Dépannage du message d'erreur dans Unity Connection dans Serviceability

Table des matières

Introduction

Ce document décrit comment dépanner un message d'erreur courant de Cisco Unity Connection sur la page de facilité de maintenance.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Unity Connection (CUC)
- Gestion des certificats pour serveurs unifiés

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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

Dans Cisco Unity Connection, lorsqu'un nouveau noeud est installé, un utilisateur et un mot de passe doivent être attribués, cet utilisateur est créé et stocké dans la base de données Cisco Unity.

Cette erreur apparaît pour différentes raisons, et rend impossible l'utilisation de la page de facilité de maintenance.

Étapes de dépannage

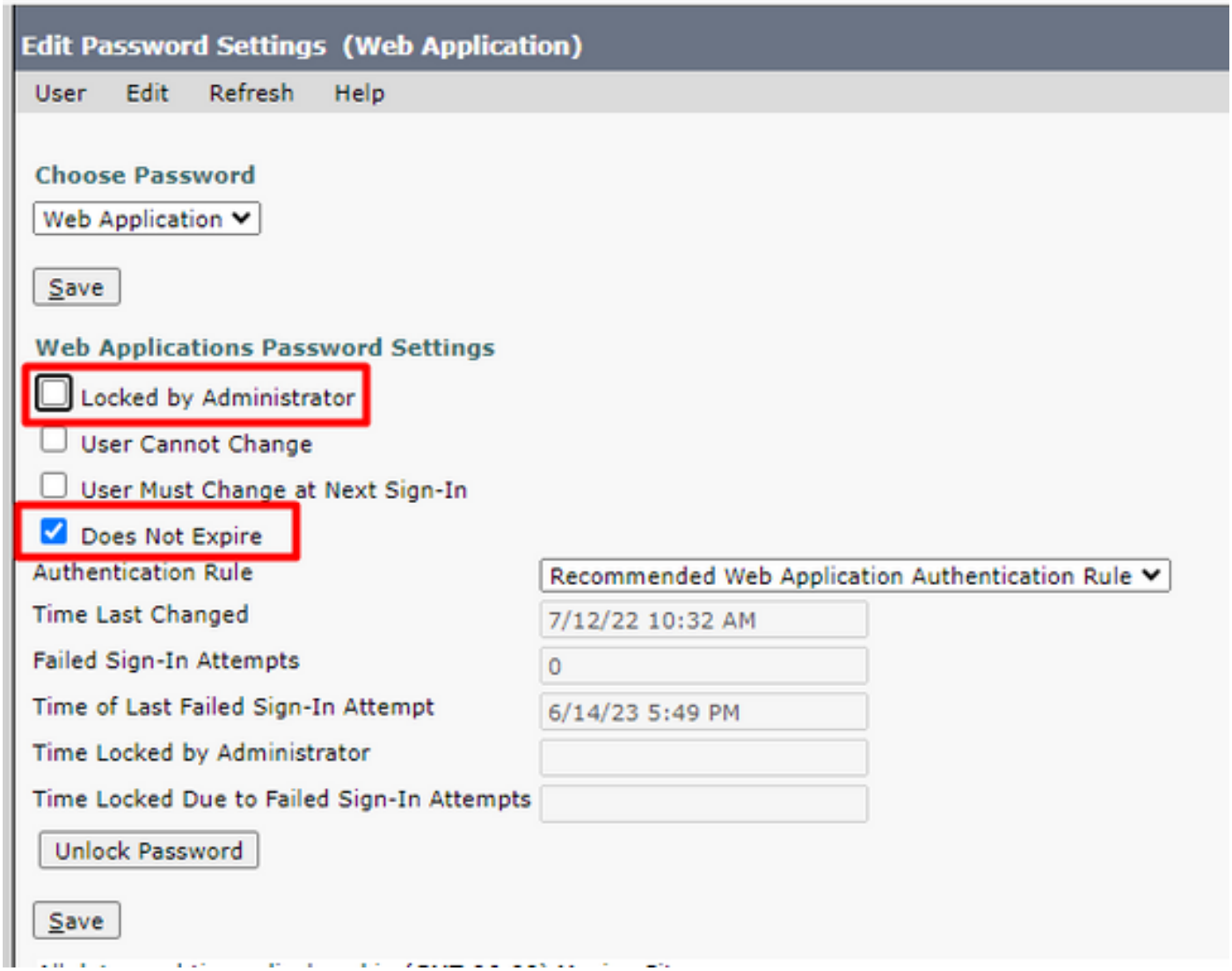
Afin de commencer à dépanner le problème, vous devez d'abord aller à l'utilisateur administrateur qui a été créé lors de l'installation de Unity :

Processus 1

Accédez à Cisco Unity Connection Administration > Go > Users > Select administration user > Edit > Password Settings

Décochez la case Verrouillé par l'administrateur pour déverrouiller le compte d'utilisateur.

Cochez la case Ne pas expirer pour éviter l'expiration du mot de passe.



Cliquez sur Déverrouiller le mot de passe > Enregistrer.

Accédez à la page Cisco Unity Connection Serviceability.

Processus 2

Si le problème peut encore être répliqué :

Accédez à Cisco Unity Connection Administration > Go > Users > Select the administrator user > Edit > Change Password et entrez un nouveau mot de passe.

Accédez à la page Cisco Unity Connection Serviceability et vérifiez si elle est accessible.

Processus 3

Si le problème persiste :

Accédez à Cisco Unified OS Administration > Go > Security > Certificate Management et vérifiez si les certificats Ipsec et Tomcat ne sont pas expirés.

Si les certificats ont expiré, ils doivent être régénérés.

Processus de régénération :

- Auto-signé:processus de régénération de certificat auto-signé
- CA -signed:processus de régénération des certificats signés CA

Processus 4

Si les certificats sont signés par une autorité de certification, vous devez vérifier si Cisco Unity Connection ne correspond pas à l'ID de bogue Cisco CSCvp31528.

Si Unity correspond, effectuez les solutions de contournement suivantes :

Solution 1

Demandez à l'autorité de certification de signer le certificat de serveur sans l'extension critique du nom alternatif de l'objet X509v3 et laissez les autres extensions en l'état.

Solution 2

Demandez à l'autorité de certification de signer le certificat du serveur et d'ajouter l'extension spécifiée en regard pour le faire fonctionner.
Contraintes de base X509v3 : critiques

Solution 3

Utiliser des certificats auto-signés, ce n'est pas toujours la solution idéale pour tous.

Solution 4

Comme l'une des dernières solutions de contournement disponibles, mettez à niveau vers la version qui contient le correctif du défaut et générez le CSR sur la version fixe et faites-le signer par CA comme il est connu avec le processus normal.

Processus 5

Sur CUC CLI :

1. Récupérez l'objectID de l'utilisateur administrateur d'application par défaut dans la base de données Unity Connection.

```
run cuc dbquery unitydirdb select name, value from vw_configuration where name='DefaultAdministrator'
```

Sortie de commande :

```
name                  value
--------------------  -------------------------------------
DefaultAdministrator  XXXX-XXXX-XXXXX-XXXX
```

2. Récupérez l'alias associé à l'objectID administrateur d'application par défaut. Dans une requête, remplacez le champ objectid='XXXX-XXXX-XXXXX-XXXX' par la valeur du résultat précédent.

```
run cuc dbquery unitydirdb select alias,objectid from vw_user where objectid='XXXX-XXXX-XXXXX-XXXX'
```

Sortie de commande :

```
alias     objectid
-----   -----------------------------------
admin   XXXX-XXXX-XXXXX-XXXX
```

3. Confirmez que le type de chiffrement est 4 pour l'authentification Web pour l'utilisateur administrateur d'application par défaut (le type d'identification 3 est pour le mot de passe d'application Web).

```
run cuc dbquery unitydirdb select objectid, userobjectid, credentialtype, encryptiontype from tbl_crede
```

Sortie de commande :

```
objectid                             userobjectid                         credentialtype encryptionty
------------------------------------ ------------------------------------ -------------- ------------
ZZZZZ-ZZZZZ-ZZZZZ-ZZZZZ                XXXX-XXXX-XXXXX-XXXX                          3              4
TTTTT-TTTTT-TTTTT-TTTTT                XXXX-XXXX-XXXXX-XXXX                          4              3
```

Si le type de cryptage = 3, passez à 4.

```
run cuc dbquery unitydirdb update tbl_credential set encryptiontype = "4" where objectid = "ZZZZZ-ZZZZZ
```

5. Le mot de passe doit être modifié car l'ancien mot de passe chiffrait l'utilisateur avec le type 3

```
utils cuc reset password <accountalias>
```

6. Redémarrez Tomcat via CLI

```
utils service restart Cisco Tomcat
```

Vérifiez si la page de maintenance est accessible.

Si le problème persiste, collectez les journaux Tomcat CUC à partir de RTMT.

Pour ce faire :

1. Ouvrez RTMT.
2. Insérez Cisco Unity Connection IP/Hostname.
3. Insérer l'utilisateur et le mot de passe.

4. Double-cliquez sur Collecter les fichiers. La fenêtre Collect Files (recueillir les fichiers) s’ouvre pour sélectionner les applications et les services UCM.

5. Dans Select UCM Services/Applications (sélectionner les services et les applications UCM), cochez la case de la colonne All Servers (tous les serveurs) pour :

- Cisco Tomcat

Informations connexes

- Assistance technique et téléchargements Cisco

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.