Generieren und Extrahieren der RCA-Datei aus dem Cisco DNA Center

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie die Root Cause Analysis (RCA)-Datei erstellt und aus dem Cisco Digital Network Architecture (DNA) Center extrahiert wird.

Hintergrundinformationen

Sie benötigen CLI-Zugriff auf das Cisco DNA Center. Um sich mit der CLI bei Cisco DNA Center anzumelden, müssen Sie über Secure Socket Shell (SSH) eine Verbindung zur Management-IP-Adresse Ihres Cisco DNA Center mit `maglev` als Benutzername auf Port `2222`.

Achten Sie auf die eingeschränkte Shell-Funktion, die in 2.3.2.x hinzugefügt wurde und es Ihnen nicht erlaubt, viele Befehle auszuführen, bis Sie sie deaktivieren. Weitere Informationen zum vorübergehenden Deaktivieren der eingeschränkten Shell finden Sie in diesem Dokument.

Generieren der RCA-Datei in einem Single-Node-Cluster

Schritt 1: Melden Sie sich bei der Cisco DNA Center-CLI an Port 2222 an. Verwenden Sie `maglev` als Benutzername, es sei denn, der Benutzername wurde zum Zeitpunkt der Ersteinrichtung geändert. Führen Sie dann die `rca` aus.

<#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':




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




/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 den neueren Cisco DNA Center-Versionen (2.3.4.x und höher) können Sie Folgendes ausführen: $ 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
```

Hinweis: Die RCA-Datei wird generiert und gespeichert in /data/rca. Die Erstellung der Datei dauert in der Regel etwa 20 Minuten. Der Dateiname muss das folgende Format haben: maglev-

-rca

.tar.gz

.

Generieren der RCA-Datei in einem N-Node-Cluster

Tipp: Wenn Sie einen funktionierenden n-Knoten-Cluster haben, werden die Services verteilt. Wenn die Dienste verteilt werden, enthält die RCA eines einzelnen Knotens keine Protokolle von Diensten, die auf anderen Knoten ausgeführt werden. Wenn Sie z. B. den Dienst A auf Knoten-1 ausführen und die RCA von Knoten-2 erhalten, sind die Protokolle von Dienst A nicht enthalten. Es wird daher empfohlen, die RCA-Datei aller Knoten im Cluster zu erfassen und einzubeziehen, wenn das TAC eine RCA Datei.

Wenn Sie einen Cluster mit drei Knoten haben und das rca auf einem beliebigen Gerät fordert Sie das Cisco DNA Center zur Eingabe einer Cluster-IP-Adresse auf. Geben Sie an der Eingabeaufforderung die clusterübergreifende IP-Adresse des Knotens ein, von dem Sie die RCA abrufen möchten.

In diesem Beispiel befinden sich die IP-Adressen zwischen Clustern im Bereich 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
================================================================
Done

================================================================
Verifying administration access
================================================================
```

Cluster: 10.1.1.3

```
[administration] username for 'https://10.1.1.3:443': admin
[administration] password for 'admin':




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
```

Nachdem Sie die rca Befehl, werden die von Ihnen angegebenen IP-Adressen zwischen Clustern zwischengespeichert in /home/maglev/.maglevconf. Wenn Sie das nächste Mal die rca verwendet Cisco DNA Center denselben Knoten, um die RCA-Informationen abzurufen.

<#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/
â€¦ rca continuedâ€¦
```

Wenn Sie die rca auf einem anderen Knoten, müssen Sie den im Cisco DNA Center konfigurierten Kontext löschen. Anschließend werden Sie aufgefordert, eine neue IP-Adresse zwischen den Clustern auszuwählen, und Sie können die IP-Adresse des anderen Knotens definieren.

<#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': <
```

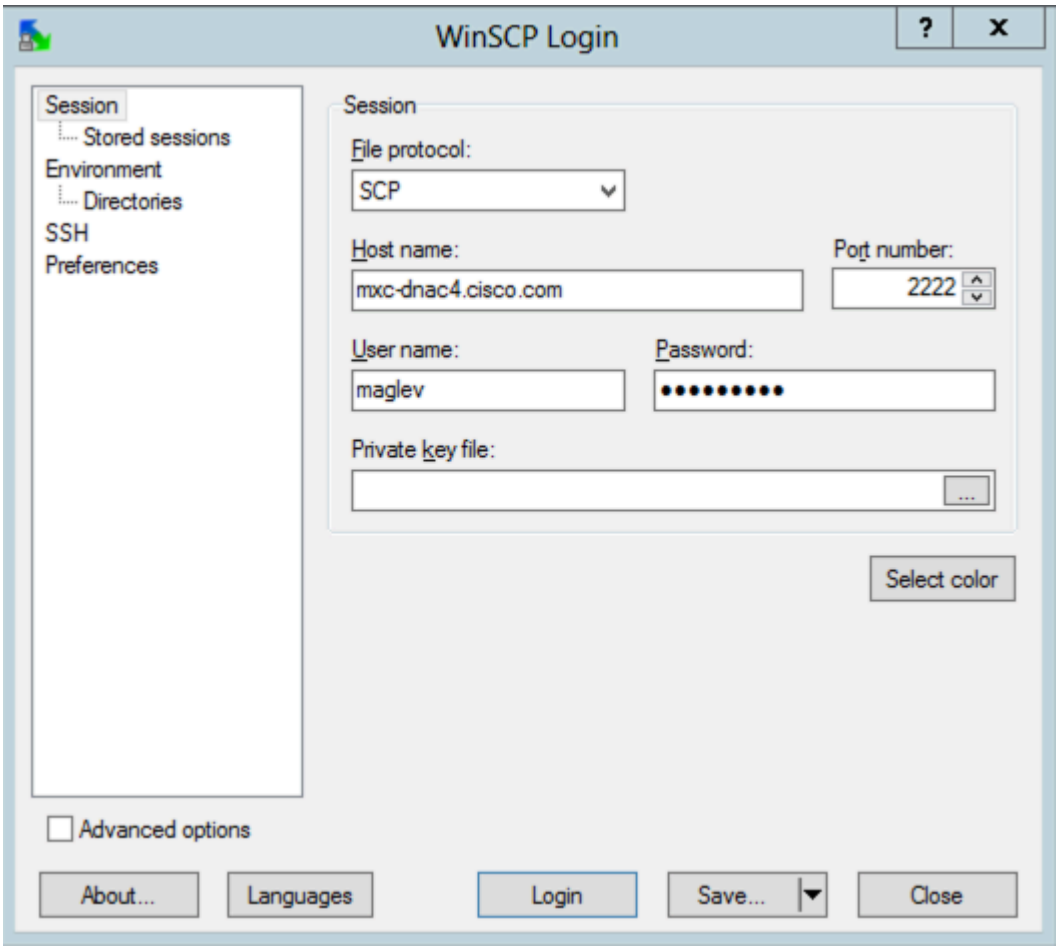
type your admin password

```
>
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
```

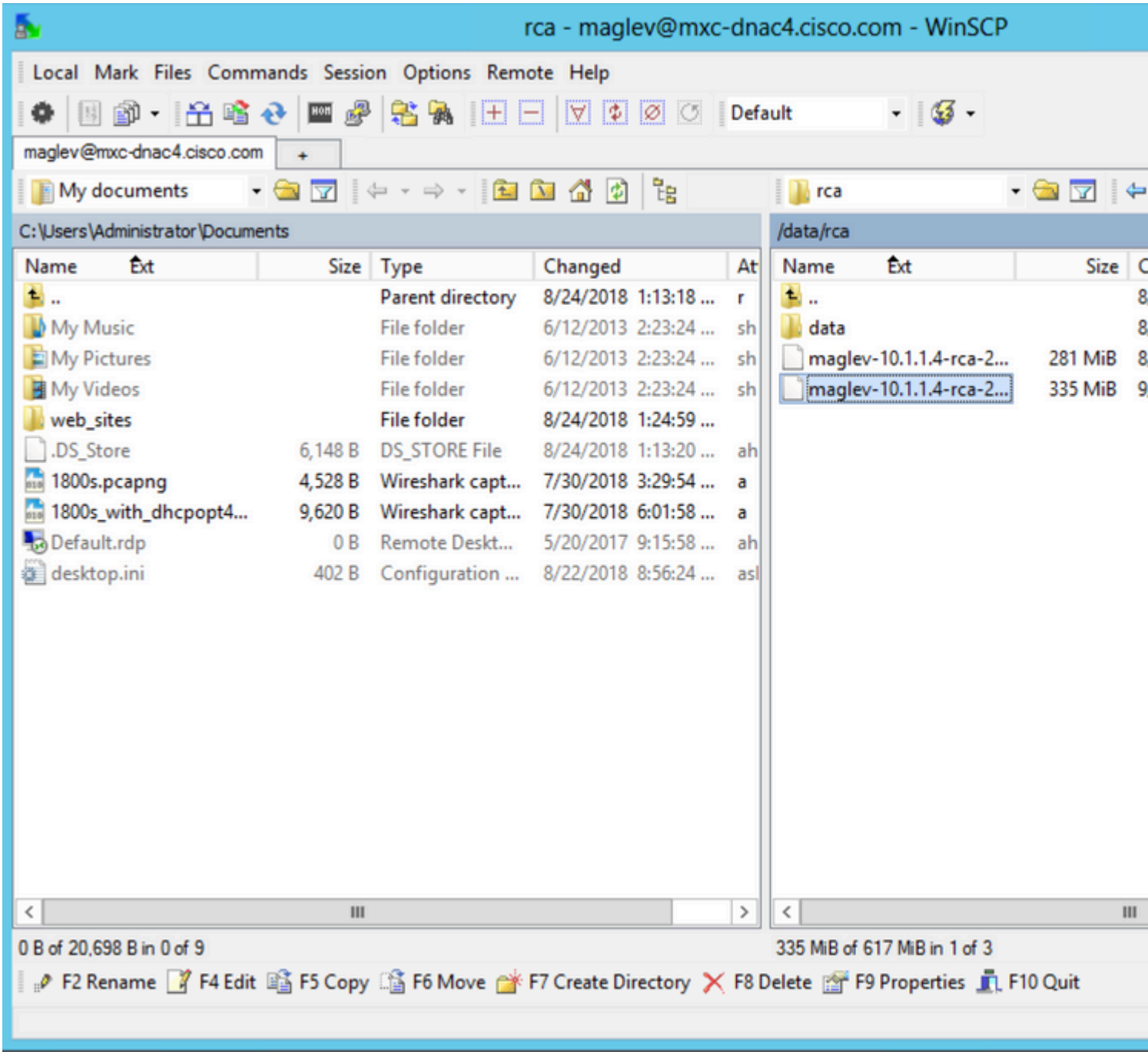
Extrahieren der RCA-Datei auf einem Windows-Computer

Schritt 1: Laden Sie WinSCP oder Ihren bevorzugten SCP-Client herunter.

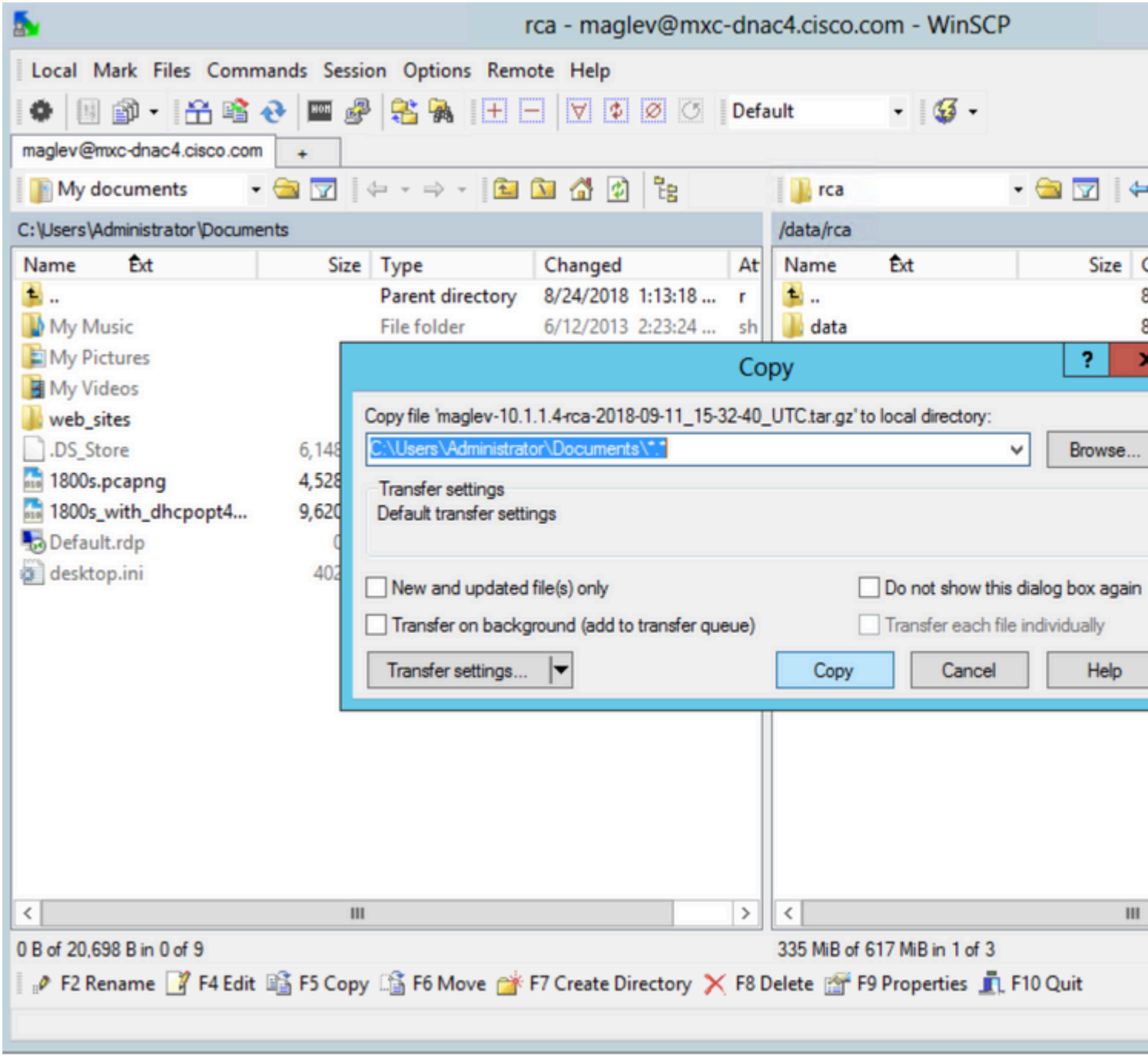
Schritt 2: Melden Sie sich mit Ihren CLI-Anmeldeinformationen beim Cisco DNA Center an, und wählen Sie SCP als Dateiprotokoll, und wählen Sie die Portnummer 2222 aus.



Schritt 3: Navigieren Sie zum /data/rca Ordner.



Schritt 4: Kopieren Sie die RCA-Datei auf Ihren lokalen Computer.



Extrahieren der RCA-Datei auf einem Mac- oder Linux-Computer

> **Hinweis**: In diesem Beispiel wird die Cisco DNA Center IP-Adresse wie folgt aufgelöst: mxc-dnac4.cisco.com. Ersetzen Sie diesen Hostnamen durch den FQDN (Fully Qualified Domain Name) oder die IP-Adresse Ihrer Cisco DNA Center-Appliance.

Schritt 1: Öffnen Sie eine Terminalsitzung, und kopieren Sie dann die RCA-Datei mit dem Namen maglev-10.1.1.4-rca-2018-09-11_15-32-40_UTC.tar.gz auf der Cisco DNA Center-Appliance im /data/rca in das aktuelle Arbeitsverzeichnis auf Ihrem 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 der RCA-Datei auf einen Mac- oder Linux-Computer

Verwenden Sie in der CLI der Cisco DNA Center-Appliance folgende Syntax:

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

Nachfolgend finden Sie ein Beispiel für den in der Übung verwendeten Befehl:

<#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:u660kUomvMParNkcPIm7oXrDp84rilP5CM9wCWCFOAE.
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:
```

```
maglev-10.1.1.4-rca-2018-09-11_15-32-40_UTC.tar.gz
```

RCA-Datei in TAC-SR hochladen

Sie können das Uploader für Ticket-Dateien verwenden, um die RCA-Datei über einen Browser in einen TAC Service Request (SR) hochzuladen, der auf Ihrem Computer vorhanden ist. Geben Sie bei Bedarf die Vorgangsnummer an.

RCA-Datei auf TAC-SR übertragen

Es gibt zwei Optionen, um eine Datei (z. B. die RCA) direkt von einer Cisco DNA Center-Appliance auf einen TAC SR hochzuladen. In beiden Optionen ist der Benutzername die SR-Nummer, und das Kennwort

ist ein Token, der für jeden SR eindeutig ist. Der Benutzername/das Passwort ist immer in einer Notiz am Anfang Ihres SR vorhanden und kann auch aus SCM abgerufen werden. Weitere Informationen zum Token finden Sie unter Uploads von Kundendateien an das Cisco Technical Assistance Center.

Beispielausgabe von einem 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: Datei über HTTPS hochladen (Schnellste Option und nutzt Port 443)

Schritt 1: Testen Sie, ob eine Verbindung von Ihrer Cisco DNA Center-Appliance zu cxd.cisco.com über Port 443. So führen Sie den Test durch:

<#root>

```
$
```

nc -zv cxd.cisco.com 443

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

Hinweis: Wenn der Test fehlschlug, können Sie Ihre Datei nicht mit dieser Methode hochladen.

Schritt 2: Wenn der Test erfolgreich war, laden Sie die Datei mithilfe des folgenden Befehls über HTTPS hoch:

<#root>

```
$ curl â€“T â€œ
```

```
â€¢ -u
```

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

(Wenn Sie eine detailliertere Ansicht des Uploads anzeigen möchten, fügen Sie -v Option. Beispiel: 'curl -vT â€¦'.)

Beispiele:

```
<#root>

$

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


Enter host password for user '688046089':









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

Option 2: Laden Sie die Datei über SCP hoch (nutzt Port 22)

Schritt 1: Testen Sie, ob eine Verbindung von Ihrer Cisco DNA Center-Appliance zu cxd.cisco.com über Port 22. So führen Sie den Test durch:

```
<#root>

$

nc -zv cxd.cisco.com 22


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

Hinweis: Wenn der Test fehlschlug, können Sie Ihre Datei nicht mit dieser Methode hochladen.

Schritt 2: Wenn der Test erfolgreich war, laden Sie die Datei mithilfe des folgenden Befehls über SCP hoch:

```
<#root>

$ scp
```

```
@cxd.cisco.com:
```

Beispiele:

<#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 SHA256:3c8Vi3Ms2AITZlNzkBccR1pvE5ie9oMs64Uh0uhRado.
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:
```

```
test.txt

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.