Generate and Extract the RCA File from Cisco DNA Center

Contents

Introduction

This document describes how to create and extract the Root Cause Analysis (RCA) file from the Cisco Digital Network Architecture (DNA) Center.

Background Information

You must have CLI access to Cisco DNA Center. In order to log in to Cisco DNA Center with the CLI, you must connect via Secure Socket Shell (SSH) to the management IP address of your Cisco DNA Center with `maglev` as the username on port `2222`.

Beware of the restricted shell feature that was added in 2.3.2.x that does not allow you to run many commands until you disable it. In order to disable the restricted shell temporarily in 2.3.2.x or 2.3.3.x, refer to this document. In 2.3.4.0 and later the restricted shell can not be disabled.

Generate the RCA File in a Single-Node Cluster

Step 1. Log in to the Cisco DNA Center CLI on port 2222. Use the `maglev` as the username, unless the username was modified at the time of the initial setup. Then run the `rca` command.

<#root>

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

sudo

rca

```
[sudo] password for maglev:

================================================================
Verifying ssh/sudo access
================================================================
Done

================================================================
Verifying administration access
================================================================
[administration] password for 'admin':
```

<type your admin password>

```
User 'admin' logged into 'kong-frontend.maglev-system.svc.cluster.local' successfully

================================================================
RCA package created on Tue Sep 11 15:32:47 UTC 2018
================================================================

2018-09-11 15:32:47 | INFO | Generating log for 'date'...
tar: Removing leading `/' from member names
/etc/cron.d/
/etc/cron.d/clean-journal-files
<snip>
/data/rca/maglev-x.x.x.x-rca-2018-09-11_15-32-40_UTC/docker_inspect_k8s_platform-ui_platform-ui-2963217
/data/rca/maglev-x.x.x.x-rca-2018-09-11_15-32-40_UTC/sudo_ethtool_calife1d52fff20.log
2018-09-11 15:43:14 | INFO | Cleaning up RCA temp files...
```

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) ~
```

In the newer Cisco DNA Center releases (2.3.4.x and later), you have the ability to perform `$ 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
```

Note: The RCA file is generated and stored in `/data/rca`. It usually takes around 20 minutes to create the file. The filename must have this format: `maglev-<inter-cluster link IP address>-rca<date and time>.tar.gz`.

Generate the RCA File in an N-Node Cluster

Tip: When you have a functional n-node cluster, services are distributed. When the services are distributed, the RCA from an individual node does not include logs from services that run on other nodes. For example, if you have service A that runs on node-1 and you get the RCA from node-2, the logs from service A are not included. Therefore, it is recommended that you capture and include the RCA file of all nodes in the cluster when the TAC requests an RCA file.

When you have a 3-node cluster and you run the rca command on any device, the Cisco DNA Center prompts you for a cluster IP address. At the prompt, enter the inter-cluster IP address of the node that you want to retrieve the RCA from.

In this example, the inter-cluster IP addresses are in the 10.1.1.0/29 range.

```
<#root>

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

rca


================================================================
Verifying ssh/sudo access
================================================================
Done

================================================================
Verifying administration 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

================================================================
RCA package created on Wed May 30 18:24:44 UTC 2018
================================================================

2018-05-30 18:24:44 | INFO | Generating log for 'date'...
tar: Removing leading `/' from member names
/etc/cron.d/
/etc/cron.d/run-remedyctl
```

After you run the rca command, the inter-cluster IP addresses that you specified are cached in /home/maglev/.maglevconf. The next time you run the rca command, Cisco DNA Center uses the same node in order to get the RCA information.

```
<#root>

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

rca
```

```
[sudo] password for maglev:

================================================================
Verifying ssh/sudo access
================================================================
Done

================================================================
Verifying administration access
================================================================
[administration] password for 'admin': <
```

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 18:23:46 UTC 2018
================================================================

2018-05-30 18:23:46 | INFO | Generating log for 'date'...
tar: Removing leading `/' from member names
/etc/cron.d/
… rca continued…
```

If you need to run the rca command on a different node, you must delete the context that is configured in Cisco DNA Center, then you are asked to choose a new inter-cluster IP address and you can define the IP address of the other node.

<#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 May 2018 18:24:18 UTC
; maglev 73529
;--------------------------------------------------------------------

[global]


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

rca

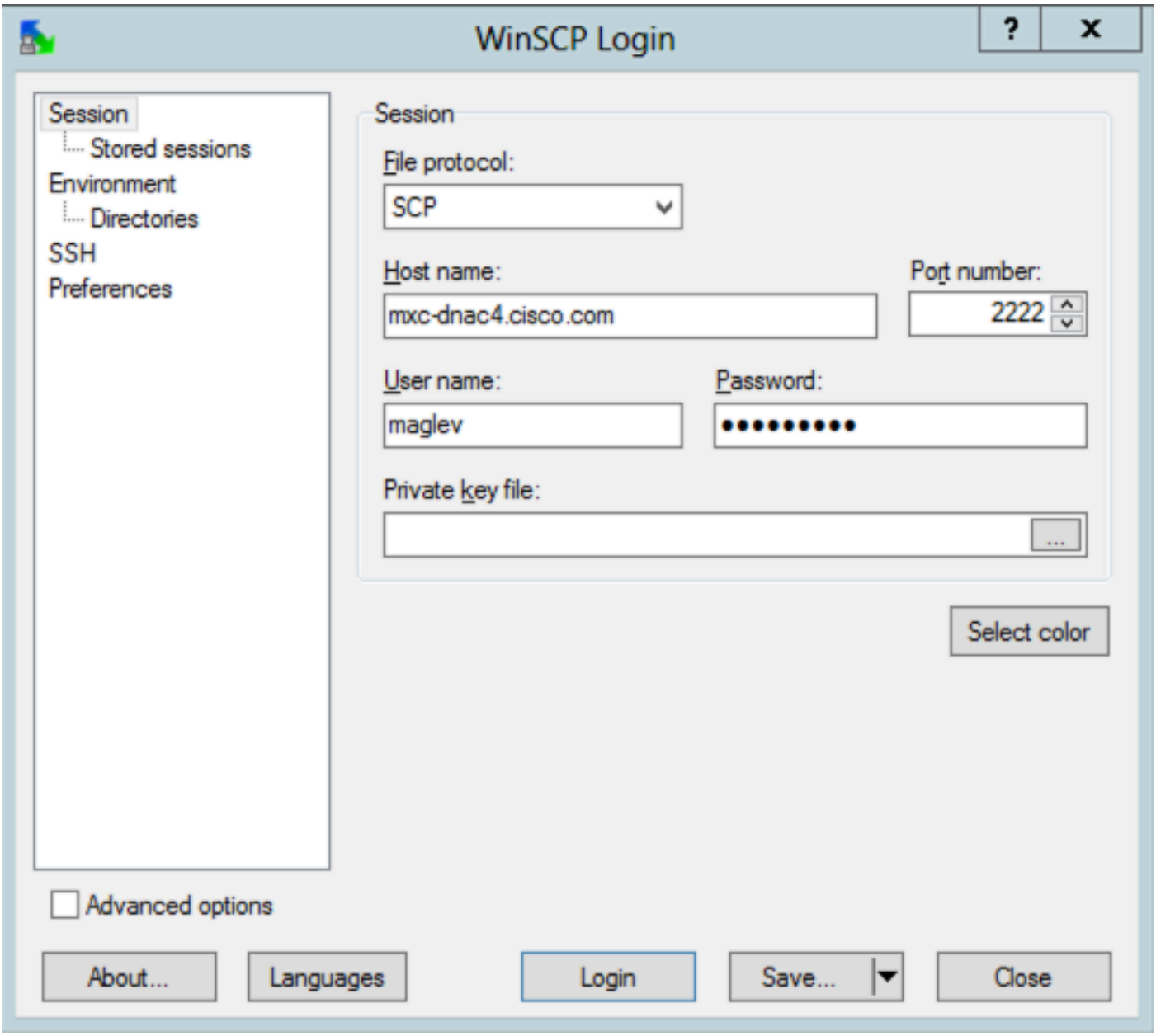
```
================================================================
```

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

================================================================
Verifying administration access
================================================================
Cluster:

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

================================================================
RCA package created on Wed May 30 18:24:44 UTC 2018
================================================================

2018-05-30 18:24:44 | INFO | Generating log for 'date'...
tar: Removing leading `/' from member names
/etc/cron.d/
/etc/cron.d/run-remedyctl
```

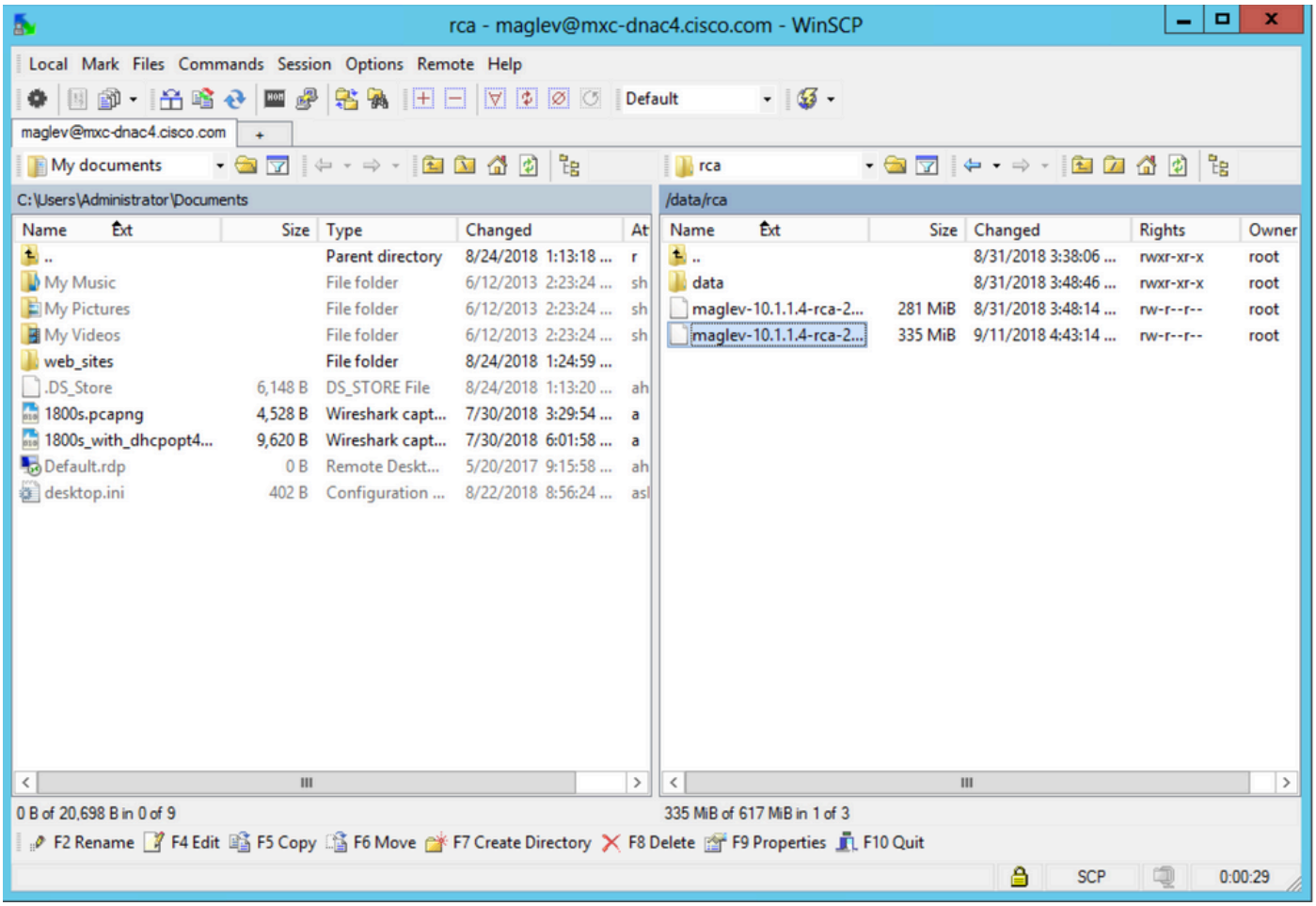
Extract the RCA File on a Windows Computer

Step 1. Download WinSCP or your favorite SCP client.

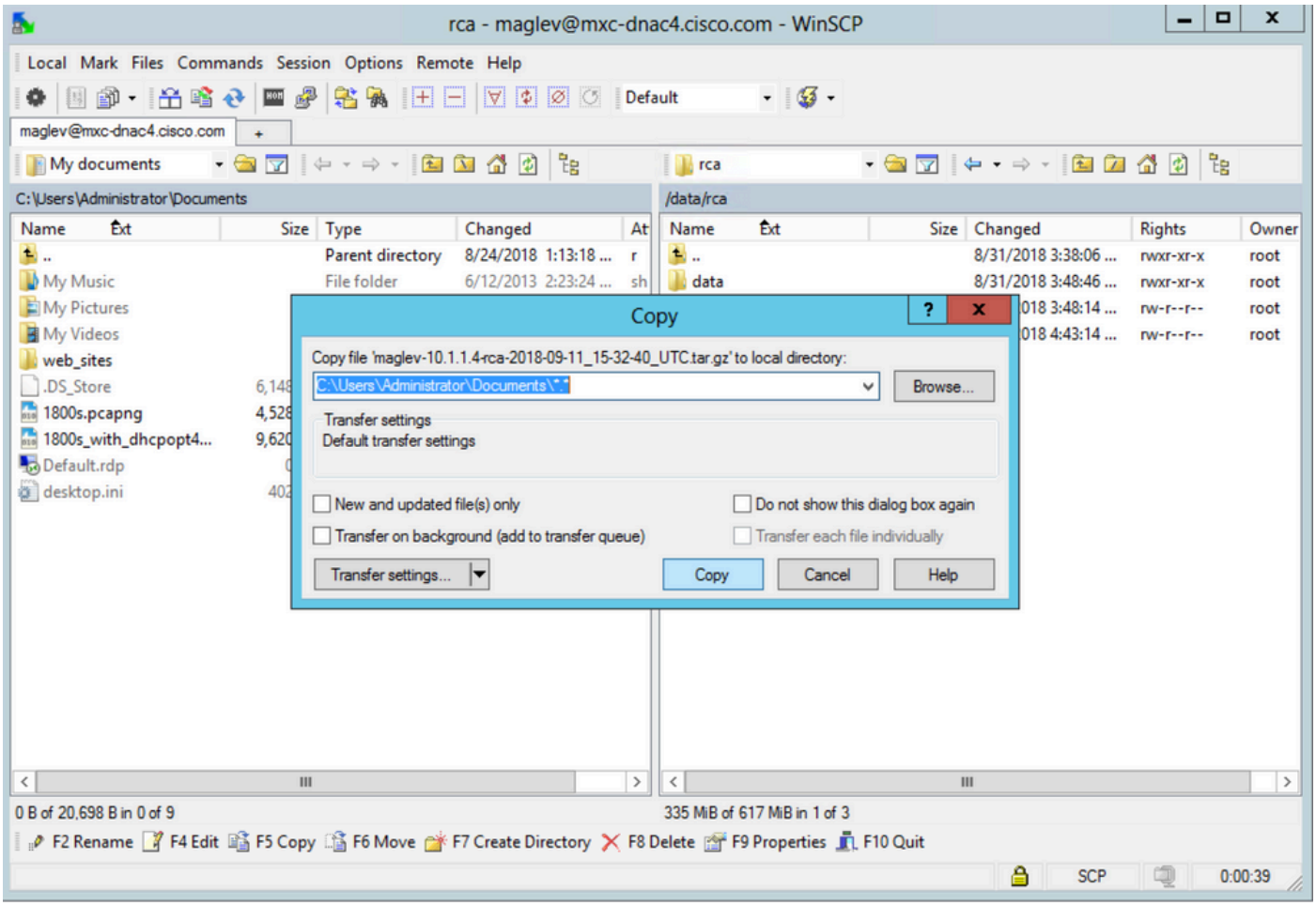
Step 2. Log in to Cisco DNA Center with your CLI credentials, choose SCP as the file protocol, and choose the port number 2222.



Step 3. Navigate to the /data/rca folder.



Step 4. Copy the RCA file to your local computer.



Extract the RCA File on a Mac or Linux Computer

Note: In this example, the Cisco DNA Center IP address resolves to mxc-dnac4.cisco.com. Replace this hostname with the Fully Qualified Domain Name (FQDN) or IP address of your Cisco DNA Center appliance.

Step 1. Open a terminal session, then perform these steps to copy the RCA file named maglev-10.1.1.4-rca-2018-09-11_15-32-40_UTC.tar.gz stored on the Cisco DNA Center appliance in the /data/rca directory to the present working directory on your computer.

<#root>

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

scp -P 2222 maglev@mxc-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@mxc-dnac4.cisco.com's password: <

type your maglev password>

maglev-10.1.1.4-rca-2018-09-11_15-32-40_UTC.tar.gz
ALECARRA-M-P1Z8:~ alecarra$
```

Push the RCA File to a Mac or Linux Computer

From the CLI of the Cisco DNA Center appliance, use this syntax:

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

Here is an example of the command used in the lab:

```
<#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 SHA256:u66OkUomvMParNkcPIm7oXrDp84rilP5CM9wCWCFOAE.
Are you sure you want to continue connecting (yes/no)?

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
```

Upload the RCA File to a TAC SR

You can use the Case File Uploader tool in order to upload the RCA file to a TAC Service Request (SR) that exists on your computer via a browser. Specify the case number where required.

Push the RCA File to the TAC SR

There are two options in order to upload a file (such as the RCA) directly from a Cisco DNA Center appliance to a TAC SR). In both options, the username is the SR number and the password is a token unique to every SR. The username/password is always present in a note at the start of your SR, and can also be retrieved from SCM. For more details on the token, refer to Customer File Uploads to Cisco Technical Assistance Center.

Sample output from a 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
```

Option 1. Upload the File via HTTPS (Fastest Option and Uses Port 443)

Step 1. Test whether you have connectivity from your Cisco DNA Center appliance to cxd.cisco.com via port 443. Here is one way to perform the test:

```
<#root>

$

nc -zv cxd.cisco.com 443


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

Note: If the test failed, you cannot use this method to upload your file.

Step 2. If the test succeeded, upload the file via HTTPS with the use of this command:

```
<#root>

$ curl -T “

<filename with path>

” -u

<SR number>

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

(If you want to see a more detailed view of the upload, then add the -v option. For example, 'curl -vT ...'.)

For example:

```
<#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) ~
$
```

Restricted Shell

Since the restricted shell prevents the use of CURL, we employ rca copy, which leverages scp, to enable secure file transfer to cxd.cisco.com.

```
$ rca copy --files maglev-10.1.1.233-rca-2024-03-06_14-07-36_UTC.tar.gz 6969XXXXX@cxd.cisco.com:/
FIPS mode initialized
Warning: Permanently added the ECDSA host key for IP address '10.209.135.105' to the list of known host
6969XXXXX6@cxd.cisco.com's password:
maglev-10.1.1.233-rca-2024-03-06_14-07-36_UTC.tar.gz
```

Option 2. Upload the File via SCP (Uses Port 22)

Step 1. Test whether you have connectivity from your Cisco DNA Center appliance to cxd.cisco.com via port 22. Here is one way to perform the test:

<#root>

$

nc -zv cxd.cisco.com 22

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

Note: If the test failed, you cannot use this method to upload your file.

Step 2. If the test succeeded, upload the file via SCP with the use of this command:

<#root>

$ scp

<local filename with path>

<SR number>

@cxd.cisco.com:

For example:

<#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 SHA256:3c8Vi3Ms2AITZlNzkBccR1pvE5ie9oMs64UhOuhRado.
```

```
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) ~
$
```