

Configurer la sauvegarde et la restauration à partir de l'interface utilisateur graphique dans CUCM

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Sauvegarde](#)

[Restaurer](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit la configuration requise pour **Backup** et **Restore** dans **CUCM** à partir du **Graphic User Interface (GUI)**.

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

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

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Cisco Unified Communications Manager version 10.5.2.15900-8

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

LES Disaster Recovery System (DRS), qui peut être appelé à partir de CUCM Administration, fournit des fonctionnalités complètes de sauvegarde et de restauration des données pour tous les serveurs

du cluster. Le DRS permet de planifier régulièrement des sauvegardes de données automatiques ou appelées par l'utilisateur.

DRS restaure ses propres paramètres (périphérique de sauvegarde et paramètres de planification) dans le cadre de la sauvegarde/restauration de la plateforme. DRS sauvegarde et restaure le `drfDevice.xml` et `drfSchedule.xml` fichiers. Lorsque le serveur est restauré avec ces fichiers, il n'est pas nécessaire de reconfigurer le périphérique de sauvegarde et la planification DRS.

Les **Disaster Recovery System** inclut les fonctionnalités suivantes :

- Une interface utilisateur pour effectuer des tâches de sauvegarde et de restauration
- Architecture de système distribué avec fonctions de sauvegarde et de restauration
- Sauvegardes planifiées
- Archiver les sauvegardes sur un lecteur de bande physique ou un serveur SFTP distant

Les **Disaster Recovery System** contient deux fonctions clés, **Master Agent (MA)** et **Local Agent (LA)**.

Les **Master Agent** coordonne les activités de sauvegarde et de restauration avec **Local Agents**. Le système active automatiquement le **Master Agent** et **Local Agent** sur tous les noeuds du cluster.

Cluster CUCM (cela implique les noeuds CUCM et le **Cisco Instant Messaging & Presence (IM&P)** serveurs) doivent remplir les conditions suivantes :

- **Port 22** afin d'établir la communication avec le serveur SFTP
- Confirmé que le **IPsec** et **Tomcat** les certificats ne sont pas expirés. Afin de vérifier la validité des certificats, naviguer jusqu'à **Cisco Unified OS Administration > Security > Certificate Management**

Remarque : afin de régénérer les certificats ipsec et Tomcat, utilisez la [Procédure pour régénérer les certificats dans CUCM](#)

- Assurez-vous que la configuration de la réplication de base de données est terminée et qu'elle n'affiche aucune erreur ou incohérence provenant du serveur de publication CUCM et des serveurs de publication IM&P.

Les paramètres du serveur SFTP doivent couvrir les exigences suivantes :

- Les identifiants de connexion sont disponibles
- Il doit être accessible à partir du serveur CUCM
- Les fichiers sont inclus dans le chemin sélectionné lors d'une restauration

Configurer

Sauvegarde

Les **Disaster Recovery System** effectue une sauvegarde au niveau du cluster, ce qui signifie qu'il collecte les sauvegardes pour tous les serveurs d'un cluster CUCM vers un emplacement central et archive les données de sauvegarde sur un périphérique de stockage physique.

Étape 1. Pour créer des unités de sauvegarde sur lesquelles les données sont enregistrées, accédez à **Disaster Recovery System > Backup > Backup Device**.

Étape 2. Sélectionner **Add New**; définir un **Backup Device Name** et saisissez les valeurs 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* BackupDevice1

Select Destination*

Network Directory

Host name/IP address	10.1.89.107
Path name	/
User name	administrator
Password	*****
Number of backups to store on Network Directory	2 ▾

Save Back

Étape 3. Créer et modifier des plannings de sauvegarde afin de sauvegarder des données. Naviguez jusqu'à Backup > Scheduler.

Étape 4. Définir un Schedule Name. Sélectionnez le Device Name et vérifiez la Features selon votre scénario.

Disaster Recovery System
For Cisco Unified Communications Solutions

Navigation Disaster Rec
admin | Search Documents

Backup ▾ Restore ▾ Help ▾

Scheduler

Save Set Default Disable Schedule Enable Schedule Back

Status
Status:Ready

Schedule Name
Schedule Name* DailyBackUp

Select Backup Device
Device Name* BackupDevice1 ▾

Select Features*

CDR_CAR UCM PLM

Étape 5. Configurez une sauvegarde planifiée en fonction de votre scénario.

Start Backup at*

Date: 2019 Jun 18 Time: 00 Hour 00 Minute

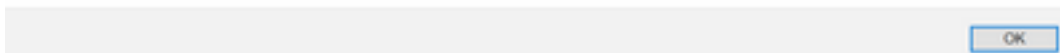
Frequency*

Once
 Daily
 Weekly
 Monthly

Monday Tuesday Wednesday Thursday
 Friday Saturday Sunday

Étape 6. Sélectionner **save** et notez l'avertissement comme indiqué dans l'image. Sélectionner **ok** afin d'avancer.

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.



Étape 7. Une fois que c'est **Backup Schedule** est créé, sélectionnez **Enable Schedule** .

Scheduler

Status

Disabled

Schedule Name

Schedule Name*

Étape 8. Patientez jusqu'à ce que l'état passe à **Enabled**.

Disaster Recovery System
For Cisco Unified Communications Solutions

Backup ▾ Restore ▾ Help ▾

Scheduler

Status

Enabled

Schedule Name

Schedule Name*

Étape 9. Si une sauvegarde manuelle est requise, accédez à **Backup > Manual Backup**.

Étape 10. Sélectionnez le **Device Name** et vérifiez la **Features** selon votre scénario.



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*

Select Features *

- CDR_CAR
- UCM
- PLM

Étape 11. Sélectionner **Start Backup** et l'opération s'affiche en cours.

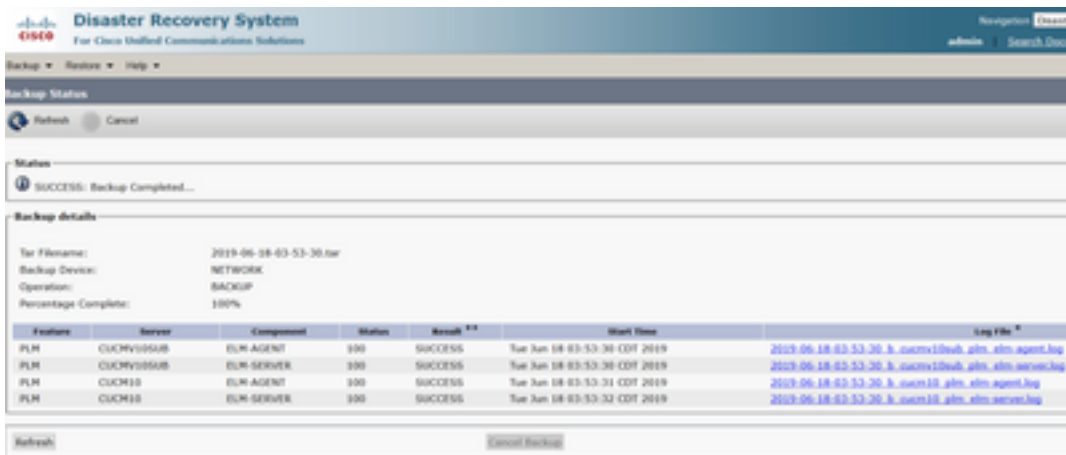
The screenshot shows the Disaster Recovery System interface during a backup operation. The status bar indicates "Backup operation in progress for server [XXXXXXXX], please wait...". Below this, the "Backup Details" section provides the following information:

- For Platform: 2019-06-18 03:53:38 AM
- Backup Device: NETWORK
- Operation: BACKUP
- Percentage Complete: 0%

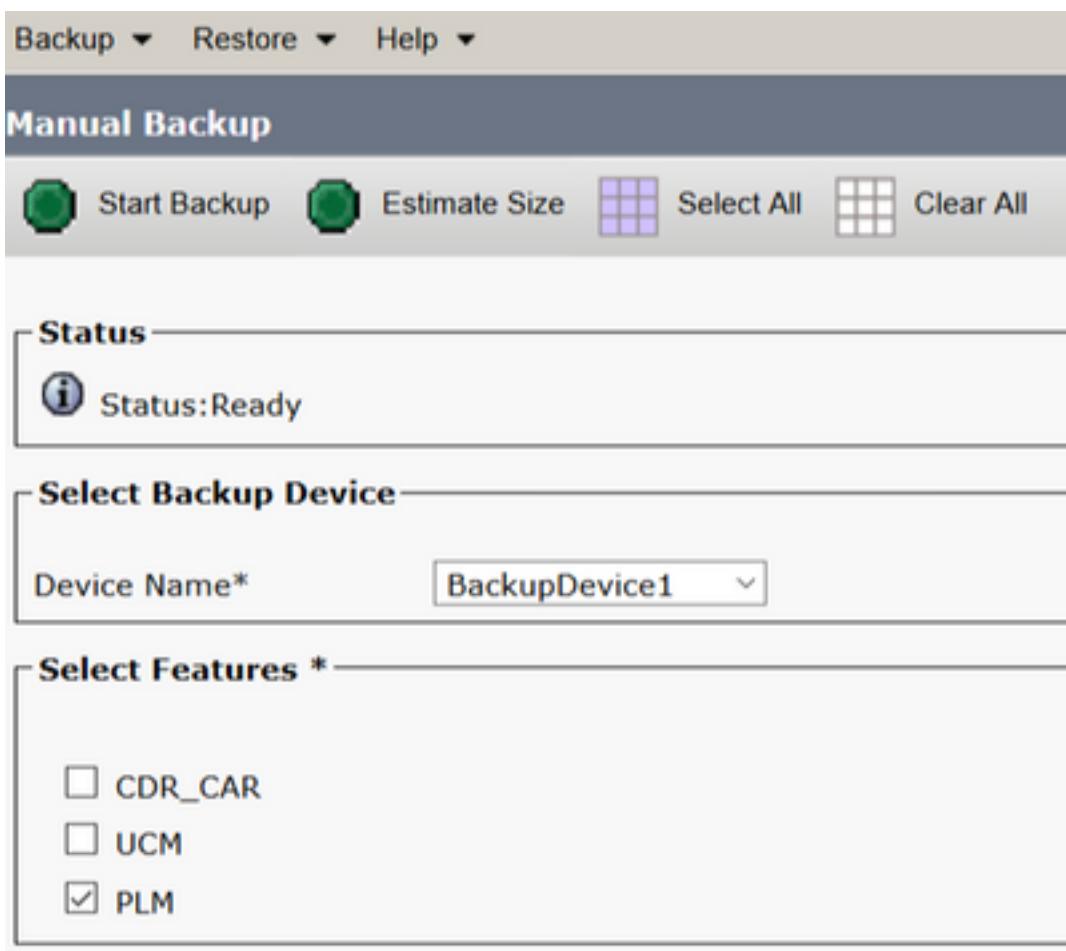
Platform	Server	Component	ID	Status	Health	Start Time	Log File
PLM	CUKRV0004	ELM AGENT	0	Active	---	Tue Jun 18 03:53:30 CDT 2019	
PLM	CUKRV0004	ELM SERVER	0	---	---		
PLM	CUKRV0004	ELM AGENT	0	---	---		
PLM	CUKRV0004	ELM SERVER	0	---	---		

Buttons: Refresh, Cancel Backup

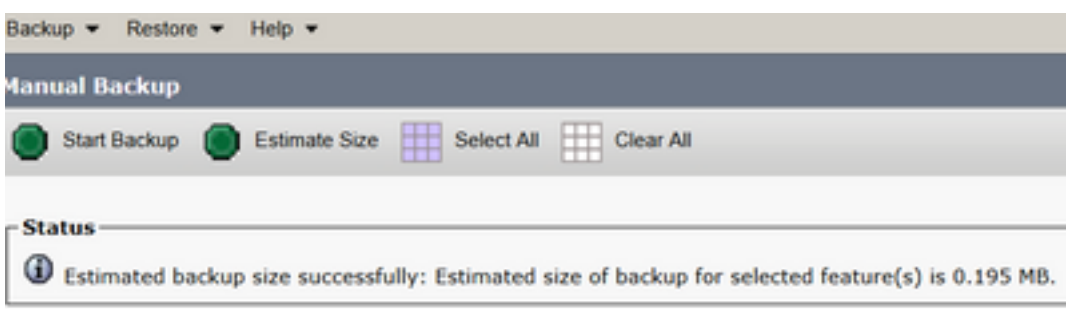
Étape 12. Lorsque la sauvegarde manuelle est terminée, le message de fin s'affiche.



Étape 13. Pour estimer la taille du fichier tar de sauvegarde utilisé par le périphérique SFTP, sélectionnez Estimate Size.

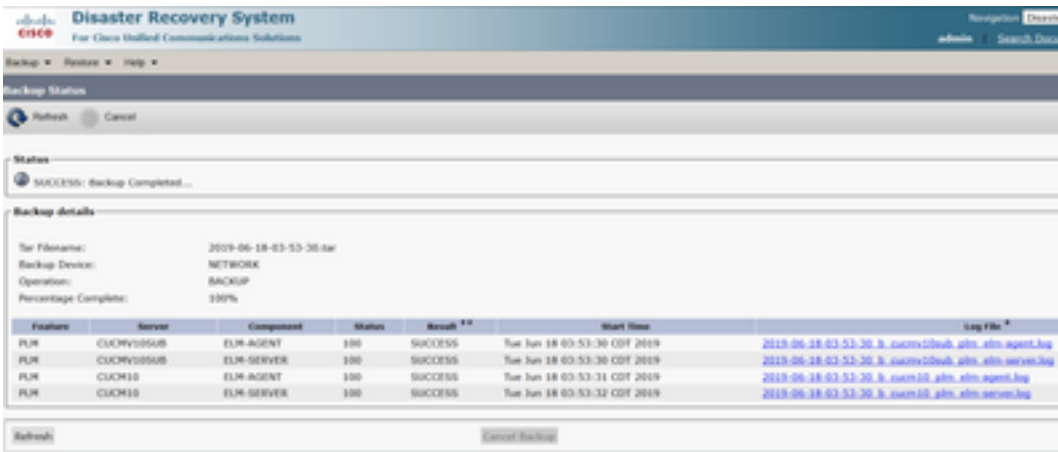


Étape 14. La taille estimée s'affiche comme illustré dans l'image

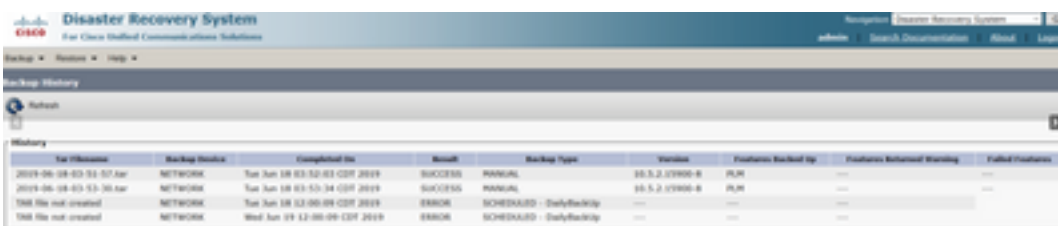


Remarque : la fonction Taille estimée est calculée en fonction des sauvegardes précédentes réussies et peut varier au cas où la configuration aurait été modifiée depuis la dernière sauvegarde.

Étape 15. Pour vérifier l'état de la sauvegarde pendant son exécution, accédez à **Backup > Backup Status**.



Étape 16. Pour consulter les procédures de sauvegarde effectuées dans le système, accédez à **Backup > History**.



Restaurer

Restaurations DRS principalement `drfDevice.xml` et `drfSchedule.xml` fichiers. Cependant, lorsqu'une restauration des données système est effectuée, vous pouvez choisir les noeuds du cluster qui doivent être restaurés.

Remarque : le périphérique de sauvegarde (serveur SFTP) doit être déjà configuré afin de récupérer les fichiers tar de celui-ci et de restaurer le système avec ces fichiers.

Étape 1. Naviguez jusqu'à **Disaster Recovery System > Restore > Restore Wizard**.

Étape 2. Sélectionnez le **Device Name** qui stocke le fichier de sauvegarde à utiliser pour la restauration. Sélectionner **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

Étape 3. Sélectionnez le **Backup File** dans la liste affichée des fichiers disponibles, comme illustré dans l'image. Le fichier de sauvegarde sélectionné doit inclure les informations à restaurer.



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

Back Next Cancel

Étape 4. Dans la liste des fonctionnalités disponibles, sélectionnez la fonctionnalité à restaurer.

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

Status:Ready

Select Features*

PLM

Backed up components in TAR:

Feature	Server
PLM	CUCM105UB ELM-AGENT
PLM	CUCM105UB ELM-SERVER
PLM	CUCM10 ELM-AGENT
PLM	CUCM10 ELM-SERVER

Étape 5. Sélectionnez les nœuds dans lesquels appliquer la restauration.



Remarque : la restauration en une étape permet la restauration de l'ensemble du cluster si le serveur de publication a déjà été reconstruit ou nouvellement installé. Cette option n'est visible QUE si le fichier de sauvegarde sélectionné pour la restauration est le fichier de sauvegarde du cluster et que les fonctionnalités choisies pour la restauration incluent la ou les fonctionnalités enregistrées auprès des noeuds d'éditeur et d'abonné.

Étape 6. Sélectionner **Restore** pour démarrer le processus et l'état de restauration est mis à jour.



Étape 7. Pour vérifier l'état de la restauration, accédez à **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

Étape 8. Restore Status modifications apportées à SUCCESS lorsqu'il est terminé.

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

Étape 9. Pour que les modifications prennent effet, le système doit être redémarré.

```
admin:utils system restart

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

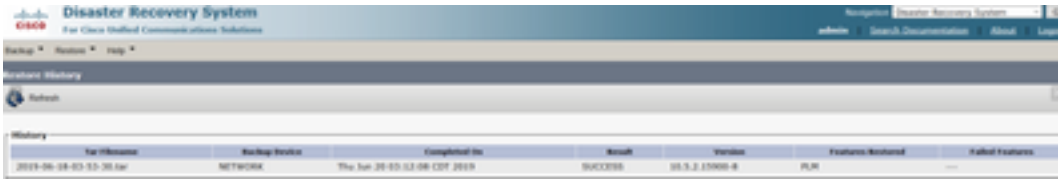
Appliance is being Restarted ...
Warning: Restart could take up to 5 minutes.
Stopping Service Manager...
- Service Manager shutting down services... Please Wait
Restart operation appears to be stuck

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!
```

Conseil : utilisez une procédure prise en charge afin de redémarrer le système [Arrêter ou redémarrer le système](#)

Étape 10. Afin de consulter les procédures de restauration effectuées dans le système, accédez à **Restore > History**.



The screenshot shows the 'Disaster Recovery System' interface. At the top, there is a navigation bar with 'Home', 'Search & Documentation', 'About', and 'Logout'. Below this is a 'Restore History' section with a 'Refresh' button. The main content is a table with the following columns: 'Restore ID', 'Restore Name', 'Completed On', 'Result', 'Version', 'Features Restored', and 'Failed Features'. A single row is visible with the following data: '2019-06-24-03:53:30 for', 'NETWORK', 'Thu Jun 20 03:53:08 CDT 2019', 'SUCCESS', '10.5.2.1000-6', 'PLN', and '...'.

Restore ID	Restore Name	Completed On	Result	Version	Features Restored	Failed Features
2019-06-24-03:53:30 for	NETWORK	Thu Jun 20 03:53:08 CDT 2019	SUCCESS	10.5.2.1000-6	PLN	...

Dépannage

Cette section fournit des informations pour dépanner votre configuration.

Le cluster CUCM (qui implique les noeuds CUCM et les serveurs Cisco Instant Messaging & Presence (IM&P)) doit répondre aux exigences suivantes :

- Port 22 afin d'établir la communication avec le serveur SFTP
- Confirmé que le IPsec et Tomcat les certificats ne sont pas expirés. Afin de vérifier la validité des certificats, naviguer jusqu'à **Cisco Unified OS Administration > Security > Certificate Management**

Remarque : pour régénérer les certificats ipsec et Tomcat, utilisez la [procédure pour régénérer les certificats dans CUCM](#)

- Assurez-vous que la configuration de la réplication de base de données est terminée et qu'elle n'affiche aucune erreur ou incohérence provenant du serveur de publication CUCM et des serveurs de publication IM&P.
- Validez l'accessibilité entre les serveurs et le serveur SFTP.
- Vérifiez que tous les serveurs du cluster sont authentifiés à l'aide de la commande `show network cluster`.

Lorsque des échecs de sauvegarde ou de restauration sont signalés et qu'une assistance supplémentaire est requise, cet ensemble de journaux doit être collecté et partagé avec le centre d'assistance technique (TAC) :

- Journaux principaux Cisco DRF
- Journaux locaux Cisco DRF
- Journaux d'échec de la page État actuel de DRF
- Horodatage de l'émission

Informations connexes

- [Serveurs SFTP pris en charge](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.