



Dépanner le connecteur d'attributs dynamiques

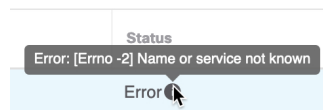
Comment résoudre les problèmes liés à l'utilisation du connecteur d'attributs dynamiques, y compris en utilisant les outils fournis.

- [Dépanner les messages d'erreur, à la page 1](#)
- [Outils de dépannage, à la page 3](#)
- [Obtenir de manière manuelle un certificat de Chaîne d'autorité de certification \(CA\), à la page 5](#)

Dépanner les messages d'erreur

Problème : erreur de nom ou de service inconnu

Cette erreur est affichée sous forme d'infobulle lorsque vous passez la souris sur une condition d'erreur sur un adaptateur ou un connecteur. Voici un exemple ; le vôtre peut être différent.



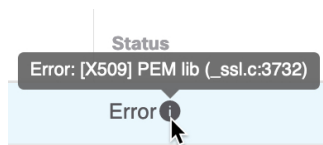
Solution : modifiez le connecteur et vérifiez la présence :

- d'une barre oblique à la fin d'un nom d'hôte
- (On-Prem Firewall Management Center adaptateur uniquement). Un modèle au début d'un nom d'hôte (par exemple, `https://`)
- Vérifiez que le mot de passe est correct
- Dans le cas On-Prem Firewall Management Center d'un adaptateur, Vérifiez le contenu du champ **Certificat du serveur FMC**.

Pour en savoir plus, consultez [Obtenir de manière manuelle un certificat de Chaîne d'autorité de certification \(CA\)](#).

Problème : [X509 PEM lib]

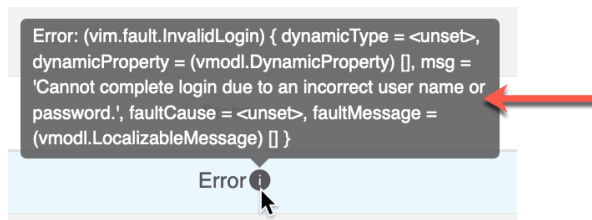
Cette erreur est affichée sous forme d'infobulle lorsque vous passez la souris sur une condition d'erreur dans un connecteur.



Solution : modifiez le connecteur et vérifiez la chaîne CA. Pour en savoir plus, consultez [Obtenir de manière manuelle un certificat de Chaîne d'autorité de certification \(CA\)](#).

Problème : nom d'utilisateur ou mot de passe incorrect

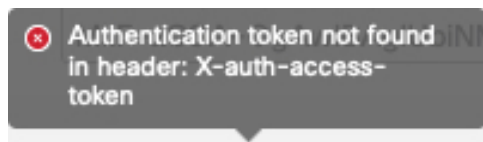
Cette erreur est affichée sous forme d'infobulle lorsque vous passez la souris sur une condition d'erreur dans un connecteur.



Solution : modifiez le connecteur et changez le nom d'utilisateur ou le mot de passe.

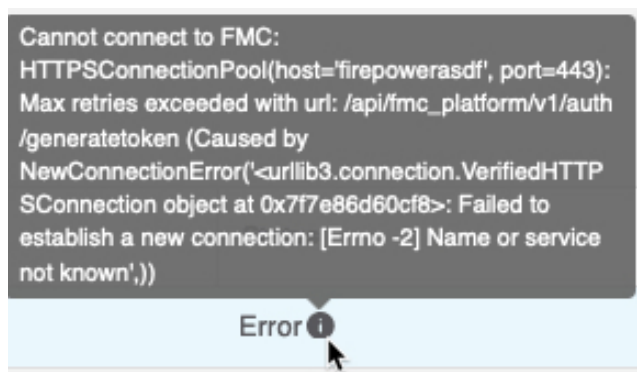
Problème : le jeton d'authentification n'a pas été trouvé dans l'en-tête.

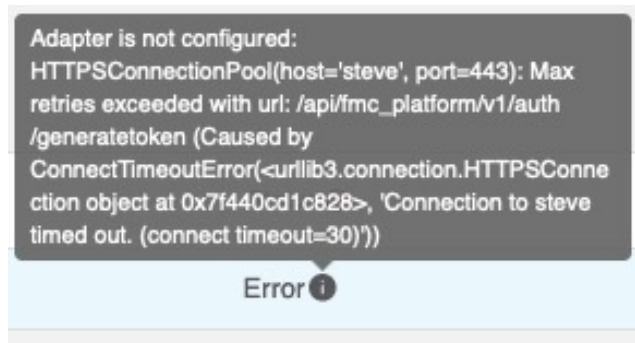
Cette erreur s'affiche lorsque vous essayez de tester la connexion avec un utilisateur d'adaptateur qui ne dispose pas de privilèges suffisants sur centre de gestion :



Problème : erreur de dépassement de délai ou de nombre maximal de tentatives pour un adaptateur.

Cette erreur est affichée sous forme d'infobulle lorsque vous passez la souris sur une condition d'erreur dans un adaptateur.





Solution : effectuez toutes les opérations suivantes :

- Vérifiez que le centre de gestion fonctionne et qu'il est accessible à partir de connecteur d'attributs dynamiques.
- Vérifier le contenu du champ **Certificat du serveur FMC**.
- Assurez-vous que la valeur saisie dans le champ **IP** correspond exactement au nom commun du certificat.

Pour en savoir plus, consultez [Obtenir de manière manuelle un certificat de Chaîne d'autorité de certification \(CA\)](#).

Outils de dépannage

Pour vous aider à effectuer un dépannage avancé et à travailler avec l'assistance technique de Cisco, nous mettons à votre disposition les outils de dépannage suivants. Pour utiliser ces outils, connectez-vous en tant qu'utilisateur quelconque à l'hôte Ubuntu sur lequel le connecteur d'attributs dynamiques fonctionne.

Vérifier l'état du conteneur

Pour vérifier l'état des conteneurs Docker de connecteur d'attributs dynamiques, saisissez les commandes suivantes :

```
cd ~/csdac/app
sudo ./muster-cli status
```

Voici un exemple de sortie :

```
===== CORE SERVICES =====
      Name                               Command                               State    Ports
-----
muster-bee      ./docker-entrypoint.sh run ...      Up              50049/tcp, 50050/tcp
muster-etcd     etcd                                  Up              2379/tcp, 2380/tcp
muster-ui       /docker-entrypoint.sh runs ...      Up (healthy)
0.0.0.0:443->8443/tcp, :::443->8443/tcp
muster-ui-backend ./docker-entrypoint.sh run ...      Up              50031/tcp

===== CONNECTORS AND ADAPTERS =====
      Name                               Command                               State    Ports
-----
muster-adapter-fmc.1 ./docker-entrypoint.sh run ...      Up              50070/tcp
muster-connector-vcenter.1 ./docker-entrypoint.sh run ...      Up              50070/tcp
```

Arrêter, démarrer ou redémarrer les conteneurs Docker de Connecteur d'attributs dynamiques

Si le `./muster-cli status` indique que les conteneurs sont en panne ou pour redémarrer les conteneurs en cas de problème, vous pouvez saisir les commandes suivantes :

Arrêter et redémarrer :

```
cd ~/csdac/app
sudo ./muster-cli stop
sudo ./muster-cli start
```

Démarrer seulement :

```
cd ~/csdac/app
sudo ./muster-cli start
```

Activer la journalisation du débogage et générer des fichiers de dépannage

Si l'assistance technique de Cisco vous le conseille, activez la journalisation du débogage et générez des fichiers de dépannage comme suit :

```
cd ~/csdac/app
sudo ./muster-cli debug-on
sudo ./muster-cli ts-gen
```

Le nom du fichier de dépannage est `ts-bundle-horodatage.tar` et est créé dans le même répertoire.

Le tableau suivant indique l'emplacement des fichiers de dépannage et des journaux dans le fichier de dépannage.

Emplacement	Ce qu'il contient
<code>/csdac/app/ts-bundle-timestamp (horodatage)/info</code>	Contenu de la base de données <code>etcd</code>
<code>/csdac/app/ts-bundle-timestamp (horodatage)/logs</code>	Fichiers journaux des conteneurs
<code>/csdac/app/ts-bundle-timestamp (horodatage)/status.log</code>	État du conteneur, versions et état de l'image

Vérifier les objets dynamiques

Pour vérifier que vos connecteurs créent des objets sur le centre de gestion, vous pouvez utiliser la commande suivante sur le centre de gestion en tant qu'administrateur :

```
sudo tail -f /var/opt/CSCOPx/MDC/log/operation/usmsharedsvcs.log
```

Exemple : création réussie d'un objet

```
26-Aug-2021 12:41:35.912, [INFO], (DefenseCenterServiceImpl.java:1442)
com.cisco.nm.vms.api.dc.DefenseCenterServiceImpl, ajp-nio-127.0.0.1-9009-exec-10
** REST Request [ CSM ]
** ID : 18b25356-fd6b-4cc4-8d27-bbccb52a6275
** URL: POST /audit
{
  "version": "7.1.0",
  "requestId": "18b25356-fd6b-4cc4-8d27-bbccb52a6275",
  "data": {
    "userName": "csdac-centos7",
    "subsystem": "API",
    "message": "POST
https://myfmc.example.com/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f
/object/dynamicobjects Created (201) - The request has been fulfilled and resulted in a new
resource being created",
    "sourceIP": "192.0.2.103",
```

```
"domainUuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f",
"time": "1629981695431"
},
"deleteList": []
}
```

Obtenir de manière manuelle un certificat de Chaîne d'autorité de certification (CA)

Si vous ne pouvez pas récupérer automatiquement la chaîne de l'autorité de certification, utilisez l'une des procédures suivantes spécifiques au navigateur pour obtenir une chaîne de certificat utilisée pour se connecter en toute sécurité à vCenter, NSX ou à Centre de gestion.

La *chaîne de certificats* est constituée du certificat racine et de tous les certificats subordonnés.

Vous devez utiliser l'une de ces procédures pour vous connecter aux éléments suivants :

- vCenter ou NSX

Il n'est pas nécessaire d'obtenir une chaîne de certificats pour se connecter à Azure ou AWS.

- Centre de gestion

Avant d'utiliser cette procédure, consultez la section relative à l'extraction automatique de la chaîne de l'autorité de certification dans :

- [Créer un connecteur vCenter](#)

Obtenir une chaîne de certificats - Mac (Chrome et Firefox)

Utilisez cette procédure pour obtenir une chaîne de certificats à l'aide des navigateurs Chrome et Firefox sur Mac OS.

1. Ouvrez une fenêtre de terminal.
2. Entrez la commande suivante.

```
security verify-cert -P url[:port]
```

où url est l'URL (y compris le schéma) de vCenter ou de Centre de gestion. Par exemple :

```
security verify-cert -P https://myvcenter.example.com
```

Si vous accédez à vCenter ou à centre de gestion en utilisant NAT ou PAT, vous pouvez ajouter un port comme suit :

```
security verify-cert -P https://myvcenter.example.com:12345
```

3. Enregistrer l'ensemble de la chaîne de certificats dans un fichier texte en clair.

- *Inclure* tous les délimiteurs----DÉBUT DU CERTIFICAT----- et -----FIN DU CERTIFICAT-----.
- *Exclure* tout texte superflu (par exemple, le nom du certificat et tout texte contenu dans les crochets d'angle (< et >) ainsi que les crochets eux-mêmes.

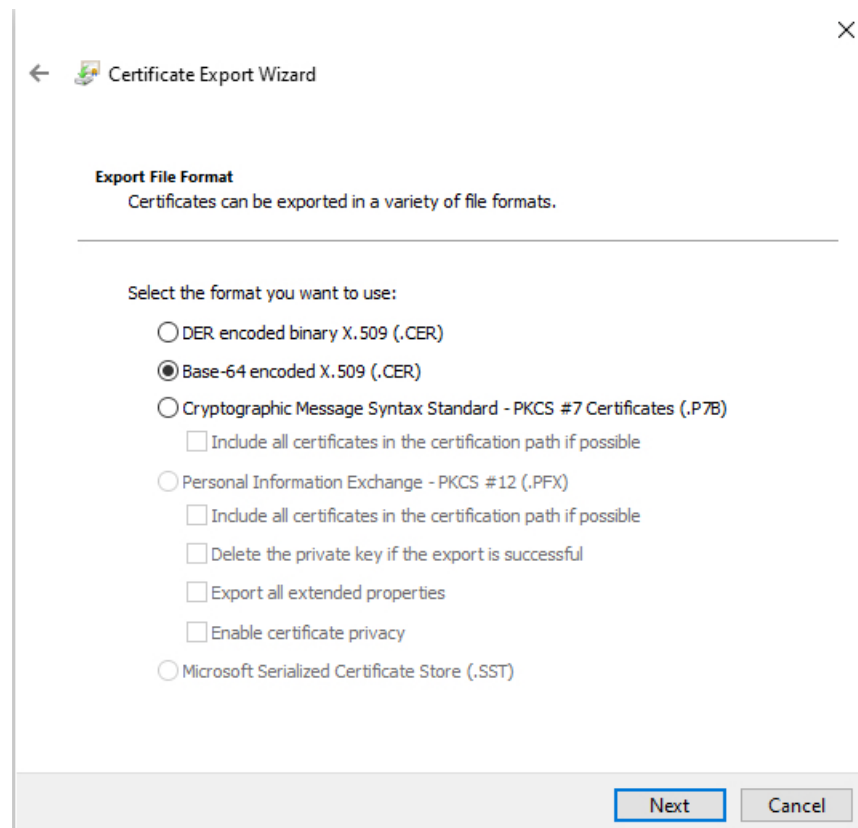
4. Répétez ces tâches pour le vCenter et le Centre de gestion.

Obtenir une chaîne de certificats - Windows Chrome

Utilisez cette procédure pour obtenir une chaîne de certificats à l'aide du navigateur Chrome sous Windows.

1. Se connecter à vCenter ou à Centre de gestion en utilisant Chrome.
2. Dans la barre d'adresse du navigateur, cliquez sur le cadenas à gauche du nom d'hôte.
3. Cliquez sur **Certificats**.
4. Cliquez sur l'onglet **Chemin de certification**.
5. Cliquez sur le premier certificat de la chaîne.
6. Cliquez sur **Afficher le certificat**.
7. Cliquez sur l'onglet **Détails**.
8. Cliquez sur **Copier dans un fichier**.
9. Suivez les invites pour créer un fichier de certificat au format CER qui inclut l'ensemble de la chaîne de certificats.

Lorsque vous êtes invité à choisir un format de fichier d'exportation, cliquez sur **Base 64-Encoded X.509 (.CER)** comme le montre la figure suivante.



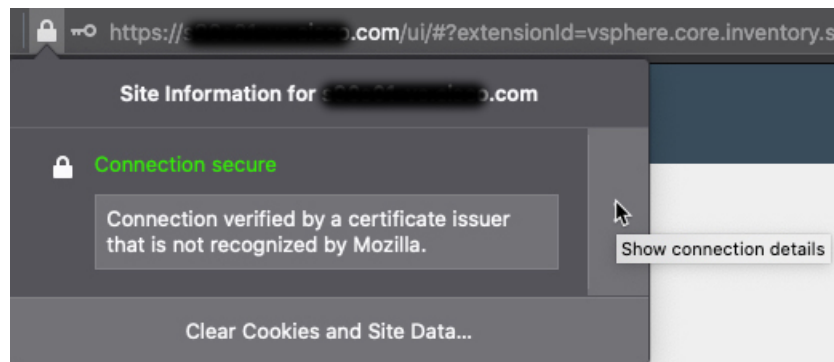
10. Suivez les invites pour terminer l'exportation.
11. Ouvrez le certificat dans un éditeur de texte.

12. Répétez le processus pour tous les certificats de la chaîne.
Vous devez coller chaque certificat dans l'éditeur de texte dans l'ordre, du premier au dernier.
13. Répétez ces tâches pour le vCenter et le FMC.

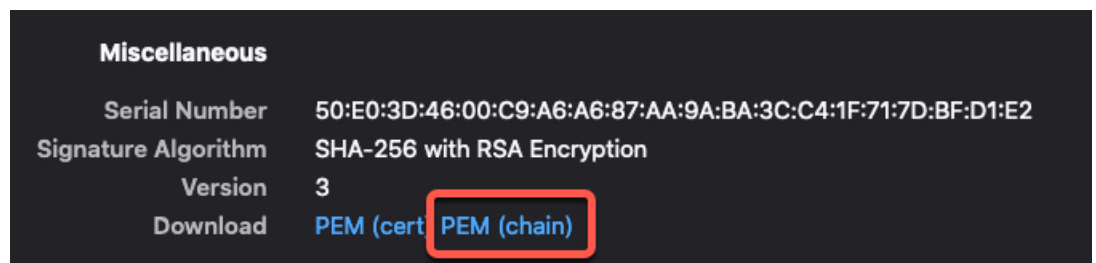
Obtenir une chaîne de certificats - Firefox sous Windows

La procédure suivante permet d'obtenir une chaîne de certificats pour le navigateur Firefox sous Windows ou Mac OS.

1. Connectez-vous à vCenter ou à Centre de gestion en utilisant Firefox.
2. Cliquez sur le cadenas à gauche du nom de l'hôte.
3. Cliquez sur la flèche droite (**Afficher les détails de la connexion**). La figure suivante présente un exemple.



4. Cliquez sur **Plus d'informations**.
5. Cliquez sur **Afficher le certificat**.
6. Si la boîte de dialogue résultante comporte des onglets, cliquez sur l'onglet correspondant à l'autorité de certification de premier niveau.
7. Faites défiler jusqu'à la section Divers.
8. Cliquez sur **PEM (chaîne)** sur la ligne Téléchargement. La figure suivante présente un exemple.



9. Enregistrez le fichier.
10. Répétez ces tâches pour le vCenter et le Centre de gestion.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d'incohérence, la version anglaise du présent contenu prévaudra.