

Dépannage de Cisco HCI avec les problèmes de connexion du fournisseur de matériel Nutanix

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Dépannage](#)

[Délai de contexte dépassé](#)

[Résolution de noms DNS correcte](#)

[La machine virtuelle de Prism Central ne peut pas se connecter à Intersight CVA / PVA](#)

[Commandes réseau pour tester la connectivité](#)

[Les Détails D'Authentification Fournis Ne Sont Pas Valides](#)

[Impossible d'extraire la liste de CLUF](#)

[Informations connexes](#)

Introduction

Ce document décrit comment dépanner les problèmes de connexion des fournisseurs de matériel de Nutanix Foundation Central à Cisco Intersight.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes .

- Connaissance de base de la connectivité réseau.
- Compréhension de base des clés API Intersight.
- Compte Intersight avec au moins les privilèges d'administrateur du serveur.



E-mail

Sign out



Account and role

Change

Server Administrator



Region

intersight-aws-us-east-1

Access details

User settings



Remarque : Intersight fournit un contrôle d'accès basé sur les rôles (RBAC) pour autoriser ou restreindre l'accès système à un utilisateur, en fonction des rôles et des privilèges de l'utilisateur. Un rôle d'utilisateur dans Intersight représente un ensemble de privilèges dont dispose un utilisateur pour effectuer un ensemble d'opérations et fournit un accès granulaire aux ressources. Intersight fournit un accès basé sur les rôles à des utilisateurs individuels ou à un ensemble d'utilisateurs sous Groupes.

Composants utilisés

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

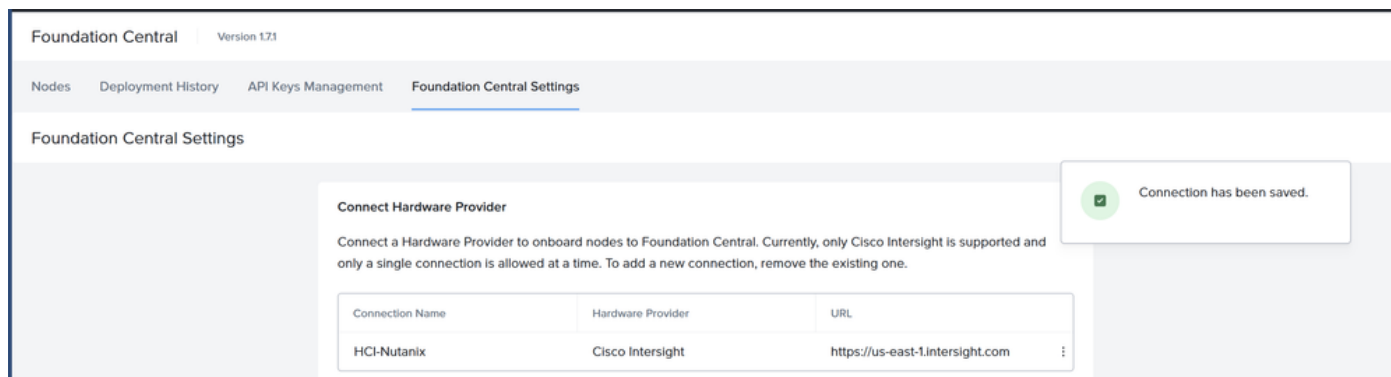
- Foundation Central 1.7.1 ou version ultérieure.
- Intersight SAAS, CVA et PVA.

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.

Informations générales

Il est nécessaire de connecter Foundation Central à Cisco Intersight en tant que fournisseur de matériel pour déployer la solution Cisco HCI avec Nutanix dans Intersight Standalone Mode ISM ou Intersight Managed Mode IMM.



Mode autonome Intersight : les noeuds sont connectés à une paire de commutateurs ToR (Top-of-Rack) et les serveurs sont gérés de manière centralisée à l'aide de Cisco Intersight®. Bien qu'un minimum de trois noeuds soit requis pour déployer un cluster Nutanix standard, nous proposons également une option de déploiement d'un cluster à noeud unique et d'un cluster à deux noeuds pour les sites en périphérie et les filiales et les situations dans lesquelles un fabric réseau hautes performances est déjà installé.

Mode géré Intersight : le mode géré Intersight unifie les fonctionnalités des systèmes UCS et la flexibilité basée sur le cloud d'Intersight, unifiant ainsi l'expérience de gestion des systèmes autonomes et connectés à Fabric Interconnect. Le modèle de gestion Intersight normalise la gestion des politiques et des opérations pour les interconnexions de fabric UCS-FI-6454, UCS-FI-64108, UCS-FI-6536, UCSX-S9108-100G et les serveurs Cisco UCS série C (M5, M6, M7, M8) et Cisco UCS série X (M6, M7, M8).

Dépannage

Délai de contexte dépassé

"Échec de la validation de la connexion avec les détails d'authentification donnés : Échec de la récupération de la clé API : délai de contexte dépassé."

Connect Hardware Provider

Connection Details

Connection Name

HCI-Nutanix-API-KEY

Only the special characters - . _ are allowed

Hardware Provider

Cisco Intersight

Intersight Deployment Type

☒ SaaS
☐ Connected/Private Virtual Appliance

Intersight Region & URL

North America

https://us-east-1.intersight.com

h connection and

Failed to validate connection with the given auth details:

Failed to fetch the API Key:

Get "https://us-east-1.intersight.com/api/v1/iam/Api"

Assurez-vous que vous disposez d'une connectivité appropriée entre Prism Central et Foundation Central vers les URL suivantes via les ports 443 TCP/UDP et 80 TCP.

Région	URL	URL requises par les connecteurs de périphériques
Amérique du Nord	intersight.com	svc.intersight.com
	us-east-1.intersight.com	svc.us-east-1.intersight.com
	Ips :	svc-static1.intersight.com
	52.223.48.112	ucs-starship.com*
	99.83.178.202	ucs-connect.com*
EMEA	Intersight.com	
	eu-central-1.intersight.com	svc.eu-central-1.intersight.com
	Ips :	svc-static1.eu-central-1.intersight.com
	52.223.57.109	
	99.83.140.236	



Remarque : Cisco Intersight prend en charge deux régions : la région d'Amérique du Nord existante (us-east-1) et la région Europe, Moyen-Orient et Afrique (EMEA) (eu-central-1).

Pour valider les informations précédentes, connectez-vous par SSH à votre machine virtuelle Prism Central ou Foundation Central et exécutez une commande curl sur les URL et les ports mentionnés.

```
curl -v -k https://svc.intersight.com
```

```

admin@NTNX-10-31-123-88-A-PCVM:~$ curl -v -k https://svc.intersight.com
* About to connect() to svc.intersight.com port 443 (#0)
*   Trying 2600:9000:a60c:6a4d:2d28:e9be:e3e:f0cf...
* Connected to svc.intersight.com (2600:9000:a60c:6a4d:2d28:e9be:e3e:f0cf) port 443 (#0)
* Initializing NSS with certpath: sql:/etc/pki/nssdb
* skipping SSL peer certificate verification
* SSL connection using TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
* Server certificate:
*   subject: CN=us-east-1.intersight.com
*   start date: Apr 01 00:00:00 2025 GMT
*   expire date: Apr 30 23:59:59 2026 GMT
*   common name: us-east-1.intersight.com
*   issuer: CN=Amazon RSA 2048 M03,O=Amazon,C=US
> GET / HTTP/1.1
> User-Agent: curl/7.29.0
> Host: svc.intersight.com
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Tue, 09 Sep 2025 18:53:00 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 82
< Connection: keep-alive
< Set-Cookie: AWSALB=W9cqyvSaX/07+KZ4058CopaQB1JlMCo4TYocbNpCwsDBaDH/xquxQcaFXKe14m9SUn6/KJCRooj8o5BR/Q5w0Y4fxCLFL3ShwUNjehUjTf6EF0AY7AXD19WaiDlu; Expires=Tue, 16 Sep 2025 18:53:00 GMT; Path=/
< Set-Cookie: AWSALBCORS=W9cqyvSaX/07+KZ4058CopaQB1JlMCo4TYocbNpCwsDBaDH/xquxQcaFXKe14m9SUn6/KJCRooj8o5BR/Q5w0Y4fxCLFL3ShwUNjehUjTf6EF0AY7AXD19WaiDlu; Expires=Tue, 16 Sep 2025 18:53:00 GMT; Path=/; SameSite=None; Secure
< X-Starship-Traceid: A5c88567814c27739a26fa67a590716182
* Connection #0 to host svc.intersight.com left intact
svc.intersight.com is alive and healthy at 2025-09-09 18:53:00.934344289 +0000 UTCadmin@NTNX-10-31-123-88-A-PCVM:~$ █

```

Test de connectivité de boucle réussi.

Si la commande curl échoue, vérifiez auprès de votre équipe de pare-feu que les URL et les ports sont autorisés dans le pare-feu ou la liste d'accès.

```

admin@NTNX-10-31-123-88-A-PCVM:~$ curl -v -k https://svc.intersight.com
* About to connect() to svc.intersight.com port 443 (#0)
*   Trying 2600:9000:a60c:6a4d:2d28:e9be:e3e:f0cf...
* No route to host
*   Trying 2600:9000:a706:c634:41:731c:ad1e:bf00...
* No route to host
*   Trying 99.83.178.202...
* Connection timed out
*   Trying 52.223.48.112...
* After 86287ms connect time, move on!
* Failed connect to svc.intersight.com:443; Operation now in progress
* Closing connection 0
curl: (7) Failed connect to svc.intersight.com:443; Operation now in progress
admin@NTNX-10-31-123-88-A-PCVM:~$ █

```

Échec du test de connectivité de boucle.

Résolution de noms DNS correcte

Certains pare-feu ou listes d'accès nécessitent l'ajout de l'adresse IP de résolution à partir des URL mentionnées. Ces deux URL sont résolues en adresses IPv4 et IPv6 :

- 52.223.48.112
- 99.83.178.202
- 2600:9000:a60c:6a4d:2d28:e9be:e3e:f0cf
- 2600:9000:a706:c634:41:731c:ad1e:bf00

Vous pouvez le valider à l'aide de la commande nslookup.

```
nslookup svc.intersight.com
```

```
admin@NTNX-10-31-123-88-A-PCVM:~$ nslookup svc.intersight.com
Server:          10.31.123.60
Address:         10.31.123.60#53

Non-authoritative answer:
Name:   svc.intersight.com
Address: 52.223.48.112
Name:   svc.intersight.com
Address: 99.83.178.202
Name:   svc.intersight.com
Address: 2600:9000:a60c:6a4d:2d28:e9be:e3e:f0cf
Name:   svc.intersight.com
Address: 2600:9000:a706:c634:41:731c:ad1e:bf00

admin@NTNX-10-31-123-88-A-PCVM:~$ █
```

nslookup, commande

La machine virtuelle de Prism Central ne peut pas se connecter à Intersight CVA / PVA

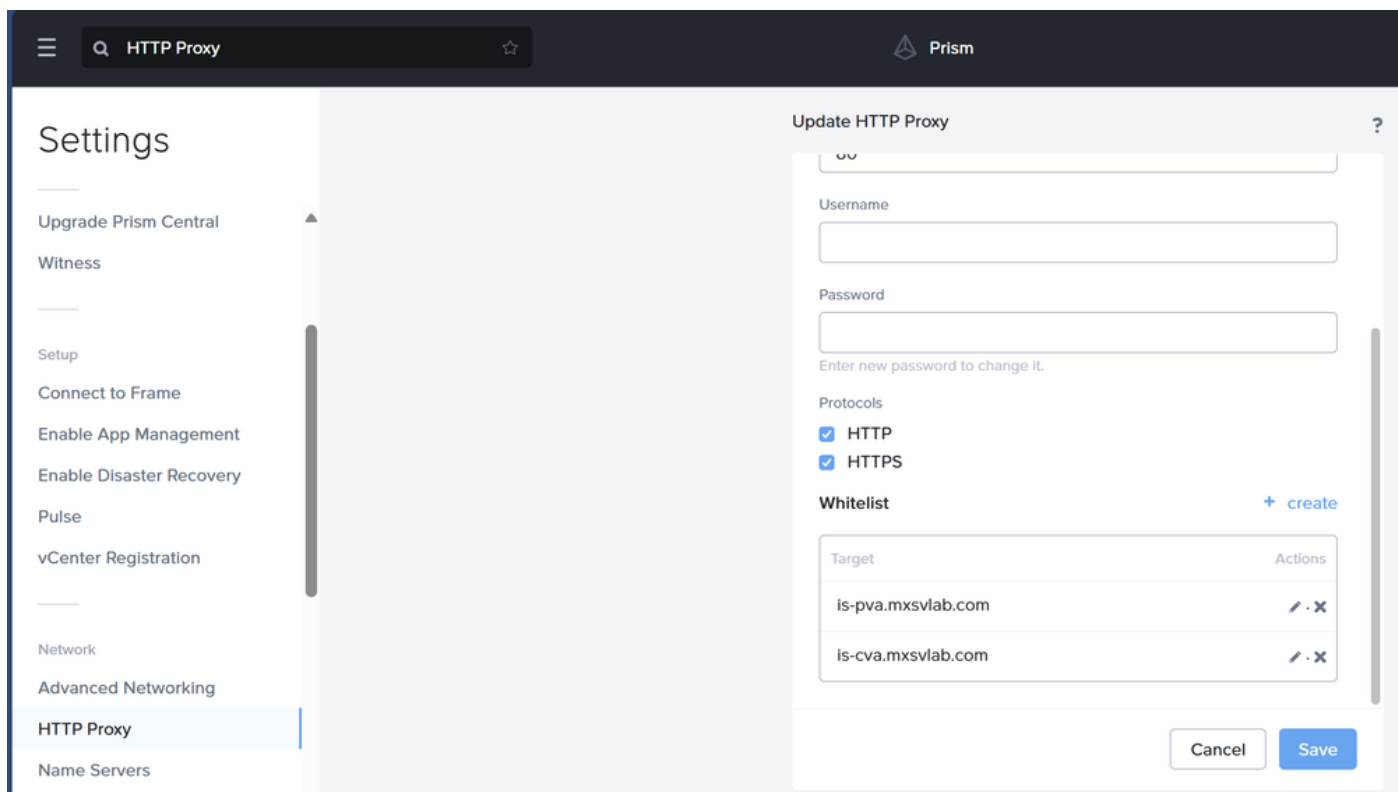
En cas de connexion directe de Prism Central à Intersight CVA / PVA, assurez-vous d'autoriser la connexion sur le port 443.

Si PC VM dispose d'un proxy configuré pour se connecter à Internet pour des tâches telles que les téléchargements de logiciels ou LCM, vous devez mettre en liste blanche le nom de domaine complet Intersight CVA / PVA et l'adresse IP dans les paramètres du proxy Prism Central.



Remarque : Une entrée de liste blanche est un hôte unique identifié par une adresse IP ou un réseau identifié par l'adresse réseau et le masque de sous-réseau. L'ajout d'une entrée de liste blanche signifie « ignorer les paramètres de proxy pour cette adresse ou ce réseau ».

Pour corriger ce problème dans Prism Central, accédez à : Settings > Network > HTTP Proxy > Click on pencil icon to edit > Whitelist.



Proxy HTTP

Vous pouvez vérifier si ces étapes ont réussi en testant la connectivité à Intersight CVA / PVA avec une commande curl.

```
curl -v -k https://is-pva.mxsvlab.com
```

```
curl -v -k https://is-pva.mxsvlab.com
* Trying 192.168.1.100:443...
* Connected to is-pva.mxsvlab.com (192.168.1.100) port 443
* ALPN: curl offers http/1.1
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
* TLSv1.3 (IN), TLS handshake, Certificate (11):
* TLSv1.3 (IN), TLS handshake, CERT verify (15):
* TLSv1.3 (IN), TLS handshake, Finished (20):
* TLSv1.3 (OUT), TLS handshake, Finished (20):
* SSL connection using TLSv1.3 / TLS_AES_256_GCM_SHA384
* ALPN: server accepted http/1.1
```

Essai de bouclage

Commandes réseau pour tester la connectivité

Commande	Description
----------	-------------

<pre>curl -v -k https://<URL de l'aperçu> curl -v -k https://svc.intersight.com</pre>	Tester la connectivité vers une URL Intersight requise
<pre>curl -v -k --proxy <adresse proxy>:<port> <URL de l'aperçu> curl -v -k --proxy http://proxy.esl.cisco.com:8080 https://svc.intersight.com</pre>	Tester la connectivité lorsque le proxy est requis
<pre>curl -4 6 -v -k https://<URL de l'aperçu> curl -4 -v -k https://svc.intersight.com</pre>	Spécifier le test de connectivité à l'adressage IPV4 ou IPV6
<pre>tracpath <Intersight IP> tracpath 99.83.178.202</pre>	Trace les paquets vers un hôte de destination
<pre>nslookup <URL> nslookup svc.Intersight.com</pre>	Détermine l'adresse IP associée à une adresse spécifique

Les Détails D'Authentification Fournis Ne Sont Pas Valides

"Impossible d'enregistrer les données d'authentification du gestionnaire matériel : Les détails d'authentification fournis ne sont pas valides. Veuillez fournir une clé API et un secret valides."

Connect Hardware Provider

North Americahttps://us-east-1.intersight.com

Connection Credentials

You can find the API key ID and secret key on the Cisco Intersight Settings page. Currently, only Open API schema version 3 is supported.

Intersight API Key ID

62ed7649

Intersight Secret Key

-----BEGIN EC PRIVATE KEY-----
HAgEAMBMGByqGSM49AgEGCCqGSM49AwEHBG0waw

Hide

CancelConnect

Failed to save hardware manager auth data: Auth details provided are invalid. Please provide valid API Key and secret

Vous devez confirmer qu'il n'y a pas d'erreurs typographiques ou de caractères manquants lors de la saisie ou du collage de la clé secrète Intersight, sinon la connexion au fournisseur de matériel échoue.

View API Key



This is the only one time that the secret key can be viewed or downloaded. You cannot recover them later. However, you can create new access keys at any time.

API Key ID



62ed7649

Secret Key



-----BEGIN EC PRIVATE KEY-----

MIGHAgEAMBMGBByqGSM49AgEGCCqGSM49AwEHBG0waw

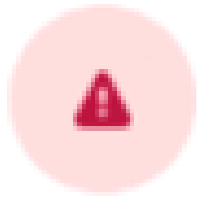


I have downloaded the Secret Key.

Close

Impossible d'extraire la liste de CLUF

"Échec de la validation de la connexion avec les détails d'authentification donnés : Impossible d'extraire la liste de CLUF. Échec avec erreur : Votre jeton a expiré en raison d'une inactivité au cours des 30 derniers jours."



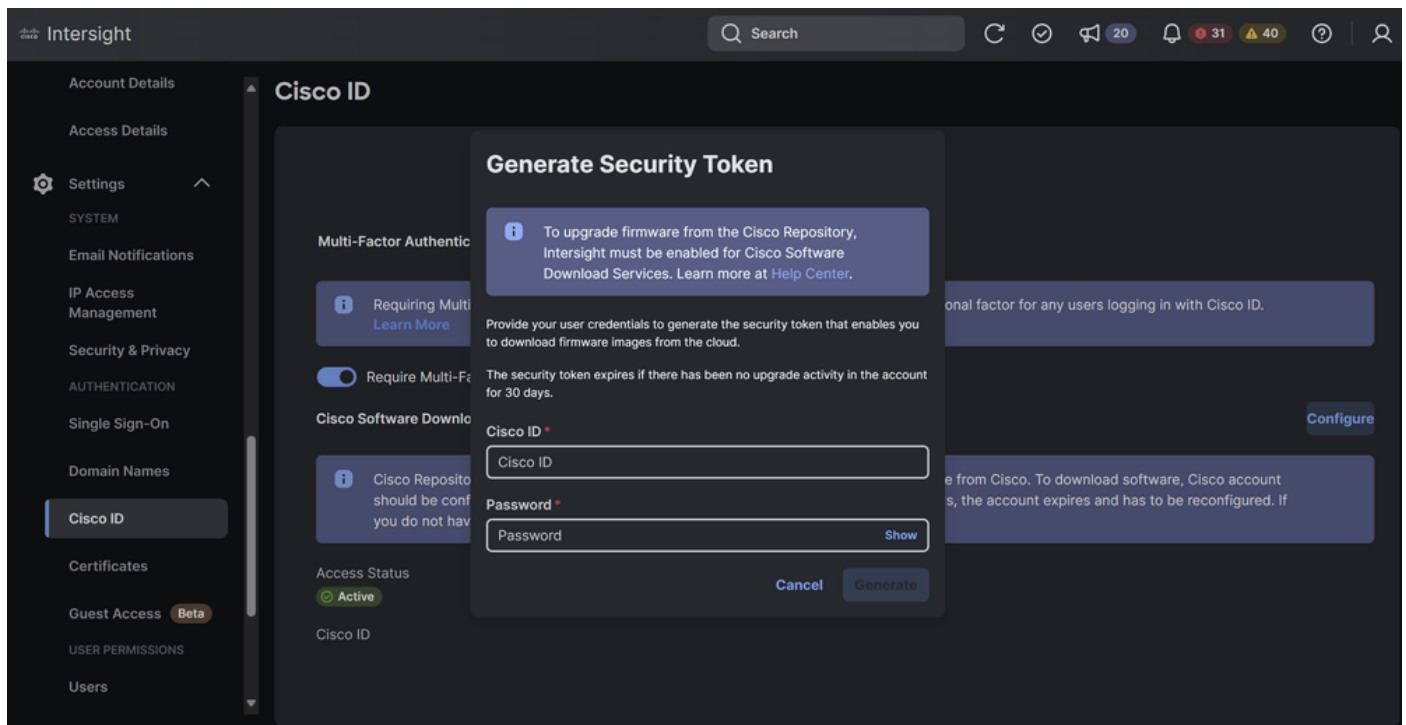
Failed to validate connection
with the given auth details:
Unable to fetch the EULA list.
Failed with error: Your token has
expired due to inactivity in the
last 30 days. Provide your Cisco

Lors de la phase d'intégration des noeuds, vous pouvez rencontrer une erreur « Failed to connect to INTERSIGHT hardware manager with UUID » ou « Your user credentials may have expired ». Ceci apparaît en cas de problème de compte Intersight concernant le CLUF.



Remarque : À partir d'aujourd'hui, l'acceptation du CLUF est REQUISE pour ISM. Cela va changer à l'avenir puisque nous ne dépendons plus du CLUF pour les téléchargements de micrologiciels.

Pour corriger ce problème dans Intersight, accédez à : Settings > Cisco ID > Configure > Enter Cisco ID and Password.



Informations connexes

- [Organisations et rôles dans Intersight](#)
- [Configuration des ports](#)
- [URL de point de terminaison requises pour demander des cibles](#)
- [Accorder l'accès au référentiel de logiciels Cisco et accepter le CLUF](#)

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.