

Fehlerbehebung bei Fehlermeldungen in Unity Connection im Servicebereich

Inhalt

- [Einleitung](#)
- [Voraussetzungen](#)
- [Anforderungen](#)
- [Verwendete Komponenten](#)
- [Hintergrundinformationen](#)
- [Phasen der Fehlerbehebung](#)
- [Prozess 1](#)
- [Prozess 2](#)
- [Prozess 3](#)
- [Regenerationsprozess:](#)
- [Prozess 4](#)
- [Probleumgehung 1](#)
- [Probleumgehung 2](#)
- [Probleumgehung 3](#)
- [Prozess 5](#)
- [Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die Fehlerbehebung bei einer allgemeinen Cisco Unity Connection-Fehlermeldung auf der Wartungsseite beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Unity Connection (CUC)
- Zertifikatsverwaltung für einheitliche Server

Verwendete Komponenten

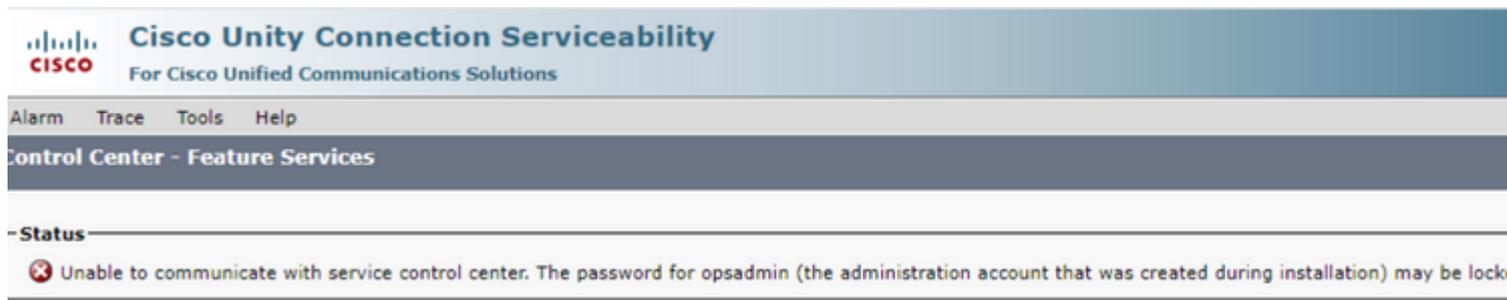
Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Wenn in Cisco Unity Connection ein neuer Knoten installiert wird, müssen ein Benutzer und ein Kennwort zugewiesen werden. Der Benutzer wird erstellt und in der Cisco Unity-Datenbank gespeichert.

Dieser Fehler tritt aus verschiedenen Gründen auf und macht es unmöglich, die Wartungsseite zu verwenden.



Phasen der Fehlerbehebung

Um mit der Fehlerbehebung zu beginnen, müssen Sie zuerst den Administratorbenutzer aufrufen, der bei der Installation von Unity erstellt wurde:

Prozess 1

Navigieren Sie zu **Cisco Unity Connection Administration > Go > Users > Select administration user > Edit > Password Settings**

Deaktivieren Sie das Kontrollkästchen **Durch Administrator gesperrt**, um das Benutzerkonto zu entsperren.

Aktivieren Sie das Kontrollkästchen **Läuft nicht ab**, um zu verhindern, dass das Kennwort abläuft.

Klicken Sie auf **Kennwort entsperren > Speichern**.

Navigieren Sie zur Seite Cisco Unity Connection Serviceability.

Prozess 2

Wenn das Problem weiterhin repliziert werden kann:

Navigieren Sie zu **Cisco Unity Connection Administration > Go > Users > Select the administrator user > Edit > Change Password**, und geben Sie ein neues Kennwort ein.

Navigieren Sie zur Seite "Serviceability" von Cisco Unity Connection, und prüfen Sie, ob darauf zugegriffen werden kann.

Prozess 3

Wenn das Problem weiterhin besteht:

Navigieren Sie zu **Cisco Unified OS Administration > Go > Security > Certificate Management**, und überprüfen Sie, ob die Ipsec- und Tomcat-Zertifikate nicht abgelaufen sind.

Wenn Zertifikate abgelaufen sind, müssen sie neu generiert werden.

Regenerationsprozess:

- Selbstsigniert: [Prozess zur Regenerierung selbstsignierter Zertifikate](#)
- CA -signiert: [Neugenerierung eines CA-signierten Zertifikats](#)

Prozess 4

Wenn die Zertifikate CA-signiert sind, müssen Sie überprüfen, ob Cisco Unity Connection nicht mit der Cisco Bug-ID [CSCvp31528](#) übereinstimmt.

Wenn Unity übereinstimmt, führen Sie die folgenden Workarounds aus:

Problemumgehung 1

Bitten Sie die Zertifizierungsstelle, das Serverzertifikat ohne die kritische Erweiterung des X509v3 Subject Alternative Name (Alternativer Name des X509v3-Betreffs) zu signieren, und lassen Sie andere Erweiterungen unverändert.

Problemumgehung 2

Bitten Sie die Zertifizierungsstelle, das Serverzertifikat zu signieren und die als Nächstes angegebene Erweiterung hinzuzufügen, damit es funktioniert.

X509v3-Basiseinschränkungen: kritisch

Problemumgehung 3

Verwenden Sie selbstsignierte Zertifikate, es ist nicht immer die richtige Lösung für alle.

Lösung 4

Als eine der letzten verfügbaren Problemumgehungen sollten Sie ein Upgrade auf Release durchführen, das die Behebung des Fehlers enthält, und das CSR für eine feste Version generieren und von der Zertifizierungsstelle signieren lassen, wie es beim normalen Prozess bekannt ist.

Prozess 5

Über die CUC-CLI:

1. Rufen Sie die objectID des Standardanwendungsadministratorbenutzers aus der Unity Connection-Datenbank ab.

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

Befehlsausgabe:

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

2. Rufen Sie den Alias ab, der mit der objectID des Standardanwendungsadministrators verknüpft ist. Ersetzen Sie bei der Abfrage das Feld objectid='XXXX-XXXX-XXXXX-XXXX' durch den Wert in der vorherigen Ausgabe.

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

Befehlsausgabe:

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

3. Bestätigen Sie, dass der Verschlüsselungstyp für die Webauthentifizierung für den Standardbenutzer des Anwendungsadministrators 4 ist (Anmeldeinformationstyp 3 ist für das Kennwort der Webanwendung).

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

Befehlsausgabe:

objectid	userobjectid	credentialtype	encryptiontype
-----	-----	-----	-----
ZZZZZ-ZZZZZ-ZZZZZ-ZZZZZ	XXXX-XXXX-XXXXX-XXXX	3	4
TTTTT-TTTTT-TTTTT-TTTTT	XXXX-XXXX-XXXXX-XXXX	4	3

Wenn Verschlüsselungstyp = 3 ist, ändern Sie den Wert in 4.

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

5. Das Kennwort muss geändert werden, da der Benutzer beim alten Kennwort mit Typ 3 verschlüsselt wurde.

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

6. Tomcat über CLI neu starten

```
utils service restart Cisco Tomcat
```

Überprüfen Sie, ob die Wartungsseite verfügbar ist.

Wenn das Problem weiterhin besteht, sammeln Sie CUC Tomcat-Protokolle von RTMT.

Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie RTMT.
2. Cisco Unity Connection-IP/Hostname einfügen.
3. Geben Sie den Benutzer und das Kennwort ein.
4. Doppelklicken Sie **auf Dateien sammeln**. Das Fenster "Dateien sammeln" wird geöffnet. Es wird auf "UCM-Dienste/Anwendungen auswählen" zugegriffen.
5. Aktivieren Sie in UCM-Dienste/Anwendungen auswählen das Kontrollkästchen in der Spalte Alle Server für:
 - Cisco Tomcat

Zugehörige Informationen

- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.