

# Gere e extraia o arquivo RCA do Cisco DNA Center

## Contents

---

[Introdução](#)

[Informações de Apoio](#)

[Gerar o arquivo RCA em um cluster de nó único](#)

[Gerar o arquivo RCA em um cluster N-Node](#)

[Extraia o arquivo RCA em um computador com Windows](#)

[Extraia o arquivo RCA em um computador Mac ou Linux](#)

[Envie o arquivo RCA para um computador Mac ou Linux](#)

[Carregar o arquivo RCA em um TAC SR](#)

[Envie o arquivo RCA para o TAC SR](#)

[Opção 1. Carregar o arquivo via HTTPS \(opção mais rápida e usa a porta 443\)](#)

[Shell Restrito](#)

[Opção 2. Fazer upload do arquivo via SCP \(usa a porta 22\)](#)

---

## Introdução

Este documento descreve como criar e extrair o arquivo de análise da causa raiz (RCA) do Cisco Digital Network Architecture (DNA) Center.

## Informações de Apoio

Você deve ter acesso de CLI ao Cisco DNA Center. Para fazer logon no Cisco DNA Center com a CLI, você deve se conectar via Secure Socket Shell (SSH) ao endereço IP de gerenciamento do Cisco DNA Center com `maglev` o nome de usuário na porta 2222.

Cuidado com o recurso de shell restrito que foi adicionado ao 2.3.2.x, que não permite executar vários comandos até que você o desative. Para desativar temporariamente o shell restrito no 2.3.2.x ou 2.3.3.x, consulte [este documento](#). No 2.3.4.0 e posterior, o shell restrito não pode ser desativado.

Gerar o arquivo RCA em um cluster de nó único

Etapa 1. Faça login na CLI do Cisco DNA Center na porta 2222. Use o `maglev` como o nome de usuário, a menos que o nome de usuário tenha sido modificado no momento da configuração inicial. Em seguida, execute o comando `rca`.

```
<#root>
```

```
[Tue Sep 11 15:08:48 UTC] maglev@10.1.1.1 (maglev-master-1) ~ $
```

```
sudo
```

```
rca

[sudo] password for maglev: ===== Verifying
<type your admin password>

User 'admin' logged into 'kong-frontend.maglev-system.svc.cluster.local' successfully =====
Created RCA package: /data/rca/maglev-x.x.x.x-rca-2018-09-11_15-32-40.UTC.tar.gz

[Tue Sep 11 15:43:14 UTC] maglev@10.1.1.1 (maglev-master-1) ~
```

Nas versões mais recentes do Cisco DNA Center (2.3.4.x e posterior), você pode executar o \$ rca copy.

```
$ rca --help
```

Help:

rca - root cause analysis collection utilities

Usage: rca [COMMAND] [ARGS]...

Commands:

- clear - clear RCA files
- copy - copy rca files to specified location
- exec - collect RCA
- view - restricted filesystem view

---

 **Observação:** o arquivo RCA é gerado e armazenado no /data/rca. Geralmente, leva cerca de 20 minutos para criar o arquivo. O nome do arquivo deve ter este formato: maglev-<inter-cluster link IP address>-rca<date and time>.tar.gz.

---

Gerar o arquivo RCA em um cluster N-Node

---

 **Dica:** quando você tem um cluster funcional de n nós, os serviços são distribuídos. Quando os serviços são distribuídos, o RCA de um nó individual não inclui logs de serviços que são executados em outros nós. Por exemplo, se você tiver o serviço A executado no nó 1 e obtiver o RCA do nó 2, os registros do serviço A não serão incluídos. Portanto, é recomendável capturar e incluir o arquivo RCA de todos os nós no cluster quando o TAC solicitar um RCA arquivo.

---

Quando você tiver um cluster de 3 nós e executar o comandorca em qualquer dispositivo, o Cisco DNA Center solicitará um endereço IP do cluster. No prompt, insira o endereço IP entre clusters do nó do qual deseja recuperar o RCA.

Neste exemplo, os endereços IP entre clusters estão no intervalo 10.1.1.0/29.

```
<#root>
```

```
[Wed May 30 18:24:26 UTC] maglev@10.1.1.2 (maglev-master-10) ~ $
```

```
rca

===== Verifying ssh/sudo access =====
```

Cluster: 10.1.1.3

```
[administration] username for 'https://10.1.1.3:443': admin [administration] password for 'admin':  
<type your admin password>  
User 'admin' logged into '10.1.1.3' successfully =====
```

Depois de executar o rca comando, os endereços IP entre clusters especificados são armazenados em cache /home/maglev/.maglevconf. Na próxima vez que você executar o comandorca, o Cisco DNA Center usará o mesmo nó para obter as informações de RCA.

<#root>

```
[Wed May 30 18:23:37 UTC] maglev@10.1.1.2 (maglev-master-10) ~ $
```

```
rca  
[sudo] password for maglev: ===== Verifying  
type the admin password  
>  
User 'admin' logged into '10.1.1.3' successfully <-- it automatically logged into the cluster previously  
===== RCA package created on Wed May 30 18:2
```

Se precisar executar o comandorca em um nó diferente, você deverá excluir o contexto configurado no Cisco DNA Center. Em seguida, você será solicitado a escolher um novo endereço IP entre clusters e poderá definir o endereço IP do outro nó.

<#root>

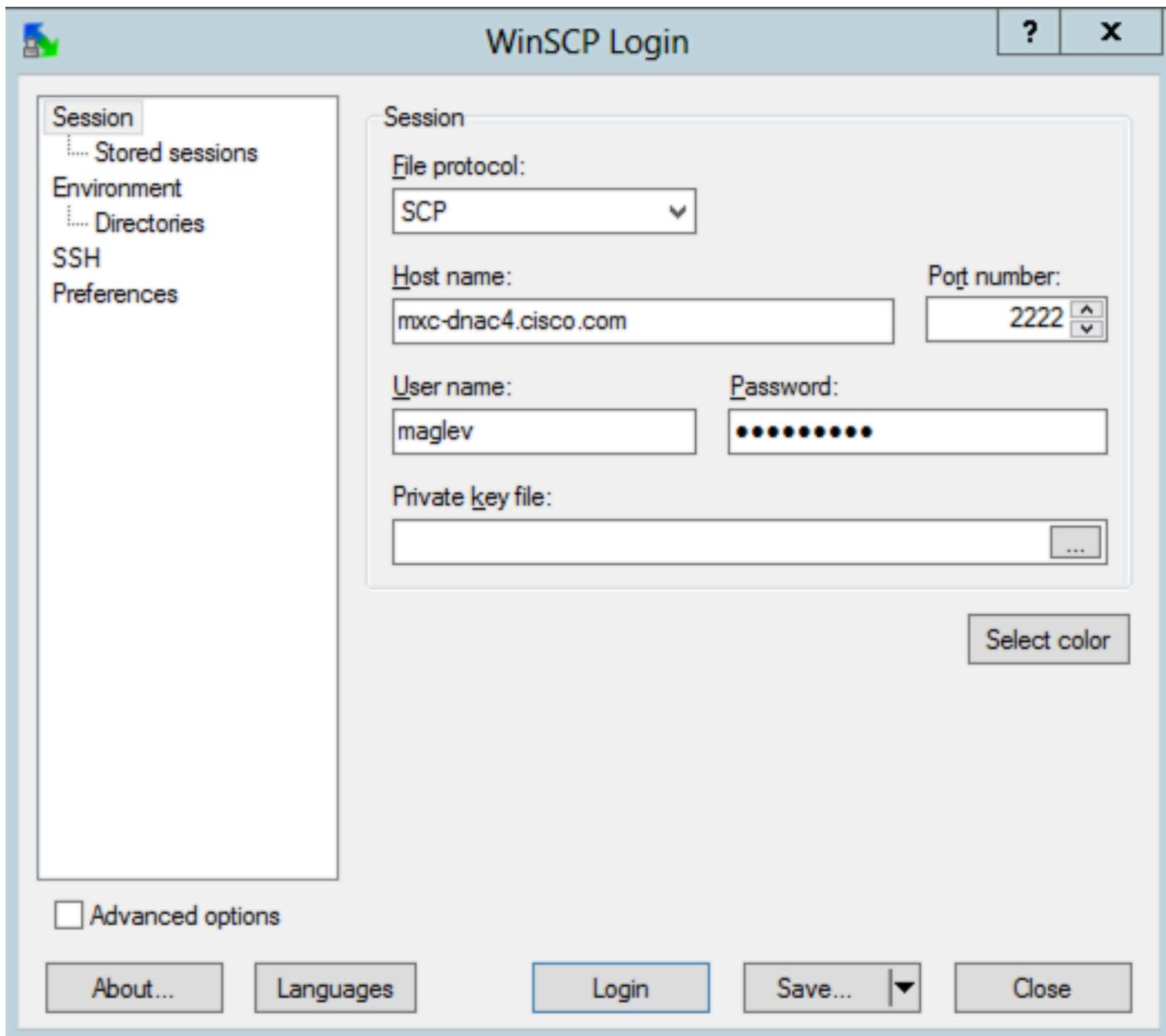
```
[Wed May 30 18:24:10 UTC] maglev@10.1.1.2 (maglev-master-10) ~ $
```

```
sudo maglev context delete maglev-1  
Removed command line context 'maglev-1' [Wed May 30 18:24:18 UTC] maglev@10.1.1.2 (maglev-master-10) ~  
more /home/maglev/.maglevconf  
;----- ; Modified by Maglev: Wed, 30 M  
rca  
===== Verifying ssh/sudo access =====  
10.1.1.2 <-- now it asks for the new cluster IP address  
[administration] username for 'https://10.1.1.2:443': admin [administration] password for 'admin': <  
type your admin password  
> User 'admin' logged into '10.1.1.2' successfully =====
```

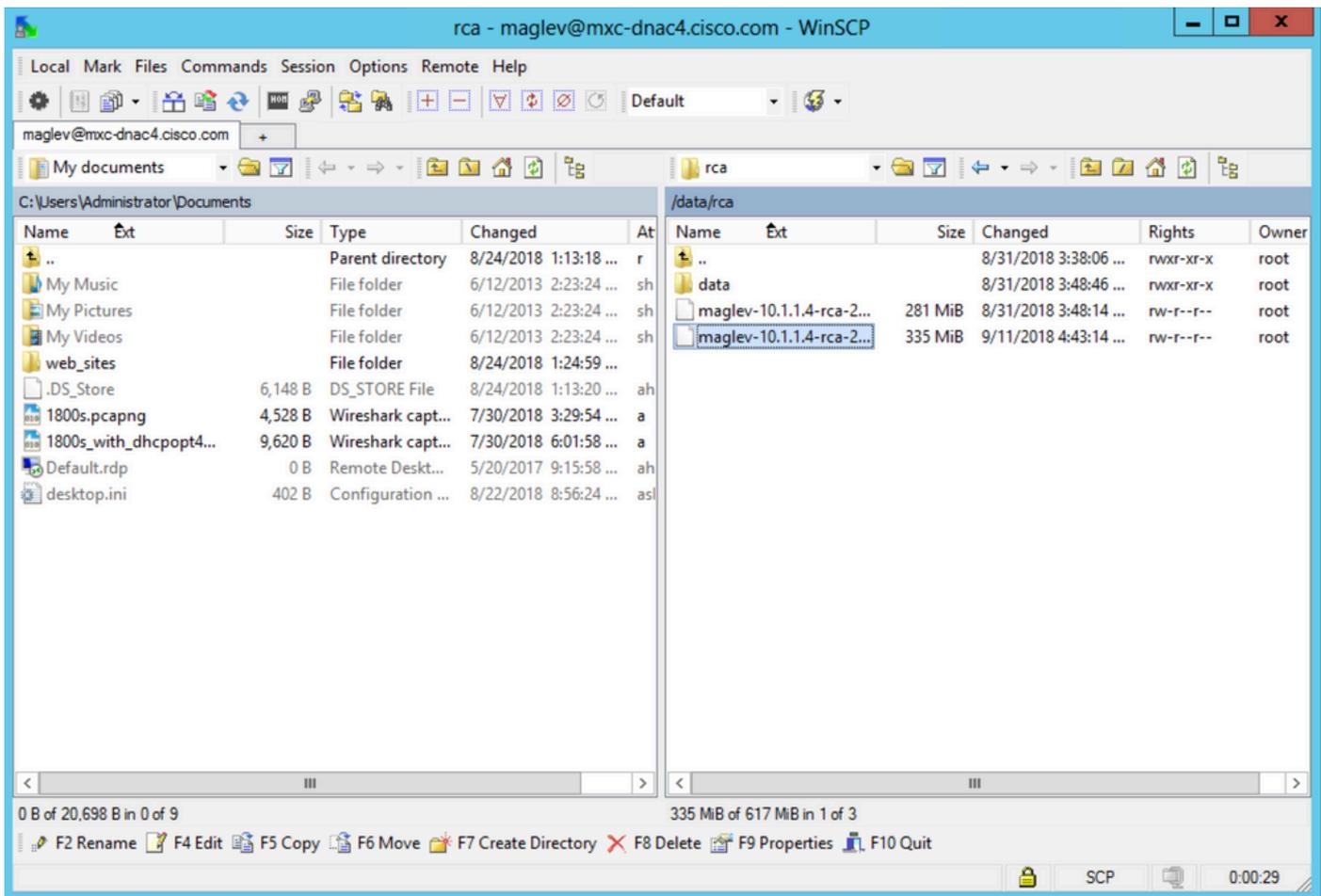
Extraia o arquivo RCA em um computador com Windows

Etapa 1. Baixe o [WinSCP](#) ou seu cliente SCP favorito.

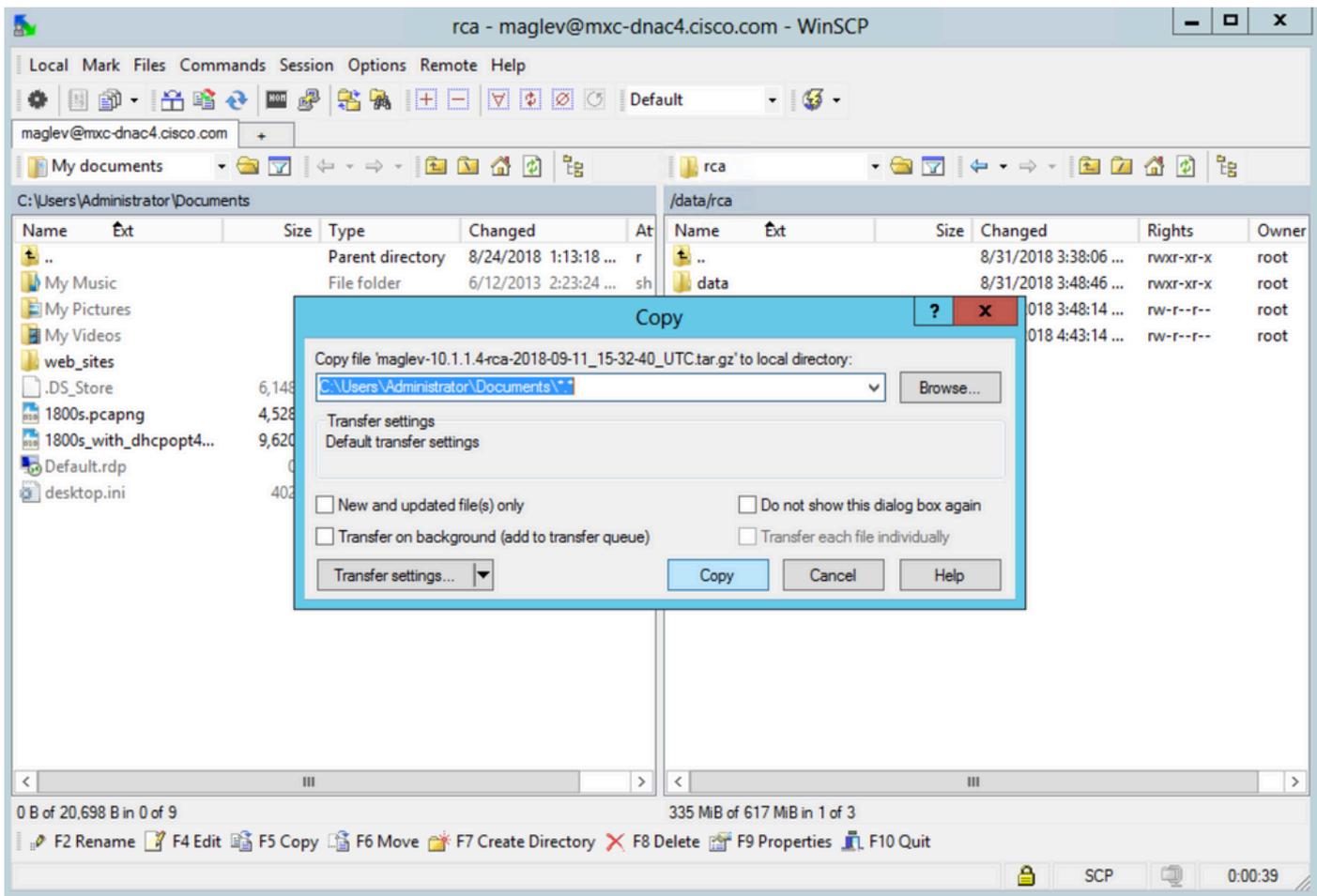
Etapa 2. Faça login no Cisco DNA Center com suas credenciais de CLI, escolha SCP como o protocolo de arquivo e escolha o número de porta 2222.



Etapa 3. Navegue até a /data/rca pasta.



Etapa 4. Copie o arquivo RCA para o computador local.



Extraia o arquivo RCA em um computador Mac ou Linux

**Observação:** neste exemplo, o endereço IP do Cisco DNA Center é resolvido como mxc-dnac4.cisco.com. Substitua esse nome de host pelo FQDN (Fully Qualified Domain Name, Nome de domínio totalmente qualificado) ou pelo endereço IP do dispositivo Cisco DNA Center.

Etapa 1. Abra uma sessão de terminal e, em seguida, execute estas etapas para copiar o arquivo RCA chamado maglev-10.1.1.4-rca-2018-09-11\_15-32-40.UTC.tar.gz armazenado no dispositivo Cisco DNA Center no diretório/data/rca para o diretório de trabalho atual no computador.

```
<#root>
```

```
ALECARRA-M-P1Z8:~ alecarra$
```

```
scp -P 2222 maglev@mx-c-dnac4.cisco.com:/data/rca/maglev-10.1.1.4-rca-2018-09-11_15-32-40.UTC.tar.gz ./
```

```
Welcome to the Maglev Appliance maglev@mx-c-dnac4.cisco.com's password: <
```

```
type your maglev password>
```

```
maglev-10.1.1.4-rca-2018-09-11_15-32-40.UTC.tar.gz 100% 335MB 3.3MB/s 01:41 ALECARRA-M-P1Z8:~ alecarra$
```

Envie o arquivo RCA para um computador Mac ou Linux

Na CLI do dispositivo Cisco DNA Center, use esta sintaxe:

```
$ scp /data/rca/<RCA file name> <Mac/Linux username>@<Mac/Linux IP address>:<path to save the file>
```

Aqui está um exemplo do comando usado no laboratório:

```
<#root>
```

```
$
```

```
scp /data/rca/maglev-10.1.1.4-rca-2018-09-11_15-32-40.UTC.tar.gz alecarra@10.24.133.238:/Users/alecarra/
```

```
The authenticity of host '10.24.133.238 (10.24.133.238)' can't be established. ECDSA key fingerprint is
```

```
yes
```

```
Warning: Permanently added '10.24.133.238' (ECDSA) to the list of known hosts. Password:
```

```
<type your Linux or Mac user password>
```

```
maglev-10.1.1.4-rca-2018-09-11_15-32-40.UTC.tar.gz 100% 335MB 3.7MB/s 01:32
```

Carregar o arquivo RCA em um TAC SR

Você pode usar a [ferramenta Carregador de arquivo de caso](#) para carregar o arquivo RCA em uma Solicitação de serviço (SR) do TAC que existe em seu computador através de um navegador. Especifique o número do caso quando necessário.

Envie o arquivo RCA para o TAC SR

Há duas opções para carregar um arquivo (como o RCA) diretamente de um dispositivo Cisco DNA Center para um TAC SR. Em ambas as opções, o nome de usuário é o número de SR e a senha é um token exclusivo para cada SR. O nome de usuário/senha está sempre presente em uma nota no início do seu SR, e também pode ser recuperado do SCM. Para obter mais detalhes sobre o token, consulte [Uploads de arquivo do cliente para o Cisco Technical Assistance Center](#).

Exemplo de saída de um SR:

Subject: 688046089: CXD Upload Credentials

You can now upload files to the case using FTP/FTPS/SCP/SFTP/HTTPS protocols and the following details:

Hostname: cxd.cisco.com

Username: 688046089

Password: gX\*\*\*\*\*P7

Opção 1. Carregar o arquivo via HTTPS (opção mais rápida e usa a porta 443)

Etapa 1. Teste se você tem conectividade do seu dispositivo Cisco DNA Center para `cxd.cisco.com` via porta 443. Esta é uma maneira de executar o teste:

```
<#root>
```

```
$
```

```
nc -zv cxd.cisco.com 443
```

```
Connection to cxd.cisco.com 443 port [tcp/https] succeeded!
```

```
$
```



**Observação:** se o teste falhar, você não poderá usar este método para fazer upload do arquivo.

---

Etapa 2. Se o teste for bem-sucedido, carregue o arquivo via HTTPS com o uso deste comando:

```
<#root>
```

```
$ curl -T "
```

```
<filename with path>
```

```
" -u
```

```
<SR number>
```

```
https://cxd.cisco.com/home/
```

(Se quiser ver uma exibição mais detalhada do carregamento, adicione a `-v` opção. Por exemplo, `'curl -vT ...'`.)

Por exemplo:

```
<#root>
```

```
$
```

```
curl -T "./test.txt" -u 688046089 https://cxd.cisco.com/home/
```

```
Enter host password for user '688046089':
```

```
<Type your CXD Upload password, unique to a Service Request, here>
```

```
[Tue Dec 10 13:35:47 UTC] maglev@10.1.1.1(maglev-master-1) ~
```

```
$
```

Shell Restrito

Como o shell restrito impede o uso de CURL, empregamos rca copy, que utiliza scp, para permitir a transferência segura de arquivos para cxd.cisco.com.

```
$ rca copy --files maglev-10.1.1.233-rca-2024-03-06_14-07-36.UTC.tar.gz 6969XXXXXX@xcd.cisco.com:/
FIPS mode initialized
Warning: Permanently added the ECDSA host key for IP address '10.209.135.105' to the list of known hosts.
6969XXXXXX6@xcd.cisco.com's password:
maglev-10.1.1.233-rca-2024-03-06_14-07-36.UTC.tar.gz
```

Opção 2. Fazer upload do arquivo via SCP (usa a porta 22)

Etapa 1. Teste se você tem conectividade do seu dispositivo Cisco DNA Center para cxd.cisco.com via porta 22. Esta é uma maneira de executar o teste:

```
<#root>
$
nc -zv cxd.cisco.com 22

Connection to cxd.cisco.com 22 port [tcp/ssh] succeeded!
$
```



**Observação:** se o teste falhar, você não poderá usar este método para fazer upload do arquivo.

---

Etapa 2. Se o teste for bem-sucedido, carregue o arquivo via SCP com o uso deste comando:

```
<#root>
$ scp
<local filename with path>

<SR number>
@xcd.cisco.com:
```

Por exemplo:

```
<#root>
$
```

```
scp ./test.txt 688046089@cxd.cisco.com:
```

```
The authenticity of host 'cxd.cisco.com (X.X.X.X)' can't be established.  
RSA key fingerprint is SHA256:3c8Vi3Ms2AITZ1NzkBccR1pvE5ie9oMs64Uh0uhRado.  
Are you sure you want to continue connecting (yes/no)?
```

```
yes
```

```
Warning: Permanently added 'cxd.cisco.com,X.X.X.X' (RSA) to the list of known hosts.  
688046089@cxd.cisco.com's password:
```

```
<Type your CXD Upload password, unique to a service request, here>
```

```
test.txt
```

```
[Tue Dec 10 13:44:27 UTC] maglev@10.1.1.1 (maglev-master-1) ~  
$
```

## 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.