

Konfigurieren von Backup und Wiederherstellung über GUI in CUCM

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Backup](#)

[Wiederherstellen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument werden die Setup-Anforderungen für **Backup** und **Restore** Funktionen in **CUCM** von der **Graphic User Interface (GUI)**.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- **Cisco Unified Communications Manager**
- **Secure File Transfer Protocol (SFTP)**

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- **Cisco Unified Communications Manager Version 10.5.2.15900-8**

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 verstehen.

Hintergrundinformationen

Die Fehlermeldung **Disaster Recovery System (DRS)**, der von der CUCM-Verwaltung aufgerufen werden kann, bietet vollständige Funktionen für Datensicherung und Wiederherstellung für alle Server im Cluster. Das DRS ermöglicht regelmäßig geplante automatische oder vom Benutzer aufgerufene

Datensicherungen.

DRS stellt seine eigenen Parameter (Backup-Geräte- und Zeitplanparameter) als Teil der Backup-/Wiederherstellungsplattform wieder her. DRS sichert und stellt das `drfDevice.xml` und `drfSchedule.xml` Dateien. Wenn der Server mit diesen Dateien wiederhergestellt wird, ist es nicht erforderlich, das DRS-Sicherungsgerät neu zu konfigurieren und einen Zeitplan zu erstellen.

Die Fehlermeldung **Disaster Recovery System** bietet folgende Funktionen:

- Eine Benutzeroberfläche zur Durchführung von Backup- und Wiederherstellungsaufgaben
- Verteilte Systemarchitektur mit Backup- und Wiederherstellungsfunktionen
- Geplante Backups
- Archivierung von Backups auf einem physischen Bandlaufwerk oder einem Remote-SFTP-Server

Die Fehlermeldung **Disaster Recovery System** enthält zwei Schlüsselfunktionen, **Master Agent (MA)** und **Local Agent (LA)**.

Die Fehlermeldung **Master Agent** koordiniert Backup- und Wiederherstellungsaktivitäten mit **Local Agents**. Das System aktiviert automatisch die **Master Agent** und **Local Agent** auf allen Knoten im Cluster.

CUCM-Cluster (dies betrifft die CUCM-Knoten und die **Cisco Instant Messaging & Presence (IM&P) Server**) müssen folgende Anforderungen erfüllen:

- **Port 22** offen, um die Kommunikation mit dem SFTP-Server herzustellen.
- Validierte, dass die **IPsec** und **Tomcat** Zertifikate sind nicht abgelaufen. Um die Gültigkeit der Bescheinigungen zu überprüfen, fliegen nach **Cisco Unified OS Administration > Security > Certificate Management**

Hinweis: Verwenden Sie das [Verfahren](#) zum Regenerieren von IPsec- und Tomcat-Zertifikaten [in CUCM](#).

- Stellen Sie sicher, dass die Datenbankreplikation eingerichtet wurde und keine Fehler oder Diskrepanzen zwischen den CUCM Publisher- und den IM&P Publisher-Servern zeigt.

Die SFTP-Servereinstellungen müssen die folgenden Anforderungen erfüllen:

- Anmeldeinformationen sind verfügbar.
- Sie muss vom CUCM-Server aus erreichbar sein.
- Dateien werden in den Pfad eingefügt, der bei der Wiederherstellung ausgewählt wird

Konfigurieren

Backup

Die Fehlermeldung **Disaster Recovery System** führt ein Backup auf Cluster-Ebene durch, d. h. es sammelt Backups für alle Server in einem CUCM-Cluster an einem zentralen Standort und archiviert die Backup-Daten auf einem physischen Speichergerät.

Schritt 1: Um Backup-Devices zu erstellen, auf denen Daten gespeichert werden, navigieren Sie zu **Disaster Recovery System > Backup > Backup Device**.

Schritt 2: Auswählen **Add New**; definieren Sie **Backup Device Name** und geben Sie die SFTP-Werte ein.
Save

The screenshot shows the 'Backup Device' configuration page in the Cisco Disaster Recovery System. At the top, there is a navigation bar with 'Backup', 'Restore', and 'Help' menus. Below this is a header for 'Backup Device' with 'Save' and 'Back' buttons. The main content area is divided into sections: 'Status' (Status: Ready), 'Backup device name' (Backup device name*: BackupDevice1), and 'Select Destination*' (Network Directory). The Network Directory section includes fields for Host name/IP address (10.1.89.107), Path name (/), User name (administrator), Password (masked with dots), and Number of backups to store on Network Directory (2). At the bottom, there are 'Save' and 'Back' buttons.

Schritt 3: Erstellen und bearbeiten Sie Backup-Zeitpläne, um Daten zu sichern. Navigieren Sie zu **Backup > Scheduler**.

Schritt 4: Definieren eines **Schedule Name**. Wählen Sie **Device Name** und überprüfen Sie **Features** basierend auf Ihrem Szenario.

The screenshot shows the 'Scheduler' configuration page in the Cisco Disaster Recovery System. At the top, there is a navigation bar with 'Backup', 'Restore', and 'Help' menus. Below this is a header for 'Scheduler' with 'Save', 'Set Default', 'Disable Schedule', 'Enable Schedule', and 'Back' buttons. The main content area is divided into sections: 'Status' (Status: Ready), 'Schedule Name' (Schedule Name*: DailyBackUp), 'Select Backup Device' (Device Name*: BackupDevice1), and 'Select Features *'. The Select Features section includes checkboxes for CDR_CAR, UCM (checked), and PLM.

Schritt 5: Konfigurieren Sie ein zeitgesteuertes Backup basierend auf Ihrem Szenario.

Start Backup at*

Date: 2019 Jun 18 Time: 00 Hour 00 Minute

Frequency*

Once
 Daily
 Weekly
 Monthly

Monday Tuesday Wednesday Thursday
 Friday Saturday Sunday

Schritt 6: Auswählen **save** und beachten Sie die Warnung, wie im Bild dargestellt. Auswählen **ok** um voranzukommen.



Schritt 7. Sobald dies möglich ist **Backup Schedule** wird erstellt, wählen Sie **Enable Schedule** .

Scheduler

Save Set Default Disable Schedule Enable Schedule Back

Status
Disabled

Schedule Name
Schedule Name* DailyBackUp

Schritt 8: Warten Sie, bis der Status auf geändert wird. **Enabled**.

Disaster Recovery System
For Cisco Unified Communications Solutions

Backup Restore Help

Scheduler

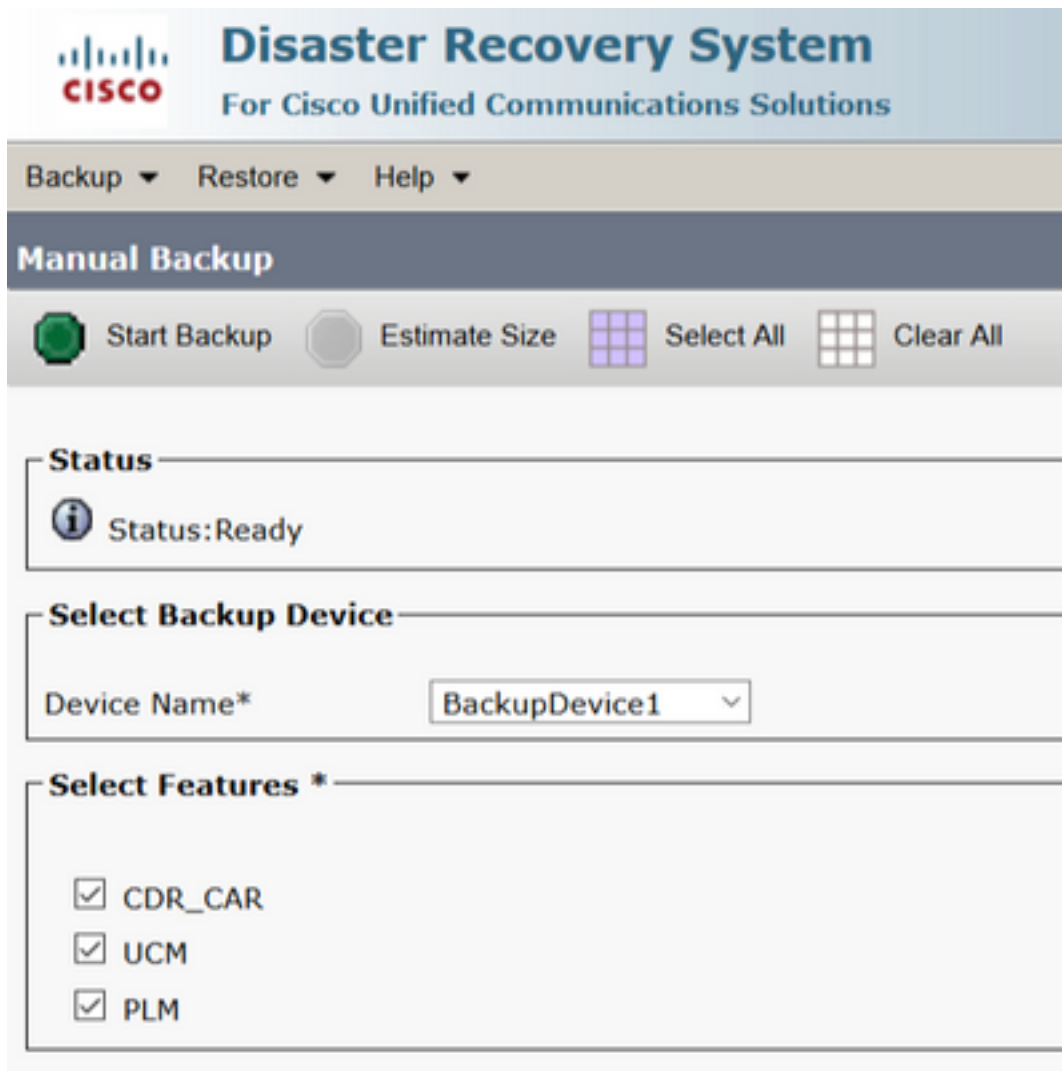
Save Set Default Disable Schedule Enable Schedule Back

Status
Enabled

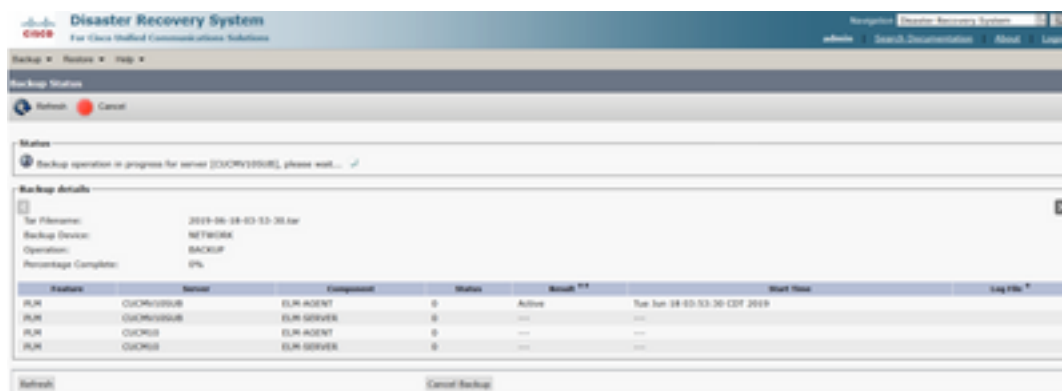
Schedule Name
Schedule Name* DailyBackUp

Schritt 9. Wenn eine manuelle Sicherung erforderlich ist, navigieren Sie zu **Backup > Manual Backup**.

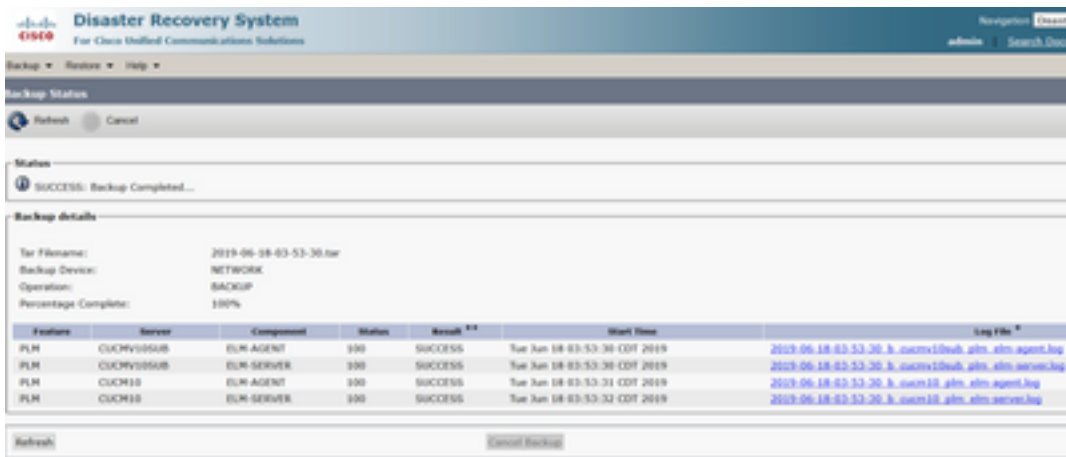
Schritt 10. Wählen Sie **Device Name** und überprüfen Sie **Features** basierend auf Ihrem Szenario.



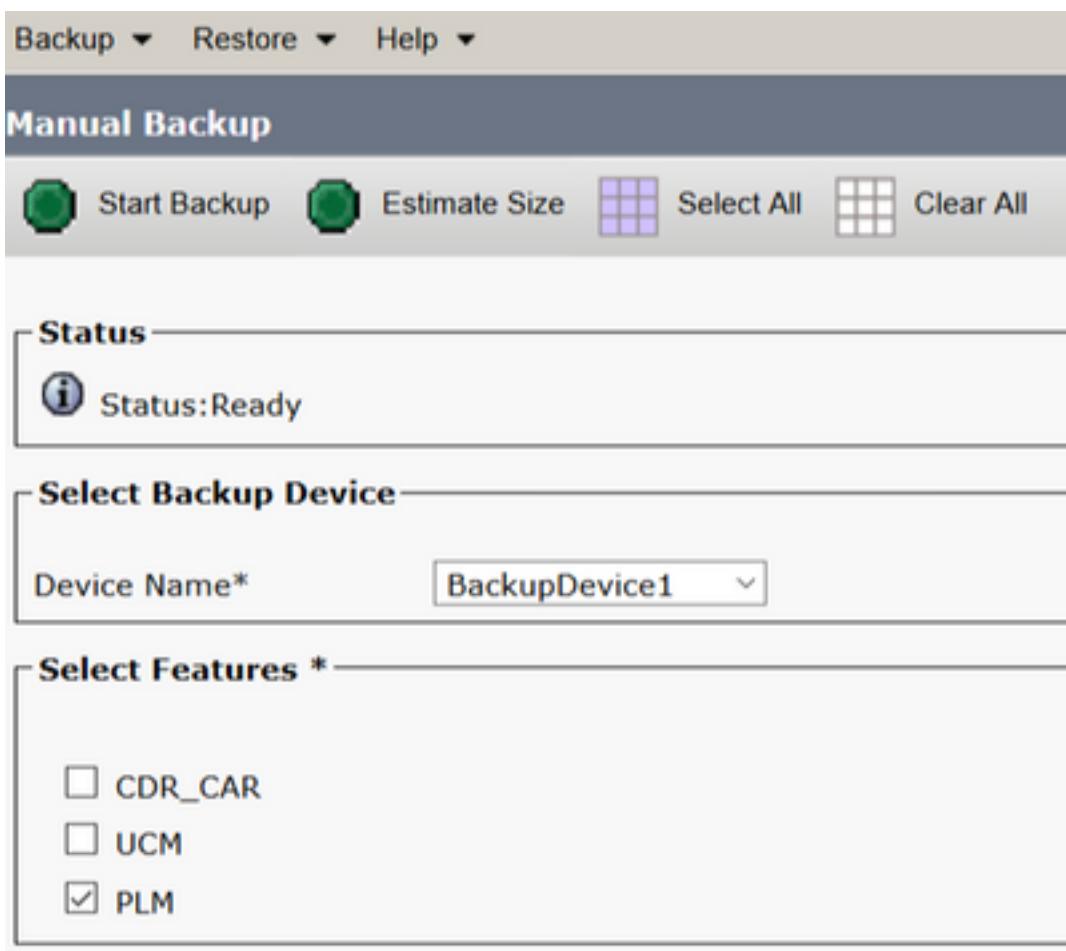
Schritt 11. Auswählen **Start Backup** und der Vorgang wird angezeigt.



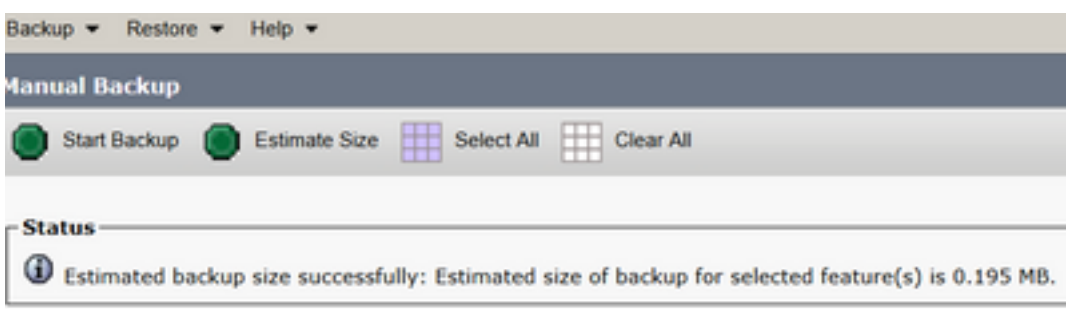
Schritt 12: Wenn die manuelle Sicherung abgeschlossen ist, wird die Abschlussmeldung angezeigt.



Schritt 13: Um die Größe der Backup-TAR-Datei zu schätzen, die vom SFTP-Gerät verwendet wird, wählen Sie Estimate Size.

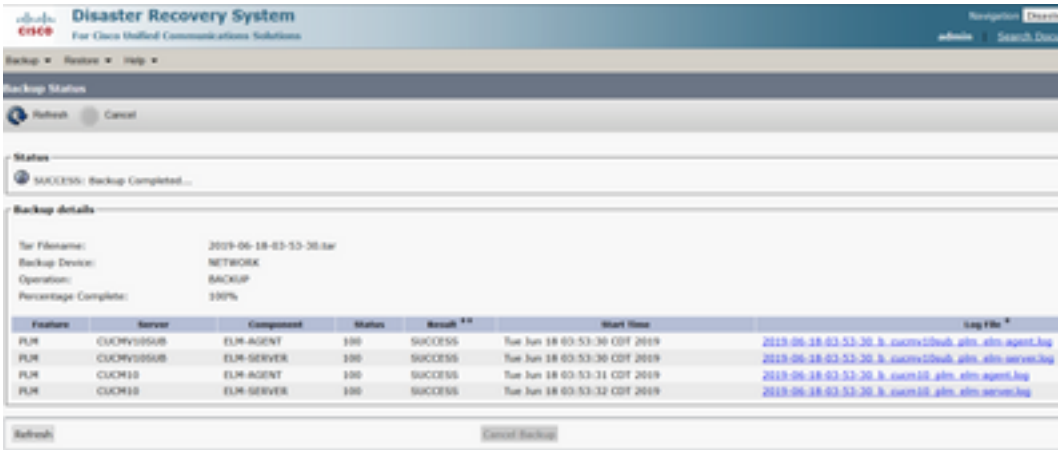


Schritt 14: Die Größe der Schätzung wird wie im Bild dargestellt angezeigt.

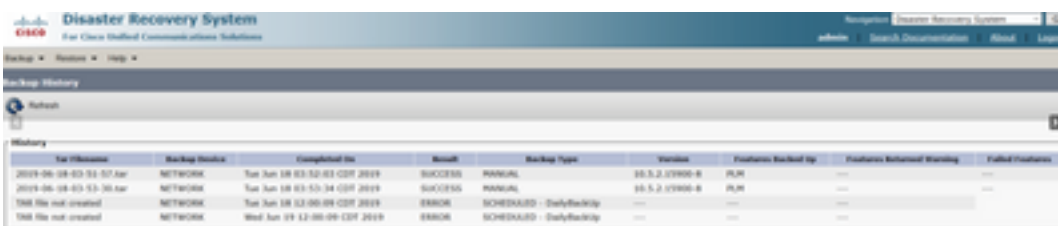


Hinweis: Die Funktion zur Größenschätzung wird auf der Grundlage früherer erfolgreicher Sicherungen berechnet und kann variieren, falls die Konfiguration seit der letzten Sicherung geändert wurde.

Schritt 15: Um den Status der Sicherung während der Ausführung einer Sicherung zu überprüfen, navigieren Sie zu **Backup > Backup Status**.



Schritt 16: Um die im System ausgeführten Sicherungsverfahren anzuzeigen, navigieren Sie zu **Backup > History**.



Wiederherstellen

DRS stellt hauptsächlich wieder her `drfDevice.xml` und `drfSchedule.xml` Dateien. Wenn jedoch eine Systemdatenwiederherstellung durchgeführt wird, können Sie auswählen, welche Knoten im Cluster wiederhergestellt werden sollen.

Hinweis: Das Sicherungsgerät (SFTP-Server) muss bereits konfiguriert sein, um die TAR-Dateien abzurufen und das System mit diesen Dateien wiederherzustellen.

Schritt 1: Navigieren Sie zu **Disaster Recovery System > Restore > Restore Wizard**.

Schritt 2: Wählen Sie **Device Name** in dem die für die Wiederherstellung zu verwendende Sicherungsdatei gespeichert wird. Auswählen **Next**.



Disaster Recovery System

For Cisco Unified Communications Solutions

Backup ▾ Restore ▾ Help ▾

Step1 Restore - Choose Backup device



Next



Cancel

Status



Status:Ready

Select Backup Device

Device Name*

-- Not Selected -- ▾

-- Not Selected --

SFTP_1

BackupDevice1

Next

Cancel

Schritt 3: Wählen Sie **Backup File** aus der angezeigten Liste der verfügbaren Dateien, wie im Bild dargestellt. Die ausgewählte Sicherungsdatei muss die wiederherzustellenden Informationen enthalten.



Disaster Recovery System

For Cisco Unified Communications Solutions

Backup ▾ Restore ▾ Help ▾

Step2 Restore - Choose the Backup Tar File

Back Next Cancel

Status

Status:Ready

Select Backup Archive**

Select Backup File*

-- Tar file list --

-- Tar file list --

2019-06-18-03-51-57

2019-06-18-03-53-30

Schritt 4: Wählen Sie aus der Liste der verfügbaren Funktionen die wiederherzustellende Funktion aus.

Disaster Recovery System
For Cisco Unified Communications Solutions

Backup ▾ Restore ▾ Help ▾

Step3 Restore - Select the Type of Restore

Back Select All Clear All Next Cancel

Status: Ready

Select Features*

PLM

Backed up components in TAR:

Feature	Server
PLM	CUCM10SUB ELM-AGENT
PLM	CUCM10SUB ELM-SERVER
PLM	CUCM10 ELM-AGENT
PLM	CUCM10 ELM-SERVER

Schritt 5: Wählen Sie die Knoten aus, auf die die Wiederherstellung angewendet werden soll.



Hinweis: Mit der Wiederherstellung in einem Schritt kann der gesamte Cluster wiederhergestellt werden, wenn Publisher bereits neu erstellt oder neu installiert wurde. Diese Option ist NUR sichtbar, wenn die für die Wiederherstellung ausgewählte Sicherungsdatei die Sicherungsdatei des Clusters ist und die für die Wiederherstellung ausgewählten Funktionen die Funktion(en) enthalten, die sowohl bei den Publisher- als auch bei den Subscriber-Knoten registriert ist.

Schritt 6: Auswählen **Restore** , um den Prozess zu starten, und der Wiederherstellungsstatus wird aktualisiert.



Schritt 7. Um den Status der Wiederherstellung zu überprüfen, navigieren Sie zu **Restore > Current Status**.

Disaster Recovery System
For Cisco Unified Communications Solutions

Backup > Restore > Help

Restore Status

Refresh

Status

Restoring server [CUCMV10SUB], please wait... %

Restore details

Tar Filename: 2019-06-18-03-53-30.tar
Backup Device: NETWORK
Operation: RESTORE
Percentage Complete: 50%

Feature	Server	Component	Status	Result **	Start Time	Log File *
PLM	CUCMV10SUB	ELM-AGENT	100	SUCCESS	Thu Jun 20 03:09:51 CDT 2019	2019-06-20-03-09-29_r_cucmv10sub_plm_elm-agent.log
PLM	CUCMV10SUB	ELM-SERVER	0	Active	Thu Jun 20 03:09:51 CDT 2019	

Refresh

Schritt 8: Restore Status Änderungen an success wenn sie abgeschlossen ist.

Disaster Recovery System
For Cisco Unified Communications Solutions

Backup > Restore > Help

Restore Status

Refresh

Status

SUCCESS: Restore Completed...

Restart Required

Please restart the server(s) [CUCMV10SUB] before performing the next restore for changes to take effect. In case of a cluster, restart the entire cluster.
Note: If you have restored system to be in FIPS mode, please note it has been enabled, but has not taken effect yet. FIPS mode will be active only after next reboot.

Restore details

Tar Filename: 2019-06-18-03-53-30.tar
Backup Device: NETWORK
Operation: RESTORE
Percentage Complete: 100%

Feature	Server	Component	Status	Result **	Start Time	Log File *
PLM	CUCMV10SUB	ELM-AGENT	100	SUCCESS	Thu Jun 20 03:09:51 CDT 2019	2019-06-20-03-09-29_r_cucmv10sub_plm_elm-agent.log
PLM	CUCMV10SUB	ELM-SERVER	100	SUCCESS	Thu Jun 20 03:09:51 CDT 2019	2019-06-20-03-09-29_r_cucmv10sub_plm_elm-server.log

Schritt 9. Damit die Änderungen wirksam werden, muss das System neu gestartet werden.

```
admin:utils system restart

Do you really want to restart ?
Enter (yes/no)? yes

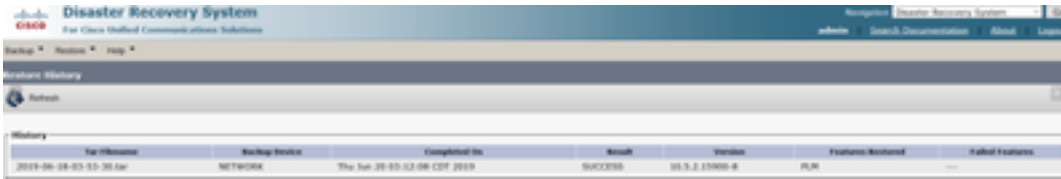
Appliance is being Restarted ...
Warning: Restart could take up to 5 minutes.
Stopping Service Manager...
- Service Manager shutting down services... Please Wait
Restart operation appears to be stuck

Would you like to force the Restart?
continue Restart (yes/no)?
Broadcast message from admin@CUCMV10SUB
(unknown) at 3:19 ...

The system is going down for reboot NOW!
```

Tip: Verwenden Sie ein unterstütztes Verfahren, um das System neu zu starten
[Herunterfahren oder Neustart des Systems](#)

Schritt 10. Um die im System ausgeführten Wiederherstellungsvorgänge anzuzeigen, navigieren Sie zu **Restore > History**.



Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung bei Ihrer Konfiguration.

Der CUCM-Cluster (dies umfasst die CUCM-Knoten und die Cisco Instant Messaging & Presence (IM&P)-Server) muss folgende Anforderungen erfüllen:

- **Port 22** offen, um die Kommunikation mit dem SFTP-Server herzustellen.
- Validierte, dass die **IPsec** und **Tomcat** Zertifikate sind nicht abgelaufen. Um die Gültigkeit der Bescheinigungen zu überprüfen, fliegen nach **Cisco Unified OS Administration > Security > Certificate Management**

Hinweis: Verwenden Sie das [Verfahren](#) zum Regenerieren von IPsec- und Tomcat-Zertifikaten [in CUCM](#).

- Stellen Sie sicher, dass die Datenbankreplikation eingerichtet wurde und keine Fehler oder Diskrepanzen zwischen den CUCM Publisher- und den IM&P Publisher-Servern zeigt.
- Überprüfen Sie die Erreichbarkeit zwischen den Servern und dem SFTP-Server.
- Überprüfen Sie mit dem Befehl, ob alle Server im Cluster authentifiziert sind. **show network cluster**.

Wenn Fehler bei der Sicherung oder Wiederherstellung gemeldet werden und weitere Unterstützung erforderlich ist, müssen diese Protokolle gesammelt und an das Technical Assistance Center (TAC) weitergegeben werden:

- Cisco DRF-Masterprotokolle
- Lokale Cisco DRF-Protokolle
- Fehlerprotokolle von der Seite Aktueller Status von DRF
- Zeitstempel der Ausgabe

Zugehörige Informationen

- [Unterstützte SFTP-Server](#)

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.