

可維護性中的Unity Connection中的錯誤消息故障排除

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[要排除故障的階段](#)

[流程1](#)

[流程2](#)

[流程3](#)

[再生過程：](#)

[流程4](#)

[解決方法1](#)

[解決方法2](#)

[解決方法3](#)

[流程5](#)

[相關資訊](#)

簡介

本文檔介紹如何對可維護性頁面上常見的Cisco Unity Connection錯誤消息進行故障排除。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Unity Connection(CUC)
- 適用於整合伺服器的憑證管理

採用元件

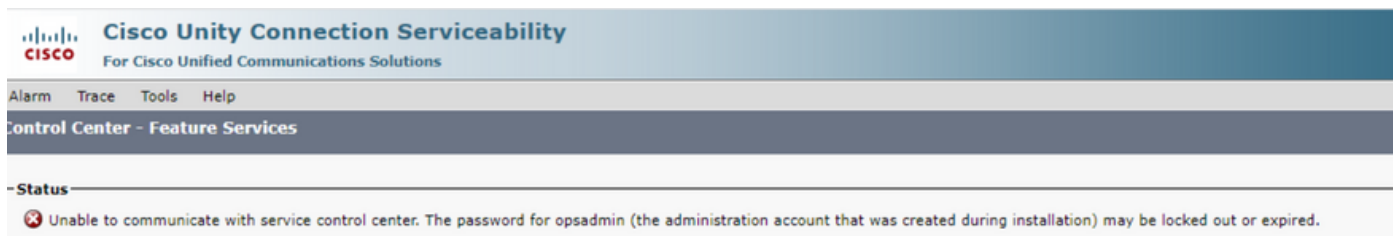
本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

在Cisco Unity Connection中，當安裝新節點時，必須分配使用者和密碼，此使用者將被建立並儲存在Cisco Unity資料庫中。

出現此錯誤的原因各不相同，因此無法使用可維護性頁面。



要排除故障的階段

若要開始排除故障，首先需要轉到安裝Unity時建立的管理員使用者：

流程1

導航到Cisco Unity Connection Administration > Go > Users > Select administration user > Edit > Password Settings

取消選中Locked by Administrator覈取方塊以解鎖使用者帳戶。

選中Does Not Expire覈取方塊以避免密碼過期。

Edit Password Settings (Web Application)

User Edit Refresh Help

Choose Password

Web Application ▼

Save

Web Applications Password Settings

Locked by Administrator

User Cannot Change

User Must Change at Next Sign-In

Does Not Expire

Authentication Rule Recommended Web Application Authentication Rule ▼

Time Last Changed 7/12/22 10:32 AM

Failed Sign-In Attempts 0

Time of Last Failed Sign-In Attempt 6/14/23 5:49 PM

Time Locked by Administrator

Time Locked Due to Failed Sign-In Attempts

Unlock Password

Save

按一下Unlock Password > Save。

導航至Cisco Unity Connection Serviceability頁面。

流程2

如果問題仍然存在：

導航到Cisco Unity Connection Administration > Go > Users > Select the administrator user > Edit > Change Password，然後輸入新密碼。

導航至Cisco Unity Connection Serviceability頁面，驗證其是否可訪問。

流程3

如果問題仍然存在：

導覽至Cisco Unified OS Administration > Go > Security > Certificate Management，然後驗證Ipsec和Tomcat證書是否未過期。

如果證書已過期，必須重新生成證書。

再生過程：

- 自簽名：自簽名的證書再生過程
- CA — 簽名：CA簽名的證書再生過程

流程4

如果憑證是CA簽署，則需要驗證Cisco Unity Connection是否與Cisco錯誤ID [CSCvp31528](#)相符。

如果Unity匹配，請執行下面的解決方法：

解決方法1

要求CA在沒有X509v3使用者替代名稱的關鍵副檔名的情況下簽署伺服器證書，並讓其他副檔名保持原樣。

解決方法2

請CA對伺服器證書進行簽名，並新增旁邊指定的副檔名使其起作用。
X509v3基本限制：關鍵

解決方法3

使用自簽名證書，它並不總是適合所有使用者的解決方案。

解決方法4

作為最後一個可用的變通方法之一，請升級到「版本」，其中包含缺陷的修復；然後，在固定版本上產生CSR，並由CA簽署，如同使用正常流程所知的。

流程5

在CUC CLI上：

1.從Unity Connection資料庫中檢索預設應用程式管理員使用者的objectID。

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

命令輸出：

name	value
DefaultAdministrator	XXXX-XXXX-XXXXX-XXXX

2.檢索與預設應用程式管理員objectID關聯的別名。查詢時將欄位objectid='XXXX-XXXX-XXXXX-XXXX'替換為先前輸出中的值。

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

命令輸出：

alias	objectid
admin	XXXX-XXXX-XXXXX-XXXX

3.確認預設應用程式管理員使用者的Web身份驗證的加密型別為4 (Credentialtype 3用於Web應用程式密碼)。

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

命令輸出：

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

如果加密型別= 3，則更改為4。

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

5.必須更改密碼，因為舊密碼已使用型別3對使用者進行了加密

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

6.通過CLI重新啟動Tomcat

```
utils service restart Cisco Tomcat
```

驗證可維護性頁面是否可訪問。

如果問題仍然存在，請從RTMT收集CUC Tomcat日誌。

為此，請執行以下操作：

1. 開啟RTMT。
2. 插入Cisco Unity Connection IP/主機名。
3. 插入使用者和密碼。
4. 按兩下「Collect Files(收集檔案)」。將開啟「收集檔案」視窗以選擇UCM服務/應用程式。
5. 在選擇UCM服務/應用程式中，點選所有伺服器列中的覈取方塊：

- Cisco Tomcat

相關資訊

- [思科技術支援與下載](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。