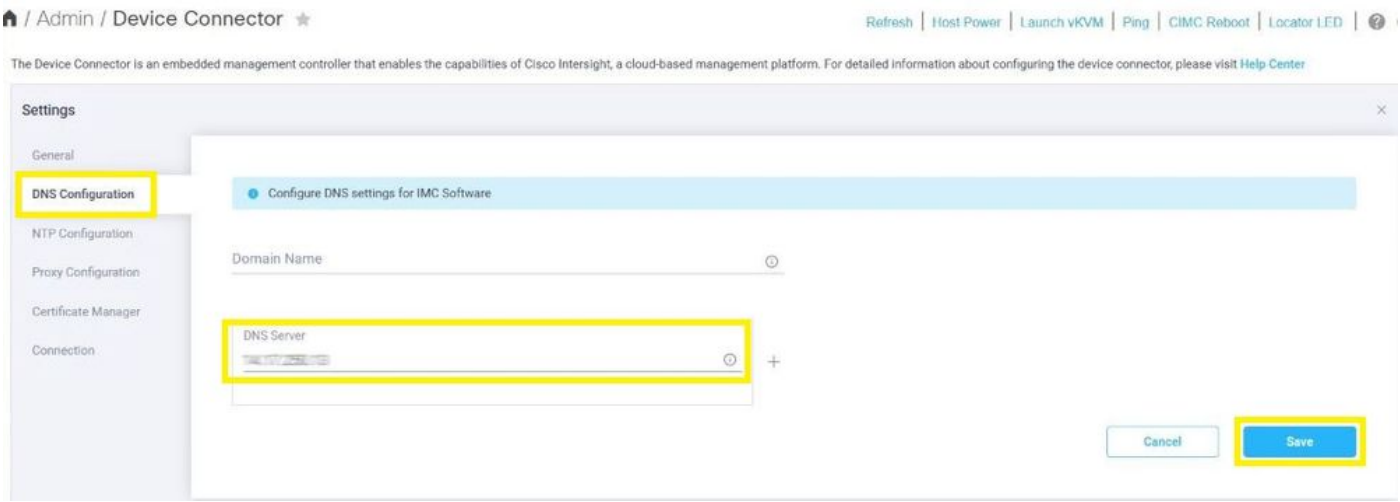


Étape 3. Lancez l'interface utilisateur graphique CIMC et accédez à **Admin** > **Device Connector.** Si **Device Connector** est désactivé, choisissez **Turn On.** Une fois activé, sélectionnez **Settings.**

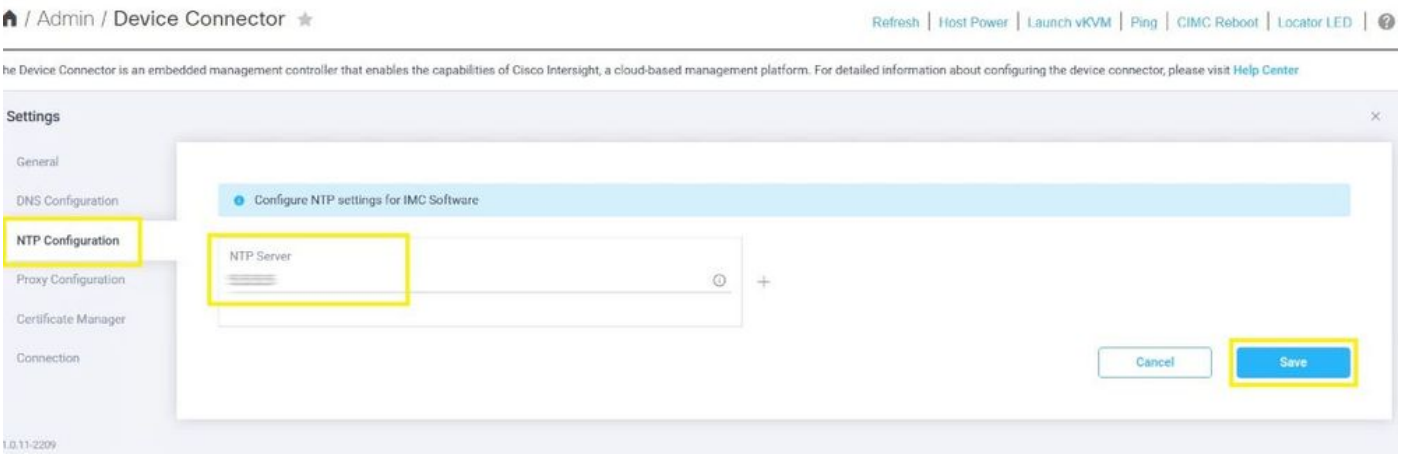
Conseil : dans l'interface utilisateur graphique de CIMC, naviguez jusqu'à **Chassis** > **Summary** et comparez les **Firmware Version** pour confirmer que la configuration minimale requise pour le micrologiciel est respectée et que Cisco Intersight la demande. Utilisez ce lien pour vérifier la configuration minimale requise pour votre modèle de serveur spécifique : Intersight Supported Systems. Si le microprogramme ne répond pas à la configuration minimale requise à revendiquer, exécutez un utilitaire de mise à niveau de l'hôte (HUU) sur le serveur, voir ici : Processus de l'utilitaire de mise à niveau de l'hôte Cisco.



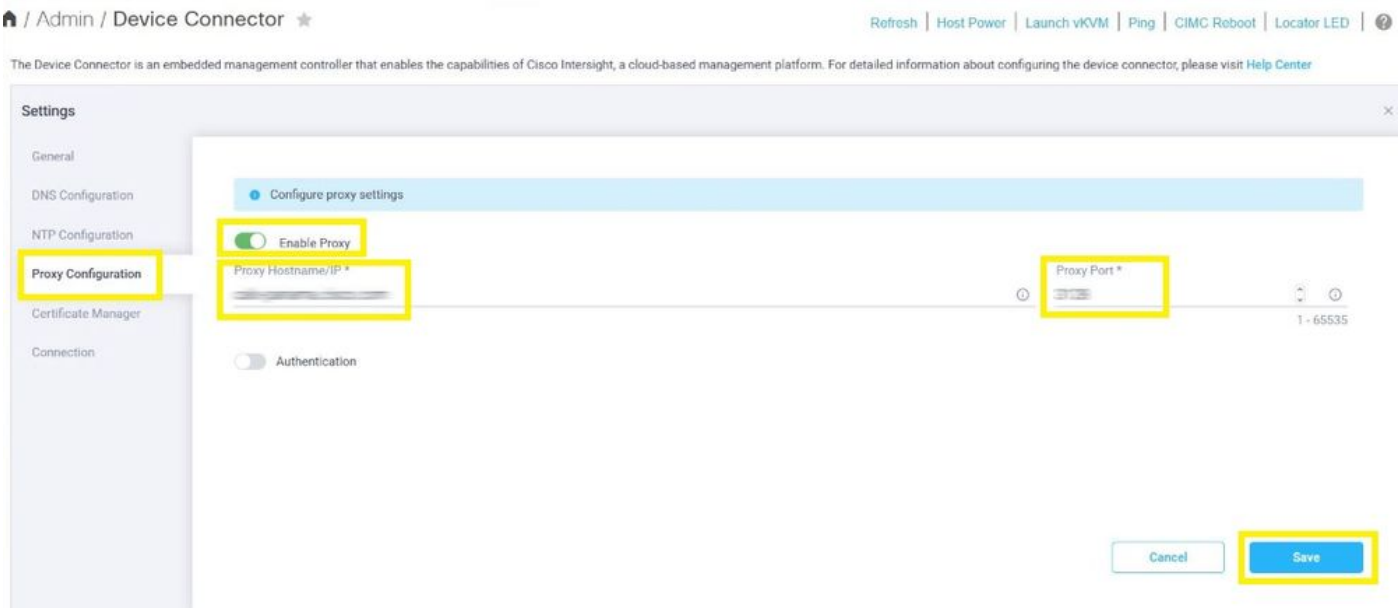
Étape 3.1. Naviguez jusqu'**Admin** > **Device Connector** > **Settings** > **DNS Configuration**à et configurez le **DNS Server** et sélectionnez **Save** comme indiqué dans cette image.



Étape 3.2. Naviguez jusqu'à **Admin** > **Device Connector** > **Settings** > **NTP Configuration.** Configure the **NTP Server** address per the environment et sélectionnez **Save** comme indiqué dans cette image.

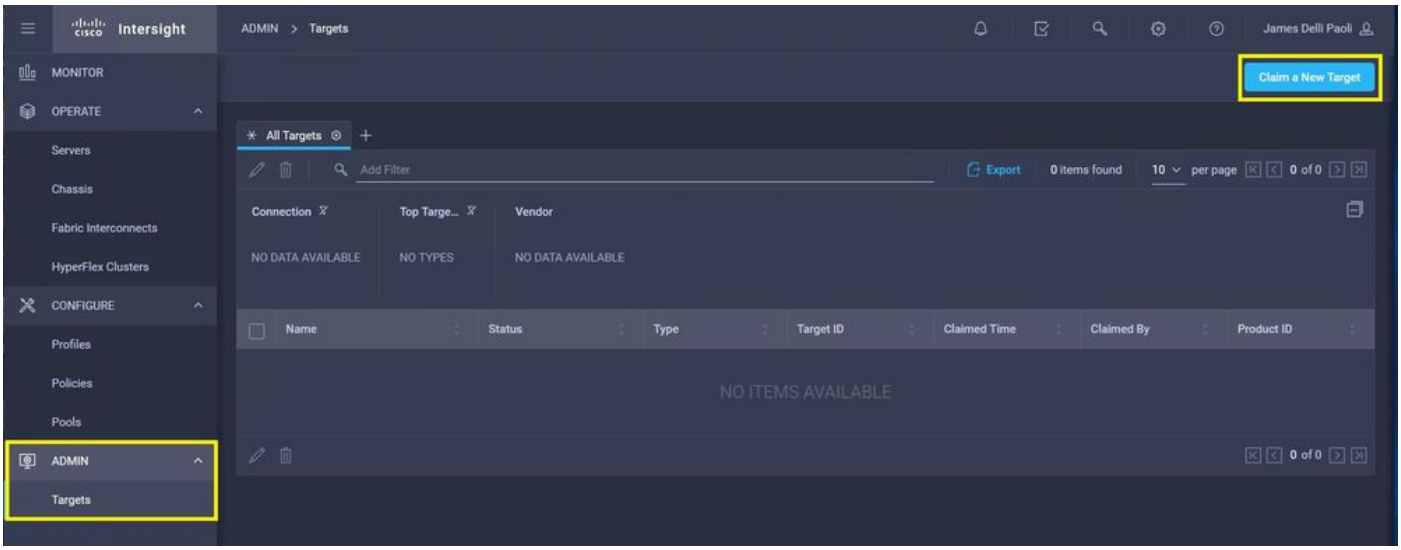


Étape 3.3. Si nécessaire, configurez un proxy pour accéder à Cisco Intersight. Naviguez jusqu'à **Admin** > **Device Connector** > **Settings** > **Proxy Configuration** > **Enable Proxy.** Configurer le **Proxy Hostname/IP** et le **Proxy Port** , puis sélectionnez **Save.**



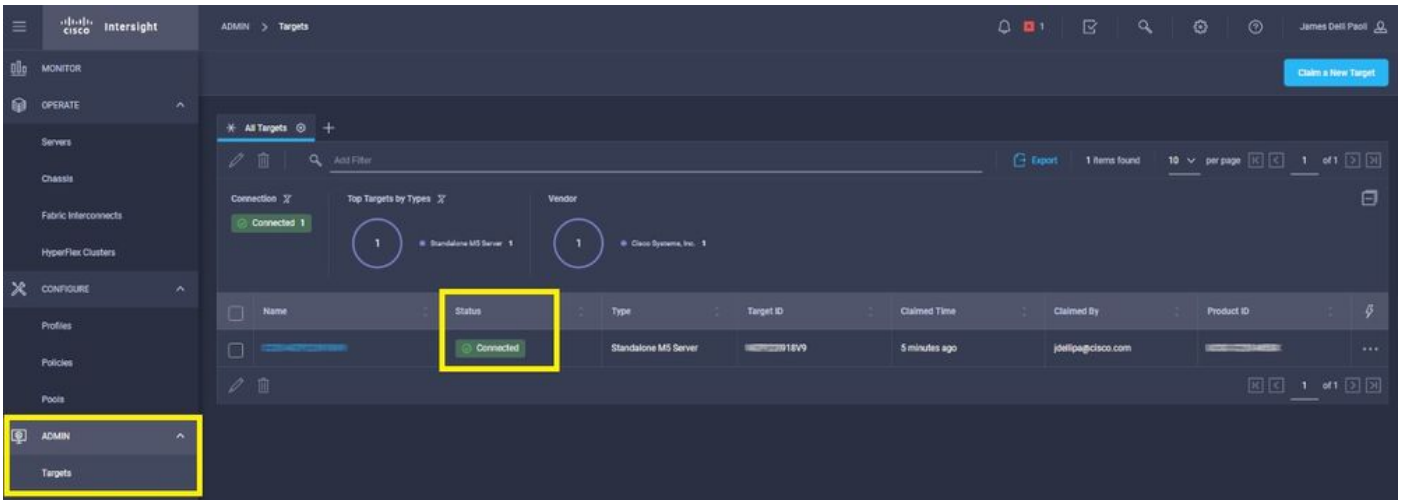
Étape 4. Sélectionnez **Admin** > **Device Connector** et copiez le **Device ID** et **Claim Code.** copiez les deux dans un bloc-notes ou un fichier texte pour une utilisation ultérieure.

Étape 5. Lancez Cisco Intersight et naviguez jusqu'à **Admin > Targets > Claim a New Target > Cisco UCS Server (Standalone) > Start.** Enter the **Device ID** et **Claim Code** qui a été copié à partir de l'interface utilisateur graphique CIMC, puis sélectionnez **Claim.**



Remarque : si le serveur fait partie d'un groupe de ressources spécifique, sélectionnez-le à cette étape.

Étape 6. Naviguez jusqu'à **Admin > Targets.** Une demande d'indemnisation réussie affiche le **Status > Connected,** comme illustré dans cette image.



Vérification de base pour les problèmes de revendication de périphérique

Remarque : pour obtenir une liste complète des conditions d'erreur et des mesures correctives, cliquez sur le lien Conditions d'erreur et mesures correctives du connecteur de périphérique.

Description des états de connexion des connecteurs de périphériques	Explication de l'état de connexion du connecteur	Corrections possibles
Revendiqué	La connexion à la plate-forme Cisco Intersight est réussie et vous avez demandé la connexion.	S/O
Non réclamé	La connexion à la plate-forme Cisco Intersight est réussie, mais le point d'extrémité n'est pas encore revendiqué.	Vous pouvez demander une connexion non demandée via Cisco Intersight.
Désactivé Administrativement	Indique que le connecteur de périphérique/gestion Intersight a été désactivé sur le terminal.	Activez le connecteur de périphérique sur le point d'extrémité.
DNS mal configuré	DNS n’a pas été configuré correctement dans CIMC ou n’a pas été configuré du tout.	Indique qu'aucun des serveurs de noms DNS configurés sur le système n'est accessible.

		Vérifiez que vous avez entré des adresses IP valides pour les serveurs de noms DNS.
Erreur de résolution DNS Intersight	DNS est configuré mais ne peut pas résoudre le nom DNS d'Intersight.	Cliquez sur ce lien pour voir si Intersight est en cours de maintenance : Intersight Status. Si Intersight est opérationnel, cela indique probablement que le nom DNS du service Intersight n'est pas résolu.
Erreur réseau UCS Connect	Indique les configurations réseau non valides.	Vérifiez et confirmez : MTU est correct de bout en bout, les ports 443 et 80 sont autorisés, le pare-feu autorise toutes les adresses IP physiques et virtuelles, DNS et NTP sont configurés sur le terminal.
Erreur de validation du certificat	Le terminal refuse d'établir une connexion à la plate-forme Cisco Intersight car le certificat présenté par la plate-forme Cisco Intersight n'est pas valide.	Certificat expiré ou non encore valide : vérifiez que le protocole NTP est correctement configuré et que l'heure du périphérique est synchronisée avec l'heure universelle coordonnée. Vérifiez que DNS est correctement configuré. Si un proxy Web transparent est en cours d'utilisation, vérifiez que le certificat n'a pas expiré. Le nom de certificat présenté par le serveur Web ne correspond pas au nom DNS du service Intersight : vérifiez que DNS est correctement configuré. Contactez votre administrateur de proxy Web pour vérifier que le proxy Web transparent est correctement configuré. Plus précisément, le nom du certificat présenté par le proxy Web doit correspondre au

		nom DNS du service Intersight (svc.intersight.com). Le certificat a été émis par une autorité de certification (CA) non approuvée : vérifiez que DNS est correctement configuré. Contactez votre administrateur Web ou infosec pour vérifier que le proxy Web transparent est correctement configuré. Plus précisément, le nom du certificat présenté par le proxy Web doit correspondre au nom DNS du service Intersight.

Connectivité réseau générale requise par Cisco Intersight

- Une connexion réseau à la plate-forme Intersight est établie à partir du connecteur de périphérique du point d'extrémité
- Vérifiez si un pare-feu est introduit entre la cible gérée et Intersight, ou si les règles d'un pare-feu actuel ont changé. Cela peut entraîner des problèmes de connexion de bout en bout entre le terminal et Cisco Intersight. Si les règles sont modifiées, assurez-vous qu'elles autorisent le trafic à travers le pare-feu.
- Si vous utilisez un proxy HTTP pour acheminer le trafic hors de vos locaux et si vous avez apporté des modifications à la configuration du serveur proxy HTTP, veillez à modifier la configuration du connecteur de périphérique pour refléter les modifications. Cette opération est nécessaire car Intersight ne détecte pas automatiquement les serveurs proxy HTTP.
- Configurez DNS et résolvez le nom DNS. Le connecteur de périphérique doit pouvoir envoyer des requêtes DNS à un serveur DNS et résoudre les enregistrements DNS. Le connecteur de périphérique doit être en mesure de convertir svc.intersight.com en adresse IP.
- Configurez NTP et vérifiez que l'heure du périphérique est correctement synchronisée avec un serveur de temps.

Remarque : pour obtenir une liste complète des exigences de connectivité d'Intersight, reportez-vous à la section Exigences de connectivité réseau d'Intersight.

Informations connexes

- Cibles de demande Cisco Intersight Getting Started
- Systèmes pris en charge par Cisco Intersight SaaS
- PID pris en charge par Cisco Intersight SaaS
- Connectivité réseau requise pour Cisco Intersight

- Vidéos de formation Cisco Intersight
- ID de bogue Cisco CSCvw76806 - Un serveur C-Series autonome peut échouer à se déclarer dans Cisco Intersight si sa version de connecteur de périphérique est inférieure à 1.0.9.
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.