

Cisco DNA CenterからのRCAファイルの生成と抽出

内容

[はじめに](#)

[背景説明](#)

[単一ノードクラスタでのRCAファイルの生成](#)

[NノードクラスタでのRCAファイルの生成](#)

[WindowsコンピュータでのRCAファイルの抽出](#)

[MacまたはLinuxコンピュータでのRCAファイルの抽出](#)

[RCAファイルをMacまたはLinuxコンピュータにプッシュする](#)

[RCAファイルのTAC SRへのアップロード](#)

[RCAファイルをTAC SRにプッシュする](#)

[オプション 1HTTPS経由でファイルをアップロードする（最速のオプションでポート443を使用）](#)

[制限付きシェル](#)

[オプション 2SCP経由でのファイルのアップロード（ポート22を使用）](#)

はじめに

このドキュメントでは、Cisco Digital Network Architecture(DNA)Centerから根本原因分析(RCA)ファイルを作成して抽出する方法について説明します。

背景説明

Cisco DNA CenterへのCLIアクセスが必要です。CLIを使用してCisco DNA Centerにログインするには、Secure Socket Shell(SSH)を介して、Cisco DNA Centerの管理IPアドレスに接続し、ポートのユーザ名としてmaglevを使用する必要があります。

2.3.2.xで追加された制限付きシェル機能には注意してください。この機能を無効にするまで、多くのコマンドを実行できません。

2.3.2.xまたは2.3.3.xで制限付きシェルを一時的に無効にするには、[このドキュメント](#)を参照してください。2.3.4.0以降では、制限付きシェルを無効にすることはできません。

単一ノードクラスタでのRCAファイルの生成

ステップ 1：ポート2222でCisco DNA Center CLIにログインします。初期セットアップ時にユーザ名が変更されていない限りmaglev、をユーザ名として使用します。次に、rcaコマンドを実行します。

```
<#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) ~
```

新しいCisco DNA Centerリリース (2.3.4.x以降) では、次の機能を実行でき\$ rca copyます。


```
$ 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
```

 注:RCAファイルが生成され、に保存され/data/rcaます。通常、ファイルの作成には約20分かかります。ファイル名は次の形式にする必要がありmaglev-<inter-cluster link IP address>-rca<date and time>.tar.gzます。

NノードクラスタでのRCAファイルの生成

 ヒント : 機能しているnノードクラスタがある場合、サービスは分散されます。サービスが分散されると、個々のノードのRCAには、他のノードで実行されるサービスのログは含まれません。たとえば、node-1でサービスAを実行していて、node-2からRCAを取得する場合、サービスAからのログは含まれません。そのため、TACがファイルを要求する際には、クラスタ内のすべてのノードのRCAファイルをキャプチャして含めることを推奨RCAします。

3ノードクラスタがあり、任意のデバイスでコマンドを実行するとrca、Cisco DNA CenterはクラスタIPアドレスの入力を求めるプロンプトを表示します。プロンプトで、RCAを取得するノードのクラスタ間IPアドレスを入力します。

この例では、クラスタ間IPアドレスは10.1.1.0/29の範囲にあります。

```
<#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 =====

コマンドを実行すると、指定したクラスタ間IPアドレスがキャッシュされ/home/maglev/.maglevconfに保存されます。次にこのコマンドを実行するとrca、Cisco DNA Centerは同じノードを使用してRCA情報を取得します。

<#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

別のノードでコマンドを実行する必要がある場合rca、Cisco DNA Centerで設定されているコンテキストを削除する必要があります。その後、新しいクラスタ間IPアドレスを選択するように求められ、他のノードのIPアドレスを定義できます。

<#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': <

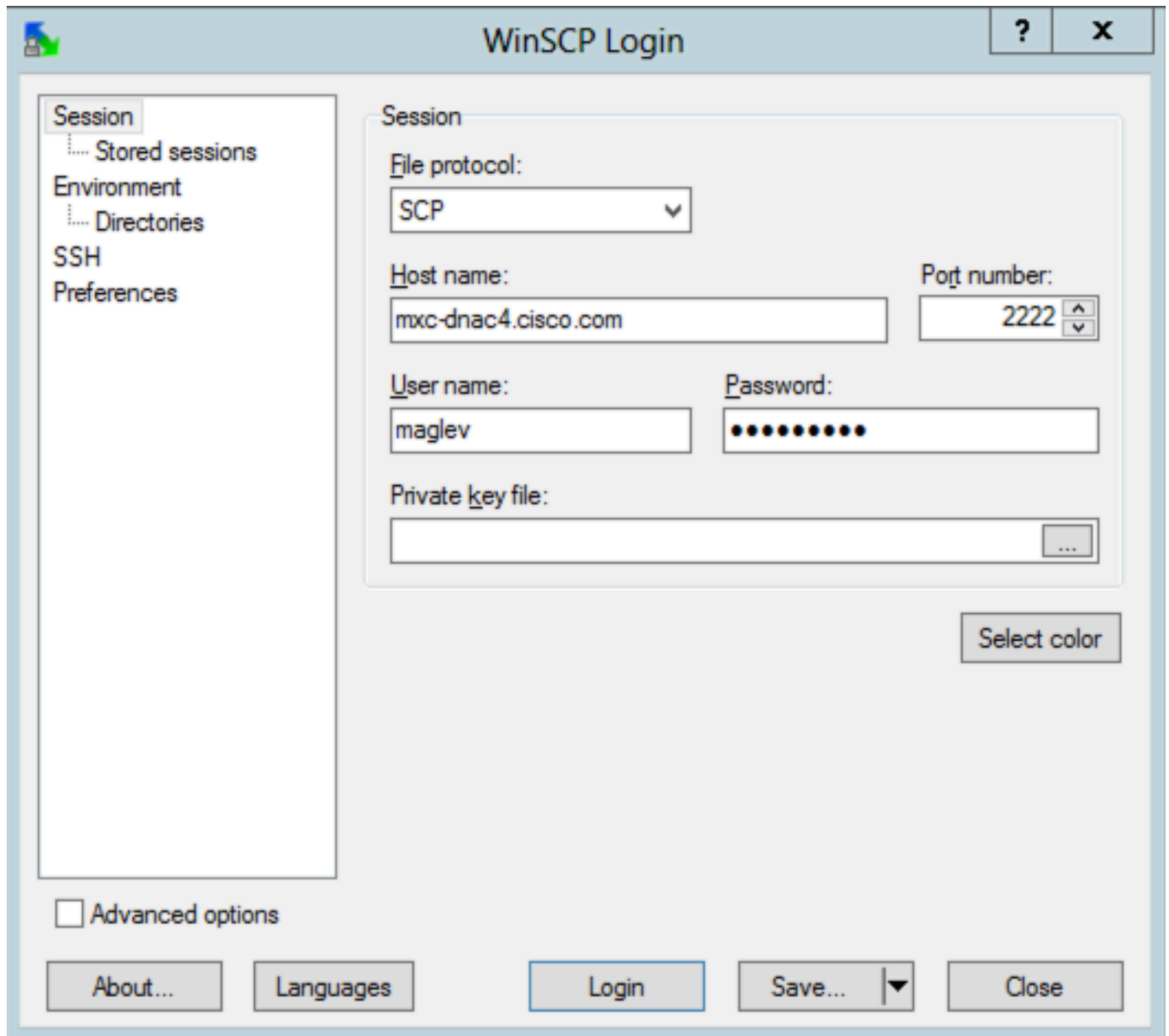
type your admin password

> User 'admin' logged into '10.1.1.2' successfully =====

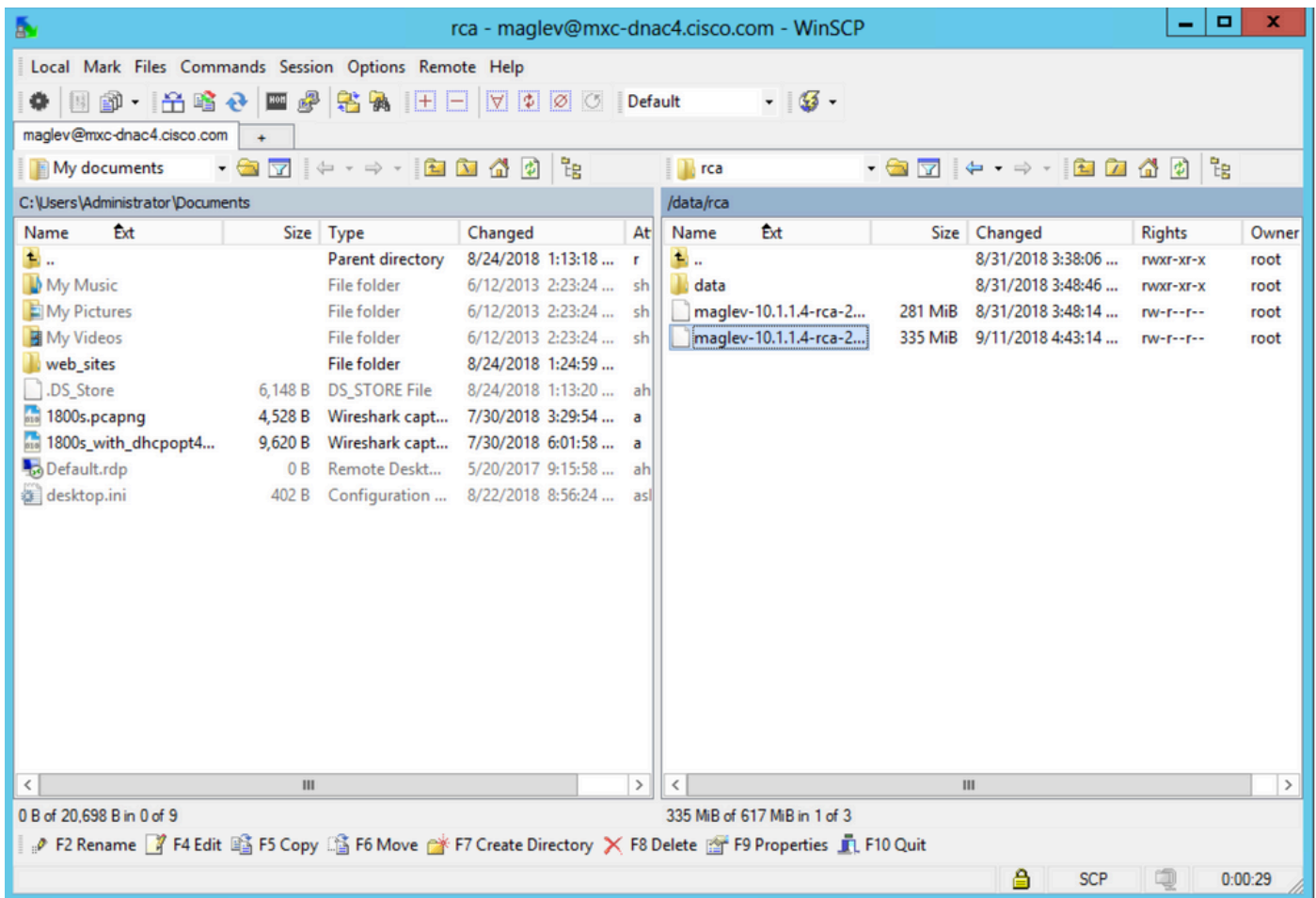
WindowsコンピュータでのRCAファイルの抽出

ステップ 1 : [WinSCP](#)または任意のSCPクライアントをダウンロードします。

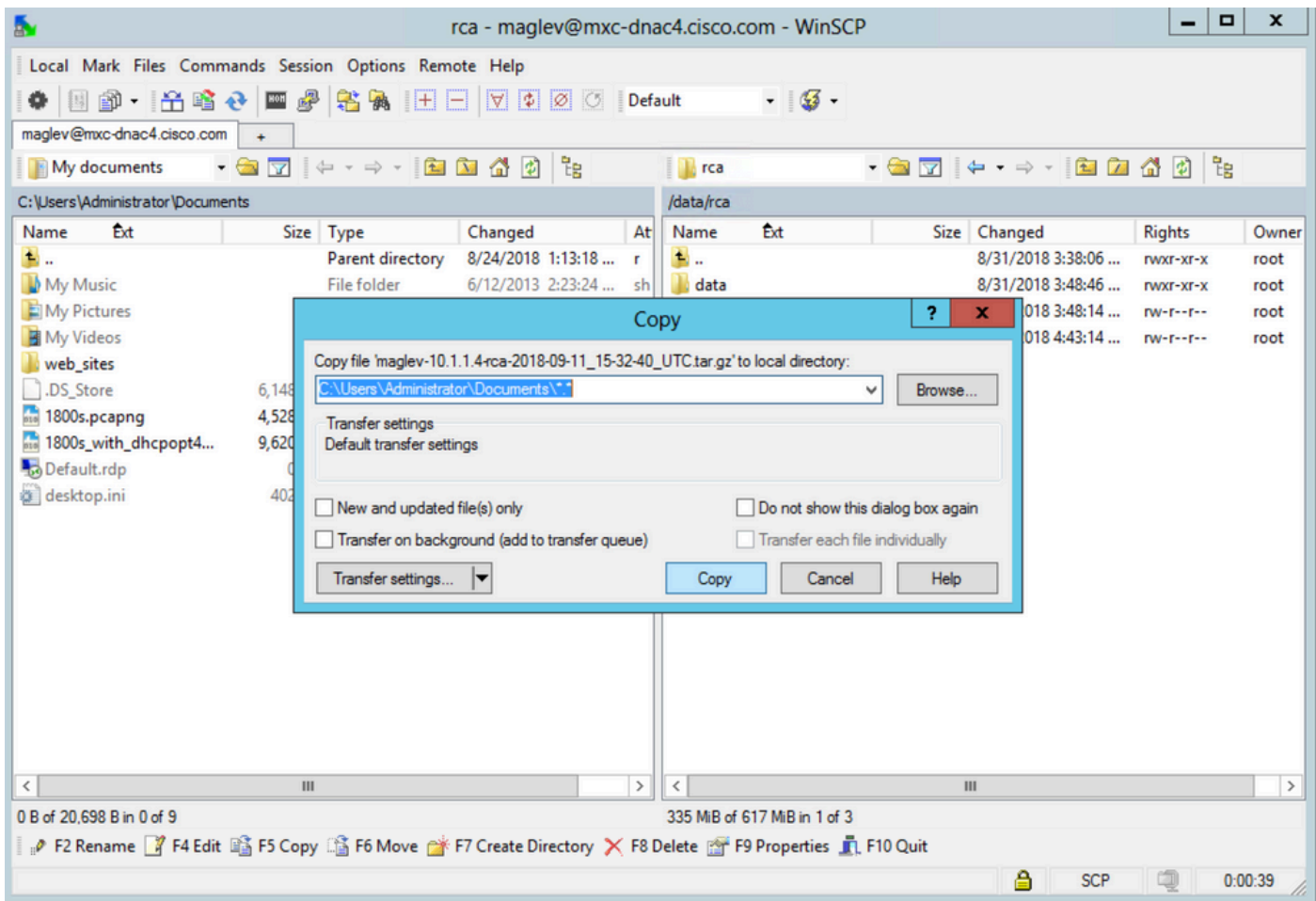
ステップ 2 : CLIクレデンシャルを使用してCisco DNA Centerにログインし、ファイルプロトコルとしてSCPを選択し、ポート番号2222を選択します。




ステップ 3 : フォルダに移動/data/rcaします。



ステップ 4 : RCAファイルをローカルコンピュータにコピーします。



MacまたはLinuxコンピュータでのRCAファイルの抽出

 注：この例では、Cisco DNA CenterのIPアドレスはに解決されmx-c-dnac4.cisco.comます。このホスト名を、使用しているCisco DNA Centerアプライアンスの完全修飾ドメイン名(FQDN)またはIPアドレスに置き換えます。

ステップ 1：ターミナルセッションを開き、次の手順を実行して、Cisco DNA Centerアプライアンスに保存されているmaglev-10.1.1.4-rca-2018-09-11_15-32-40.UTC.tar.gzという名前のRCAファイルを/data/rca、コンピュータの現在の作業ディレクトリにコピーします。

<#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$
```

RCAファイルをMacまたはLinuxコンピュータにプッシュする

Cisco DNA CenterアプライアンスのCLIから、次の構文を使用します。

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

ラボで使用するコマンドの例を次に示します。

```
<#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
```

RCAファイルのTAC SRへのアップロード

[Case File Uploaderツール](#)を使用して、RCAファイルをブラウザ経由でお客様のコンピュータに存在するTACサービスリクエスト (SR)にアップロードできます。必要に応じてケース番号を指定します。

RCAファイルをTAC SRにプッシュする

ファイル (RCAなど) をCisco DNA CenterアプライアンスからTAC SRに直接アップロードするには、2つのオプションがあります。どちらのオプションでも、ユーザ名はSR番号で、パスワードは各SRに固有のトークンです。ユーザ名/パスワードは、SRの開始時に常にメモに含まれ、SCMから取得することもできます。トークンの詳細については、「[Cisco Technical Assistance Centerへの顧客ファイルのアップロード](#)」を参照してください。

SRからの出力例：

```
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
```

オプション 1HTTPS経由でファイルをアップロードする (最速のオプションでポート443を使用)

ステップ 1 : Cisco DNA Center アプライアンスからポート443経由で接続できるかどうかをテスト cxd.cisco.com します。テストを実行する方法の1つを次に示します。

```
<#root>
```

```
$
```

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

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

```
$
```



注 : テストが失敗した場合、この方法を使用してファイルをアップロードすることはできません。

ステップ 2 : テストが成功したら、次のコマンドを使用してHTTPS経由でファイルをアップロードします。

```
<#root>
```

```
$ curl -T "
```

```
<filename with path>
```

```
" -u
```

```
<SR number>
```

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

(アップロードの詳細ビューを表示する場合は、-v オプションを追加します。たとえば、「curl -vT ...」と入力します)。

例 :

```
<#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) ~
```

```
$
```

制限付きシェア

制限付きシェルはCURLの使用を妨げるため、scpを利用するrca copyを採用して、cxd.cisco.comへの安全なファイル転送を可能にしています。

```
$ rca copy --files maglev-10.1.1.233-rca-2024-03-06_14-07-36.UTC.tar.gz 6969XXXXXX@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 hosts.
6969XXXXXX6@cxd.cisco.com's password:
maglev-10.1.1.233-rca-2024-03-06_14-07-36.UTC.tar.gz
```

オプション 2SCP経由でのファイルのアップロード (ポート22を使用)

ステップ 1 : Cisco DNA Centerアプライアンスからポート22経由でへの接続が確立されているかどうかをテストcxd.cisco.comします。テストを実行する方法の1つを次に示します。

```
<#root>
```

```
$
```

```
nc -zv cxd.cisco.com 22
```

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

```
$
```



注 : テストが失敗した場合、この方法を使用してファイルをアップロードすることはできません。

ステップ 2 : テストが成功したら、次のコマンドを使用してSCP経由でファイルをアップロードします。

```
<#root>
```

```
$ scp
```

```
<local filename with path>
```

```
<SR number>
```

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

例 :

```
<#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:

<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) ~
\$

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。