

Configurazione di backup e ripristino dalla GUI in CUCM

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Backup](#)

[Ripristina](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive i requisiti di impostazione per **Backup e Restore** caratteristiche in CUCM dal **Graphic User Interface (GUI)**.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- **Cisco Unified Communications Manager versione 10.5.2.1590-8**

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

OSPF (Open Shortest Path First) **Disaster Recovery System (DRS)**, che può essere richiamato da CUCM Administration, fornisce funzionalità complete di backup e ripristino dei dati per tutti i server del cluster. DRS consente di eseguire backup di dati pianificati in modo regolare, automatici o richiamati dall'utente.

DRS ripristina i propri parametri (dispositivo di backup e parametri di pianificazione) come parte del backup/ripristino della piattaforma. DRS esegue il backup e ripristina `drfDevice.xml` e `drfSchedule.xml` file. Quando il server viene ripristinato con questi file, non è necessario riconfigurare il dispositivo di backup DRS e la pianificazione.

OSPF (Open Shortest Path First) **Disaster Recovery System** include le seguenti funzionalità:

- Un'interfaccia utente per l'esecuzione delle operazioni di backup e ripristino
- Architettura di sistema distribuita con funzioni di backup e ripristino
- Backup pianificati
- Archiviazione dei backup su un'unità a nastro fisica o su un server SFTP remoto

OSPF (Open Shortest Path First) **Disaster Recovery System** contiene due funzioni chiave, **Master Agent (MA)** e **Local Agent (LA)**.

OSPF (Open Shortest Path First) **Master Agent** coordina l'attività di backup e ripristino con **Local Agents**. Il sistema attiva automaticamente **Master Agent** e **Local Agent** in tutti i nodi del cluster.

cluster CUCM (che comprende i nodi CUCM e il **Cisco Instant Messaging & Presence (IM&P)** server) devono soddisfare i seguenti requisiti:

- Port 22 aperto per stabilire la comunicazione con il server SFTP
- È stato verificato che **IPsec** e **Tomcat** certificati non scaduti.

Per verificare la validità dei certificati, n passa a **Cisco Unified OS Administration > Security > Certificate Management**

Nota: per rigenerare i certificati ipsec e Tomcat, utilizzare la [procedura per rigenerare i certificati in CUCM](#)

- Verificare che l'installazione di Replica di database sia stata completata e che non vengano visualizzati errori o mancate corrispondenze dai server di pubblicazione CUCM e di pubblicazione IM&P.

Le impostazioni del server SFTP devono soddisfare i seguenti requisiti:

- Credenziali di accesso disponibili
- Deve essere raggiungibile dal server CUCM
- I file vengono inclusi nel percorso selezionato quando viene eseguito un ripristino

Configurazione

Backup

OSPF (Open Shortest Path First) **Disaster Recovery System** esegue un backup a livello di cluster, ovvero raccoglie i backup di tutti i server di un cluster CUCM in una posizione centrale e archivia i dati di backup in un dispositivo di storage fisico.

Passaggio 1. Per creare dispositivi di backup su cui vengono salvati i dati, passare a **Disaster Recovery System > Backup > Backup Device**.

Passaggio 2. Seleziona **Add New**; definizione di un **Backup Device Name** e immettere i valori SFTP. **Save**



Disaster Recovery System

For Cisco Unified Communications Solutions

Backup ▾ Restore ▾ Help ▾

Backup Device

 Save  Back

Status

 Status:Ready

Backup device name

Backup device name™

Select Destination*

Network Directory

Host name/IP address	<input type="text" value="10.1.89.107"/>
Path name	<input type="text" value="/"/>
User name	<input type="text" value="administrator"/>
Password	<input type="password" value="*****"/>

Number of backups to store on Network Directory ▾

Passaggio 3. Creare e modificare pianificazioni di backup per eseguire il backup dei dati. Passa a **Backup > Scheduler**.

Passaggio 4. Definire un **Schedule Name**. Selezionare il **Device Name** e controllare la **Features** in base allo scenario.

The screenshot shows the Cisco Disaster Recovery System Scheduler configuration interface. At the top, there is a navigation bar with the Cisco logo and the text "Disaster Recovery System For Cisco Unified Communications Solutions". The user is logged in as "admin". Below the navigation bar, there are tabs for "Backup", "Restore", and "Help". The main heading is "Scheduler". Below the heading, there are several action buttons: "Save", "Set Default", "Disable Schedule", "Enable Schedule", and "Back". The "Back" button is highlighted in green. The configuration fields are as follows:

- Status:** Status: Ready
- Schedule Name:** Schedule Name*
- Select Backup Device:** Device Name*
- Select Features:** CDR_CAR UCM PLM

Passaggio 5. Configurare un backup pianificato in base allo scenario.

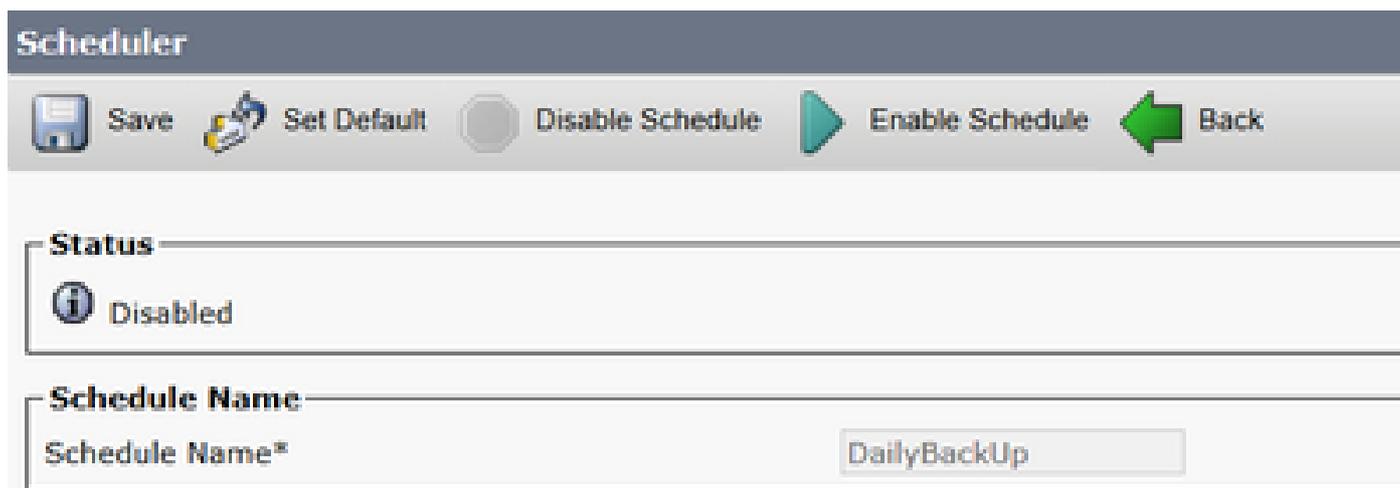
The screenshot shows the configuration page for the Scheduler, focusing on the "Start Backup at" and "Frequency" sections. The "Start Backup at" section has a date field set to "2019 Jun 18" and a time field set to "00:00". The "Frequency" section has radio buttons for "Once", "Daily", "Weekly", and "Monthly". The "Daily" option is selected. Below the "Daily" option, there are checkboxes for each day of the week: "Monday", "Tuesday", "Wednesday", "Thursday", "Friday", "Saturday", and "Sunday".

Passaggio 6. Seleziona **Save** e notare l'avviso come mostrato nell'immagine. Seleziona **OK** per andare avanti.

The DRS Backup archive encryption depends on the current security password. During a restore, you could be prompted to enter this security password if this password has been changed.

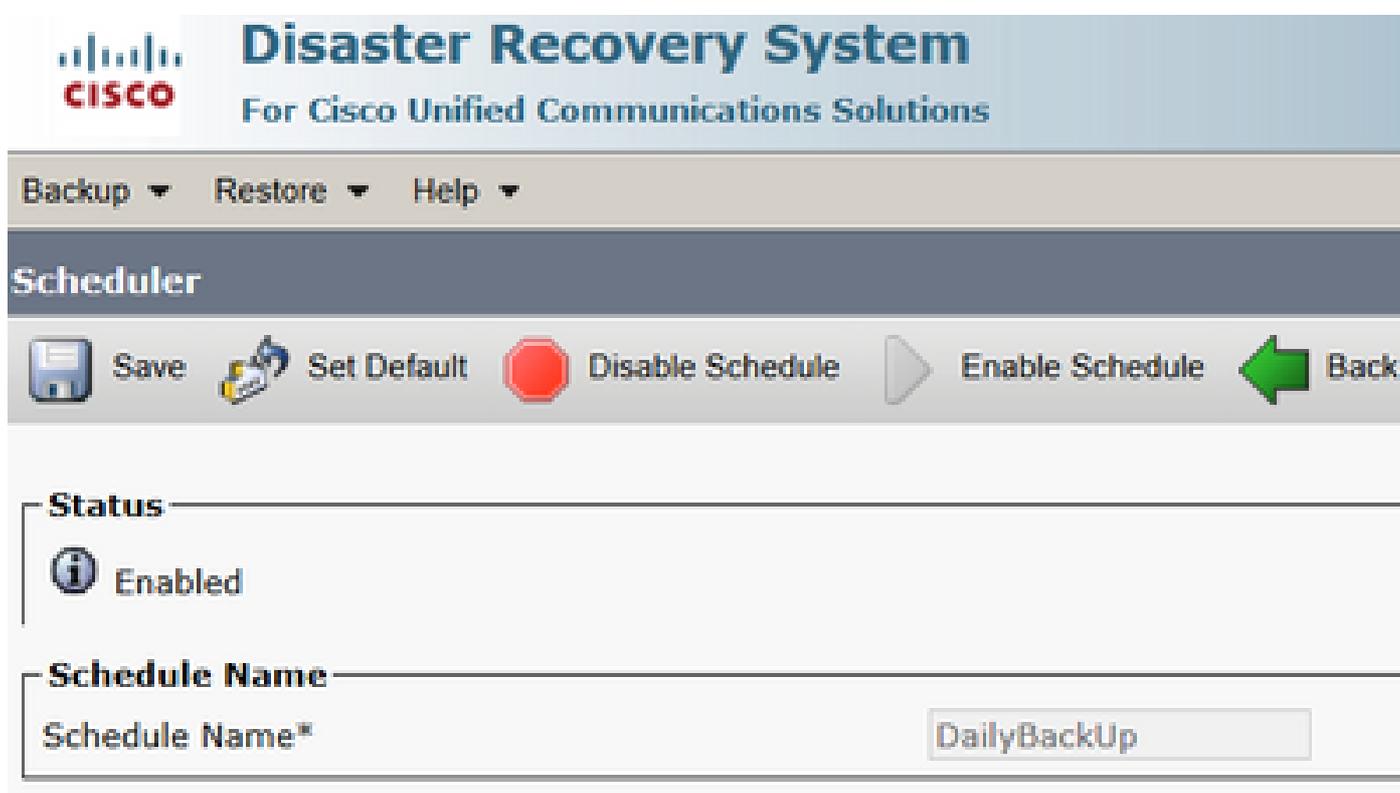
The screenshot shows a single button labeled "OK" in a light blue box.

Passaggio 7. Una volta che Backup Schedule viene creato, selezionare Enable Schedule .



The screenshot shows the 'Scheduler' configuration page. At the top, there is a navigation bar with buttons: 'Save', 'Set Default', 'Disable Schedule', 'Enable Schedule', and 'Back'. The 'Enable Schedule' button is highlighted with a green arrow. Below the navigation bar, the 'Status' field is set to 'Disabled'. The 'Schedule Name' field is set to 'DailyBackUp'.

Passaggio 8. Attendere che lo stato venga modificato in Enabled.



The screenshot shows the 'Disaster Recovery System' configuration page. At the top, there is a navigation bar with buttons: 'Backup', 'Restore', and 'Help'. Below the navigation bar, the 'Scheduler' configuration page is visible. The 'Status' field is now set to 'Enabled'. The 'Schedule Name' field is still set to 'DailyBackUp'. The 'Enable Schedule' button is highlighted with a green arrow.

Passaggio 9. Se è necessario un backup manuale, passare a Backup > Manual Backup.

Passaggio 10. Selezionare il Device Name e controllare la Features in base allo scenario.



Disaster Recovery System

For Cisco Unified Communications Solutions

Backup ▾ Restore ▾ Help ▾

Manual Backup



Start Backup



Estimate Size



Select All



Clear All

Status



Status:Ready

Select Backup Device

Device Name*

BackupDevice1 ▾

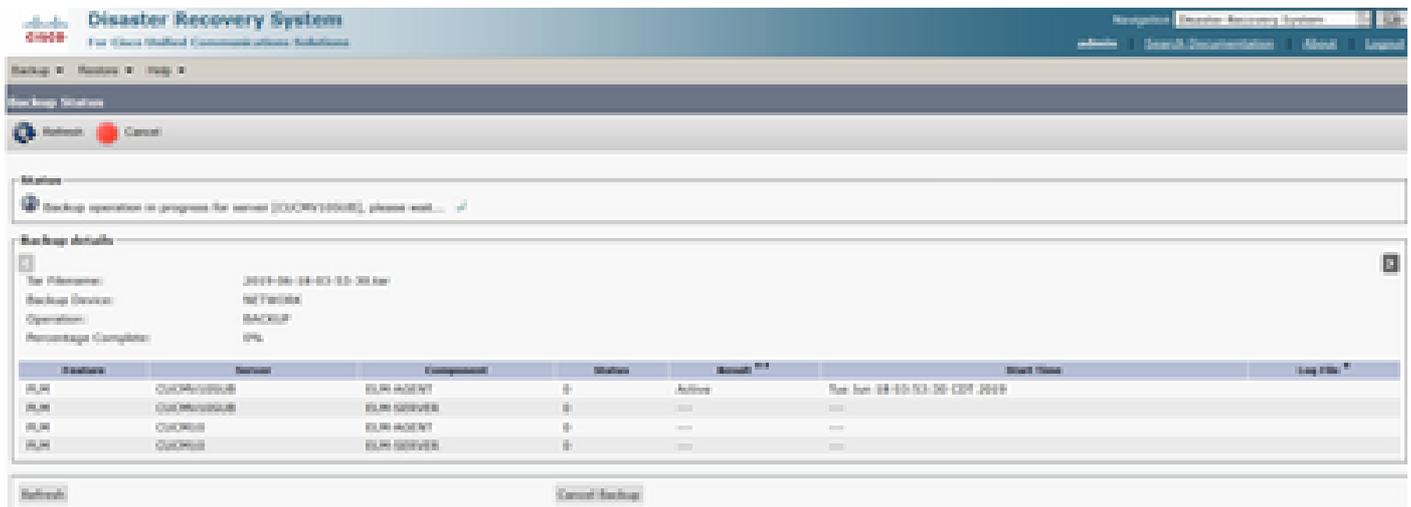
Select Features *

CDR_CAR

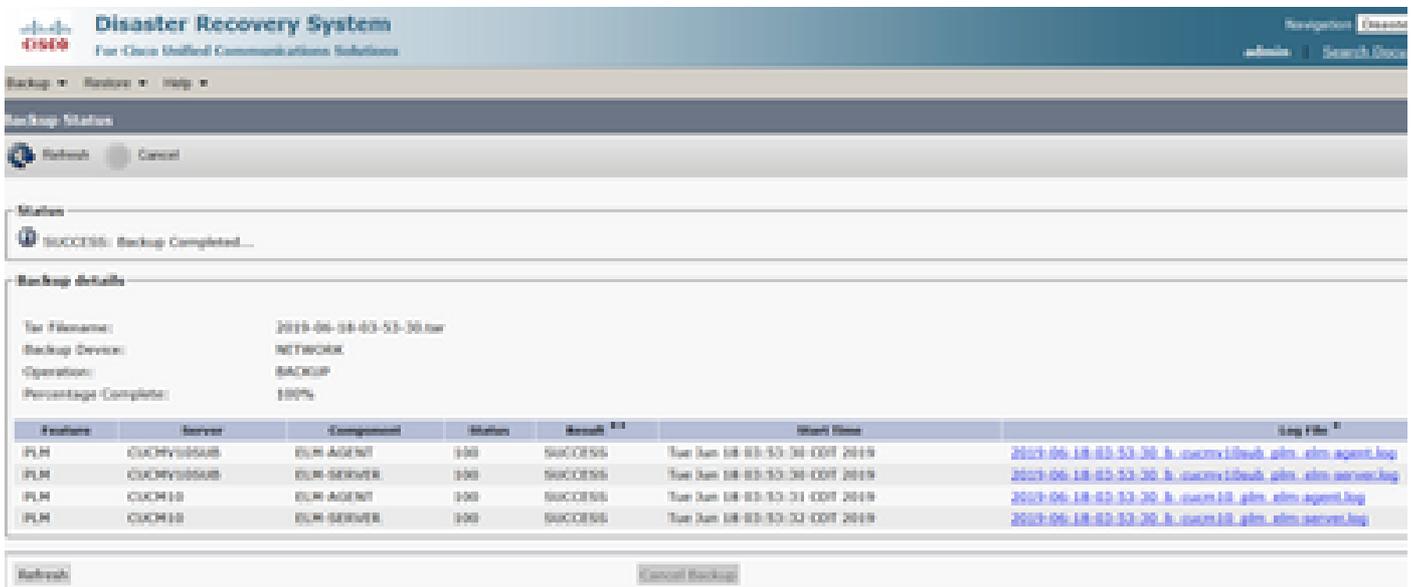
UCM

PLM

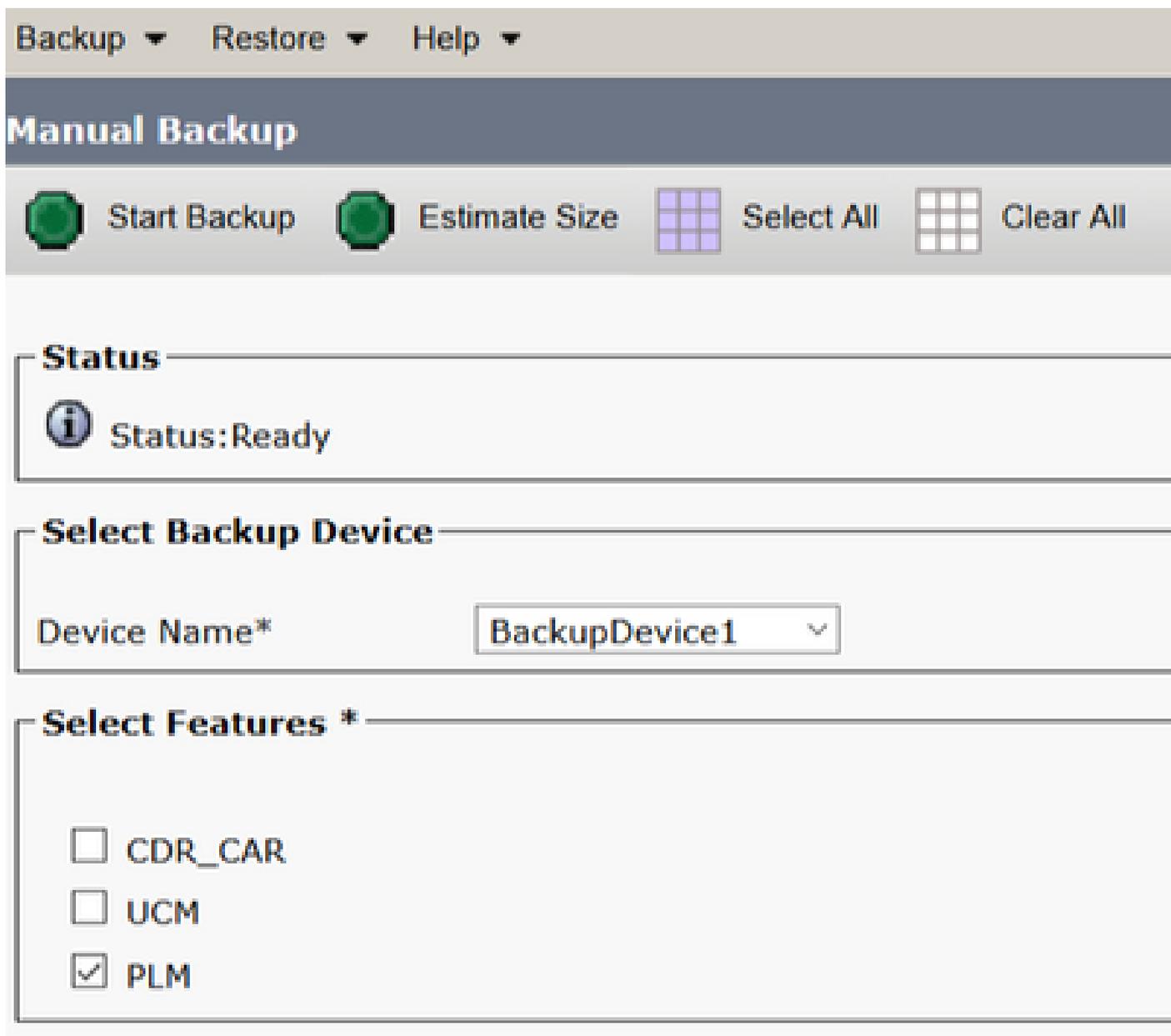
Passaggio 11. Seleziona **Start Backup** e l'operazione è in corso.



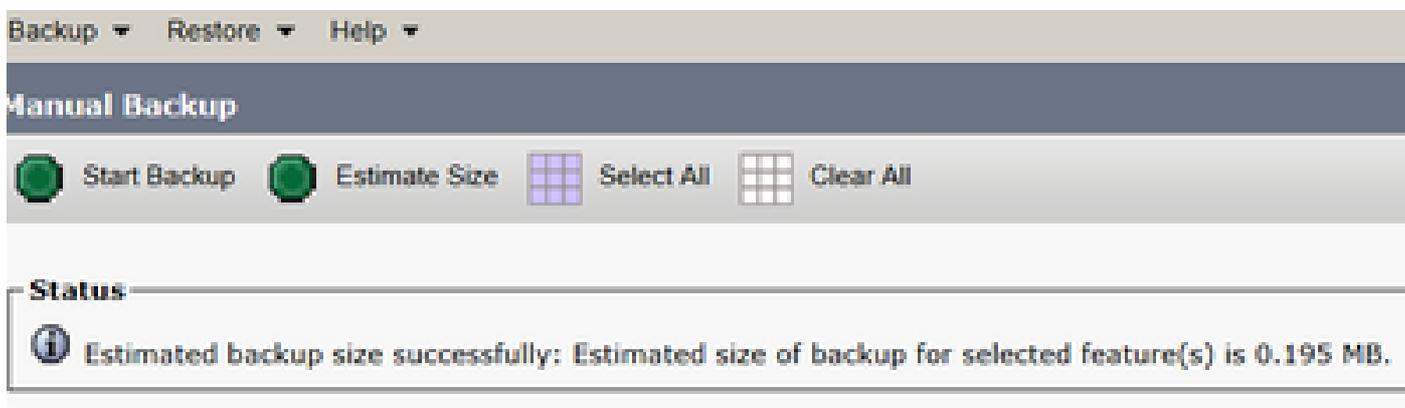
Passaggio 12. Una volta completato il backup manuale, viene visualizzato il messaggio di completamento.



Passaggio 13. Per stimare le dimensioni del file tar di backup utilizzato dal dispositivo SFTP, selezionate Estimate Size.



Passaggio 14. Le dimensioni stimate vengono visualizzate come mostrato nell'immagine



Nota: la funzione Stima dimensioni viene calcolata in base ai backup precedenti riusciti e

può variare nel caso in cui la configurazione sia stata modificata dall'ultimo backup.

Passaggio 15. Per controllare lo stato del backup durante l'esecuzione di un backup, passare a **Backup > Backup Status**.

Disaster Recovery System
For Cisco Unified Communications Solutions

Backup > Restore > Help

Backup Status

Refresh Cancel

Status
SUCCESS: Backup Completed...

Backup details

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

Feature	Server	Component	Status	Result	Start Time	Log File
EUCM100A0	EUCM100A0	EUM-AGENT	100	SUCCESS	Tue Jun 18 03:53:30 CDT 2019	2019-06-18-03-53-30_b_eucm100a0_pdm_eum-agent.log
EUCM100A0	EUCM100A0	EUM-SERVER	100	SUCCESS	Tue Jun 18 03:53:30 CDT 2019	2019-06-18-03-53-30_b_eucm100a0_pdm_eum-server.log
EUCM10	EUCM10	EUM-AGENT	100	SUCCESS	Tue Jun 18 03:53:31 CDT 2019	2019-06-18-03-53-30_b_eucm10_pdm_eum-agent.log
EUCM10	EUCM10	EUM-SERVER	100	SUCCESS	Tue Jun 18 03:53:32 CDT 2019	2019-06-18-03-53-30_b_eucm10_pdm_eum-server.log

Refresh Cancel Backup

Passaggio 16. Per consultare le procedure di backup eseguite nel sistema, passare a **Backup > History**.

Disaster Recovery System
For Cisco Unified Communications Solutions

Backup > Restore > Help

Backup History

Refresh

Tar Filename	Backup Device	Completed On	Result	Backup Type	Version	Features Backed Up	Features Backed Up Warning	Failed Features
2019-06-18-03-53-30.tar	NETWORK	Tue Jun 18 03:53:31 CDT 2019	SUCCESS	MANUAL	06.5.2.00000-B	PLM	---	---
2019-06-18-03-53-30.tar	NETWORK	Tue Jun 18 03:53:34 CDT 2019	SUCCESS	MANUAL	06.5.2.00000-B	PLM	---	---
tar file not created	NETWORK	Tue Jun 18 03:00:00 CDT 2019	ERROR	SCHEDULED - DailyBackup	---	---	---	---
tar file not created	NETWORK	Wed Jun 19 12:00:00 CDT 2019	ERROR	SCHEDULED - DailyBackup	---	---	---	---

Ripristina

Ripristini DRS principalmente `drfDevice.xml` e `drfSchedule.xml` file. Tuttavia, quando viene eseguito il ripristino dei dati di sistema, è possibile scegliere i nodi del cluster che devono essere ripristinati.

Nota: per recuperare i file tar dal dispositivo di backup (server SFTP) e ripristinare il sistema con questi file, è necessario che il dispositivo di backup (server SFTP) sia già configurato.

Passaggio 1. Passa a **Disaster Recovery System > Restore > Restore Wizard**.

Passaggio 2. Selezionare il **Device Name** che archivia il file di backup da utilizzare per il ripristino. Seleziona **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

Passaggio 3. Selezionare il **Backup File** dall'elenco visualizzato dei file disponibili, come mostrato nell'immagine. Il file di backup selezionato deve includere le informazioni da ripristinare.



Disaster Recovery System

For Cisco Unified Communications Solutions

Backup ▾ Restore ▾ Help ▾

Step2 Restore - Choose the Backup Tar File

Back Next Cancel

Status

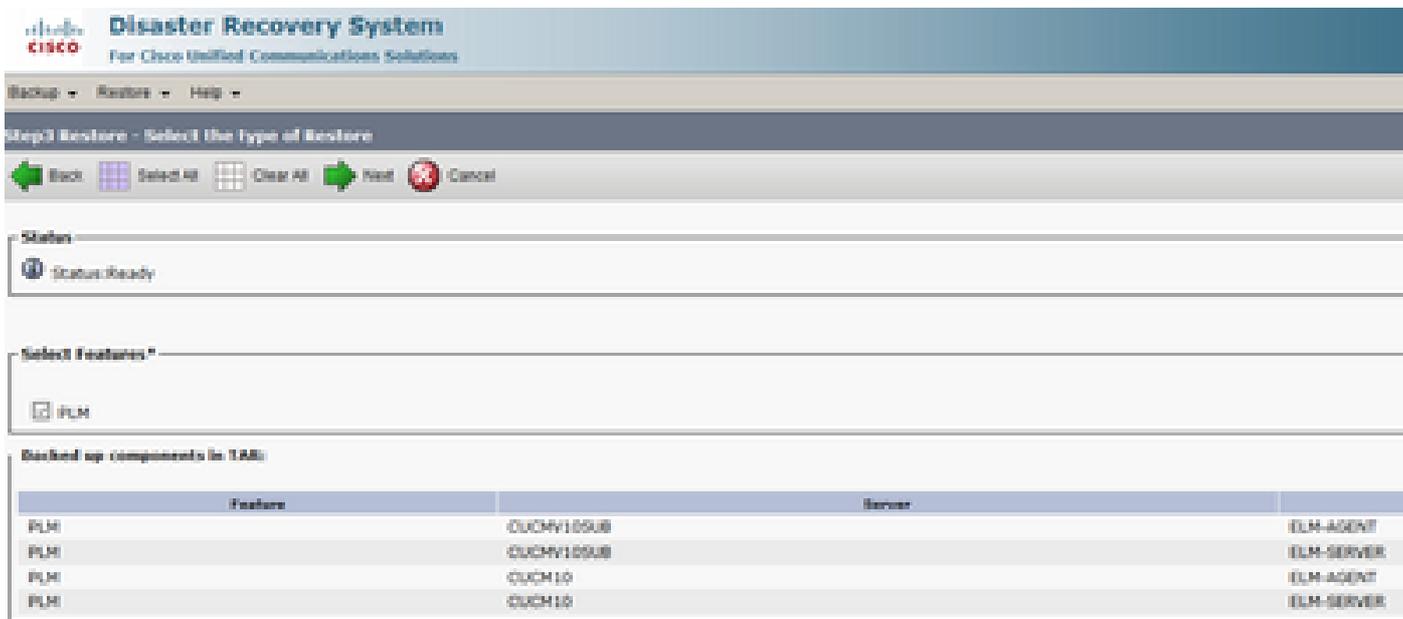
Status:Ready

Select Backup Archive**

Select Backup File*

-- Tar file list --	▾
-- Tar file list --	
2019-06-18-03-51-57	
2019-06-18-03-53-30	

Passaggio 4. Dall'elenco delle feature disponibili, selezionate la feature da ripristinare.



Passaggio 5. Selezionare i nodi in cui applicare il ripristino.



Nota: il ripristino in un unico passaggio consente di ripristinare l'intero cluster se il server di pubblicazione è già stato ricostruito o è stato installato di recente. Questa opzione è visibile SOLO se il file di backup selezionato per il ripristino è il file di backup del cluster e le funzionalità scelte per il ripristino includono quelle registrate sia con i nodi del server di pubblicazione che con quelli del sottoscrittore.

Passaggio 6. Seleziona **Restore** per avviare il processo e lo stato di ripristino viene aggiornato.



Disaster Recovery System

For Cisco Unified Communications Solutions

Backup ▾ Restore ▾ Help ▾

Restore Status



Status

Reading backup from media

Restore details

Tar Filename: 2019-06-18-03-53-30.tar
Backup Device: NETWORK
Operation: RESTORE
Percentage Complete: 0%

Passaggio 7. Per verificare lo stato del ripristino, passare a **Restore > Current Status**.

Disaster Recovery System

Navigation | Logout

Home | Search | Disaster

Backup ▾ Restore ▾ Help ▾

Restore Status

Status

Restoring server [COPY10000], please wait...

Restore Details

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

Instance	Server	Component	Status	Result	Start Time	Log File
PLM	CUCM10000B	PLM-AGENT	100	SUCCESS	Thu Jun 20 03:09:51 CDT 2019	2019-06-20-03-09-29_r_cucm10000b_plm_rlm_agent.log
PLM	CUCM10000B	PLM-SERVER	0	Active	Thu Jun 20 03:09:51 CDT 2019	

Passaggio 8. Restore Status modifiche a SUCCESS al termine dell'operazione.

Disaster Recovery System
For Cisco Unified Communications Solutions

Navigation | Dashboard
admin | Search Docu

Backup | Restore | Help

Restore Monitor

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 systems 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

Run Filename: 2019-06-20-03-29-29.r
Backup Device: NETWORK
Operation: RESTORE
Percentage Complete: 100%

Hostname	Server	Component	Status	Result **	Start Time	Log File *
RUN	CUCMV10SUB	ELM-AGENT	100	SUCCESS	Thu Jun 20 03:29:14 CDT 2019	2019-06-20-03-29-29.r_cucmv10sub_plm_elm-agent.log
RUN	CUCMV10SUB	ELM-SERVER	100	SUCCESS	Thu Jun 20 03:29:14 CDT 2019	2019-06-20-03-29-29.r_cucmv10sub_plm_elm-server.log

Passaggio 9. Per rendere effettive le modifiche, è necessario riavviare il sistema.

```
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!
```

Suggerimento: utilizzare una procedura supportata per riavviare il sistema. [Arrestare o riavviare il sistema](#)

Passaggio 10. Per consultare le procedure di ripristino eseguite nel sistema, passare a **Restore > History**.

Backup	Backup Status	Completed On	Result	Version	Features/Backupset	Initial Features
2017-08-08 08:53:13-28.6a1	SUCCESS	Thu Jul 28 10:13:08 CDT 2017	SUCCESS	08.0.0.1.0000-4	PLM	---

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Il cluster CUCM (che interessa i nodi CUCM e i server Cisco Instant Messaging & Presence (IM&P)) deve soddisfare i seguenti requisiti:

- Port 22 aperto per stabilire la comunicazione con il server SFTP
- È stato verificato che IPsec e Tomcat certificati non scaduti.

Per verificare la validità dei certificati, npassa a **Cisco Unified OS Administration > Security > Certificate Management**

Nota: per rigenerare i certificati ipsec e Tomcat, utilizzare la [procedura per rigenerare i certificati in CUCM](#)

- Verificare che l'installazione di Replica di database sia stata completata e che non vengano visualizzati errori o mancate corrispondenze dai server di pubblicazione CUCM e di pubblicazione IM&P.
- Verificare la raggiungibilità tra i server e il server SFTP.
- Convalida l'autenticazione di tutti i server del cluster tramite il comando `show network cluster`.

Quando vengono segnalati errori di backup o ripristino e è necessaria ulteriore assistenza, questo gruppo di registri deve essere raccolto e condiviso con il centro di assistenza tecnica (TAC, Technical Assistance Center):

- Registri master DRF Cisco
- Registri locali DRF Cisco
- Registri degli errori dalla pagina Stato corrente DRF
- Timestamp del problema

Informazioni correlate

- [Server SFTP supportati](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).