

Configurar backup e restauração da GUI no CUCM

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Fazer backup](#)

[Restaurar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve os requisitos de configuração para Backup e Restore recursos no CUCM do Graphic User Interface (GUI).

Prerequisites

Requirements

A Cisco recomenda o conhecimento destes tópicos:

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

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Cisco Unified Communications Manager versão 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O Disaster Recovery System (DRS), que pode ser chamado do CUCM Administration, fornece recursos completos de backup e restauração de dados para todos os servidores no cluster. O DRS permite backups de dados automáticos ou chamados pelo usuário programados regularmente.

O DRS restaura seus próprios parâmetros (dispositivo de backup e parâmetros de programação) como parte do backup/restauração da plataforma. O DRS faz backup e restaura o `drfDevice.xml` e `drfSchedule.xml` arquivos. Quando o servidor é restaurado com esses arquivos, não há necessidade de reconfigurar o dispositivo e o agendamento de backup do DRS.

O **Disaster Recovery System** inclui os seguintes recursos:

- Uma interface de usuário para executar tarefas de backup e restauração
- Uma arquitetura de sistema distribuída com funções de backup e restauração
- Backups agendados
- Arquivar backups em um drive de fita física ou servidor SFTP remoto

O **Disaster Recovery System** contém duas funções principais, **Master Agent (MA)** e **Local Agent (LA)**.

O **Master Agent** coordena a atividade de backup e restauração com **Local Agents**. O sistema ativa automaticamente o **Master Agent** e **Local Agent** em todos os nós no cluster.

Cluster do CUCM (envolve os nós do CUCM e o **Cisco Instant Messaging & Presence (IM&P)** servidores) devem atender a estes requisitos:

- **Port 22** aberto para estabelecer a comunicação com o servidor SFTP
- Validou que o **IPsec** e **Tomcat** os certificados não expiraram. Para verificar a validade dos certificados, navegue até **Cisco Unified OS Administration > Security > Certificate Management**

Observação: para gerar novamente certificados ipsec e Tomcat, use o [Procedimento para gerar novamente certificados no CUCM](#)

- Verifique se a configuração da replicação de banco de dados foi concluída e se não mostra erros ou incompatibilidades nos servidores do Publicador CUCM e do Publicador IM&P.

As configurações do servidor SFTP devem cobrir estes requisitos:

- As credenciais de login estão disponíveis
- Deve ser acessível a partir do servidor CUCM
- Os arquivos são incluídos no caminho selecionado quando uma restauração é executada

Configurar

Fazer backup

O **Disaster Recovery System** executa um backup em nível de cluster, o que significa que ele coleta backups de todos os servidores em um cluster do CUCM para um local central e arquiva os dados de backup em um dispositivo de armazenamento físico.

Etapa 1. Para criar dispositivos de backup nos quais os dados são salvos, navegue até **Disaster Recovery System > Backup > Backup Device**.

Etapa 2. Selecionar **Add New**; definir um **Backup Device Name** e insira os valores de 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

Etapa 3. Crie e edite programações de backup para fazer backup dos dados. Navegue até **Backup > Scheduler**.

Etapa 4. Defina um **Schedule Name**. Selecione a opção **Device Name** e verifique a **Features** com base no seu cenário.

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

Etapa 5. Configure um backup agendado com base no seu cenário.

Start Backup at*

Date: 2019 Jun 18 Time: 00 Hour 00 Minute

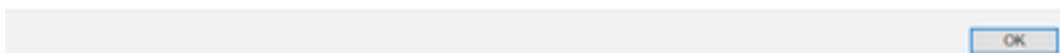
Frequency*

Once
 Daily
 Weekly
 Monthly

Monday Tuesday Wednesday Thursday
 Friday Saturday Sunday

Etapa 6. Selecionar **save** e observe o aviso conforme mostrado na imagem. Selecionar **OK** para avançar.

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.



Passo 7. Uma vez que um **Backup Schedule** é criado, selecione **Enable Schedule**.

Scheduler

Status

i Disabled

Schedule Name

Schedule Name*

Etapa 8. Aguarde até que o status seja alterado para **Enabled**.

Disaster Recovery System
For Cisco Unified Communications Solutions

Backup ▾ Restore ▾ Help ▾

Scheduler

Status

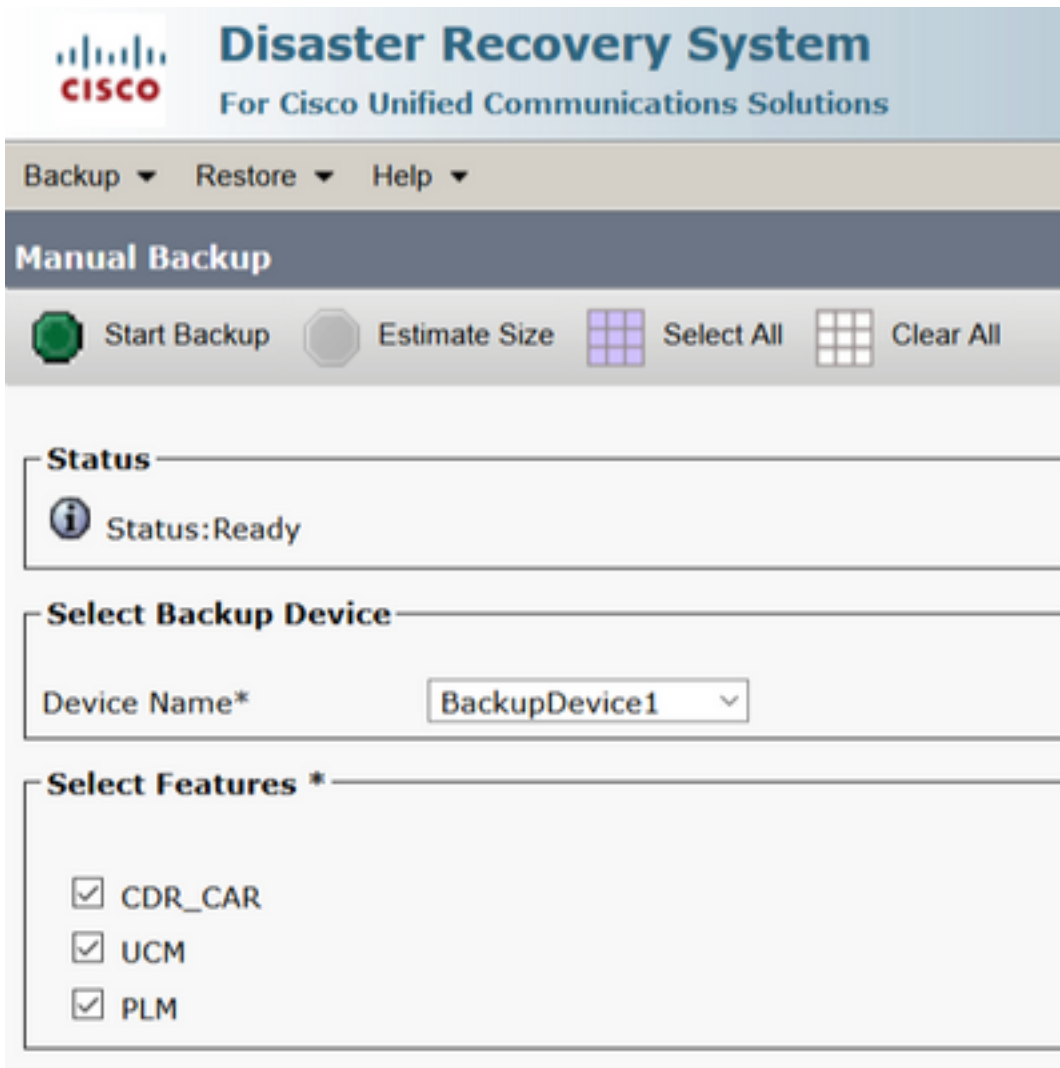
i Enabled

Schedule Name

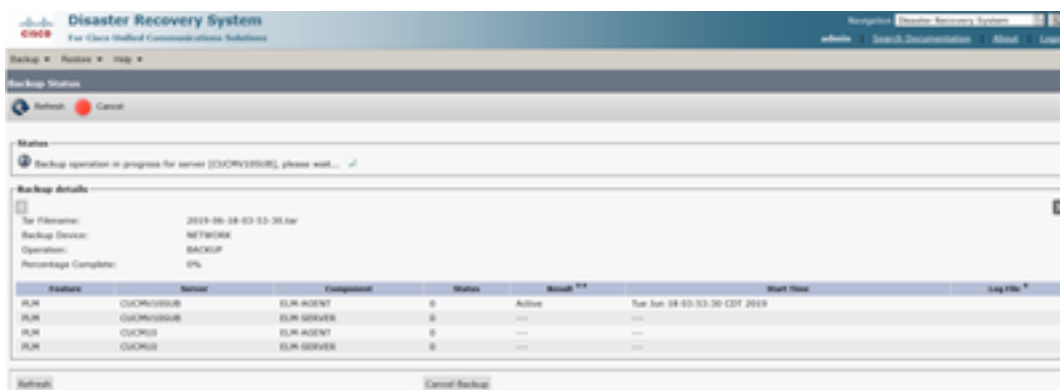
Schedule Name*

Etapa 9. Se um backup Manual for necessário, navegue até **Backup > Manual Backup**.

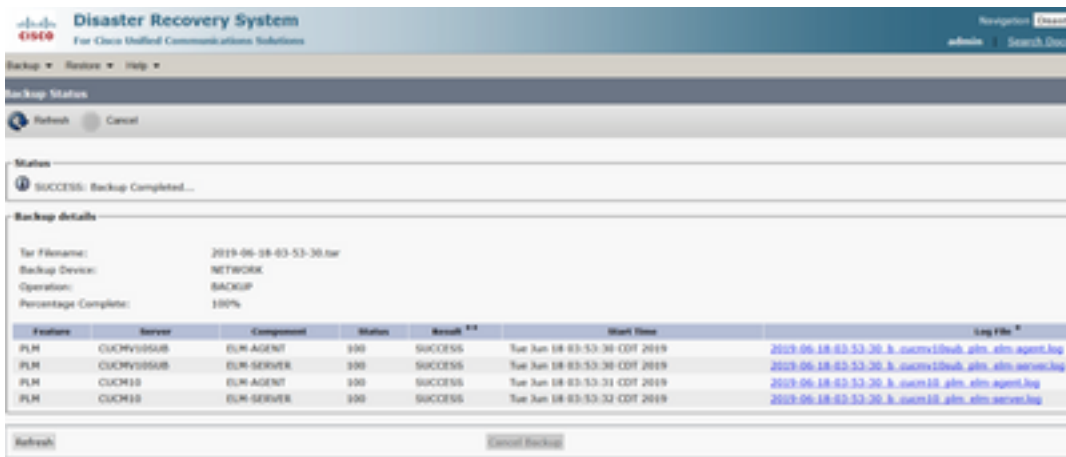
Etapa 10. Selecione a opção **Device Name** e verifique a **Features** com base no seu cenário.



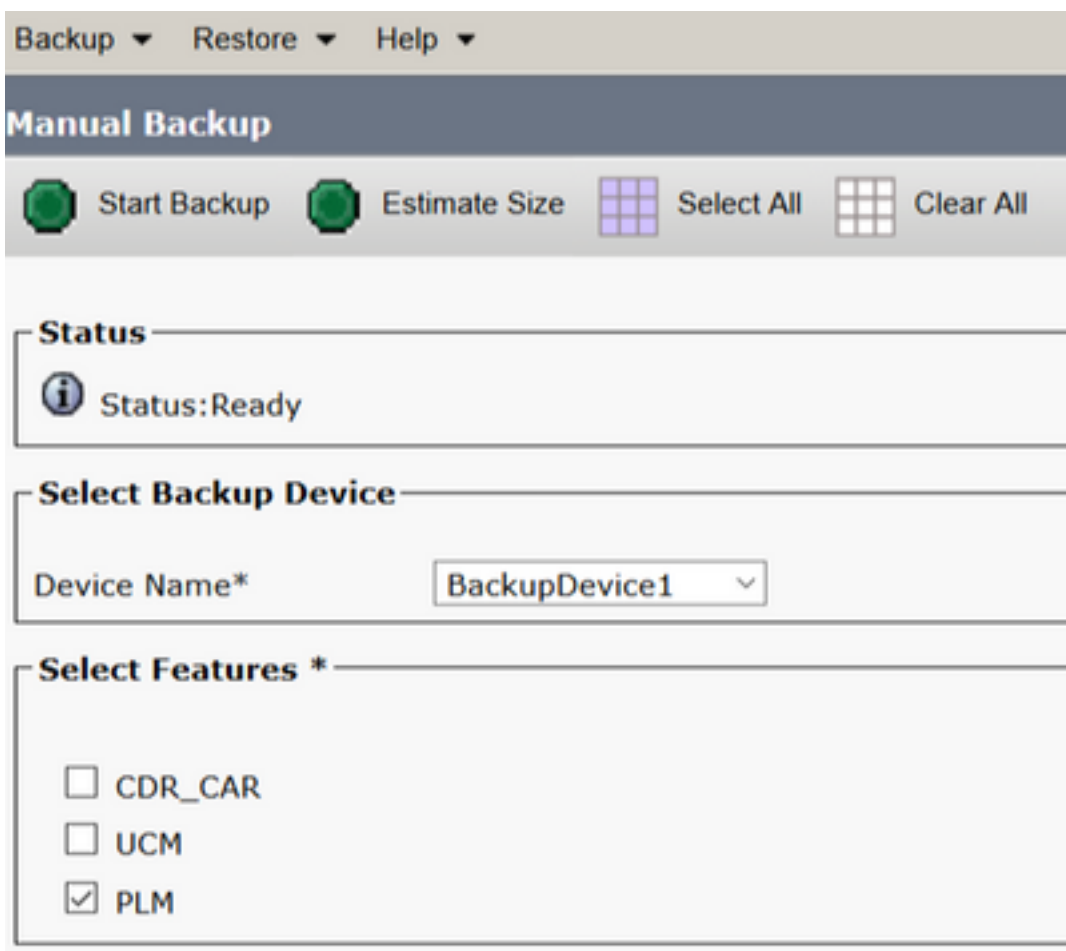
Etapa 11. Selecionar **Start Backup** e a operação é exibida em andamento.



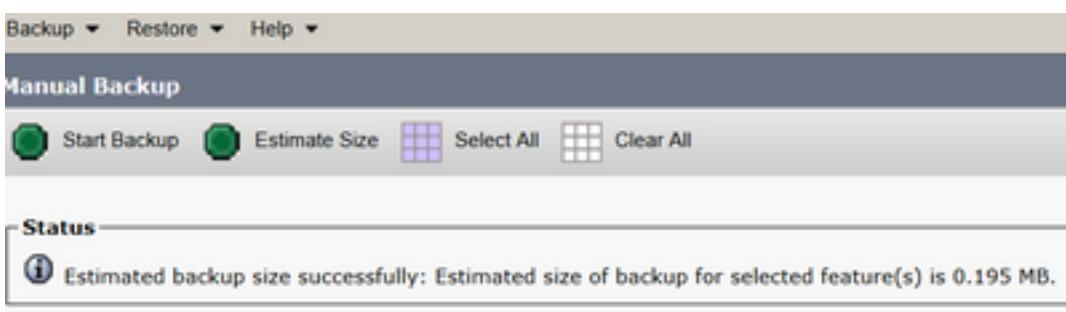
Etapa 12. Quando o backup manual estiver concluído, a mensagem de conclusão será exibida.



Etapa 13. Para estimar o tamanho do arquivo tar de backup que o dispositivo SFTP usa, selecione Estimate Size.

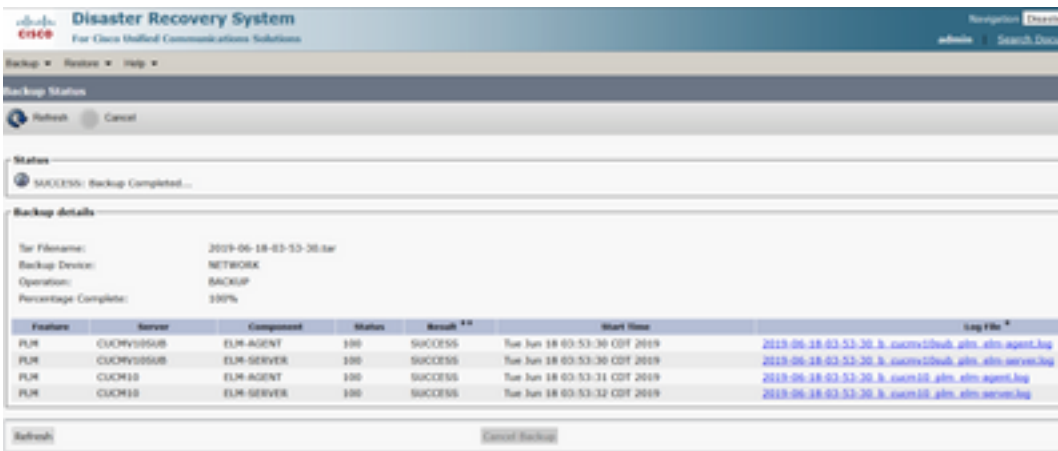


Etapa 14. O tamanho da estimativa é exibido conforme mostrado na imagem

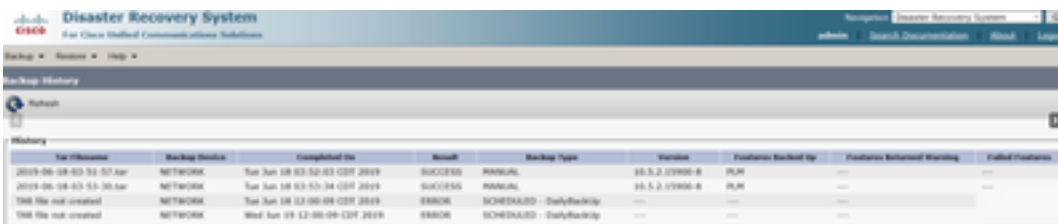


Observação: a função Estimar Tamanho é calculada com base em backups bem-sucedidos anteriores e pode variar caso a configuração tenha sido alterada desde o último backup.

Etapa 15. Para verificar o Status do Backup enquanto um backup é executado, navegue até **Backup > Backup Status**.



Etapa 16. Para consultar os procedimentos de backup executados no sistema, navegue até **Backup > History**.



Restaurar

Restaurações DRS principalmente `drfDevice.xml` e `drfSchedule.xml` arquivos. No entanto, quando uma restauração de dados do sistema é executada, você pode escolher quais nós no cluster precisam ser restaurados.

Observação: o dispositivo de backup (servidor SFTP) já deve estar configurado para recuperar os arquivos tar dele e restaurar o sistema com esses arquivos.

Etapa 1. Navegue até **Disaster Recovery System > Restore > Restore Wizard**.

Etapa 2. Selecione a opção **Device Name** que armazena o arquivo de backup a ser usado para a restauração. Selecionar **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

Etapa 3. Selecione a opção **Backup File** na lista exibida de arquivos disponíveis, como mostrado na imagem. O arquivo de backup selecionado deve incluir as informações a serem restauradas.



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

Etapa 4. Na lista de recursos disponíveis, selecione o recurso a restaurar.

Disaster Recovery System
For Cisco Unified Communications Solutions

Backup ▾ Restore ▾ Help ▾

Step3 Restore - Select the Type of Restore

Back 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

Etapa 5. Selecione os nós nos quais aplicar a restauração.



Observação: a restauração em uma etapa permite a restauração do cluster inteiro se o Publicador já tiver sido reconstruído ou instalado recentemente. Essa opção ficará visível SOMENTE se o arquivo de backup selecionado para restauração for o arquivo de backup do cluster e os recursos escolhidos para restauração incluírem os recursos registrados nos nós do editor e do assinante.

Etapa 6. Selecionar **Restore** para iniciar o processo e o status Restaurar é atualizado.



Passo 7. Para verificar o status da restauração, navegue até **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

Etapa 8. Restore Status alterações em SUCCESS quando estiver concluída.

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

Etapa 9. Para que as alterações entrem em vigor, o sistema deve ser reiniciado.

```
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!
```

Dica: use um procedimento com suporte para reiniciar o sistema [Desligue ou reinicie o sistema](#)

Etapa 10. Para consultar os procedimentos de restauração executados no sistema, navegue até **Restore > History**.

Start Time	Backup Status	Completed On	Result	Version	Features Restored	Failed Features
2019-06-24 03:53:30 for	NETWORK	The Jul 20 03:53:08 CDT 2019	SUCCESS	10.5.2.10000-6	PLN	---

Troubleshoot

Esta seção fornece informações para solucionar problemas da sua configuração.

O cluster do CUCM (que envolve os nós do CUCM e os servidores de mensagens instantâneas e presença (IM&P) da Cisco) deve atender a estes requisitos:

- Port 22 aberto para estabelecer a comunicação com o servidor SFTP
- Validou que o IPsec e Tomcat os certificados não expiraram. Para verificar a validade dos certificados, navegue até **Cisco Unified OS Administration > Security > Certificate Management**

Observação: para gerar novamente certificados ipsec e Tomcat, use o [Procedimento para gerar novamente certificados no CUCM](#)

- Verifique se a configuração da replicação de banco de dados foi concluída e se não mostra erros ou incompatibilidades nos servidores do Publicador CUCM e do Publicador IM&P.
- Valide a acessibilidade entre os servidores e o servidor SFTP.
- Valide se todos os servidores no cluster estão autenticados com o comando `show network cluster`.

Quando falhas de backup ou restauração são relatadas e é necessária assistência adicional, este conjunto de registros deve ser coletado e compartilhado com o Centro de Assistência Técnica (TAC):

- Logs principais do Cisco DRF
- Registros locais do Cisco DRF
- Registros de falhas da página Status atual do DRF
- Carimbo de data/hora da emissão

Informações Relacionadas

- [Servidores SFTP suportados](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.