

排除CER備份失敗並出現錯誤消息故障

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[疑難排解](#)

[日誌收集](#)

[日誌分析](#)

[糾正措施](#)

[案例 1](#)

[案例 2](#)

[相關資訊](#)

簡介

本文檔介紹如何對Cisco Emergency Responder(CER)無法備份並在狀態下顯示錯誤消息進行故障排除。

必要條件

需求

思科建議瞭解以下主題：

- 思科緊急回應端
- 對安全憑證的基本瞭解

採用元件

本檔案中的資訊是根據以下軟體版本：

- 思科緊急回應端11.5.4.60000-5

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

在群集模式下部署的CER可能無法備份，並顯示錯誤消息「無法聯絡伺服器」。主代理或本地代理可能關閉」。

舉例來說：

The screenshot shows a 'Backup Status' window with a 'Refresh' button and a 'Cancel' button. Below the buttons, there is a 'Status' section with a warning icon and the text: 'WARNING: Unable to contact server. Master or Local Agent could be down, Backup Completed...'. Underneath is the 'Backup details' section, which includes the following information:

- Tar Filename: 2023-06-21-08-02-15.tar
- Backup Device: [Redacted]
- Operation: BACKUP
- Percentage Complete: 52%

Below this information is a table with the following columns: Feature, Server, Component, Status, Result **, Start Time, and Log File *. The table contains 8 rows, all of which show a status of 0 and a result of 'Unable to contact server. Master or Local Agent could be down'.

Feature	Server	Component	Status	Result **	Start Time	Log File *
CER			0	Unable to contact server. Master or Local Agent could be down	---	
CER			0	Unable to contact server. Master or Local Agent could be down	---	
CER			0	Unable to contact server. Master or Local Agent could be down	---	
CER			0	Unable to contact server. Master or Local Agent could be down	---	
CER			0	Unable to contact server. Master or Local Agent could be down	---	
CER			0	Unable to contact server. Master or Local Agent could be down	---	
CER			0	Unable to contact server. Master or Local Agent could be down	---	
CER			0	Unable to contact server. Master or Local Agent could be down	---	

CER備份錯誤消息

受影響的版本是11.x及更高版本。

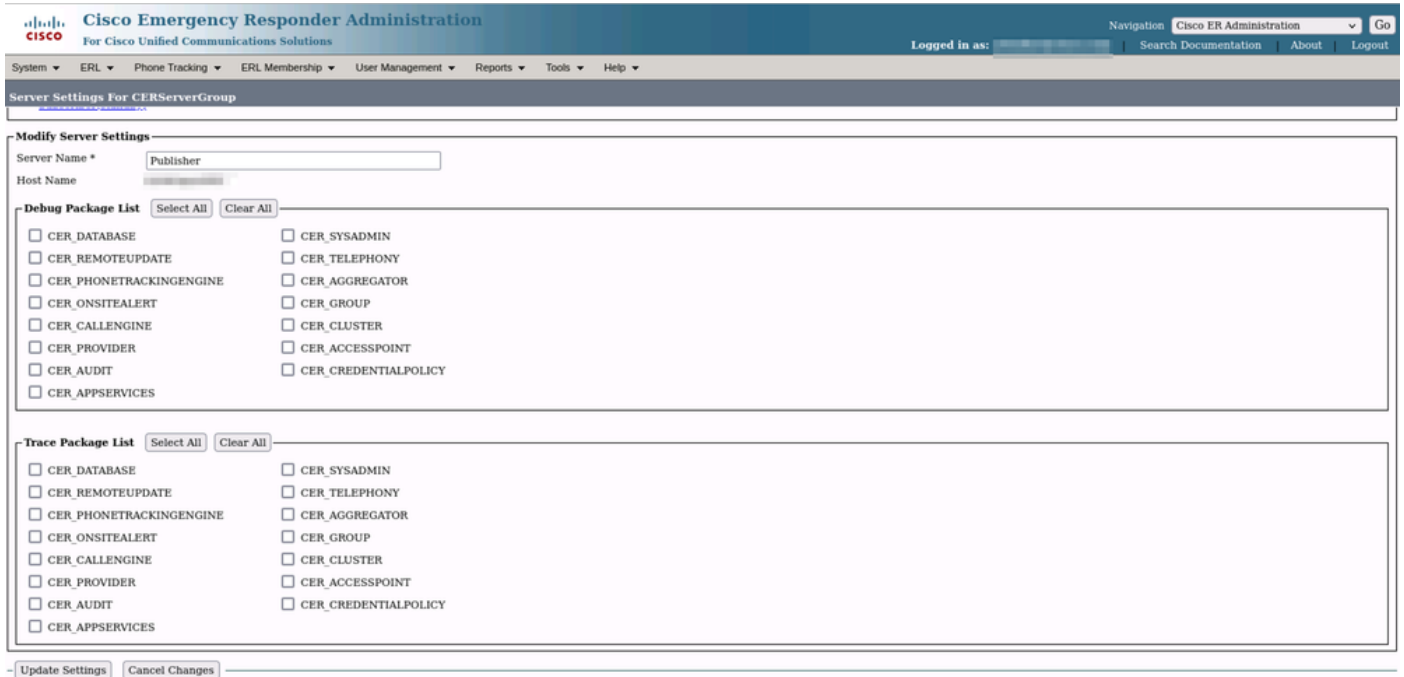
疑難排解

日誌收集

發生這種情況時，請收集日誌以嘗試收集儘可能多的資訊，以嘗試確定問題的根源並確定解決該問題的正確行動計畫。

收集日誌之前，請啟用詳細跟蹤和調試，完成以下步驟：

1. 登入到CER管理網頁。
2. 導覽至System > Server Settings。預設情況下，CER發佈伺服器處於選中狀態。如果還需要CER訂閱伺服器日誌，則可以更改該發佈伺服器。
3. 按一下「調試包清單」和「跟蹤包清單」部分的全選。
4. 按一下「Update Settings」。

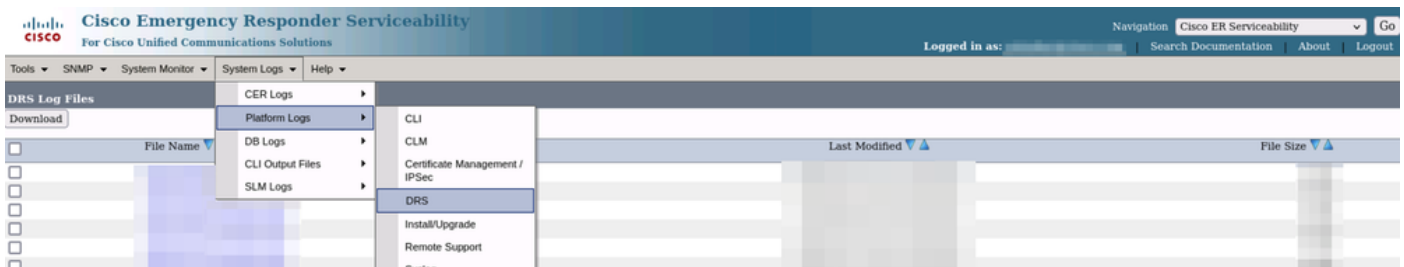


CER啟用調試和跟蹤

現在，請重複這個問題。

複製問題後，請繼續從Cisco ER可維護性網頁收集適用於複製嘗試的DRS日誌，完成以下步驟：

1. 在Navigation中選擇Cisco ER Serviceability。
2. 導航到System Logs > Platform Logs > DRS。



CER收集DRS日誌

日誌分析

在分析日誌時，我們開始看到伺服器嘗試與它的對等體建立連線的位置，並且我們看到日誌中的錯誤消息，指出故障的原因。

在CER發佈器DRF MA日誌中：

2023-06-21 07:58:58,148 DEBUG [Thread-16] - drfNetServerClient: drfQueryTruststore: IPsec trustStore中的條目數：1

2023-06-21 07:58:58,148 DEBUG [Thread-16] - drfNetServerClient: drfQueryTruststore — 每20小時運行一次Query truststore

2023-06-21 07:58:58,168錯誤[NetServerWorker] - drfNetServerWorker.drfNetServerWorker：無法建立到客戶端的輸入/輸出流收到嚴重警報：錯誤證書

2023-06-21 08:04:46,274 DEBUG [NetServerWorker] - drfNetServer.run : 收到來自/IP:Port的客戶端套接字請求

2023-06-21 08:04:46,274 DEBUG [NetServerWorker] — 驗證客戶端請求是否來自群集中的節點

2023-06-21 08:04:46,278 DEBUG [NetServerWorker] — 已驗證的客戶端。IP = 10.10.20.25主機名 = device.test.org。請求來自群集中的節點

2023-06-21 08:04:46,278 DEBUG [NetServerWorker] - drfNetServerWorker : 要建立的套接字對象輸入流

2023-06-21 08:04:46,313錯誤[NetServerWorker] - drfNetServerWorker.drfNetServerWorker : 無法建立到客戶端的輸入/輸出流收到嚴重警報：錯誤證書

在CER發佈器DRF本地日誌中：

2023-06-21 07:58:47,453 DEBUG [main] - drfNetServerClient:Reconnect , 無法連線到主機：[X]，消息：連線被拒絕（連線被拒絕），原因：空

在此之前，我們看到連線由於證書錯誤而被拒絕。

用於為備份/恢復在節點之間建立可信連線的證書是IPSec。此時，我們已經可以確定該問題與IPSec證書過期或某個伺服器中存在不正確的證書有關。

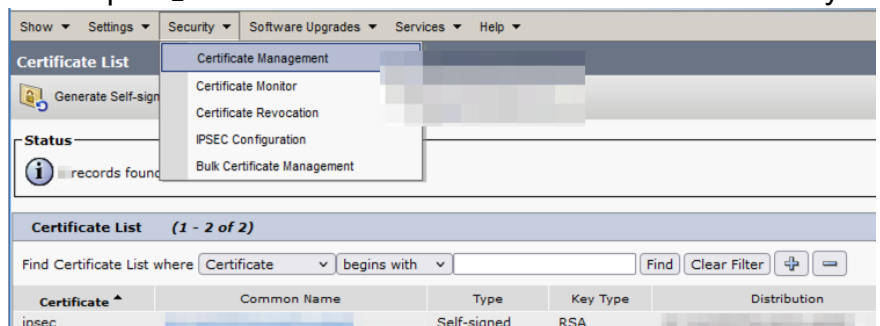
糾正措施

1. 驗證所有CER訂戶節點中IPSec信任證書的序列號(SN)，該序列號必須與CER發佈者提供的IPSec.prem的SN匹配(場景1)。
2. 確認CER Publisher節點中IPSec.pem證書的有效性。日期必須有效或者必須重新生成IPSec證書(案例2)。

案例 1

IPSec證書SN在CER已發佈訂閱伺服器和CER訂閱伺服器之間不匹配。請繼續執行以下步驟：

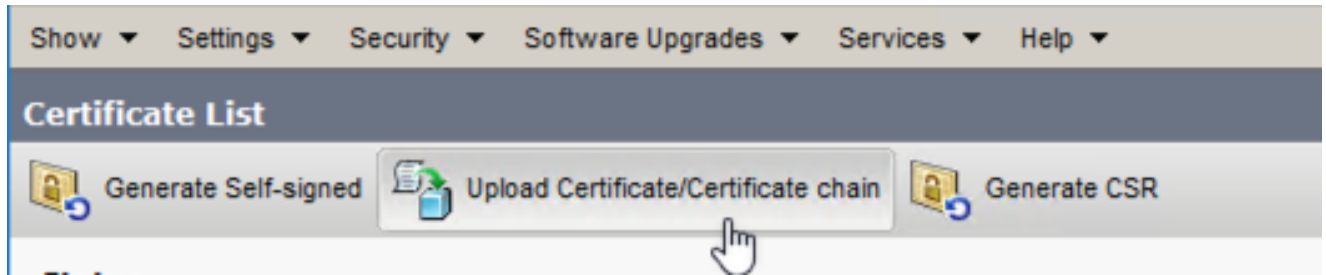
1. 刪除CER訂閱伺服器中的IPSec-trust證書，其中序列號與CER發佈伺服器中的序列號不匹配。
2. 從CER發佈器從以下路徑下載「IPSec.pem」：Cisco Unified OS Administration > Security >



Certificate Management > Find

CER ipsec.pem證書

3. 上傳路徑Cisco Unified OS Administration > Security > Certificate Management > Upload the certificate as IPSec-trust所需的CER Subscribers中的「IPSec.pem」檔案。



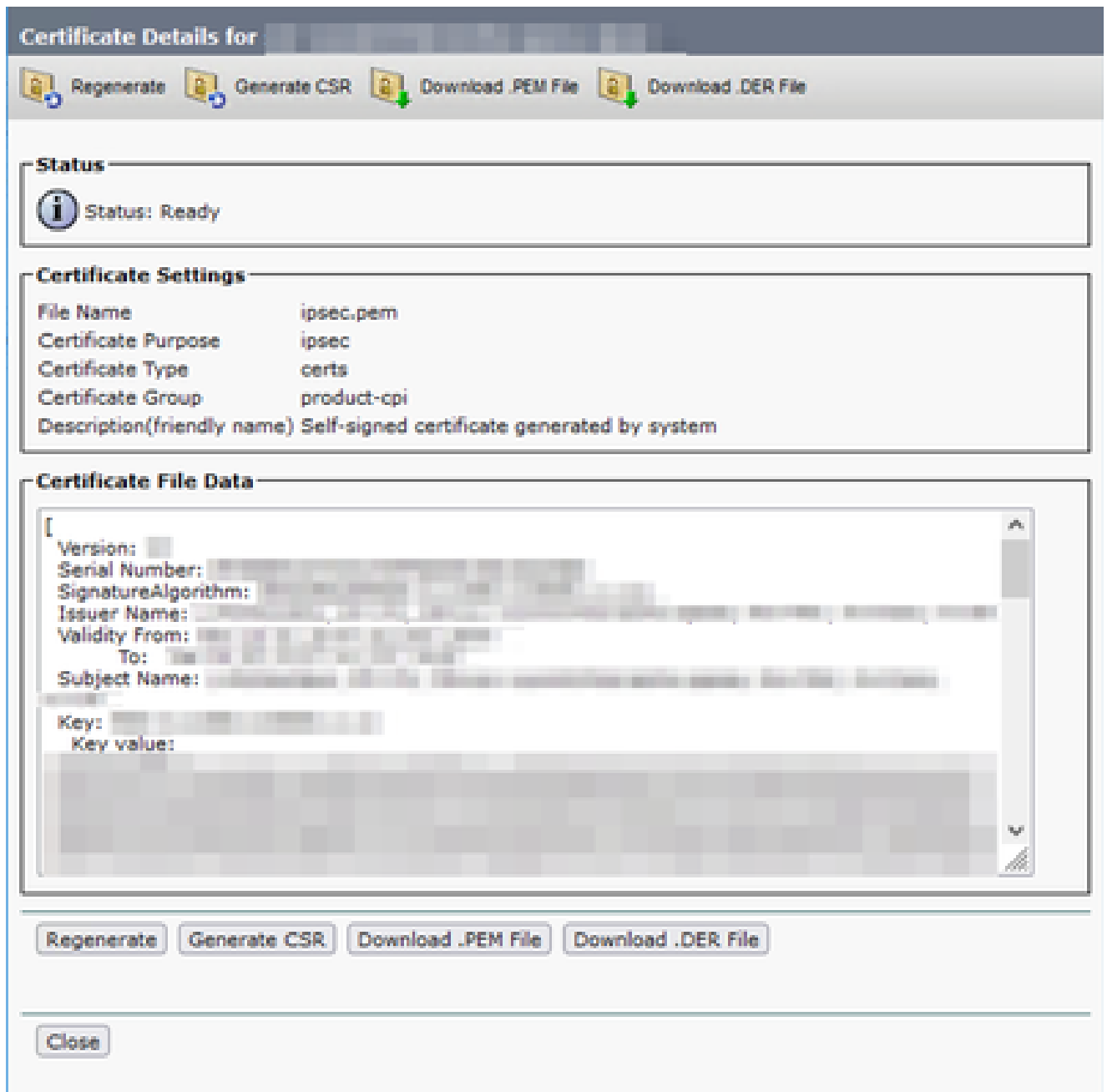
CER ipsec.trust證書上傳

4. 在所有CER節點中重新啟動DRF Local和DRF Master服務。

案例 2

IPSec已過期，需要重新生成。請繼續執行以下步驟：

1. 針對群集中的每個伺服器，導航到Cisco Unified OS Administration > Security > Certificate Management。從發佈伺服器開始，然後每個訂閱伺服器。
2. 從CER Publisher開始，按一下Find以顯示伺服器中的所有證書。
3. 按一下證書「IPSec.pem」。
4. 這將顯示Certificate資訊，然後按一下Regenerate。



CER ipsec.pem重新生成

5. 在CER發佈器中重新生成證書並顯示Success消息後，請在CER訂閱伺服器節點中重複步驟1-4。
6. 在所有節點中重新生成證書後，請重新啟動以下服務：
 - 僅CER Publisher中的Cisco DRF Master:
 - 導航至CER Serviceability > Tools > Control Center Services > Cisco DRF Master

Control Center

Control Center Services

Start

Stop

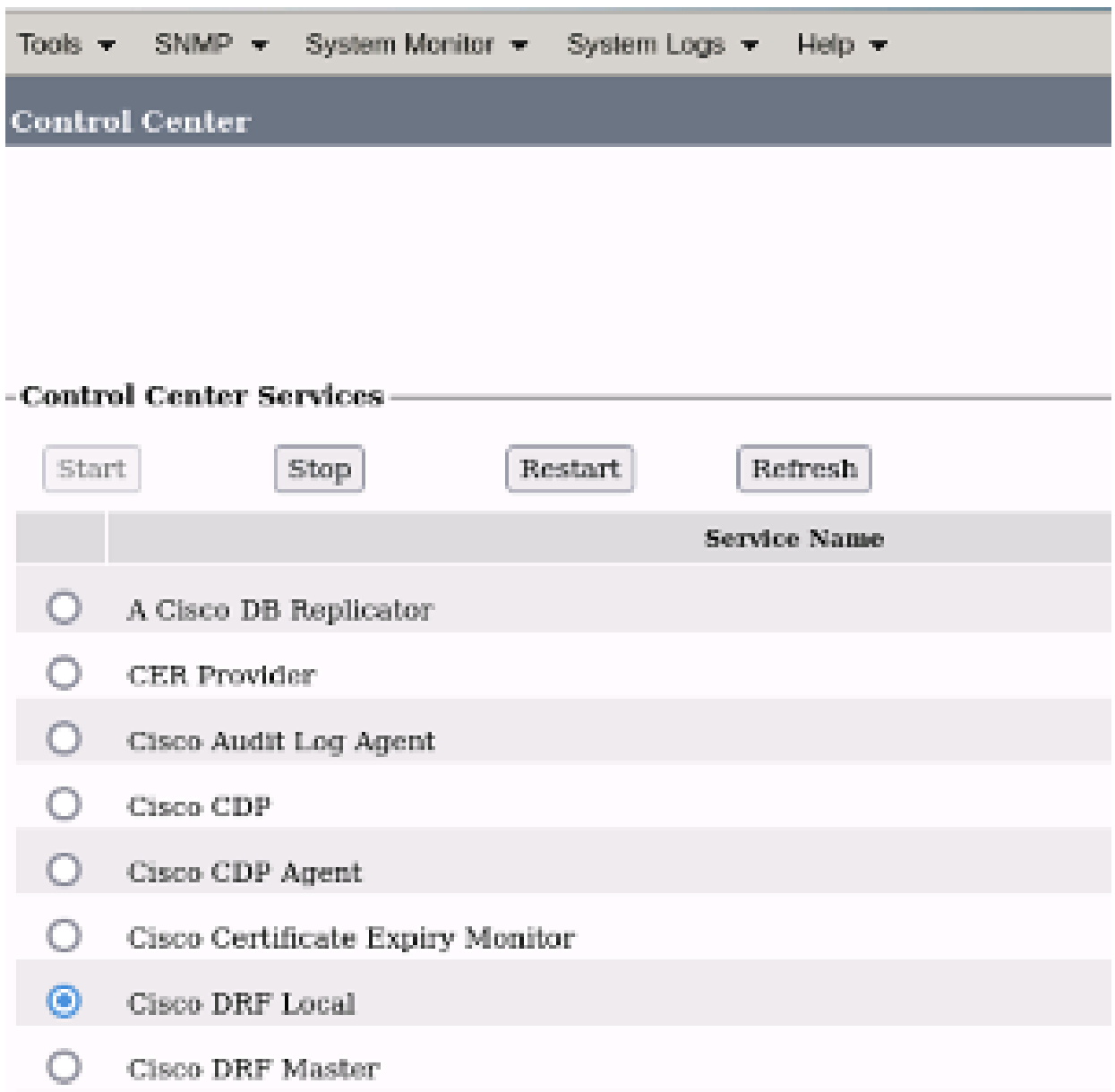
Restart

Refresh

	Service Name
<input type="radio"/>	A Cisco DB Replicator
<input type="radio"/>	CER Provider
<input type="radio"/>	Cisco Audit Log Agent
<input type="radio"/>	Cisco CDP
<input type="radio"/>	Cisco CDP Agent
<input type="radio"/>	Cisco Certificate Expiry Monitor
<input type="radio"/>	Cisco DRF Local
<input checked="" type="radio"/>	Cisco DRF Master

CER Cisco DRF主重新啟動

- Cisco DRF主服務啟用後，首先在CER發佈器中重啟Cisco DRF Local。



CER Cisco DRF本地重新啟動

- 一旦Cisco DRF Local服務在CER發佈伺服器節點中處於活動狀態，請在所有CER訂閱伺服器節點中重新啟動該服務。
7. 在所有節點上重新啟動服務後，請執行系統的手動備份：
- 導覽至Disaster Recovery System > Backup > Manual Backup。
 - 選擇備份裝置名稱。
 - 選擇備份的功能。
 - 按一下以啟動備份。

相關資訊

[如何收集CER日誌](#)

[重新生成CUCM證書](#)

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）。