Cisco Nexus Dashboard のトラブルシューティング、リリース 3.1.x

目次

便利なコマンド

システムデータへのアクセスが制限されている場合、rescue-user として任意のクラスタノードにログインできます。次のコマンドを使用して、Cisco Nexus Dashboardでさまざまな操作を実行できます。

クラスタのトラブルシューティング:

- acs health：クラスタの正常性情報と既存の問題を表示します。
- acs cluster config：クラスタの構成を表示します。
- acs show nodes：クラスタ内のすべてのノードに関する情報を表示します。
- acs show masters ：クラスタ内のプライマリ ノードに関する情報を表示します。
- acs show workers ：クラスタ内のワーカー ノードに関する情報を表示します。
- acs show standbys：クラスタ内の standby ノードに関する情報を表示します。
- acs ntp show：NTP 情報を表示します。
- acs techsupport collect -s system：インフラストラクチャのテクニカル サポート情報を収集します。
- acs techsupport collect -s cisco-mso – cNexus Dashboard Orchestrator サービスのテクニカル サポート情報を収集します。
- acs techsupport collect -s cisco-nir：Nexus Dashboard Insights サービスのテクニカル サポート情報を収集します。
- acs techsupport collect -s cisco-appcenter：App Store のテクニカル サポート情報を収集します。
- acs version：Nexus Dashboard のバージョンを返します。

デバイスのリセット:

- acs reboot：すべてのサービスと構成をそのまま使用してノードをリブートします。
- acs reboot clean： Nexus Dashboard とアプリケーションの全データを削除しますが、Nexus Dashboard のブートストラップ構成とポッド イメージは保持します。

  クリーンリブートは、すべてのノートで同時に実行する必要があります。他の 2 つの プライマリ ノードが残っている間に 1 つのノードをクリーンリブートすると、リブートされたノードが起動し、既存のクラスタから回復します。

  Nexus Dashboardクラスタを初めて起動すると、初期展開プロセスで必要なすべてのポッドイメージがインストールされます。ポッドイメージを保持すると、リブート後のクラスタの起動が高速化されます。

  クラスタ内のすべてのノードを再インストールする場合は、最初にサイトおよびアプリケーション情報をクリーンアップする必要があります。この場合、サイトがすべてのアプリケーションで無効になっており、NDクラスタから削除されていることを確認してください。

- acs reboot clean-wipe ：Nexus Dashboard およびアプリケーション イメージを含むアプリケーションの全データを削除しますが、Nexus Dashboard のブートストラップ構成は保持します。

  クラスタが再起動すると、ポッドイメージが再インストールされます。

  クラスタ内のすべてのノードを再インストールする場合は、

最初にサイトおよびアプリ情報をクリーンアップする必要があります。この場合、サイトがすべてのアプリケーションで無効になっており、NDクラスタから削除されていることを確認してください。

- acs reboot factory-reset：クラスタ ブートストラップ構成を含む Nexus Dashboard とアプリケーションの全データを削除しますが、アプリケーション イメージは保持します。

  Nexus Dashboardクラスタを初めて起動すると、初期展開プロセスで必要なすべてのポッドイメージがインストールされます。ポッドイメージを保持すると、クラスタの起動が高速化されます。

  クラスタ内のすべてのノードを再インストールする場合は、最初にサイトおよびアプリケーション情報をクリーンアップする必要があります。この場合、サイトがすべてのアプリケーションで無効になっており、NDクラスタから削除されていることを確認してください。

- acs reboot factory-wipe：アプリケーション イメージとクラスタ ブートストラップ設定を含む、Nexus Dashboard とアプリケーションの全データを削除します。

  クラスタが再起動すると、ポッドイメージが再インストールされます。

  クラスタ内のすべてのノードを再インストールする場合は、最初にサイトおよびアプリケーション情報をクリーンアップする必要があります。この場合、サイトがすべてのアプリケーションで無効になっており、NDクラスタから削除されていることを確認してください。

システムと接続に関するトラブルシューティング:

- /logs ディレクトリは rescue-user コンテナにマウントされ、標準ツールで検査できます。
- ping コマンドは、ほとんどのオプションでサポートされています。
- ip コマンドは、 ip addr show および ip route show を含む、コマンドの読み取り専用サブセットをサポートします。
- kubectl コマンドは、読み取り専用 Kubernetes コマンドをサポートします。

  たとえば、これを使用して、システムで実行されているすべてのポッドのリストを取得できます：

```
$ kubectl get pods -A
NAMESPACE        NAME                          READY STATUS RESTARTS          AGE
aaamgr           aaamgr-54494fdbc8-q8rc4       2/2   Running 0                3d3h
authy-oidc       authy-oidc-75fdf44b57-x48xr   1/1   Running 3 (3d3h ago) 3d4h
authy            authy-857fbb7fdc-7cwgg        3/3   Running 0                3d4h
cisco-appcenter apiserver-686655896d-kmqhq     1/1   Running 0                3d3h
[...]
```

- acs elasticsearch コマンドは、サービスに関するデバッグ情報を取得できるカスタム ユーティリティを呼び出します。

```
$ acs elasticsearch --name cisco-ndfc-controller-elasticsearch health
{
  "cluster_name" : "cisco-ndfc-controller-elasticsearch",
  "status" : "green",
「timed_out」 : false、
```

```
  "number_of_nodes" : 3,
  "number_of_data_nodes" : 3,
  "discovered_master" : true,
  "active_primary_shards" : 10,
  "active_shards" : 21,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0,
  "task_max_waiting_in_queue_millis" : 0,
  "active_shards_percent_as_number" : 100.0
}
```

次の例のように、kubectl コマンドを使用して、サービス固有のポッド名のリストを取得できます：

```
$ kubectl get pods -A | grep elasticsearch
cisco-ndfc-controller-elasticsearch   es-data-0   2/2   Running   0   109m
cisco-ndfc-controller-elasticsearch   es-data-1   2/2   Running   0   163m
cisco-ndfc-controller-elasticsearch   es-data-2   2/2   Running   0   104m
```

アプリケーション情報：

- acs apps instances コマンドは、クラスタで実行されているすべてのアプリケーションを表示します。
- acs apps actions コマンドは、インストール、アップグレード、削除など、アプリケーションで実行された操作履歴を表示します。

CIMCのアップグレード

Nexus Dashboardソフトウェアをアップグレードする場合は、Nexus Dashboardノードで実行されているCisco Integrated Management Controller (CIMC)のバージョンのアップグレードも必要になることがあります。

Nexus Dashboard の各リリースでサポートされている CIMC バージョンは、そのリリース固有の リリースノート に記載されています。

次の手順では、Cisco Host Upgrade Utility (HUU)を使用してNexus Dashboard CIMCをアップグレードする方法について説明します。Host Upgrade Utility の詳細については、「Upgrading the Firmware on a Cisco UCS C-Series Server Using the HUU」を参照してください。

はじめる前に

- お使いの Nexus Dashboard リリースの リリースノート で、そのリリースでサポートされている CIMC バージョンを確認してください。
- アップグレードには十分な時間を確保してください。

  アップグレードプロセスに必要な時間は、ローカルマシンとUCS-Cシャーシ間のリンクの速度、ソースおよびターゲット ソフトウェア イメージ、その他の内部コンポーネントのバージョンなど、さまざまな要因によって異なります。

- 古いファームウェアを実行している1つのノードをアップグレードして既存のクラスタに追加する場合は、クラスタのすべてのノードではなく、そのノードでのみ次の手順を実行します。
- CIMCを更新するには、CIMCのアップグレードに使用するvKVMを実行するために、ブラウザやJavaソフトウェアのバージョンの更新も必要になることがあります。

ヒ Nexus Dashboardノードはトラフィックのデータパスにないため、CIMCバージョンをアップグレードしても実稼働ネットワークには影響しません。

Nexus Dashboard CIMCソフトウェアをアップグレードするには、次の手順を実行します。

1. ブラウザを開き、CIMCのIPアドレスに移動し、CIMCのログイン情報を使用してログインします。

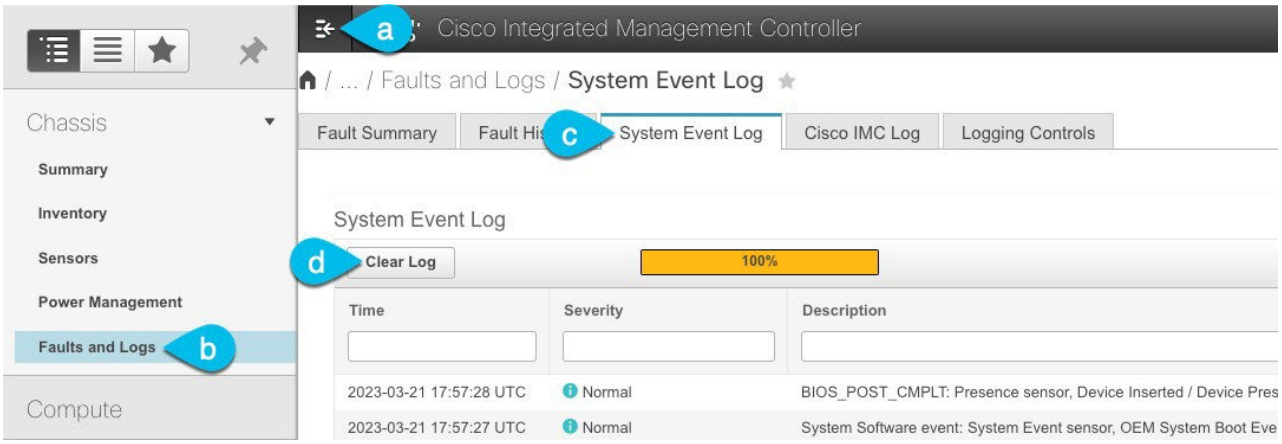
   CIMCのクレデンシャルは、Nexus Dashboard GUIのクレデンシャルとは異なる場合があること

   に注意してください。

2. **[サーバー] > [概要（Summary）]**でBIOSバージョンの最初の部分を確認し、Nexus Dashboard の UCS プラットフォームのモデルを特定します。

   Nexus Dashboardは、UCS-C220-M5およびUCS-C225-M6サーバーをサポートします。

3. 必要に応じて、既存のログをクリアします。



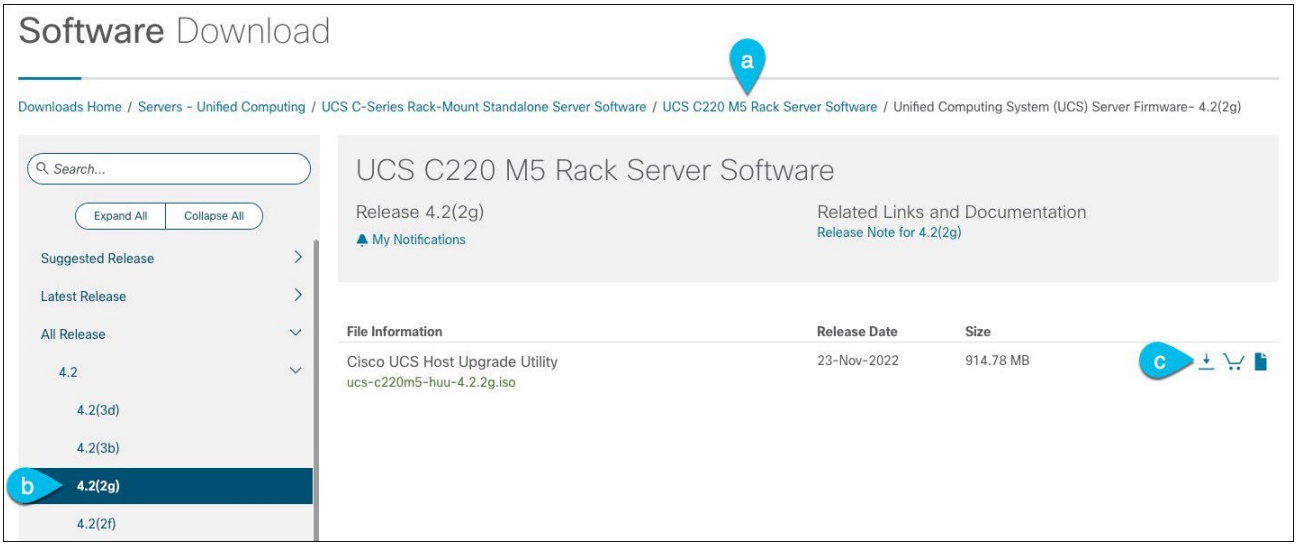
a. ハンバーガーメニューをクリックして、使用可能なオプションを表示します。

b. **[障害およびログ（Faults and Logs）]** を選択します。

c. メインペインで、**[システム イベント ログ（System Event Log）]** タブを選択し、ログが読み込まれるのを待ちます。

d. ログがいっぱいになっている場合は、**[ログのクリア（Clear Log）]** をクリックします。

4. 適切なHUU ISOイメージをダウンロードします。



a. サーバーモデルのソフトウェア ダウンロード ページに移動します。

UCS-C220-M5 の場合は、 https://software.cisco.com/download/home/286318809/type/283850974 にアクセスします。

UCS-C225-M6 の場合は、 https://software.cisco.com/download/home/286329390/type/283850974にアクセスします。

b. 左側のサイドバーで、Nexus Dashboard のターゲットリリースでサポートされているバージョンを選択します。サポートされているリリースのリストは、リリースノートに記載されています。

c. メイン ペインで、ダウンロード アイコンをクリックします。

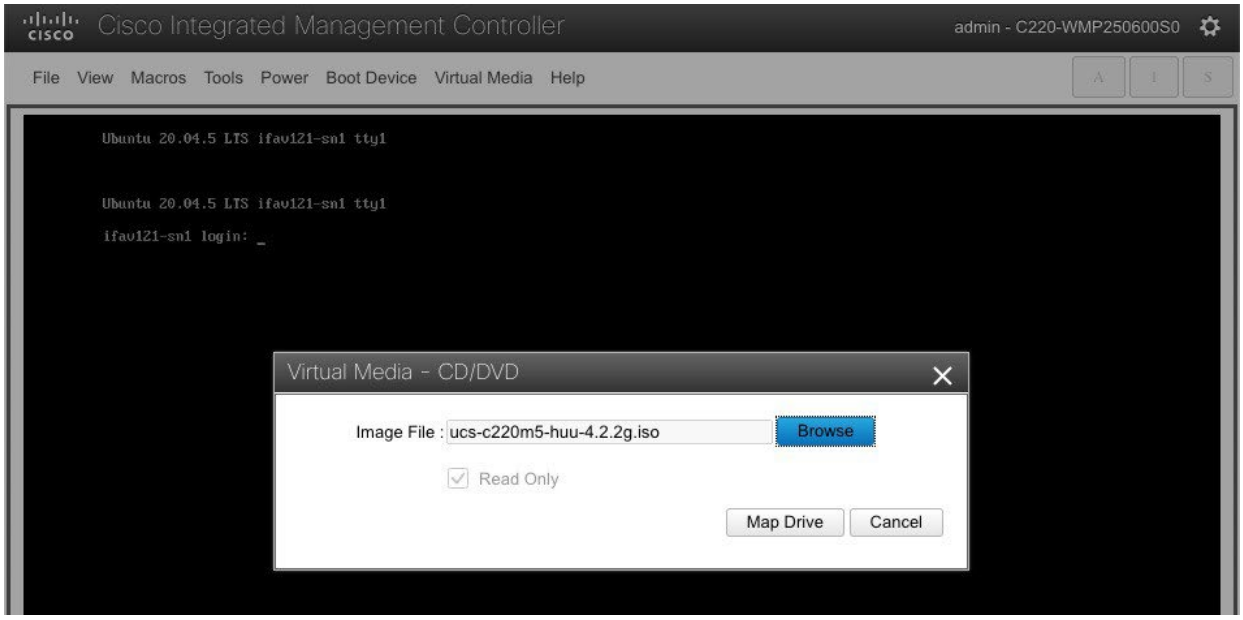
d. **[ライセンス契約を承認（Accept License Agreement）]** をクリックします。

5. CIMC GUIからKVMコンソールを起動します。

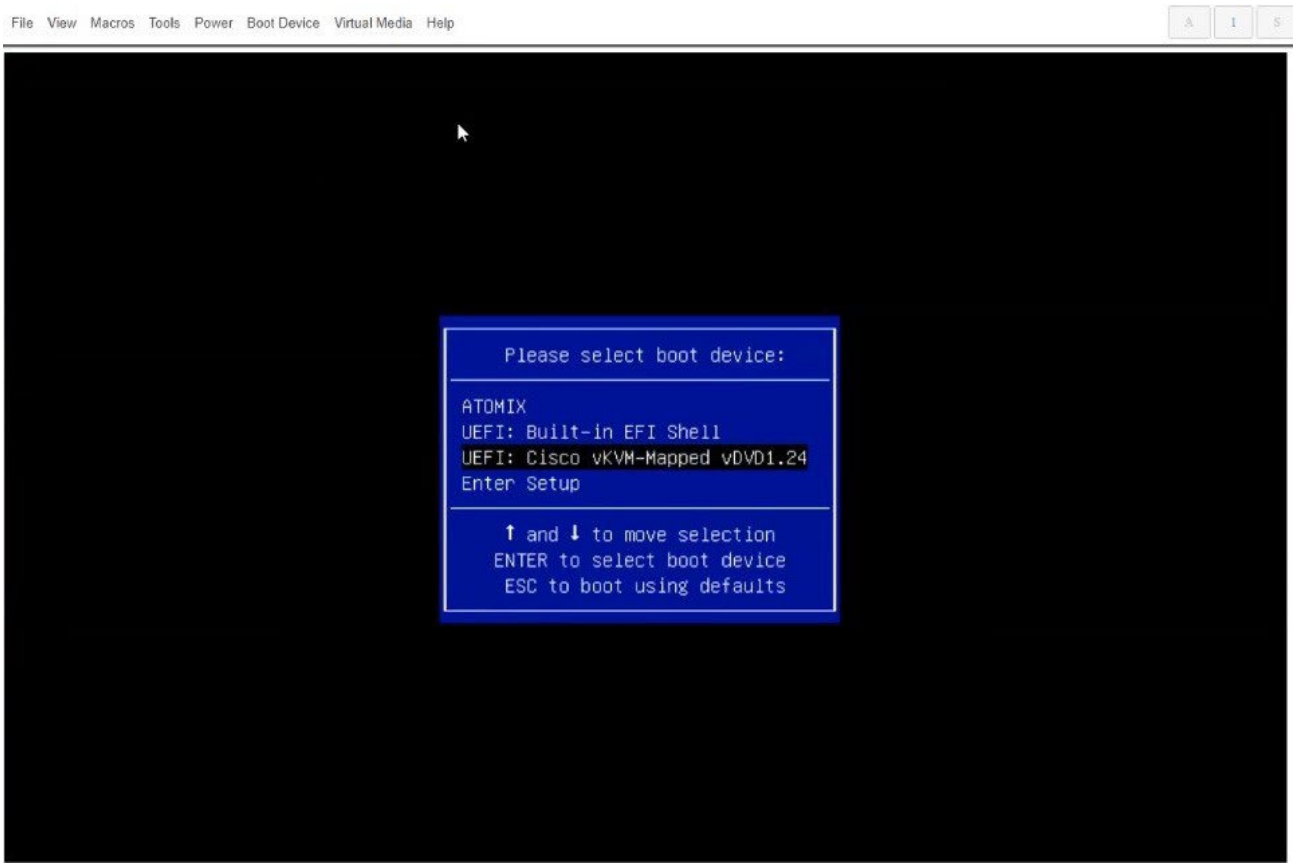
KVM コンソールを開くことができない場合は、Java

バージョンを更新する必要がある可能性があります。

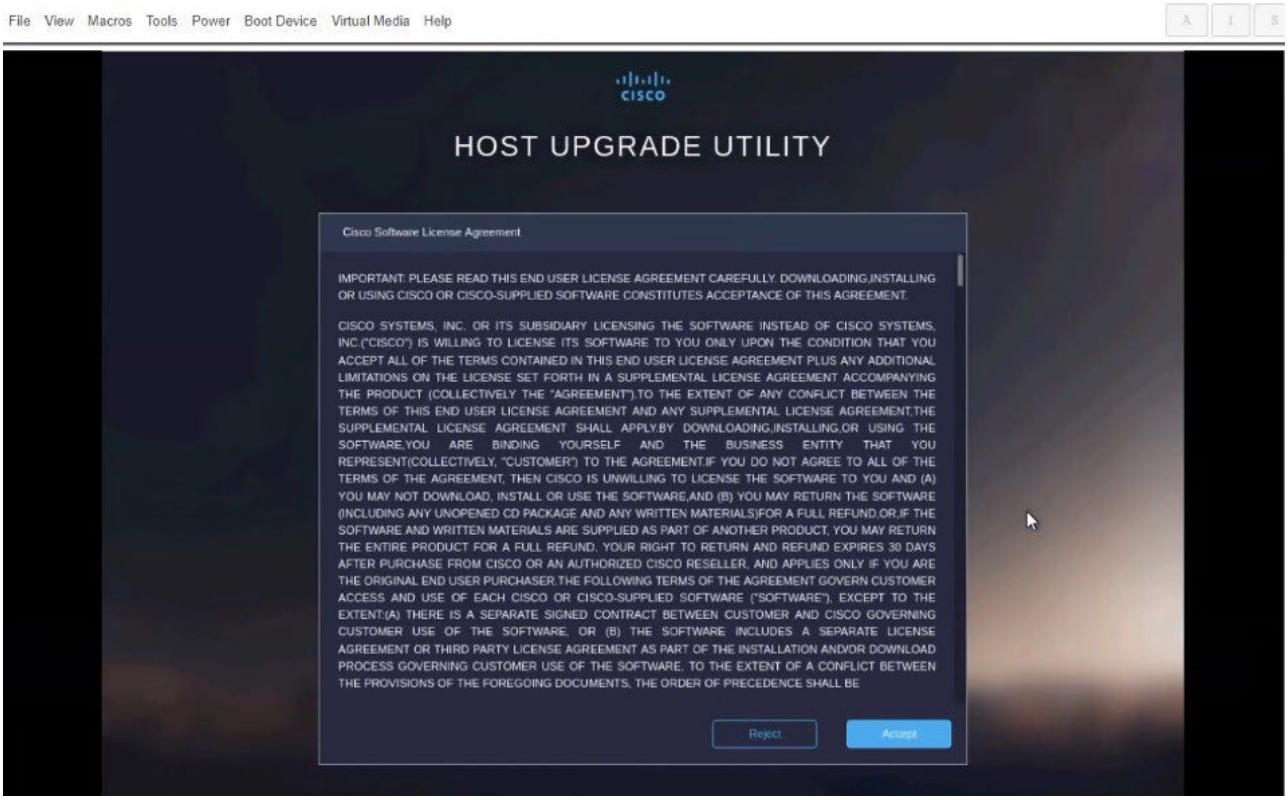
6. ステップ3でダウンロードしたHUU ISOイメージをマウントします。
   a. KVMコンソールの **[仮想メディア（Virtual Media）]** メニューから、**[仮想デバイスのアクティブ化（Activate Virtual Devices）]**を選択します。これにより、**[仮想メディア]** メニューに 仮想メディア のオプションが追加されます。
   b. KVM コンソールの **[仮想メディア]** メニューから、**CD/DVD**のマッピング を選択します。
   c. 表示された **[仮想メディア - CD/DVD]** ダイアログで、**[参照（Browse）]** をクリックし、HUUイメージを選択します。



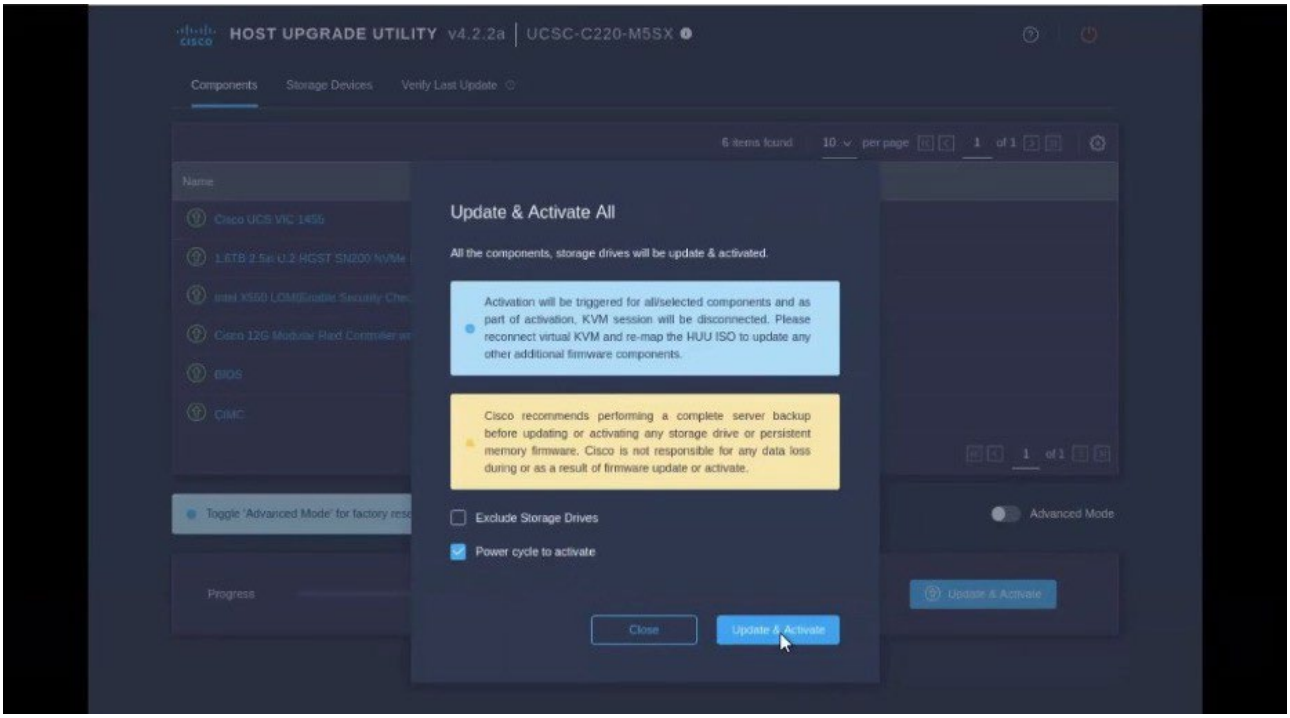
   d. 最後に、 **[マップ ドライブ（Map Drive）]** をクリックします。
7. KVM コンソールの **[電源（Power）]** メニューから、**[システムの電源再投入（Power Cycle System）]** を選択してサーバーを再起動します。
8. サーバーが起動しているときに、 **F6** を押してブートメニューを表示し、 **Cisco vKVM-Mapped vDVD** を選択します。



9. Cisco ソフトウェア ライセンス契約に同意するように求められたら、**[**同意（**Accept**）**]** を選択します。



10. **[**更新してすべてをアクティブ化（**Update & Activate All**）**]** ダイアログで、 **[**更新してアクティブ化（**Update & Activate**）**]** を選択します。



アップグレードが正常に完了したことを確認するには、GUI を使用するか、CIMC HUU を起動して **[**最後の更新の確認（**Last Update Verify**）**]** オプションを選択し、すべてのコンポーネントが正常にアップグレードされたことを確認します。

11. アップグレードが完了したら、トラステッド プラットフォーム モジュール状態(TPM)が有効

    になっていることを確認します。確認および有効化は、**[BIOS] > [BIOS** の設定（**Configure**

    BIOS）**] > [**セキュリティ（**Security**）**]** メニューで行えます。

クラスタの手動アップグレード

クラスタのアップグレードには、「ファームウェア 管理（_firmware_management_cluster_upgrades）」セクションで説明されている手順を使用することを推奨します。

ただし、単一ノード（クラスタに新しいノードを追加しているが、ノードが古いファームウェアを実行している場合）またはクラスタ全体（GUIアップグレードが成功しなかった場合）の手動アップグレードを実行する場合は、代わりに、次の手順を使用することができます。

古いファームウェアを実行している単一のノードをアップグレードして既存のクラスタに追加する場合は、クラスタ全体ではなく、そのノードに対してのみ次の手順を実行します。

1. アップグレードするノードに rescue-user としてログインします。
2. アップグレード ISO のイメージファイルを各ノードの /tmp ディレクトリにコピーします。
3. すべてのノードでアップグレードを開始します。

   すべてのノードを並行してアップグレードできます。

   ```
   # acs installer update -f /tmp/nd-dk9.3.0.1a.iso
   Warning: This command will initiate node update to new version.
   Proceed? (y/n): y
   Update in Progress ... Do not press Ctrl^C
   ```

4. ファームウェアのアップグレードが完了するまでお待ちください。

   次の手順に進む前に、すべてのノードがアップグレードの完了を待つ必要があります。

   ```
   Update succeeded, reboot your host
   ```

5. ノードのいずれかをリブートします。

   いずれかのノードをリブードする前に、先ほどの手順で言及したように、すべてのノードでアップグレードが完了していることを確認してください。

   ```
   # acs reboot
   This command will restart this device, Proceed? (y/n): y
   ```

6. アップグレードが成功したことを確認します。

   ```
   # acs health --upgrade
   All components are healthy
   ```

7. 最初のノードが正常にアップグレードされ、正常になったら、他の 2 つのノードを 1 つずつリブートします。

再起動されたノードが起動するまで待機し、次のノードを再起動する前に acs health --upgrade コマンドを使用してノードが正常であることを確認する必要があります。

8. すべてのノードが起動し、新しいバージョンで正常に稼働したら、アップグレード後のタスクを実行します。すべてのノードで次のコマンドを並行して実行できます。

```
# acs installer post-update
Warning: This command will run the post-update scripts. Proceed? (y/n): y
Update in Progress ... Do not press Ctrl^C
Post-update succeeded
```

コマンドが失敗した場合、10 分待ち、もう一度試してください。

9. アップグレード後のタスクが完了するまで待ちます。

この段階では、ノードにログインしようと試みると、UI に進行状況が表示されます。これは、最初のクラスタ展開に似ています。アップグレード後のプロセスが完了すると、通常どおりノードにログインできるようになります。

10. すべてのノードとクラスタが健全であることを検証します。

```
# acs health
All components are healthy
```

ノードの再イメージ化

Nexus Dashboardの物理ハードウェアが手元に届いた時点で、ソフトウェアイメージはあらかじめロードされています。既存のソフトウェアを設定するだけの場合は、このセクションをスキップして、「ワーカーノードの管理」または「スタンバイノードの管理」に進みます。

手動でノードを最新のソフトウェアバージョンにアップグレードする場合は、代わりに「手動アップグレード」の手順に従ってください。

ここでは、Nexus Dashboardハードウェアにソフトウェアスタックを再展開する方法について説明します。サーバーのオペレーティングシステムや GUI にアクセスできなくなるほどの致命的な障害が発生した場合や、既存のバージョンからの直接アップグレードやダウングレードがサポートされていない別のリリースを展開する場合は、次の手順を使用する必要があります。

既存のNexus Dashboard クラスタを再インストールする場合は、最初にサイトとアプリケーションの情報をクリーンアップ
する必要があります。この場合、クラスタを停止する前に、サイトがすべてのアプリケーションで無効になっており、ND クラスタから削除されていることを確認してください。

はじめる前に

- サーバーの CIMC への接続には Serial over LAN（SoL）ポートを使用する必要があります。サーバーの CIMC IP アドレスと SSH クライアントがあることを確認してください。

  CIMC 設定に関する詳細情報は、 https://www.cisco.com/c/en/us/ support/servers-unified-computing/ucs-c-series-integrated-management-controller/products- installation-and-configuration-guides-list.html で入手できます。

- Cisco Integrated Management Controller（CIMC）のサポートされているバージョンを実行していることを確認します。

  サポートされている CIMC バージョンは、ターゲット リリースの Nexus Dashboard *リリース ノート* にリストされています。CIMC のアップグレードについては、「CIMC のアップグレード」を参照してください。

リモートでホストされているイメージを使用したNexus Dashboardのインストール

Nexus Dashboardソフトウェアを再インストールするには、次の手順を実行します。

1. Cisco Nexus Dashboardイメージをダウンロードします。
   a. Nexus Dashboard ページに移動し、イメージをダウンロードします。

      https://www.cisco.com/c/en/us/support/data-center-analytics/nexus-dashboard/series.html

   b. [ダウンロード（Downloads）] タブをクリックします。
   c. ダウンロードする Nexus Dashboard のバージョンを選択します。
   d. Cisco Nexus Dashboardイメージ(nd-dk9.<version>.iso)をダウンロードします。
   e. 環境内のWebサーバーでイメージをホスティングします。

イメージをマウントするときに http URL を指定する必要があります。

2. ISOをサーバに展開します。

この手順では、サーバーの CIMC に接続する必要があります。CIMC 設定に関する詳細情報は、https://www.cisco.com/c/en/us/support/servers-unified-computing/ ucs-c-series-integrated-management-controller/products-installation-and-configuration-guides-list.html で入手できます。

a. サーバーの CIMC に SSH 接続します。

b. 仮想メディアに接続します。

```
C220-WZP21510DHS# scope vmedia
C220-WZP21510DHS /vmedia #
```

c. CIMC-Mapped vDVD にダウンロードした Nexus Dashboard イメージをマッピングします。

```
C220-WZP21510DHS /vmedia # map-www image http://<ip-address>/<path>
<image>
```

次に例を示します。

```
C220-WZP21510DHS /vmedia # map-www image http://172.31.131.47/images nd-
dk9.2.0.1.iso
```

d. イメージがマウントされていることを確認します。

```
C220-WZP21510DHS /vmedia # show mappings
Volume Map-Status Drive-Type Remote-Share Remote-File          Mount-Type
---------------- ---------- ------------ ------------------------------
image OK          [C          [<ip>/<path>] nd-dk9.2.0.1.iso www
```

e. サーバを再起動し、コンソールに接続します。

```
C220-WZP23150D4C /vmedia # exit
C220-WZP23150D4C# scope chassis
C220-WZP23150D4C /chassis # power cycle
C220-WZP23150D4C /chassis # exit
C220-WZP23150D4C# connect host
CISCO Serial Over LAN:
Press Ctrl+x to Exit the session
```

f. CIMC Web ページを開き、ログインします。

i. [KVM の起動（Launch KVM）] をクリックします。

ii. [電源（Power）]、[システムのリセット（Reset System）] の順にクリックして、ウォーム ブートを実行します。

iii. Serial over LAN セッションに戻り、そこから次の手順に進みます。

g. ブートデバイスを選択します。

次のメッセージが表示されるまで、ブートプロセスを監視します。

```
Press <F2> Setup, <F6> Boot Menu, <F7> Diagnostics, <F8> Cisco IMC Configuration,
<F12> Network Boot
```

F6 を押して、イメージ（Cisco CIMC-Mapped vDVD1）をマウントした仮想メディアデバイスを選択します。

```
/---------------------------------- \
| Please select boot device: |
|----------------------------------- |
| (Bus 05 Dev 00)PCI RAID Adapter |
| UNIGEN PHF16H0CM1-DTE PMAP |
| Cisco vKVM-Mapped vHDD1.22 |
| Cisco CIMC-Mapped vHDD1.22 |
| Cisco vKVM-Mapped vDVD1.22 |
| Cisco CIMC-Mapped vDVD1.22 |
| Cisco vKVM-Mapped vFDD1.22 |
| UEFI: Built-in EFI Shell |
| IBA GE Slot 0100 v1585 |
| IBA GE Slot 0101 v1585 |
| Enter Setup |
|----------------------------------- |
| ^ and v to move selection |
| ENTER to select boot device |
| ESC to boot using defaults |
\---------------------------------- /
```

h. ネットワークを設定します。

サーバーの初回起動時に、次の出力が表示されます。

```
+ '[' -z http://172.31.131.47/nd-dk9.2.0.1.iso ']'
++ awk -F '/|:' '{print $4}'
+ urlip=172.31.131.47
+ '[' -z 172.31.131.47 ']'
+ break
+ '[' -n http://172.31.131.47/nd-dk9.2.0.1.iso ']'
+ set +e
```

```
+ configured=0
+ '[' 0 -eq 0 ']'
+ echo 'Configuring network interface' Configuring
network interface
+ echo 'type static, dhcp, bash for a shell to configure networking, or url to re-enter
the url: '
type static, dhcp, bash for a shell to configure networking, or url to re-enter the url:
+ read -p '? ' ntype
? static ①
+ case $ntype in
+ configure_static
+ echo 'Available interfaces'
Available interfaces
+ ls -l /sys/class/net total
0
lrwxrwxrwx. 1 root root 0 Apr 26 01:21 enp1s0f0 ->
../../devices/pci0000:3a/0000:3a:00.0/0000:3b:00.0/net/enp1s0f0
lrwxrwxrwx 1 root root 0 Apr 26 01:21 enp1s0f1 ->
../../devices/pci0000:3a/0000:3a:00.0/0000:3b:00.1/net/enp1s0f1
lrwxrwxrwx 1 root root 0 Apr 26 01:21 enp1s0f4 ->
../../devices/pci0000:5d/0000:5d:00.0/0000:5e:00.0/0000:5f:01.0/0000:61:00.0/000
0:62:00.0/0000:63:00.0/net/enp1s0f4
lrwxrwxrwx. 1 root root 0 Apr 26 01:21 enp1s0f5 ->
../../devices/pci0000:5d/0000:5d:00.0/0000:5e:00.0/0000:5f:01.0/0000:61:00.0/000
0:62:00.0/0000:63:00.1/net/enp1s0f5
lrwxrwxrwx. 1 root root 0 Apr 26 01:21 lo -> ../../devices/virtual/net/lo
+ read -p 'Interface to configure: ' interface
Interface to configure: enp1s0f0 ②
+ read -p 'address: ' addr
address: 172.23.53.59/21 ③
+ read -p 'gateway: ' gw
gateway: 172.23.48.1 ④
+ ip addr add 172.23.53.59/23 dev enp1s0f0
+ ip link set enp1s0f0 up
+ ip route add default via 172.23.48.1 RTNETLINK
answers: Network is unreachable
++ seq 1 2
+ for count in '$(seq 1 2)'
+ ping -c 1 172.31.131.47
```

① IP アドレスについては、環境内に DHCP サーバーがある場合は dchp、そうでない場合は static と入力します。

② For the interface, enter the first management port (enp1s0f0).

③ static を選択した場合は、接続で使用する IP アドレスを指定します。

④ static を選択した場合は、接続で使用するゲートウェイを指定します。

3. 指定したイメージからサーバーが起動したら、使用可能な唯一のインストールオプションを選

   択します。インストールプロセスが完了するまでに最長20分かかる場合があります。

   イメージが展開されたら、「 ワーカーノード の管理」または「スタンバイノードの管理」の説明に従って、クラスタにノードを追加できます。

既存のクラスタの再構築

既存のクラスタの再構築が必要になることがあります。たとえば、データネットワークのサブネットやノードのデータIPアドレスを変更する場合などで、これにはクラスタの再展開が必要です。

1. 「バックアップと復元」の説明に従って、Nexus Dashboardクラスタ設定をバックアップします。
2. クラスタに展開されているすべてのサービスの設定をバックアップします。

   NDOについては、　　の **[操作] > [バックアップと復元]** を参照してください。

   NDIについては、 *Nexus Dashboard Insights User Guide* の **[操作] > [バックアップと復元]** を参照してください。

   NDFCについては、**NDFC**　の **[操作] > [バックアップと復元]** を参照してください。

3. クラスタが物理アプライアンスとして展開されている場合...
   a. レスキュー ユーザーとして各ノードにログインします。
   b. 各ノードで、 acs reboot factory-resetを実行します。

      これにより、ノードが工場出荷時の設定にリセットされ、再起動されます。

   c. 同じハードウェアを使用してクラスタを再展開します。

      クラスタを最初に展開したときと同じ手順を実行できます。これについては、 *Nexus Dashboard Deployment Guide* の「Deploying as Physical Appliance」の章で説明されています。

4. クラスタが仮想マシン(VM)に展開されている場合...
   a. 既存のVMの電源を切ります。

      新しいクラスタを展開し、サービスとその設定を復元するまで、既存のクラスタの VM を保持できます。その後、古いクラスタの VM を削除できます。

   b. 新しいクラスタを再展開します。

      クラスタを最初に展開したときと同じ手順を実行できます。これについては、 *Nexus Dashboard Deployment Guide* の「Deploying in VMware ESX」または「Deploying in Linux KVM」の章で説明されています。

5. 「バックアップと復元」 の説明に従って、Nexus Dashboard の構成を復元します。
6. 「サービス管理」 の説明に従って、先ほど展開したサービスをインストールします。
7. ステップ 1で作成したバックアップから各サービスの設定を復元します。

   NDOについては、　　の **[操作] > [バックアップと復元]** を参照してください。

   NDIについては、 *Nexus Dashboard Insights User Guide* の **[操作] > [バックアップと復元]** を参照してください。

   NDFCについては、**NDFC**　の **[操作] > [バックアップと復元]** を参照してください。

Zookeeper/Kafkaサービスの復旧

AppStoreエラー

Nexus Dashboard の GUI で、[サービス **> AppStore**（**Services > AppStore**）] タブにアクセスしようとすると、次のエラーが発生する場合があります。

```
{
  " error" : " There was a problem proxying the request"
}
```

原因

アプリ ストア サービスが実行されているプライマリ ノードに障害が発生すると、アプリ ストア サービスが別のマスターノードに再配置されるまでに最長5分かかる場合があります。

解決策

サービスが回復してページが更新されるまで待ちます。

イベントのエクスポート

Syslogイベントが、目的の外部イベント監視サービスに到達していません。

原因

この問題の最も一般的な原因は、Syslog 接続先サーバーが設定されていないか、正しく設定されていません。

解決策

クラスタの構成 **> Syslog*** の外部サーバーの構成が正しいことを確認してください。詳細については、「クラスタの構成」を参照してください。

原因2

リモートサーバーは特定のIPアドレスのセットからのトラフィックのみを許可しており、Nexus DashboardノードのIPアドレスからのトラフィックは許可されていません。

解決策2

外部サーバーの設定を更新して、Nexus Dashboardクラスタノードからのトラフィックを許可します。

工場出荷時の状態へのリセット

各ノードで次のコマンドを実行して、物理クラスタ全体をリセットできます。

```
# acs reboot factory-reset
```

ヒ

これを行うと、すべてのクラスタ設定とアプリケーションが失われるため、クラスタを再構築する必要があります。

仮想またはクラウド型の Nexus Dashboard クラスタをご使用の場合は、『*Cisco Nexus Dashboard 導入ガイド*』で説明されているように、すべてのノードをリセットするのではなく、既存の VM を削除してクラスタ全体を再展開することをお勧めします。

ノードIPアドレスの変更

データネット ワークの IP アドレスの変更はサポートされていません。クラスタ ノードのデータ IP アドレスを変更する場合は、クラスタを再作成する必要があります。

シングル ノード クラスタを稼働している場合、クラスタを再作成しない限り、管理 IP アドレスの変更もサポートされません。

マルチノード クラスタを稼働している場合は、次のように 1 つ以上のノードの管理 IP アドレスを変更できます。

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. メイン ナビゲーション メニューから、**[システムリソース > ノード（System Resources > Nodes）]** を選択します。
3. ノードの隣にある（**...**）メニューから、**[ノードの編集（Edit Node）]** を選択します。

   現在ログインしていないノードの IP アドレスのみを変更できることに注意してください。現行ノードの IP を変更するには、別のノードの管理 IP アドレスに移動してログインし、最後のノードまでこの手順を繰り返します。

4. ノードの **[管理ネットワーク アドレス（Management Network Address）]** と **[管理ネットワーク ゲートウェイ（Management Network Gateway）]** を更新します。たとえば、それぞれ 172.31.140.58/24 と 172.31.140.1 です。
5. **[保存（Save）]** をクリックします。

   変更はすぐに反映され、新しいIPアドレスを使用してノードにアクセスできるようになります。

クラスタ構成エラー

Nexus Dashboard でプロキシサーバーを設定または変更すると、**[クラスタ構成（Cluster Configuration）]** ページに、いくつかの cisco-mso service: Replicaset() not in desired state エラーが表示される場合があります。

原因

エラーはサービスの再起動中に表示され、30～60秒以内に自動的に解決されます。

解決策

サービスが回復してページが更新されるまで待ちます。

ログイン情報の入力を求めない二要素認証(2FA)

2要素認証を使用した最初のログイン後、その後のログイン試行ではユーザー名とパスワードの情報は要求されず、代わりに空白のページが表示されます。

原因

OIDCアプリケーションに設定されているCookieのタイムアウトが、Nexus Dashboardで設定されている認証トークンのタイムアウトよりも長くなっています。

解決策

ブラウザのキャッシュをクリアすると、認証プロセスが期待どおりに機能します。

Red Hat Enterprise Linux(RHEL)の展開

RHEL システムにログインして/logs/ndlinux/ ディレクトリを確認すると、インストール ログを表示できます。

「トラブルシューティング」のセクションで説明されている一般的なNexus Dashboardのトラブルシューティング コマンドを実行するには、最初にNexus Dashboard環境にアクセスする必要があります。

RHELシステムからNexus Dashboard環境にアクセスするには、次を実行します。

1. インストール時にYAML構成ファイルで指定したNexus Dashboardユーザーを使用してRHELシステムにログインします。
2. attach-nd コマンドを実行してNexus Dashboard環境にアクセスします。

   ```
   /usr/bin/attach-nd
   ```

   Nexus Dashboard環境にアクセスすると、このガイドの「トラブルシューティング」のセクションで説明されているすべての一般的なNexus Dashboardコマンドを使用できます。

APIC設定のインポート後にサイトに接続できない

Cisco APICサイトをNexus Dashboardにオンボーディングすると、オンボーディングを反映するようにAPIC設定が更新されます。その後、APICで以前の設定をインポートすると、サイトがNexus Dashboardまたはサービスで使用不可として表示される場合があります。

原因

以前のサイト設定には、オンボードされているNexus Dashboardクラスタに固有の情報は含まれていません。

解決策

サイトがNexus Dashboardにオンボーディングされた後、今後の設定の復元のためにAPIC設定をエクスポートすることをお勧めします。

発生後に問題を解決するには、Nexus Dashboard GUIでサイトを再登録します。

1. Nexus Dashboardクラスタにログインします。
2. **[管理コンソール（Admin Console）] > [サイト（Sites）]** に移動します。
3. サイトの横の **[アクション（Actions）]（[...]）** メニューから、**[サイトの編集（Edit Site）]** を選択します。
4. **[サイト編集（Site Edit）]** 画面で、[サイトの再登録（Re-register Site）] チェックボックスをオンにして、サイトの詳細を再度入力します。

5. **[保存（Save）]** をクリックします。

ワーカーノードまたはスタンバイノードの交換

物理クラスタへの同じプライマリ ノードの再追加

このセクションでプライマリノードを物理クラスタに再追加する方法について説明します。このシナリオは、設定のリセット（acs reboot factory-reset など）または vMedia の再インストールによって、ノードが誤ってまたは意図的に削除された場合に発生する可能性があります。

クラスタにスタンバイ ノードがある場合は、「スタンバイ ノードなしで単一のプライマリ ノードの置換」の説明に従ってスタンバイ ノードをプライマリ ノードに置き換えて、次に Adding Standby Nodes の説明に従ってプライマリ ノードを新しいスタンバイノードとして追加します。

ハードウェア障害のためにプライマリ ノードを完全に置換（RMA）する必要があるが、使用可能なスタンバイ ノードがない場合は、代わりに 「スタンバイ ノードなしで単一のプライマリ ノードの置換」で説明されている手順に従ってください。

プライマリ ノードを同じクラスタに再度追加するには、次の手順を実行します。

1. ノードが工場出荷時の設定にリセットされていることを確認します。

   ノードが不良状態の場合は、rescue-user としてノードにログインし、次のコマンドを使用してノードをリセットします。

   ```
   # acs reboot factory-reset
   ```

2. 正常なノードのいずれかの管理IPアドレスを使用してNexus DashboardGUIにログインします。
3. **[システムリソース（System Resources）] > [ノード（Nodes）]** の順に移動します。

   交換するノードが [非アクティブ（Inactive）] として UI に表示されます。

4. ノードのアクション（**[...]**）メニューから、**[登録**

   （Register）] を選択します。**[ノードの登録（Register**

   Node）] ページが開きます。

5. **[ノードの登録（Register Node）]** ページで必要な情報を入力し、**[検証（Validate）]** をクリックします。

   物理ノードの場合は、CIMC IPアドレスとログイン情報を指定する必要があります。

   仮想ノードの場合、管理 IP アドレスは保持されるため、rescue-user のパスワードのみを入力する必要があります。

6. 残りのノード情報が正確であることを確認します。
7. 登録 をクリックしてノードを再登録し、プライマリ ノードとしてクラスタに再追加します。

   ノードのブートストラップ、設定、および再追加には最大20分かかります。完了すると、ノードは UI にアクティブなプライマリ ノードとして表示されます。

スタンバイノードのない単一の仮想マスターノードの置換

ここでは、VMware ESX または Linux KVM 仮想 Nexus Dashboard クラスタでプライマリ ノードの障害から回復する方法について説明します。この手順では、置換するノードと同じフォームファクタを使用してまったく新しいNexus Dashboardノードを展開し、残りのクラスタにプライマリ ノードとして加えます。

1. 障害が発生したノードの VM の電源がオフになっていることを確認します。
2. 新しいNexus Dashboardノードを起動します。

   VMware ESX で追加のノードを起動する方法については、「VMware ESX における追加の仮想ノードの展開」を参照してください。交換するノードと同じタイプ（OVA-App または OVA-Data）のノードを起動する必要があることに注意してください。

   Linux KVM で追加のノードを起動する方法については、「Linux KVM における追加の仮想ノードの展開」を参照してください。

   ヒ 障害が発生したノードとまったく同じネットワーク設定を使用していることを確認します。

3. 新しいノードの VM の電源をオンにして、起動するまで待ちます。
4. Nexus Dashboard GUI にログインします。

   残りの正常な プライマリ ノードのいずれかの管理 IP アドレスを使用できます。

5. ノードを置換します。
   a. 左側のナビゲーション ペインから、**[**システム リソース（**System Resources**）**] [**ノード（**Nodes**）**]** を選択します。置換するノードが [非アクティブ（Inactive）] としてリスト化されます。
   b. 置換する非アクティブ プライマリ ノードの隣にある**(...)** メニューをクリックして、**[**置換（**Replace**）**]** を選択します。**[**置換（**Replace**）**]** ウィンドウが開きます。
   c. ノードの管理 **IP** アドレスとパスワードを入力し、**[**確認（**Verify**）**]** をクリックします。

      クラスタはそのノードの管理 IP アドレスに接続して接続性を確認します。

   d. **[**置換（**Replace**）**]** をクリックします。

      ノードが設定されてクラスタに参加するまでに、最大で20分かかる場合があります。

スタンバイノードのない単一の仮想プライマリノードの置換

ここでは、スタンバイ ノードのない Nexus Dashboard 物理クラスタで単一のプライマリ ノードの障害から回復する方法について説明します。この手順は、物理的に置換する必要があるハードウェアの問題を対象としていますノードのソフトウェア状態が不良の場合は、代わりに acs reboot clean コマンドを使用し、「同じ

プライマリ ノードを物理クラスタに再度追加する」 の説明に従って、同じノードをクラスタに再追加できます。

クラスタにスタンバイ ノードが設定されている場合は、「スタンバイ ノードを使った単一プライマリ ノードの置換」 の手順に従うことを推奨します。

はじめる前に

- 少なくとも 2 つのプライマリ ノードが正常であることを確認します。

  2 つのプライマリノードを使用できない場合は、「2 つのプライマリ ノードをスタンバイ ノードに置き換える」の説明に従って、クラスタを手動で復元する必要があります。

- 置換するプライマリ ノードの電源がオフになっていることを確認します。
- 「追加物理ノードの展開」の説明に従って、新しいノードを準備して展開します。
- 障害が発生したノードと同じCIMC IPアドレスとログイン情報が新しいノードに設定されていることを確認します。

  残りのプライマリノードは CIMC 情報を使用して、新しいノードで構成を復元します。

- 新しいノードの電源がオンになっていることを確認し、シリアル番号をメモ

します。障害が発生した単一のプライマリノードを置換するには、次の手順を実

行します。

1. 他のいずれかの プライマリ ノードの管理 IP を使用して、Nexus Dashboard の GUI にログインします。
2. メイン ナビゲーション メニューから、**[**システムリソース **>** ノード（System Resources > Nodes）**]** を選択します。
3. ノード リストで、置換するノードのシリアル番号を見つけ、ノードのステータスが [非アクティブ（Inactive）] と表示されていることを確認します。
4. Nexus Dashboard の **[**ノード（**Nodes**）**]** 画面で、非アクティブなノードの横にあるチェックボックスをオンにして選択します。
5. **[**アクション（**Actions**）**]** メニューから **[**置換（**Replace**）**]** を選択します。
6. **[**新しいシリアル番号（**New Serial Number**）**]** フィールドに新しいノードのシリアル番号を入力し、**[**置換（**Replace**）**]** をクリックします。

   プロセスが完了すると、古いノードのシリアル番号が新しいノードのシリアル番号に更新され、新しいマスター ノードがクラスタに正常に参加すると、ステータスが [アクティブ（Active）] に変わります。

機能不全が発生したワーカーノードまたはスタンバイノードを置換する場合は、通常のようにGUIから [非アクティブ] ノードを削除して、まったく新しいワーカーノードまたはスタンバイノードを展開します。

はじめる前に

- 置換するワーカーノードの電源がオフになっていることを確認しま

す。機能不全が発生したワーカーノードまたはスタンバイノードを置

換するには、次の手順を実行します。

1. Nexus Dashboard の **[**管理コンソール（**Admin Console**）**]** に移動します。

2. メイン ナビゲーション メニューから、**[**システムリソース **>** ノード（System Resources > Nodes）] を選択します。
3. ノード リストで、置換するノードのシリアル番号を見つけ、ノードのステータスが [非アクティブ（Inactive）] と表示されていることを確認します。
4. 横にあるチェックボックスをクリックして、非アクティブなノードを選択します。
5. **[**アクション（**Actions**）**]** メニューから **[**削除（**Delete**）**]** を選択します。

   これにより、機能不全が発生したノードがリストから削除されます。

6. 「ワーカーノードの管理」または「スタンバイノードの管理」の説明に従い、新しいノードの電源をオンにして、新しいワーカーノードまたはスタンバイノードとしてクラスタに追加します。

   古いノードを設定したときと同じ設定パラメータを使用できます。

初期クラスタブートストラップの問題

ここでは、初期クラスタ ブートストラップ プロセスのさまざまな段階について説明し、Nexus Dashboardクラスタを最初に展開する際に発生する可能性のあるいくつかの一般的な問題についてまとめます。

ノードを起動して GUI のセットアップ時に各ノードの情報を入力すると、初期ブートストラッププロセスはいくつかの段階を経て、ノードの起動、必要な情報の設定、およびクラスタの作成を実行します。ブートストラップ画面では、進行状況を追跡し、発生する可能性のある問題を示します。

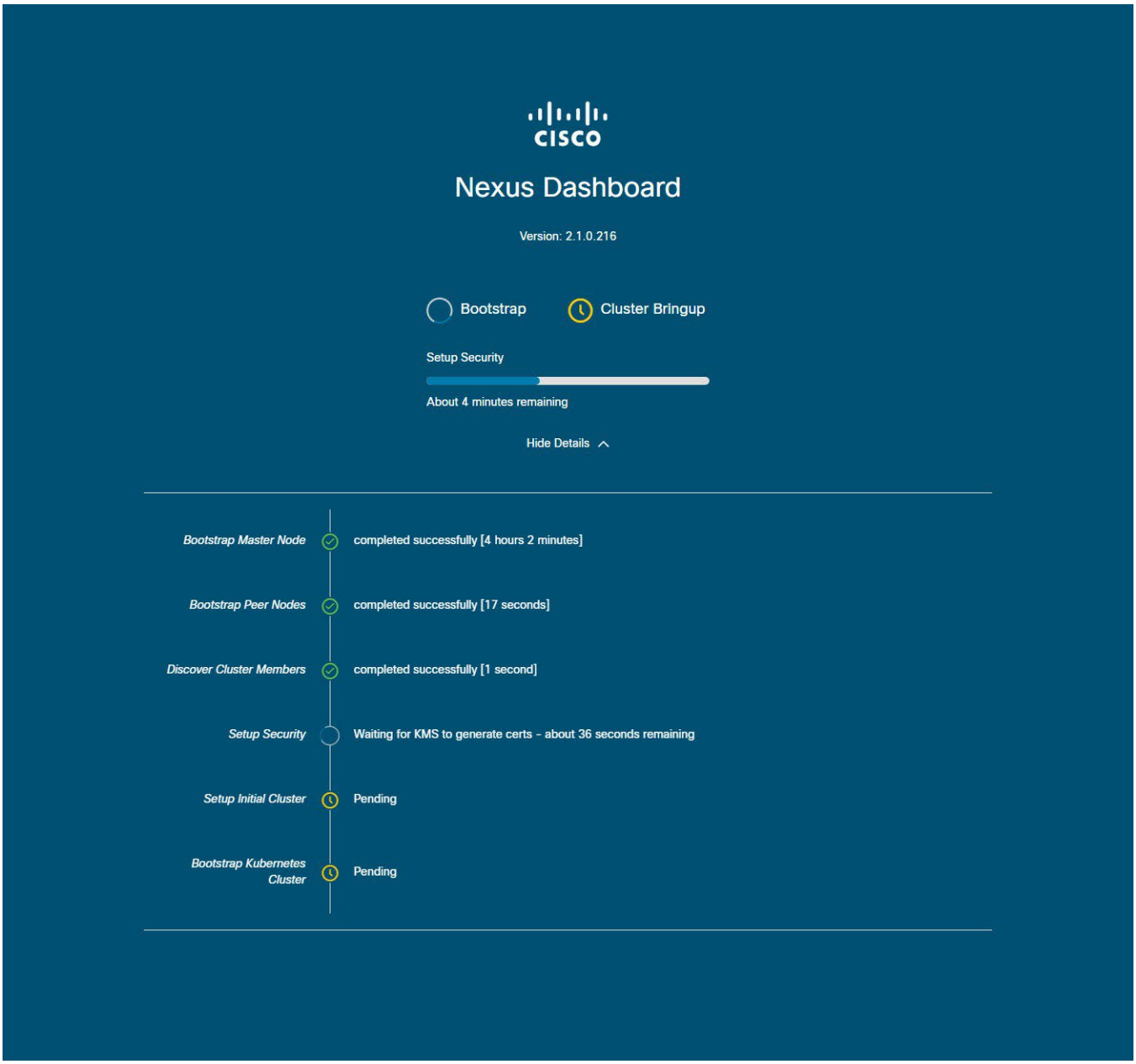


図 1. ブートストラップの進行状況

- ブートストラップ マスター ノードとブートストラップ ピア ノード：ユーザーが指定した管理ネットワークとデータ ネットワークの IP アドレスを使用して、最初のマスター ノードを起動します。次に、2番目と3番目のマスターノードをそれぞれのIPを使用して起動します。

  これらの段階のいずれかでプロセスが失敗した場合は、各ノードのコンソールに接続して、入力したすべての情報が正しいことを確認します。acs system-config コマンドを使用すると、設定内容を表示できます。

ブートストラップログ（/logs/k8/install.log）で詳細を確認することもできます。

通常、acs reboot factory-reset を使用してノードをリセットし、セットアッププロセスを再起動することで、設定不備が原因で発生した問題を解決できます。

- クラスタ メンバーの検出（Discover Cluster Members）：データ ネットワークを介してクラスタ内のすべてのマスター ノード間の接続を確立します。

  この段階の障害は通常、データネットワークIPアドレスの設定ミスと、ノードが他の2つのピアに到達できないことを示しています。

  任意のノードで acs cluster masters コマンドを使用して、指定したデータ IP を確認できます。

  コマンドが情報を返さない場合は、ip addr を使用してデータ インターフェイス（bond0br）の IP アドレスを確認し、すべてのノードの IP が他のノードから到達可能であることを確認します。

```
$ ip addr
[..]
6: bond0br: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
group default qlen 1000
    link/ether 52:54:00:e1:93:06 brd ff:ff:ff:ff:ff:ff
    inet 10.195.255.165/24 brd 10.195.255.255 scope global bond0br valid_lft
       forever preferred_lft forever
    inet6 fe80::5054:ff:fee1:9306/64 scope link
       valid_lft forever preferred_lft forever
[..]
```

- セキュリティの設定（Setup Security）：キー管理サービス（KMS）を設定して、ノード間のデータ暗号化を有効にします。

  acs cluster masters コマンドが ca cert not found エラーを返す場合、KMS の問題であることを示しています。詳細については、/logs/kms ログを確認してください。

- 初期クラスタの設定とブートストラップ Kubernetes クラスタ： こうした段階での障害は、通常、Kubernetes の問題であることを示しています。

  各ノードの /logs/k8 ログから追加の詳細情報を取得できます。

- ブートストラップの段階が完了すると、プロセスはクラスタの立ち上げの段階に進みます。

  システムの初期化からインフラサービスの準備完了待ちまでの各段階で、残りのサービスを起動してクラスタの作成を完了します。

  この段階で、いずれかのノードで acs health コマンドを使用して、正しく起動していないサービスを確認できます。次に、/logs/k8_infra/*<service>* で特定のサービスのログを確認します。

マルチクラスタ接続の問題

次のセクションでは、マルチクラスタ接続に関する一般的な問題について説明します。

複数のクラスタをまとめて接続する方法の詳細については、「マルチクラスタ接続」を参照してください。

非プライマリクラスタが再接続できない

マルチクラスタ接続グループに属していたクラスタをクリーンリブートして再展開すると、グループのプライマリクラスタはそれを認識できないため、クラスタが到達不能のままになります。

この問題を解決するには、クラスタを接続解除して再接続します。

1. プライマリクラスタにログインします。
2. 再展開したクラスタをグループから削除します。これ

   については、「クラスタの切断」を参照してください。

3. クラスタをグループに再度追加します。

   これについては、「複数のクラスタの接続」を参照してください。

古いバージョンで再展開された非プライマリクラスタ

何らかの理由で、この機能をサポートしていないバージョンのNexus Dashboardを使用して、グループ内の非プライマリクラスタの1つを再展開した場合、プライマリクラスタは引き続きそのクラスタに接続できますが、取得することはできません。 情報とUIは空白のままになります。

この問題を解決するには、そのクラスタをグループから削除します。

1. 管理 ユーザーとしてプライマリ クラスタにログインします。

   すべてのクラスタで共有されているリモートユーザーでログインすると、UIページは空白のままになります。

2. 再展開したクラスタをグループから削除します。これ

   については、「クラスタの切断」を参照してください。

3. ログアウトして、マルチクラスタ接続の管理に使用するリモートユーザーを使用して再度ログインし、UIが正しく読み込まれることを確認します。

秘密キーと自己署名証明書の生成

秘密キーの生成、証明書署名要求の作成、およびCA署名付き証明書の取得

このセクションでは、秘密キーの生成、証明書署名要求（CSR）の作成、および認証局（CA）によって署名された証明書の取得方法の例を示します。これらはNexusダッシュボードクラスタで使用します。

秘密キーと自己署名証明書の両方を生成する場合は、このセクションをスキップし、代わりに「Generating Private Key and Self-Signed Certificate」で説明されている手順に従ってください。

Nexus Dashboard GUI でキーと証明書を追加するために必要な設定手順は、「セキュリティ」の章で説明されています。

1. 秘密キーを生成します。

   OpenSSL がインストールされている任意のプラットフォームで秘密キーを生成するか、rescue-user として Nexus Dashboard ノードの 1 つに SSH で接続し、そこでこの手順を実行します。

   ```
   [rescue-user@localhost ~]$ openssl genrsa -out nd.key 2048
   Generating RSA private key, 2048 bit long modulus
   ..........................
   ..............
   e is 65537 (0x10001)
   [rescue-user@localhost ~]$ ls
   nd.key
   ```

2. 最初のステップで生成した秘密キーで署名されたCSRを生成します。

   a. 必要な情報を含む CSR 構成ファイル（csr.cfg）を作成します。設定ファイルの例を次に示します。

   ```
   [req]
   default_bits = 2048
   distinguished_name = req_distinguished_name
   req_extensions = req_ext
   prompt = no
   [req_distinguished_name]
   countryName = US
   stateOrProvinceName = Texas
   localityName = Plano
   organizationName = CSS
   organizationalUnitName = DC
   ```

```
commonName = nd.dc.css
emailAddress = no-reply@mydomain.com
[req_ext]
subjectAltName = @alt_names
[alt_names]
DNS.1 = *.dc.css
IP.1 = 10.0.0.96
IP.2 = 10.0.0.97
```

b. CSRを作成します。

```
[rescue-user@localhost ~]$ openssl req -new -key nd.key -out nd.csr -config csr.cfg
[rescue-user@localhost ~]$ ls
csr.cfg nd.csr nd.key
```

次のコマンドを使用して、生成した CSR を確認できます。

```
[rescue-user@localhost ~]$ openssl req -in nd.csr -text -noout
```

3. CA署名付き証明書を取得します。

実稼働環境では、前ステップで作成した証明書署名要求（ca.csr）をIdenTrustやDigiCertなどのパブリックCAに送り、CA署名付き証明書（ca.crt）を取得します。

4. 署名済み証明書を確認します。

次のコマンドは、生成した秘密キーと同じフォルダにCA 署名付き証明書（ca.crt）をコピーしたことを前提としています。

```
[rescue-user@localhost ~]$ openssl verify -verbose -CAfile ca.crt nd.crt
nd.crt: OK
```

5. 生成されたファイルの内容を Nexus Dashboard の GUI に追加します。

「セキュリティの構成」で説明されている手順に従って、前の手順で生成した次の 3 つのファイルの内容を入力する必要があります。

- 秘密キー（nd.key ）
- 認証局（CA）パブリック証明書（ca.crt）
- CA 署名付き証明書（nd.crt）

このセクションでは、Nexus Dashboardクラスタで秘密キーとカスタム証明書を使用する場合にそれらを生成する方法の例を示します。

CA署名付き証明書を使用する場合は、このセクションをスキップして、「

CSR、および CA 署名付き証明書の取得」を参照してください。

Nexus Dashboard GUI でキーと証明書を追加するために必要な設定手順は、「セキュリティ」の章で説明されています。

1. 秘密キーを生成します。

   OpenSSL がインストールされている任意のプラットフォームで秘密キーを生成するか、rescue-user として Nexus Dashboard ノードの 1 つに SSH で接続し、そこでこの手順を実行します。

   ```
   [rescue-user@localhost ~]$ openssl genrsa -out nd.key 2048
   Generating RSA private key, 2048 bit long modulus
   ..........................
   ..............
   e is 65537 (0x10001)
   [rescue-user@localhost ~]$ ls
   nd.key
   ```

2. 認証局(CA)キーを生成します。

   ラボやテストの目的などで自己署名CAを生成するには、次のコマンドを実行します。

   ```
   [rescue-user@localhost ~]$ openssl genrsa -out ca.key 2048
   Generating RSA private key, 2048 bit long modulus
   ...................
   ..............
   e is 65537 (0x10001)
   [rescue-user@localhost ~]$ ls
   ca.key nd.key
   ```

3. CAのCSRを生成します。

   ```
   [rescue-user@localhost ~]$ openssl req -new -key ca.key -subj
   " /CN=Self/C=US/O=Private/ST=Texas"  -out ca.csr
   [rescue-user@localhost ~]$ ls
   ca.csr ca.key nd.key
   ```

   次のコマンドを使用して、生成した CSR を確認できます。

   ```
   [rescue-user@localhost ~]$ openssl req -in ca.csr -text -noout
   ```

4. 自己署名ルート証明書を作成します。

```
[rescue-user@localhost ~]$ openssl x509 -req -in ca.csr -signkey ca.key
-CAcreateserial -out ca.crt -days 3650
Signature ok
subject=/CN=Self/C=US/O=Private/ST=Texas
Getting Private key
[rescue-user@localhost ~]$ ls
ca.crt ca.csr ca.key nd.key
```

次のコマンドを使用して、生成したルート証明書を確認できます。

```
[rescue-user@localhost ~]$ openssl x509 -in ca.crt -text -noout
```

5. 最初のステップで生成した秘密キーで署名されたCSRを生成します。
   a. 必要な情報を含む CSR 構成ファイル（csr.cfg）を作成します。設定ファ

      イルの例を次に示します。

```
[req]
default_bits = 2048
distinguished_name = req_distinguished_name
req_extensions = req_ext
prompt = no
[req_distinguished_name]
countryName = US
stateOrProvinceName = Texas
localityName = Plano
organizationName = CSS
organizationalUnitName = DC
commonName = nd.dc.css
emailAddress = no-reply@mydomain.com
[req_ext]
subjectAltName = @alt_names
[alt_names]
DNS.1 = *.dc.css
IP.1 = 10.0.0.96
IP.2 = 10.0.0.97
```

   b. CSRを作成します。

```
[rescue-user@localhost ~]$ openssl req -new -key nd.key -out nd.csr -config csr.cfg
[rescue-user@localhost ~]$ ls
```

```
ca.crt ca.csr ca.key csr.cfg nd.csr nd.key
```

次のコマンドを使用して、生成した CSR を確認できます。

```
[rescue-user@localhost ~]$ openssl req -in nd.csr -text -noout
```

6. 生成した証明書に自己署名します。

```
[rescue-user@localhost ~]$ openssl x509 -req -in nd.csr -CA ca.crt -CAkey ca.key
-CAcreateserial -out nd.crt -days 3600 Signature
ok
subject=/C=US/ST=Texas/L=Plano/O=CSS/OU=DC/CN=nd.dc.css/emailAddress=no-
reply@mydomain.com
CA 秘密キーの取得 [rescue-
user@localhost ~]$ ls
ca.crt ca.csr ca.key ca.srl csr.cfg nd.crt nd.csr nd.key
```

7. 署名済み証明書を確認します。

```
[rescue-user@localhost ~]$ openssl verify -verbose -CAfile ca.crt nd.crt
nd.crt: OK
```

8. 生成されたファイルの内容を Nexus Dashboard の GUI に追加します。

「セキュリティの構成」で説明されている手順に従って、前の手順で生成した次の 3 つのファイルの内容を入力する必要があります。

- 秘密キー（nd.key ）
- 認証局（CA）パブリック証明書（ca.crt）
- CA 署名付き証明書（nd.crt）

NDFCが管理するスイッチデバイスを交換した後のNDO設定の更新

Nexus Dashboard Fabric Controller (NDFC)ファブリックがNexus Dashboard Orchestrator (NDO)によって管理されていて、NDFCによって管理されている1つ以上のデバイスを交換した場合は、NDOが新しいスイッチのシリアル番号を認識していることを確認する必要があります。

次のセクションでは、新しいファブリック デバイスの情報を NDO と同期するために必要な手順の概要を示します。

コアまたはルートサーバー(RS)デバイスの交換

1. NDFCにログインします。
2. NDFC Easy Fabricモードの使用時にファブリック内の物理スイッチを交換するには、「Cisco NDFC Fabric Controller Configuration Guide」に記載されている返品許可（RMA）手順に従います。
3. NDOにログインします。
4. **[インフラストラクチャ] > [サイト接続]** に移動します。
5. RS/コアが存在する 全般設定 ページの コントロール プレーン構成 で 更新 をクリックします。
6. **[展開（Deploy）]** をクリックします。

リーフスイッチの交換

1. NDFCにログインします。
2. NDFC Easy Fabricモードの使用時にファブリック内の物理スイッチを交換するには、「Cisco NDFC Fabric Controller Configuration Guide」に記載されている返品許可（RMA）手順に従います。
3. NDOにログインします。
4. **[アプリケーション管理] > [スキーマ]** に移動し、そのサイト/デバイスのスキーマ/テンプレートをクリックします。
5. デバイスに存在していたVRF/ネットワークを再インポートします。
   a. **[概要を表示（View Overview）]** ドロップダウン リストで、テンプレートを選択します。
   b. **[テンプレートのプロパティ（Template Properties）]** セクションで、**[VRF]** ボックスから VRF/ネットワークをクリックします。
   c. **[インポート]** ドロップダウン リストからサイトを選択します。
   d. **[VRF]** をクリックした後、VRF を選択します。
   e. **[インポート（Import）]** をクリックします。

ボーダーゲートウェイ(BGW)デバイスの交換

1. NDFCにログインします。
2. NDFCEasy Fabric モードを使用している場合にファブリック内の物理スイッチを交換するには、

『Cisco NDFC Fabric Controller Configuration Guide』に記載されている資材返還認証（RMA）の手順に従います。

3. NDOにログインします。
4. **[インフラストラクチャ] > [サイト接続]** に移動します。
5. BGW が存在するサイトで **[更新]** をクリックし、**[展開]** をクリックします。
6. **[アプリケーション管理] > [スキーマ]** に移動し、そのサイト/デバイスのスキーマ/テンプレートをクリックします。
7. デバイスに存在していたVRF/ネットワークを再インポートします。
   a. **[概要を表示（View Overview）]** ドロップダウン リストで、テンプレートを選択します。
   b. **[テンプレートのプロパティ（Template Properties）]** セクションで、**[VRF]** ボックスから VRF/ネットワークをクリックします。
   c. **[インポート]**ドロップダウン リストからサイトを選択します。
   d. **[VRF]** をクリックした後、VRF を選択します。
   e. **[インポート（Import）]** をクリックします。

商標

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任となります。

対象製品のソフトウェア ライセンスと限定保証は、製品に添付された『Information Packet』に記載されており、この参照により本マニュアルに組み込まれるものとします。添付されていない場合には、代理店にご連絡ください。

Cisco が採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または暗黙のすべての保証を放棄します。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアルの中の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco およびCisco のロゴは、Cisco またはその関連会社の米国およびその他の国における商標または登録商標です。
商標または登録商標です。シスコの商標の一覧は、http://www.cisco.com/ go/trademarks でご確認いただけます。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」という言葉が使用されていても、シスコと他社の間にパートナー関係が存在することを意味するものではありません。（1110R）。

初版： 2023 年 1 月 31 日
最終更新日：2023 年 4 月 11 日

米国本社
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706 USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax：408 527-0883