Dépannage de la synchronisation de licence sur Catalyst SD-WAN Manager via le mode de rapport On-Prem

Table des matières

Introduction

Conditions préalables

- Exigences
- Avantages de l'utilisation de Cisco Smart Software Manager On-Prem

Erreur

Approche de dépannage

Solution de contournement

Introduction

Ce document décrit comment dépanner une erreur rencontrée lors de la synchronisation de la licence sur Catalyst SD-WAN Manager en mode de rapport On-prem.

Conditions préalables

Exigences

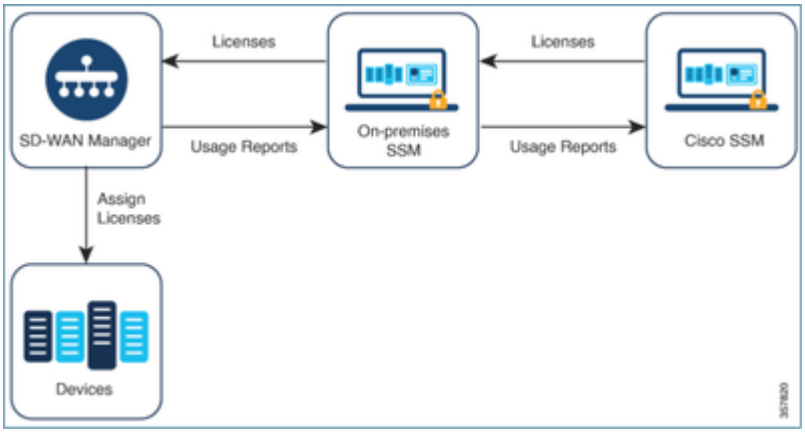
Dans les cas où Catalyst SD-WAN Manager n'est pas directement connecté à Internet, l'utilisation d'un serveur proxy peut fournir un accès à des services Internet, tels que Cisco SSM, ou à un SSM local sur site.

Version minimale : Catalyst SD-WAN Manager version 20.9.1

Cisco Smart Software Manager on-prem (SSM on-prem) est une solution Cisco Smart Licensing qui vous permet d'administrer des licences à partir d'un serveur sur votre site, au lieu d'avoir à vous connecter directement à Cisco SSM. La solution implique la configuration d'un serveur de licences sur site Cisco SSM, qui synchronise périodiquement sa base de données de licences avec Cisco SSM et fonctionne de la même manière que Cisco SSM, tout en fonctionnant localement.

Catalyst SD-WAN Manager prend en charge la gestion des licences à l'aide d'un serveur sur site Cisco SSM, à l'aide d'un mode appelé on-prem. Le mode On-prem est utile pour les organisations qui utilisent Cisco SSM on-prem pour s'adapter à une politique de sécurité stricte qui ne permet pas aux périphériques réseau de communiquer avec Cisco SSM par une connexion Internet directe.

Lorsqu'il fonctionne en mode sur site, Catalyst SD-WAN Manager synchronise les informations de licence avec le serveur de licence sur site Cisco SSM toutes les 24 heures. Au cours de cette synchronisation, Catalyst SD-WAN Manager reçoit toutes les mises à jour des licences disponibles et envoie des rapports d'utilisation des licences au serveur de licences sur site Cisco SSM. Vous pouvez synchroniser les licences à tout moment.



Avantages de l'utilisation de Cisco Smart Software Manager On-Prem

Les entreprises dont les politiques de sécurité, ou d'autres circonstances, exigent que Catalyst SD-WAN Manager ne soit pas connecté à Internet disposent de deux options pour gérer les licences Smart License Using Policy :

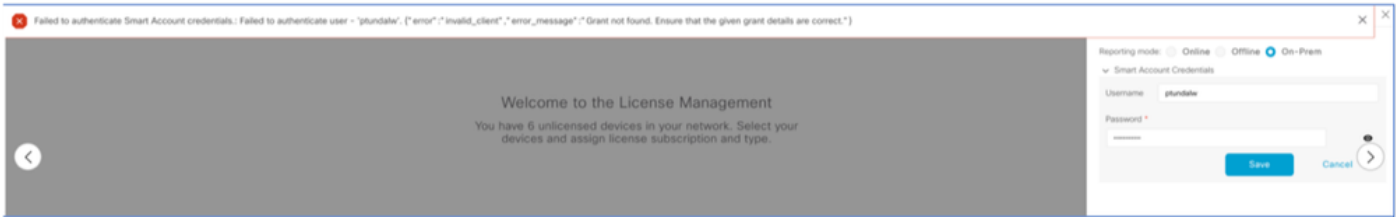
- Utilisez le mode hors connexion, qui nécessite le transfert manuel de fichiers entre Catalyst SD-WAN Manager et Cisco SSM.
- Utilisez un serveur sur site Cisco SSM accessible via une connexion au réseau local vers Catalyst SD-WAN Manager.

Ces deux méthodes permettent de transférer les informations de licence entre Cisco SSM et Catalyst SD-WAN Manager. Chaque fois qu'il est possible d'utiliser le mode sur site, ce mode offre l'avantage significatif de réduire la charge de maintenance liée au transfert manuel de fichiers entre Catalyst SD-WAN Manager et Cisco SSM, comme cela est nécessaire pour le mode hors connexion.

Erreur

Lors de la synchronisation des informations d'identification Smart à partir de l'interface utilisateur graphique de Catalyst SD-WAN Manager, vous obtenez cette erreur :

```
Failed to authenticate Smart Account credentials.: Failed to authenticate user - 'admin'. {"error":"inv
```



Approche de dépannage

- vManage doit être sur le code 20.9.1 ou ultérieur.
- Vérifiez les journaux sur le gestionnaire SD-WAN Catalyst (vmanage-server.logs) tout en plaçant les informations d'identification de compte Smart dans la section Gestion de licence du gestionnaire SD-WAN Catalyst.
- Assurez-vous que l'ID client et la clé secrète partagés par l'équipe SSM locale sont corrects.
- TCPDUMP sur l'adresse IP du serveur vManage pour CSSM
- Vérifiez que DNS est correctement configuré sur le gestionnaire SD-WAN de Catalyst et qu'il peut envoyer une requête ping à cloudsso.cisco.com
- Impliquez l'équipe SSM locale et demandez à l'équipe SSM de déboguer au niveau du serveur local.

IP de Catalyst SD-WAN Manager : 10.66.76.81 / 192.168.10.1

Adresse IP du serveur CSSM : 10.106.66.55

TCPDump sur l'adresse IP du serveur vManage pour SSM :

```
um8_vManage# tcpdump vpn 0 interface eth0 options "host 10.106.66.55 -nn -vv"

tcpdump -p -i eth0 -s 128 host 10.106.66.55 -nn -vv in VPN 0

tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 128 bytes

12:15:06.407513 IP (tos 0x0, ttl 64, id 24618, offset 0, flags [DF], proto TCP (6), length 52)

    192.168.10.1.57886 > 10.106.66.55.8443: Flags [S], cksum 0xfadb (incorrect -> 0xdf91), seq 74638621

12:15:06.651698 IP (tos 0x20, ttl 44, id 0, offset 0, flags [DF], proto TCP (6), length 52)
```

```
    10.106.66.55.8443 > 192.168.10.1.57886: Flags [S.], cksum 0x1b34 (correct), seq 2758352947, ack 746
12:15:06.651768 IP (tos 0x0, ttl 64, id 24619, offset 0, flags [DF], proto TCP (6), length 40)
    192.168.10.1.57886 > 10.106.66.55.8443: Flags [.], cksum 0xfacf (incorrect -> 0xcce1), seq 1, ack 1
12:15:06.654592 IP (tos 0x0, ttl 64, id 24620, offset 0, flags [DF], proto TCP (6), length 212)
    192.168.10.1.57886 > 10.106.66.55.8443: Flags [P.], seq 1:173, ack 1, win 229, length 172
12:15:06.899695 IP (tos 0x0, ttl 41, id 44470, offset 0, flags [DF], proto TCP (6), length 40)
    10.106.66.55.8443 > 192.168.10.1.57886: Flags [.], cksum 0xcc2d (correct), seq 1, ack 173, win 237,
12:15:06.911484 IP (tos 0x0, ttl 41, id 44471, offset 0, flags [DF], proto TCP (6), length 1420)
    10.106.66.55.8443 > 192.168.10.1.57886: Flags [.], seq 1:1381, ack 173, win 237, length 1380
12:15:06.911542 IP (tos 0x0, ttl 41, id 44472, offset 0, flags [DF], proto TCP (6), length 254)
    10.106.66.55.8443 > 192.168.10.1.57886: Flags [P.], seq 1381:1595, ack 173, win 237, length 214
12:15:06.911573 IP (tos 0x0, ttl 64, id 24621, offset 0, flags [DF], proto TCP (6), length 40)
    192.168.10.1.57886 > 10.106.66.55.8443: Flags [.], cksum 0xfacf (incorrect -> 0xc6bb), seq 173, ack
12:15:06.911598 IP (tos 0x0, ttl 64, id 24622, offset 0, flags [DF], proto TCP (6), length 40)
    192.168.10.1.57886 > 10.106.66.55.8443: Flags [.], cksum 0xfacf (incorrect -> 0xc5cf), seq 173, ack
12:15:06.923929 IP (tos 0x0, ttl 64, id 24623, offset 0, flags [DF], proto TCP (6), length 234)
    192.168.10.1.57886 > 10.106.66.55.8443: Flags [P.], seq 173:367, ack 1595, win 273, length 194
```

Journaux du serveur sur site :

```
[root@SSM-On-Prem log]# tail -f messages
Jan 13 11:13:36 SSM-On-Prem chronyd[1319]: Source 172.20.226.229https://172.20.226.229 replaced with 17
Jan 13 11:14:09 SSM-On-Prem b09c1e3b5d81: 1:M 13 Jan 2023 11:14:09.049 * 100 changes in 300 seconds. Sa
Jan 13 11:14:09 SSM-On-Prem b09c1e3b5d81: 1:M 13 Jan 2023 11:14:09.050 * Background saving started by p
Jan 13 11:14:09 SSM-On-Prem b09c1e3b5d81: 4617:C 13 Jan 2023 11:14:09.052 * DB saved on disk
Jan 13 11:14:09 SSM-On-Prem b09c1e3b5d81: 4617:C 13 Jan 2023 11:14:09.053 * RDB: 0 MB of memory used by
Jan 13 11:14:09 SSM-On-Prem b09c1e3b5d81: 1:M 13 Jan 2023 11:14:09.150 * Background saving terminated w
Jan 13 11:14:46 SSM-On-Prem 1a1fca641d0a: Redis#exists(key) will return an Integer in redis-rb 4.3. exi
Jan 13 11:14:46 SSM-On-Prem 1a1fca641d0a: [active_model_serializers] Rendered UserSerializer with Activ
Jan 13 11:14:46 SSM-On-Prem 1a1fca641d0a: method=GET path=/sessions/get_user format=json controller=Ses
Jan 13 11:14:46 SSM-On-Prem 504f06c0d581: 10.110.35.124https://10.110.35.124 - - [13/Jan/2023:11:14:46 -
```

```
Jan 13 11:17:01 SSM-On-Prem 504f06c0d581: 2023/07/13 11:17:01 [error] 47#47: *1576 connect() failed (11
Jan 13 11:17:01 SSM-On-Prem 504f06c0d581: 2023/07/13 11:17:01 [warn] 47#47: *1576 upstream server tempo
Jan 13 11:17:01 SSM-On-Prem 1a1fca641d0a: [active_model_serializers] Rendered ActiveModel::Serializer::
Jan 13 11:17:01 SSM-On-Prem 1a1fca641d0a: method=POST path=/oauth/token format=json controller=Doorkeep
Jan 13 11:17:01 SSM-On-Prem 504f06c0d581: 10.66.76.85https://10.66.76.85 - - [13/Jan/2023:11:17:01 +000
Jan 13 11:17:14 SSM-On-Prem 1a1fca641d0a: [INFO] Session expiring outcome=success
```

Se connecte à vManage en insérant les détails des comptes Smart dans la section Gestion des licences vManage :

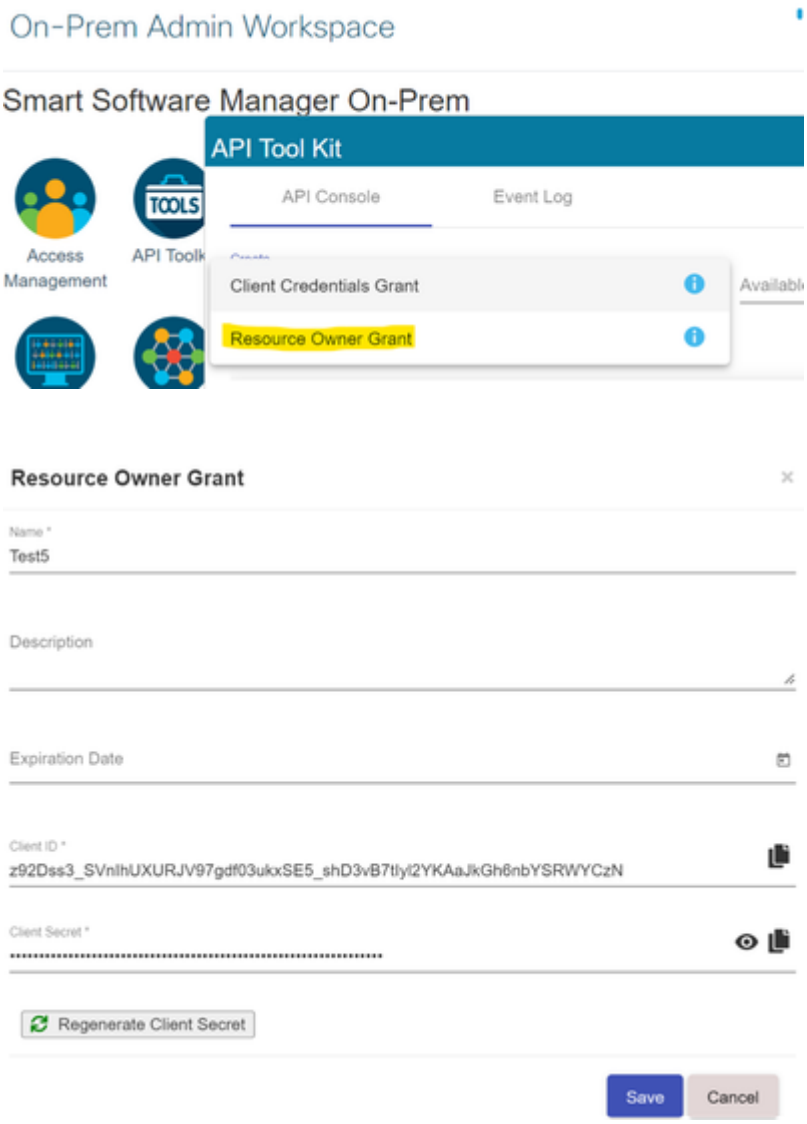
```
13-Jan-2023 17:29:02,775 IST INFO  [um8_vManage] [SmartLicensingIntegrationManager] (default task-24) |
13-Jan-2023 17:29:02,776 IST INFO  [um8_vManage] [SmartLicensingIntegrationManager] (default task-24) |
13-Jan-2023 17:29:02,780 IST INFO  [um8_vManage] [AbstractSettingsManager] (default task-24) |default|
13-Jan-2023 17:29:02,781 IST INFO  [um8_vManage] [SmartLicensingUtil] (default task-24) |default| intia
13-Jan-2023 17:29:02,781 IST INFO  [um8_vManage] [SmartLicensingUtil] (default task-24) |default| Getti
13-Jan-2023 17:29:02,793 IST INFO  [um8_vManage] [RestAPIClient] (default task-24) |default| RestAPI pr
13-Jan-2023 17:29:02,793 IST INFO  [um8_vManage] [RestAPIClient] (default task-24) |default| RestAPI pr
13-Jan-2023 17:29:02,798 IST INFO  [um8_vManage] [SmartLicensingUtil] (default task-24) |default| URL b
13-Jan-2023 17:29:02,798 IST INFO  [um8_vManage] [SmartLicensingUtil] (default task-24) |default| Query
13-Jan-2023 17:29:03,490 IST ERROR [um8_vManage] [RestAPIClient] (default task-24) |default| Failed to
13-Jan-2023 17:29:03,491 IST ERROR [um8_vManage] [SmartLicensingUtil] (default task-24) |default| Faile
13-Jan-2023 17:29:03,491 IST ERROR [um8_vManage] [SmartLicensingIntegrationRestfulResource] (default ta
```

Remarque : Vous obtenez l'erreur 403 lors de la synchronisation du compte Smart à partir de l'interface graphique utilisateur vManage, ce qui indique que le serveur comprend la demande mais refuse de l'autoriser.

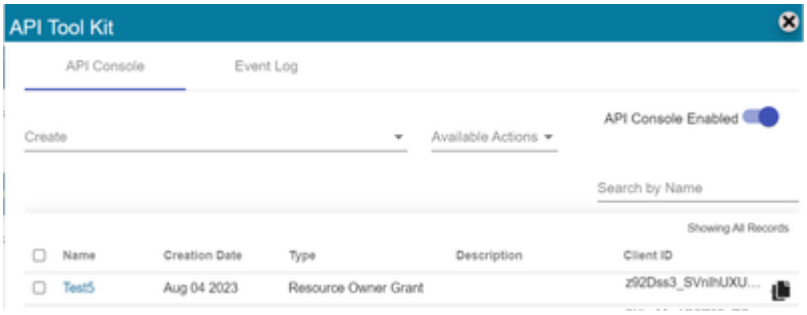
Solution de contournement

1. Connectez-vous à On Prem Server.
2. Accédez à API Tool Kit.

3. Sélectionnez Octroi propriétaire de ressources. Saisissez les détails sous Nom et sauvegardez.



4. Sélectionnez l'enregistrement enregistré (mentionné dans l'instantané précédent) et cochez Client ID et Client Secret.



5. Partagez et entrez l'ID client partagé et le Client Secret dans le portail Catalyst SD-WAN

Manager.

6. Accédez à Sync Licenses and Refresh Devices dans vManage et utilisez les mêmes informations d'identification sur prem avec lesquelles vous vous êtes connecté pour générer l'ID client et le secret client.

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.