Cisco Nexus Dashboard のトラブルシューティング、リリース 3.2.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。

- acs pwd ： rescue-user のパスワードを変更できます。

GUI の「admin」ユーザーと CLI レスキューユーザーに異なるパスワードを設定する場合は、このコマンドを使用する必要があります。GUI で admin ユーザのパスワードを変更すると、同じパスワードが rescue-user にも自動的に設定されます。

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 ：クラスタ内のセカンダリ 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 ：指定されたカテゴリのテクニカルサポート情報を収集します。
  - 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。
- acs deployment -- クラスタの展開モードを管理できます。
  - acs deployment show ：現在のクラスタでサポートされている展開モードを表示します。

```
$ acs deployment show
==========================================================================
展開名                                  サービス
--------------------------------------------------------------------------
ndfc                                  コントローラ
ndi                                 Insights
ndo                                  Orchestrator
ndfc-ndi                               Controller,Insights
```

```
ndo-ndi                         Orchestrator,Insights
=================================================================
```

- acs deployment running：現在の展開モードを表示します。

```
$ acs deployment running
Running deployment mode ndfc-ndi
```

- acs deployment clear：現在展開されているサービスを削除し、設定された展開モードを効果的に削除します。

  acs deployment running コマンドを使用して、コマンドが成功したことを確認できます。

```
$ acs deployment running
実行中の展開モードなし
```

  このコマンドを使用した後、以下で説明する acs deployment set コマンドを使用して新しい展開モードを選択できます。

- acs deployment set --mode<ndfc, ndo, ndi> -- 新しい展開モードを設定します。

  新しい展開モードを設定する前に、展開モードをクリアする必要があります。展開モードがすでに設定されている場合、このコマンドはエラーを返します。

  次の例は、説明されているすべてのコマンドを使用して、既存の展開モードを削除し、新しい展開モードを設定する方法を示しています。プロセス全体が完了するまでに最大 20分 かかる場合があります。

```
$ acs deployment show
=================================================================
展開名                                  サービス
-----------------------------------------------------------------

ndfc                            コントローラ
ndo                             オーケスト
=================================================================


$ acs deployment running
展開モード ndfc の実行


$ acs deployment clear
 警告：このコマンドは、アプリケーションのすべてのデータと状態を削除できる展開
を更新します。Proceed? (y/n): y
展開モードが正常にクリアされました。

$ acs deployment running
```

実行中の展開モードなし

$ acs deployment set --mode ndo
警告：このコマンドは、アプリケーションのすべてのデータと状態を削除できる展開を更新します。Proceed? (y/n): y
展開モードが正常に更新されました

$ acs deployment running
実行中の展開モードがありません。目的の展開モードがndoに設定されています。リリースが実行状態になるまでお待ちください。

$ acs deployment running 実行中の
展開モード ndo

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、最初にファブリック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、ファブリック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 passwd コマンドを使用して rescue-user の別のパスワードを構成した場合、pwd コマンド、パスワードは、最初のクラスターブートストラッププロセス中に構成したのパスワードにリセットされます。

- 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、最初にファブリック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、ファブリック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-0 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。

UCS サーバ ファームウェアのアップグレード

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 UCS サーバ ファームウェア（ CIMC、BIOS、 RAIDコントローラ、およびディスクおよび NIC アダプタファームウェアを含む）もアップグレードする必要があります。

Nexus Dashboard の各リリースでサポートされている UCS サーバ ファームウェア 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 ホスト アップグレード ユーティリティ (HUU) を使用して Nexus Dashbaord UCS サーバ ファームウェア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 UCS サーバ ファームウェア 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。
- UCS サーバ ファームウェアを更新するには、UCS サーバ ファームウェアのアップグレードに使用される vKVM を実行するために、ブラウザや Java ソフトウェア バージョンを更新する必要がある場合もあります。

UCS サーバ ファームウェア バージョンをアップグレードしても、Nexus Dashboard ノードがトラフィックのデータ パスに含まれていないため、実稼働ネットワークには影響しません。

Nexus Dashboard UCS サーバ ファーム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。

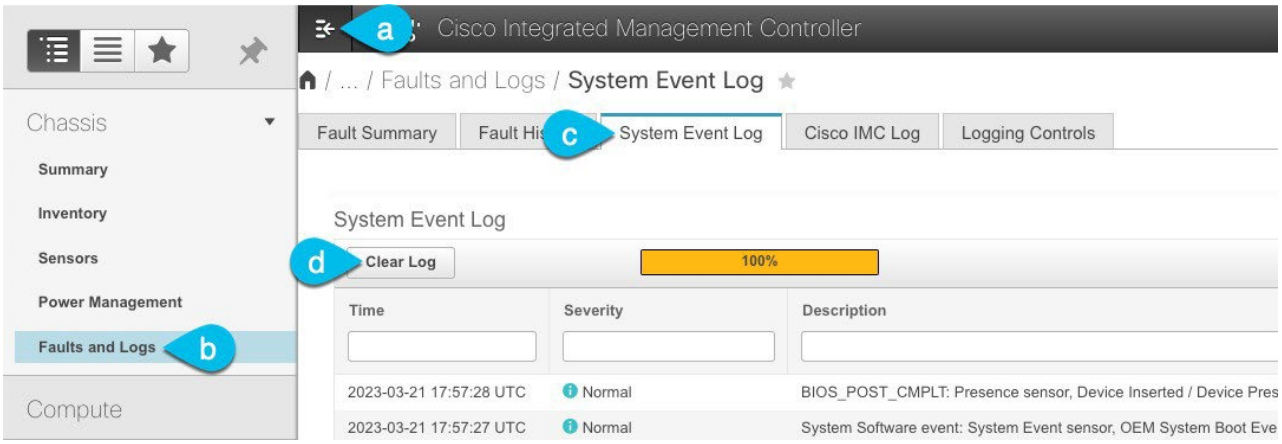
   CIMCのクレデンシャルは、Nexus Dashboard GUIのクレデンシャルとは異なる場合があること

   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。



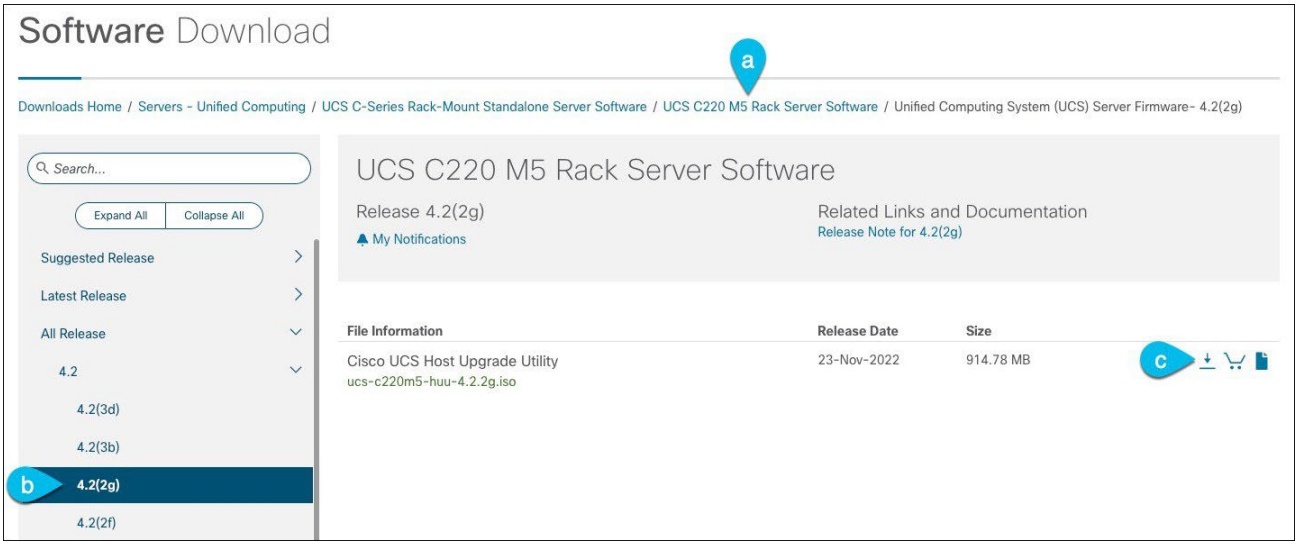
a. ハンバーガーメニューをクリックして、使用可能なオプションを表示します。

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。

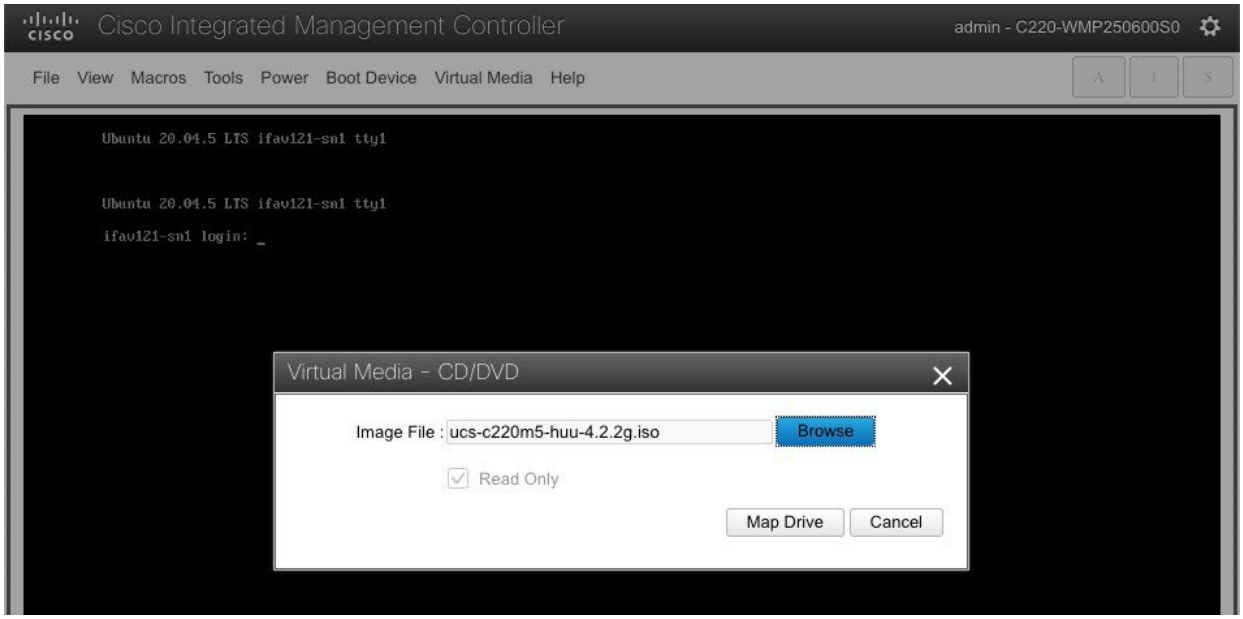
c. メイン ペインで、ダウンロード アイコンをクリックします。

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

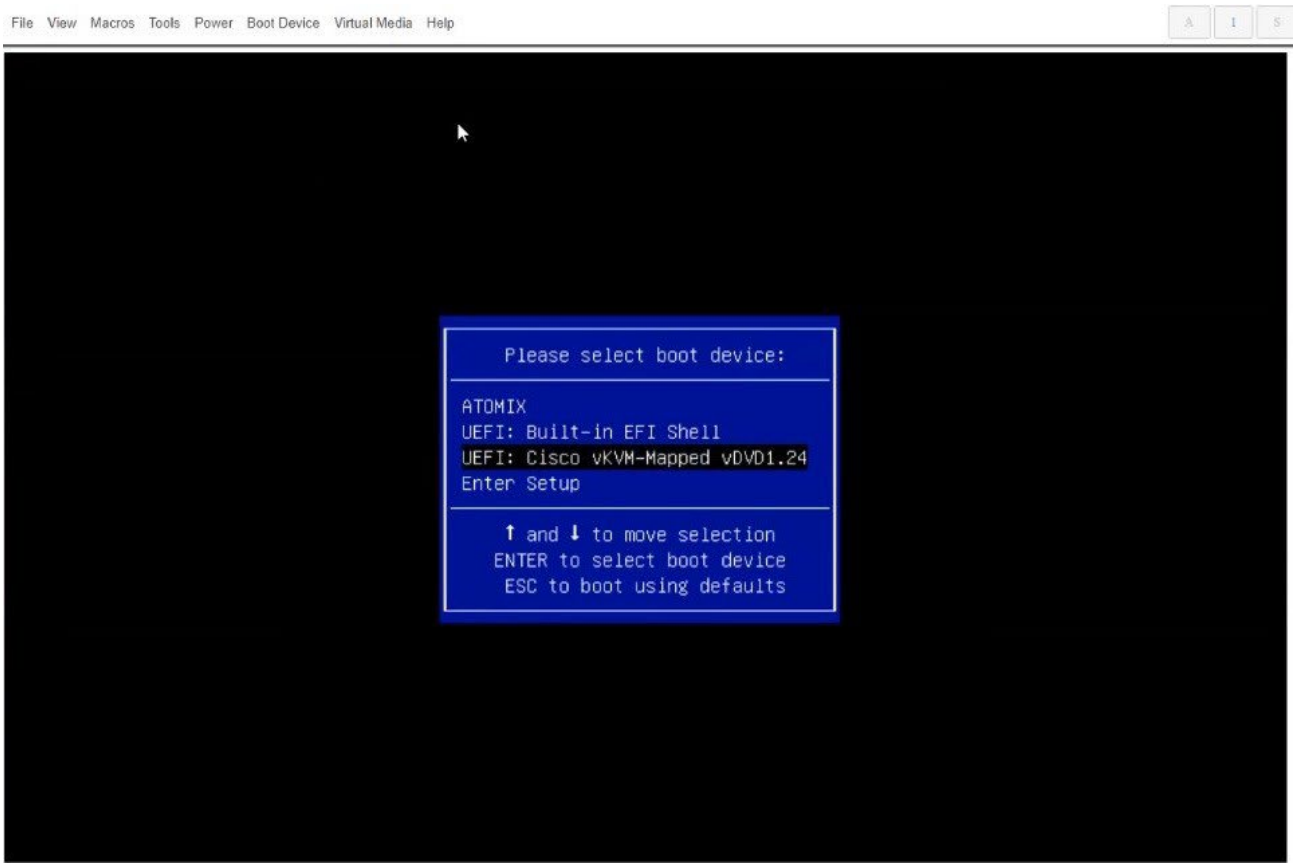
5. CIMC GUIからKVMコンソールを起動します。

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。

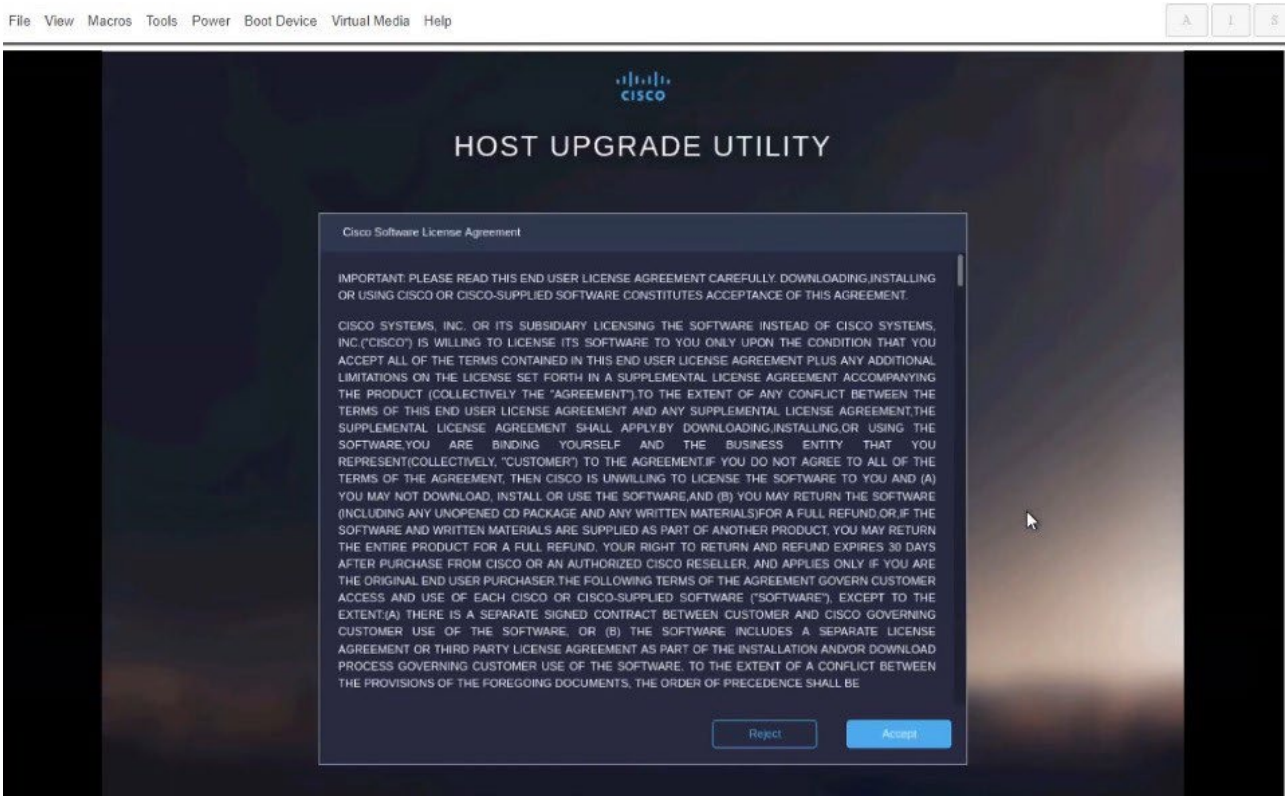
6. ステップ3でダウンロードしたHUU ISOイメージをマウントします。
   a. KVMコンソールの **[仮想メディア（Virtual Media）]** メニューから、**[仮想デバイスのアクティブ化（Activate Virtual Devices）]**を選択します。これにより、**[仮想メディア]** メニューに 仮想メディア のオプションが追加されます。
   b. KVM コンソールの **[仮想メディア]** メニューから、**CD/DVD**のマッピング を選択します。
   c. 表示された **[仮想メディア - CD/DVD]** ダイアログで、**[参照（Browse）]**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



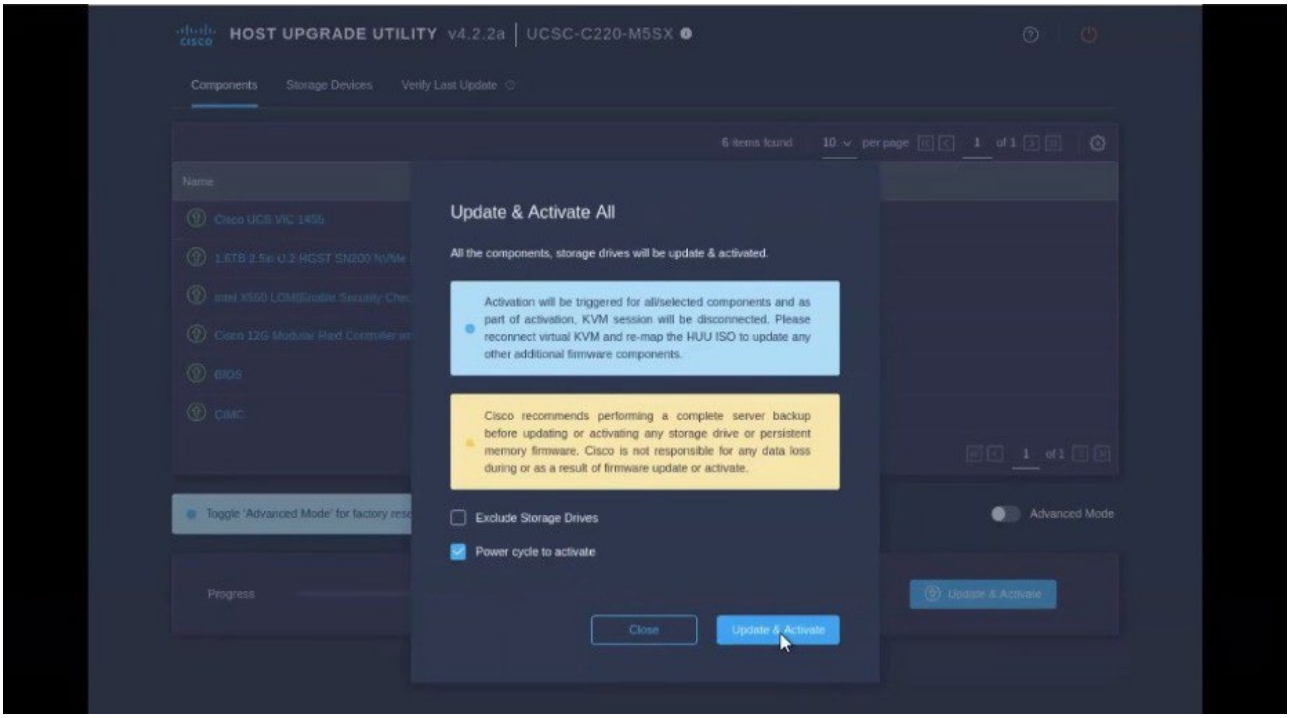
   d. 最後に、 **[マップ ドライブ（Map Drive）]** をクリックします。
7. KVM コンソールの **[電源（Power）]** メニューから、**[システムの電源再投入（Power Cycle System）]** を選択してサーバーを再起動します。
8. サーバーが起動しているときに、 **F6** を押してブートメニューを表示し、 **Cisco vKVM-Mapped vDVD** を選択します。



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、Cisco ホスト アップグレード ユーティリティ（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

Nexus Dashboard 3.1.1k で手動アップグレードを実行する場合は、Cisco TAC に連絡して、今後のアクションに関するガイダンスを入手してください。

クラスタのアップグレードには、「ファームウェア管理（クラスタの アップグレード）」（#_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. 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。

8. 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、「セカンダリ 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「クラスタの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、ファブリック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) ポートとウェブを使用する必要があるため、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。

- サポートされているバージョンの Cisco UCS サーバーファームウェアを実行していることを確認します。

  サポートされている UCS サーバ ファームウェア 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。

  UCS サーバファームウェアのアップグレードの詳細については、「UCS サーバ ファームウェアのアップグレード」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。

1	イメージのリモート ロケーションを入力します（たとえは、http://172.31.131.47/nd- dk9.2.0.1.iso）。
2	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。
3	インターフェイスの場合は、最初の管理ポート（enp1s0f0）を入力します。「enp1s0f0」と「enp1s0f1」は ND-NODE-L4 サーバーの管理ポートですが、「eno1」と「eno2」 は ND-NODE-G2 サーバーの管理ポートです。
4	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。

5	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。

```
+ read -r -p '?' url
? http://172.31.131.47/nd-dk9.2.0.1.iso (1)
+ '[' http://172.31.131.47/nd-dk9.2.0.1.iso = skip ']'
+ '[' http://172.31.131.47/nd-dk9.2.0.1.iso = '' ']'
+ '[' http = nfs: ']'
+ echo http://172.31.131.47/nd-dk9.2.0.1.iso
+ grep -q '\[.\]'
++ 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 (2)
+ 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
構成するインターフェイス：enp1s0f0 (3)
+ read -p 'address: ' addr
address: 172.23.53.59/21 (4)
```

```
+ read -p 'gateway: ' gw
gateway: 172.23.48.1 (5)
+ 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
```

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。

   が展開されたら、「 セカンダリ 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. 「Nexus Dashboard Operations」の「バックアップと復元」の説明に従って、Nexus Dashboard クラスタ構成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. 『 Nexus Dashboard Operations』の「バックアップと復元」の説明に従って、Nexus Dashboard 構成を復元します。
6. 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**　Guide の **[操作] > [バックアップと復元]**

を参照してください。

クラスタでのダイナミックリカバリの実行

セクションでは、バックアップクラスタを使用してプライマリ クラスタをダイナミックに回復する方法について説明します。この場合、1 つのクラスタは基本的にプライマリ（現用系）クラスタであり、2 番目のクラスタはバックアップ（スタンバイ）クラスタです。この状況では、2 番目のクラスタは最初のクラスタのバックアップとして特に使用できます。最初のクラスタが使用できなくなった場合、2 番目のクラスタは最初のクラスタから復元に常に使用できます。ND リリース 3.2.1 で導入された統合バックアップ機能の詳細については、「*Nexus Dashboard およびサービスの統合バックアップと復元*」の項目を参照してください。

次のセクションでは、クラスタをセットアップし、クラスタが使用できなくなった場合にダイナミックリカバリを実行するために必要な情報を提供します。

- クラスタでのダイナミックリカバリの実行に関する注意事項と制限事項
- 準備作業
- 暗号化キーの処理
- リモート ロケーションの構成
- プライマリ クラスタのバックアップ
- プライマリ クラスタの復元
- リカバリ後のタスク

クラスタでのダイナミック リカバリの実行に関する注意事項と制限事項

この状況でクラスタをダイナミックに回復する場合は、次のガイドラインと制限事項が適用されます。

- クラスタでのダイナミック リカバリの実行は、次の状況でサポートされます。
  - このダイナミック リカバリ手順では、3+3（2 つのクラスタのそれぞれに 3 つのマスターノード）または 5+5クラスタ構成のみがサポートされます。各クラスタ内のノードは、pND（物理 Nexus Dashboard）または vND（仮想 Nexus Dashboard）ノードのいずれかになります。
  - 各クラスタで異なるアプリケーションが実行されており、One ビューを介して複数のクラスタ間の接続を確立している共同ホストクラスタ。これらのタイプのクラスタでダイナミック リカバリを実行する場合は、リカバリ後のタスクで説明されているように、特定のリカバリ後のタスクを実行する必要があることに注意してください。
  - One Manage で作成されたマルチクラスタ ファブリック。詳細については、『*Managing and Monitoring Multi-Cluster Fabrics Using One Manage*』を参照してください。これらのタイプのクラスタでダイナミック リカバリを実行する場合は、リカバリ後のタスクで説明されているように、特定のリカバリ後のタスクを実行する必要があることに注意してください。
- クラスタでのダイナミック リカバリの実行は、次の状況ではサポートされません。
  - ストレッチ クラスタ。ストレッチ クラスタでは、標準規格のバックアップおよび復元オプションのみがサポートされます。

準備作業

プライマリクラスタのダイナミック リカバリに使用できるバックアップ クラスタを変更情報 に 基づいて 、 時間帯 を 自ダイナミック に設定します。「 Cisco Nexus Dashboard およびサービスの展開とアップグレード

ガイド」を参照してください。

プライマリ クラスタとバックアップ クラスタを構成する場合：

- クラスタが、「クラスタでのダイナミック リカバリの実行に関する ガイドラインと制限事項」に記載されているガイドラインに準拠していることを確認します。
- プライマリ クラスタとバックアップクラスタの両方で同じ数のノードを活用します（3 + 3 または 5 + 5クラスタ構成）。
- One Manage で作成されたマルチクラスタファブリックがある場合は、プライマリクラスタとバックアップクラスタの両方に同じ名前を使用して、プライマリクラスタのダイナミックリカバリを可能にします。リカバリ プロセスが完了したら、プライマリ クラスタに最初に使用されていたのと同じクラスタ名でスタンバイクラスタを起動します。
- 2 つのクラスタ間で通信を設定する必要はありません。バックアップ クラスタは、プライマリ クラスタの最後のバックアップを使用してプライマリ クラスタをダイナミックにリカバリできるようにするためだけに存在します。
- プライマリ クラスタとバックアップクラスタ間、および同じクラスタ上で共同ホストされるサービス間の IP アドレスのガイドラインは、いくつかの要因によって異なります。
  - 管理ネットワークの IP アドレスは、2 つのクラスタ間で異なっている必要があります。
  - クラスタでサービスを共同ホスティングしている場合は、データネットワークと永続 IP アドレスも 2 つのクラスタ間で異なっている必要があります。ただし、クラスタでサービスを共同ホスティングしていない場合は、データネットワーク IP アドレスと永続 IP アドレスを同じにすることも、2 つのクラスタ間で異なるものにすることもできます。
  - 2 つのクラスタがレイヤ 2 隣接の場合は、ノードごとに異なる永続 IP アドレスを使用する必要があります。
  - Nexus Dashboard Insights と Nexus Dashboard Fabric Controller が同じクラスタで共同ホストされている場合、通常、クラスタの 2 つのサービスに対して同じ永続 IP アドレスを使用できます。ただし、将来のある時点でクラスタでダイナミックリカバリを実行する必要がある可能性があるため、ダイナミックリカバリ後に永続 IP アドレスが重複しないように、サービス間で異なる永続 IP アドレスを使用することをお勧めします。この場合、ダイナミック回復後は永続 IP アドレスが異なることに注意してください。

暗号化キーの処理

バックアップ プロセスの特定の時点で、バックアップ ファイルの暗号化に使用される暗号化キーを入力するように求められます。後でその同じ暗号化キーを使用して、そのバックアップを復元します。

バックアップ プロセスの一部として暗号化キーを入力する場合は、その暗号化キー情報を失わないようにする必要があります。暗号化キーが失われた場合、その暗号化キーがないとバックアップを復元できないため、バックアップは役に立ちません。

リモート ロケーションの構成

リモート ロケーション情報は、統合バックアップと復元を含む、リモート ロケーションを使用するすべての機能によって参照されます。

1. ND GUI で、**[管理（Admin）] > [システム設定（System Settings）]** に移動し、**[リモート ロケーション（Remote Locations）]** タブをクリックします。

- リモート ロケーションがまだ作成されていない場合は、[リモート ロケーションが見つかりません（No Remote Locations Found）] というメッセージがページに表示されます。
- リモート ロケーションがすでに作成されている場合は、それらのリモート ロケーションが次の値でリストされます。

フィールド	説明
名前（Name）	リモート ストレージ ロケーションの名前。
ホスト	リモート ストレージ ロケーションの IP アドレス。
プロトコル	リモート ストレージ ロケーションのタイプ： ・NASストレージ ・SFTP
[ユーザ名（Username）]	リモート ロケーションのユーザー名。
Remote Path	リモート ホスト ロケーションへの絶対ファイル パス。

2. **[リモート ロケーションの追加（Add Remote Location）]**

   または **[リモート ロケーションの作成（Create Remote Location）]** をクリックします。**[リモート ストレージ ロケーションの作成（Create Remote Storage Location）]** ウィンドウが表示されます。

3. リモート ストレージ ロケーションの構成に必要な情報を入力します。

フィールド	説明
名前（Name）	リモート ストレージ ロケーションの名前を入力します。
説明	（オプション）リモート ストレージ ロケーションの説明を入力します。
リモート ストレージ ロケーションのタイプ	リモート ストレージ ロケーションのタイプの選択： ・NASストレージ ・SFTP/SCPサーバー

- 上記の [リモート ストレージ ロケーション タイプ（Remote Storage Location Type）] フィールド で [NAS ストレージ（ NAS Storage）]を選択した場合は、次の表の情報を活用します。

フィールド	説明
[プロトコル（Protocol）] リモート保管場所を読み取り/書き込みまたは 読み取り専用のどちらにするかを選択します。 ・[読み取り/書き込み（Read Write）]：このオプションを使用して、バックアップは書き込みと復元の両方が可能。 ・[読み取り専用（Read Only）]：以前に作成したバックアップを復元のみする必要がある場合は、このオプションを選択します。	ホスト名
リモート ストレージ ロケーションのホスト名を入力します。	ポート
リモート ホスト ロケーションのポートを入力します。	エクスポート パス
リモート ホスト ロケーションのエクスポート パスを入力します。	アラートしきい値
リモート ホスト ロケーションのアラートしきい値を入力します。	制限(Mi/Gi)
Kubernetes PVC を介して NAS で要求できるストレージの量を制限するために使用されます。NAS の実際のサイズは、この値と異なる場合があります。 エントリの例： 300Mi 10Gi	許可アプリケーション

- 上記の **[**リモート ストレージ ロケーション タイプ（**Remote Storage Location Type**）**]** フィールドで **[SFTP/SCP** サーバー（ **SFTP/ SCP Server**）**]** を選択した場合は、次の表の情報を活用します。

フィールド	説明
プロトコル	リモート ストレージ ロケーションのファイル 転送に使用するプロトコルを選択します。 ・ SFTP ・ SCP
ホスト名 または IP アドレス	リモート ロケーションのホスト名または IP アドレスを入力します。
デフォルトパス	バックアップ ファイルが保存されるリモート サーバのパスを指定します。 パスはスラッシュ(/ または \)文字で始まるか、絶対パスである必要があります。例： /backups/multifabric ま たは： Users/backups/multifabric
リモートポート（Remote Port）	リモート ホスト ロケーションのリモート ポートを入力します。
許可タイプ	許可タイプを選択します。 ・ パスワード ・ SSHパブリックタイプ
ユーザー名	認証ユーザ名を入力します。
パスワード	上記の **[認証タイプ（Authorization Type）]** フィールドで **[パスワード（パスワード）]** を選択した場合に使用できます。認証パスワードを入力します。
SSHキー	上記の **[認証タイプ（Authorization Type）]** フィールドで **[SSH パブリック タイプ（SSH Public Types）]** を選択した場合は、**[SSH キー（SSH Key）]** フィールドと **[パスフレーズ（Passphrase）]** フィールドを使用できます。 SSH キーを使用するには、次の手順を実行する必要があります。 1. 秘密キーと公開キーのペアを生成します（パスフレーズの有無にかかわらず）。 2. リモート ロケーションで生成された公開キーを承認します。 3. **[SSH Key]** フィールドに秘密キーを入力します。 4. **[パスフレーズ（Passphrase）]**フィールドにパスフレーズ（ステップ 1 で使用した場合）を入力します。
パスフレーズ	

4. **[保存（Save）]** をクリックします。

   [リモート ロケーション（Remote Locations）] ページに戻り、新しく作成されたリモート ロケーションがテーブルに表示されます。

- リモート ロケーション エントリを編集するには、そのリモート ロケーションのテーブルの行の末尾にある省略記号（**...**）をクリックし、**[編集（Edit）]** をクリックします。
- リモート ロケーション エントリを削除するには、テーブル内のそのリモート ロケーションの行の末尾にある省略記号（**[...]**）をクリックし、**[削除]** をクリックします。

プライマリ クラスタのバックアップ

プライマリ クラスタが使用できなくなったイベントにバックアップを使用してプライマリ クラスタを回復できるように、次の手順を活用してプライマリ クラスタをバックアップします。リカバリ プロセスは、バックアップ クラスタに関する正しい最新の情報に依存するため、次の手順を使用して現用系クラスタのバックアップを頻繁に実行します。

ここでは、プライマリ クラスタをバックアップする方法について説明します。

- プライマリ クラスタの手動バックアップ
- スケジュール バックアップの構成
- バックアップ履歴の表示

プライマリ クラスタの手動バックアップ

1. プライマリ クラスタの ND GUI にログインします。
2. 管理コンソール GUI の統合バックアップと復元ページに移動します。

   [管理（Admin）] > [バックアップと復元（Backup and Restore）]

   すでに構成されているバックアップは、**[バックアップ（Backups）]** ページに表示されます。
3. **[バックアップの作成（Create Backup）]**をクリックします。

   [バックアップの作成（Create Backup）] ペインが表示されます。
4. **[現在の展開モード（Current Deployment Mode）]** エリアに表示される情報を確認します。

   このエリアには、この Nexus Dashboard で現在実行されているサービスが表示されます。統合バックアップと復元では、このエリアに表示されるすべてのサービスがバックアップされることに注意してください。 Nexus Dashboard 内でバックアップする個々のサービスを選択することはできません。
5. **[名前（Name）]** フィールドで、このバックアップの名前を入力します。
6. **[タイプ（Type）]** フィールドで、[構成のみ（Config-Only）] または [フル（Full）] バックアップのどちらが必要かを決定します。
   - **Config-Only**：Config-Only バックアップは、以下で説明するフル バックアップよりも小さくなります。バックアップされるサービスに応じて、次の構成データが含まれます。
     - Insights：順守ルール、設定、およびその他の構成済みパラメータ
     - Orchestrator：テンプレート、設定、およびその他の構成済みパラメータ。
     - ファブリック コントローラ（Fabric Controller） ：スケジュール、テンプレート、ポリシー、およびその他の構成済みパラメータ。
   - **[完全（Full）]**：完全バックアップは大規模です。構成のみのバックアップのすべてに加えて、フル バックアップには、統計、カウンタなどの運用データも含まれます。運用データはファブリック コントローラにのみ適用され、他のサービスでは構成のみがバックアップされます。

     [完全（Full）] バックアップ タイプを使用して保存されたバックアップを復元する場合は、構成のみの復元または完全な復元のいずれかを実行できます。既存の構成があるクラスタでは完全復元を実行できないことに注意してください。この場合、既存の構成がない新しいクラスタでバックアップを復元する必要があります。

7. **[接続先（Destination）]**フィールドで、**[リモート ロケーション（Remote Location ）]** を選択して、リモート ロケーションにバックアップ データを保存します。
   この状況では、ローカル バックアップを設定しないでください。バックアップ ファイルは、使用できなくなった場合にこれらのダイナミック リカバリ手順を使用して回復する必要があるクラスタ上でローカルではなく、リモートの場所で使用できる必要があるためです。

   a. **[リモート ロケーション（Remote Location ）]** フィールドで、リストからすでに構成されているリモート ロケーションを選択するか（使用可能な場合）、**[リモート ロケーションの作成（Create Remote Location）]** をクリックします。

      [リモート ロケーションの作成（Create Remote Location）] をクリックした場合は、「リモート ロケーションの構成（Configuring Remote Locations）」の手順に従ってから、ここに戻ります。

   b. **[リモート パス（Remote Path）]** フィールドに、リモート バックアップのリモート経路を入力します。

   c. **[暗号キー（Encryption Key）]** フィールドにバックアップ ファイルに対する暗号キーを入力します。

      バックアップから復元するには、暗号化キーが必要です。詳細については、「 暗号化　キー の処理」を参照してください。

8. **[すぐにバックアップ（Backup Now）]** をクリックします。

   メインの **[バックアップ（Backups）]** ページに戻り、構成したバックアップが表示されます。

9. **[ステータス（Status）]** 列に表示される情報を活用して、バックアップのステータスをモニターします。

   バックアップの進行中は、最初はバックアップのステータスとして **[進行中（In Progress）]** と表示されます。**[詳細の表示（View Details）]** をクリックして、バックアップされている領域の詳細とバックアップの進行状況を表示します。

   しばらくすると、[ステータス（Status）] が最初に 100% に変わり、その後 **[成功（Success）]** に変わります。

10. **[名前（Name）]** 列のリンクをクリックすると、この特定のバックアップに含まれるサービスや、実行されたバックアップのタイプ（構成のみまたはフル）など、そのバックアップに関する追加情報がディスプレイれます。

    [アクション（Actions）] ドロップダウンをクリックして、このウィンドウから次のアクションを実行することもできます。

    - 削除（ 削除） ：バックアップを削除するには、このオプションを選択します。
    - ダウンロード（**Download**） ：バックアップをローカル フォルダにダウンロードするには、このオプションを選択します。
    - 復元（**Restore**） ：バックアップされた構成を復元するには、このオプションを選択します。詳細については、「プライマリ クラスタ の 復元 」を参照してください。

メインの **[バックアップ（Backups）]** ページで、リストされている任意のバックアップの省略記号（[...]）をクリックして、任意のバックアップに対して同じアクションを実行することもできます。

スケジュール バックアップの構成

1. プライマリ クラスタの ND GUI にログインします。

2. 管理コンソール GUI の統合バックアップと復元ページに移動します。

   [管理（Admin）] > [バックアップと復元（Backup and Restore）]

   すでに構成されているバックアップは、**[バックアップ（Backups）]** ページに表示されます。

3. **[バックアップ スケジュール（Backup Schedules）]** タブをクリックします。
   構成済みのスケジュールされたバックアップが一覧表示されます。

4. **[バックアップ スケジュールの作成（Create Backup Schedule）]**をクリックします。

   [バックアップの作成（Create Backup）] スライダが表示されます。

5. **[現在の展開モード（Current Deployment Mode）]** エリアに表示される情報を確認します。

   このエリアには、この Nexus Dashboard で現在実行されているサービスが表示されます。統合バックアップと復元では、このエリアに表示されるすべてのサービスがバックアップされることに注意してください。 Nexus Dashboard 内でバックアップする個々のサービスを選択することはできません。

6. **[名前（Name）]** フィールドで、このバックアップの名前を入力します。
7. **[タイプ（Type）]** フィールドで、[構成のみ（Config-Only）] または [フル（Full）] バックアップのどちらが必要かを決定します。
   - **Config-Only**：Config-Only バックアップは、以下で説明するフル バックアップよりも小さくなります。バックアップされるサービスに応じて、次の構成データが含まれます。
     - Insights：コンプライアンス ルール、設定、およびその他の構成済みパラメータ
     - Orchestrator：テンプレート、設定、およびその他の構成済みパラメータ。
     - Fabric Controller：スケジュール、テンプレート、ポリシー、およびその他の構成済みパラメータ。
   - **Full**：完全バックアップは大規模です。構成のみのバックアップのすべてに加えて、フル バックアップには、統計、カウンタなどの運用データも含まれます。運用データはファブリック コントローラにのみ適用され、他のサービスでは構成のみがバックアップされます。

     [フル（Full）] バックアップ タイプを使用して保存されたバックアップを復元する場合は、構成のみの復元またはフルの復元のいずれかを実行できます。既存の構成があるクラスタでは完全復元を実行できないことに注意してください。この場合、既存の構成がない新しいクラスタでバックアップを復元する必要があります。

8. **[リモート ロケーション（Remote Location）]** フィールドで、リストからすでに設定されているリモート ロケーションを選択するか（使用可能な場合）、**[リモート ロケーションの作成（Create Remote Location）]** をクリックします。

   [リモート ロケーションの作成（Create Remote Location）] をクリックした場合は、「リモート ロケーションの構成（Configuring Remote Locations）」の手順に従ってから、ここに戻ります。

9. **[リモート パス ファイル名（Remote Path Filename）]** フィールドに、リモートバックアップのリモート経路を入力します。
10. **[暗号キー（Encryption Key）]** フィールドにバックアップ ファイルに対する暗号キーを入力します。

    バックアップから復元するには、暗号キーが必要です。詳細については、「暗号化 キー の処理」を参照してください。

11. **[スケジューラ（Scheduler）]**エリアで、バックアップ スケジュールに使用する日時を選択します。

12. **[**頻度（**Frequency**）**]**エリアで、スケジュールされたバックアップの頻度を設定します。
    - 毎日
    - 7日ごと
    - 30日ごと
13. [作成（Create）] をクリックします。

    [バックアップ スケジュール（**Backup Schedules**）**]** ページに戻り、テーブルに新しく作成されたバックアップ スケジュール
    がリストされます。

[名前（**Name**）**]** 列のエントリをクリックすると、スケジュール済みバックアップの詳細を表示できます。**[**接続先（**Destination**）**]** 列のエントリをクリックして、リモート ロケーションの詳細を表示することもできます。

- バックアップ スケジュール エントリを編集するには、そのバックアップ スケジュール エントリのテーブルの行の末尾にある省略記号（**...**）をクリックし、**[**編集（**Edit**）**]** をクリックします。
- バックアップ スケジュール エントリを削除するには、そのバックアップ スケジュール エントリのテーブルの行の末尾にある省略記号（**[...]**）をクリックし、**[**削除（**Delete**）**]** をクリックします。

バックアップ履歴の表示

1. プライマリ クラスタの ND GUI にログインします。
2. 管理コンソール GUI の統合バックアップと復元ページに移動します。

   [管理（**Admin**）**] > [**バックアップと復元（**Backup and Restore**）**]**

   すでに構成されているバックアップは、**[**バックアップ（**Backups**）**]** ページに表示されます。
3. **[**履歴（**History**）**]**タブをクリックします。

   バックアップの履歴が次の情報とともに表示されます。
   - **[**名前（**Name**）**]** : バックアップの名前。
   - **[**日付（**Date**）**]** : バックアップに関してアクションが実行された日付。
   - **[**アクション（**Action**）**]** : バックアップに対して実行されたアクション（作成済み、削除済み、ダウンロード済み、 復元済み、 更新済みなど）。
   - **[**タイプ（**Type**）**]** : バックアップのタイプ（**[Config-Only**] または [**Full**]）。
   - **[**詳細（**Details**）**]** : 特定のバックアップに関する追加の詳細。
   - **[**ユーザー（**User**）**]** : 特定のバックアップに関連付けられているユーザー。
   - **[**ステータス（**Status**）**]** : **[**成功（**Success**）**]**、 **[**進行中（**In Progress**）**]**、**[**失敗（**Failure**）**]** などのバックアップのステータス。

プライマリ クラスタの復元

プライマリクラスタが使用できなくなった場合は、次の手順に従って、そのプライマリクラスタをバックアップ（スタンバイ）クラスタに回復します。

1. バックアップ（スタンバイ）クラスタの ND GUI にログインします。

2. 管理コンソール GUI の統合バックアップと復元ページに移動します。

   [管理（Admin）] > [バックアップと復元（Backup and Restore）]

   すでに構成されているバックアップは、**[バックアップ（Backups）]** ページに表示されます。

   プライマリ クラスタのバックアップは、バックアップ （スタンバイ）クラスタには 表示されません。この状況では 、 リモート ロケーションからバックアップ ファイル にアクセスするか、ローカルにアップロードする必要が あります。

3. 次のいずれかの方法を使用して、**[復元（Restore）]** スライダ ページにアクセスします。
   - 復元するバックアップの省略記号（[...]）をクリックし、**[復元（ 復元 ）]**を選択します。または、
   - メインの **[バックアップと復元（Backup and Restore）]** ページの右上隅にある

     [復元（Restore）] をクリックします。**[復元（Restore）]** スライド ページが表

     示されます。

4. **[送信元（Source）]** フィールドで、復元するバックアップの場所を決定します。

   特定のバックアップの省略記号（[...]）をクリックしてバックアップを復元する場合、このフィールドは編集できません。

   a. **[リモート ロケーション（Remote Location）]** フィールドで、リストからすでに構成されているリモート ロケーションを選択するか（使用可能な場合）、**[リモート ロケーションの作成（Create Remote Location）]** をクリックします。

      [リモート ロケーションの作成（Create Remote Location）] をクリックした場合は、「リモート ロケーションの構成（Configuring Remote Locations）」の手順に従ってから、ここに戻ります。通常はリモート バックアップ プロセスの一部としてリモート ロケーションを設定しますが、リモート バックアップを設定したクラスタとは異なるクラスタにいるため、復元プロセスの一部としてリモート ロケーションを設定する必要がある場合があります。この場合、この時点でリモート ロケーションを再度設定します。これにより、システムは、他のクラスタで設定したリモート バックアップを検出できるようになります。

   b. **[リモート パス（Remote Path）]** フィールドに、リモート バックアップが存在するリモート経路を入力します。

5. **[暗号キー（Encryption Key）]** フィールドにバックアップ ファイルに対する暗号キーを入力します。

   詳細については、「暗号化キーの処理」を参照してください。

6. [検証（Validation）]エリアのバックアップの行で、**[検証してアップロード（Validate and Upload）]** をクリックします。

   誤った暗号化キーを入力した場合は、検証プロセス中にエラーが発生したことを示すエラー メッセージが表示されます。バックアップ ファイル名が表示されている回線のごみ箱をクリックして検証試行を削除し、再試行します。

7. 検証の進行状況バーに 100% が表示されると、**[次へ（Next）]** ボタンが現用系になります。クリックします。
   [次へ（Next）] をクリックします。

[復元（Restore）] ウィンドウが表示され、次の情報が表示されます。

- 現在の展開モード
- バックアップ ファイルの展開モード。復元プロセスが完了した後のシステムの展開モードになります。
- バックアップ ファイルが最初に設定されたときに使用されたバックアップのタイプ

8. （オプション）**[外部サービス IP 構成を無視する（Ignore External Service IP Configuration）]** チェックボックスをオンにします。

   [外部サービスの IP 構成を無視する（Ignore External Service IP Configuration）] チェック ボックスがオンになっている場合、外部サービスの IP 構成は無視されます。この選択により、システムでバックアップを作成し、それを別の管理サブネットやデータ サブネットを持つ別のシステムに復元することができます。

9. **[復元（Restore）]** をクリックします。
   復元プロセスを開始することを確認する警告ウィンドウが表示されます。復元プロセスの実行中は、Nexus Dashboard の機能にアクセスできません。復元プロセスには数分かかる場合があります。

10. 警告ウィンドウで **[復元（Restore）]** をクリックして、復元プロセスを続行します。

    別のウィンドウが表示され、復元プロセスの進行状況が表示されます。**[タイプ（Type）]** 列のエントリの横にある矢印をクリックすると、復元プロセスの詳細が表示されます。

11. 復元プロセスが成功すると、[進行状況（Progress）] に 100% が表示され、**[履歴の表示（View History）]**
    ボタンが現用系になります。

    [履歴の表示（View History）] をクリックして **[バックアップと復元（Backup and Restore）]** ウィンドウの **[履歴（History）]**エリアに移動すると、復元プロセスが表示され、**[ステータス（Status）]** 列に **[成功（Success）]** と表示されます。

プロセスのこの時点で、スタンバイ クラスタには、以前プライマリクラスタにあった回復された情報が含まれている必要があります。リカバリの完了後に必要なタスク を完了するには、「リカバリ後のタスク」に進みます。

リカバリ後のタスク

ダイナミック リカバリ タスクを完了し、プライマリ クラスタの設定情報をスタンバイ クラスタにリカバリした後、不要な問題を回避するために、次のリカバリ後のタスクを実行します。

- 各クラスタで異なるアプリケーションが実行されている共同ホスト クラスタがあり、One ビューを介して複数のクラスタ間の接続を確立している場合は、そのプライマリ クラスタをバックアップに回復した後に、One ビューを使用してクラスタを再登録する必要があります。

  たとえば、サービスを共同ホスティングしていて、1 つのクラスタに NDI サービスがあり、別のクラスタに NDFC サービスがあるとします。NDI サービスを使用するクラスタが使用できなくなった場合は、そのクラスタを復元した後、One ビューを使用してクラスタを NDI サービスに再登録する必要があります。これらの手順については、 Nexus Dashboard Infrastructure Management の「Multi-Cluster Connectivity」セクションを参照してください。

- One Manage で作成されたマルチクラスタ ファブリックがある場合、プライマリ クラスタまたは One ビューを介してマルチクラスタ接続でセットアップされたメンバー クラスタでダイナミック リカバリが実行されると、そのファブリックのリカバリ プロセスが完了した後クラスタを使用する場合は、

クラスタをプライマリ クラスタに再登録する必要があります。

- プライマリ クラスタがリカバリ プロセスを実行した場合は、すべてのメンバー クラスタをプライマリ クラスタに再登録します。
- メンバー クラスタがリカバリ プロセスを実行した場合は、そのメンバー クラスタのみをプライマリ クラスタに再登録します。

これらの手順については、『Cisco Nexus Dashboard and Services Deployment and Upgrade Guide』を参照してください。

- 同じクラスタで NDI と NDFC を共同ホストしている場合は、クラスタが回復した後、最初にクラスタをワイプし、必要に応じてメンバー クラスタを再登録してから、 Nexus Dashboard Insights で再同期を実行します。が変更されました。

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、「システム設定」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
```

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 構成のインポート後にサイトに接続できない

Cisco APIC ファブリックを 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 構成が更新されます。その後、APIC で以前の構成をインポートすると、ファブリックが 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。

Cause

以前のファブリック構成には、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。

解像度

ファブリックが Nexus Dashboard にオンボーディングされた後、今後の構成の復元のために APIC 構成をエクスポートすることをお勧めします。

問題を発生後に解決するには、Nexus Dashboard GUI でファブリックを再登録できます。

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**）**] > [**ファブリック（**Fabrics**）**]** に移動します。
3. ファブリックの横にある **[**アクション （**...**） **]** メニューから、**[**ファブリックの編集（**Edit Fabric**）**]** を選択します。
4. **[**ファブリック 編集（**Fabric Edit**）**]** 画面で、[ファブリックの再登録（Re-register Fabric）] チェックボックスをオンにして、ファブリックの詳細を再度入力します。
5. **[**保存（**Save**）**]** をクリックします。

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、Replacing Single Primary Node with Standby Node 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。

   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。

Nexus Dashboard Insights を実行している場合、ノードを置き換えた後で、Nexus Dashboard Insights を無効にしてから再度有効にします。サービスを新しいノードに適切に再配布するには、Nexus Dashboard Insights を再起動する必要があります。

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、「Re-Adding Same Primary Node to Physical Cluster」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。
- 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。
- 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。
- UCS-C225-M6（ND-NODE-L4）ノードと ACI ファブリックを含むクラスタで 3.1.1k ソフトウェアの新規仮想メディア インストールを実行すると、NDI または NDO へのファブリックのオンボーディングが失敗するという既知の問題が存在します。 。この問題の回避策は、ソフトウェアの **3.1.1l** バージョンの新規インストールを実行することです。リリース 3.1.1k から 3.1.1l にアップグレードしても問題は解決しないので、注意してください。この問題を解決するには、3.1.1l ソフトウェアの新規インストールを実行する必要があります。
- UCS-C225-M6（ND-NODE-L4）ノードと ACI ファブリックを含むクラスタで 3.1.1k ソフトウェアの新規仮想メディア インストールを実行すると、NDI または NDO へのファブリックのオンボーディングが失敗するという既知の問題が存在します。 この問題の回避策は、ソフトウェアの **3.1.1l** バージョンの新規インストールを実行することです。リリース 3.1.1k から 3.1.1l にアップグレードしても問題は解決しないので、注意してください。この問題を解決するには、3.1.1l ソフトウェアの新規インストールを実行する必要があります。

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. 新しいノードの **CIMC IP** アドレス、CIMC ログイン ユーザー名 、および パスワード を入力し、**[**確認（**Verify**）] をクリックします。

クラスタは新しいノードの管理 IP アドレスに接続し、接続を確認し、**[**シリアル ナンバー**]** フィールドに入力します。

7. **[**置換（**Replace**）**]** をクリックして、ノードの置換を完了します。
8. **[**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。

セカンダリ ノードまたはスタンバイ ノードの交換

機能不全が発生したセカンダリ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、まったく新しいセカンダリ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

- 置換するセカンダリ 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セカンダリ 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。

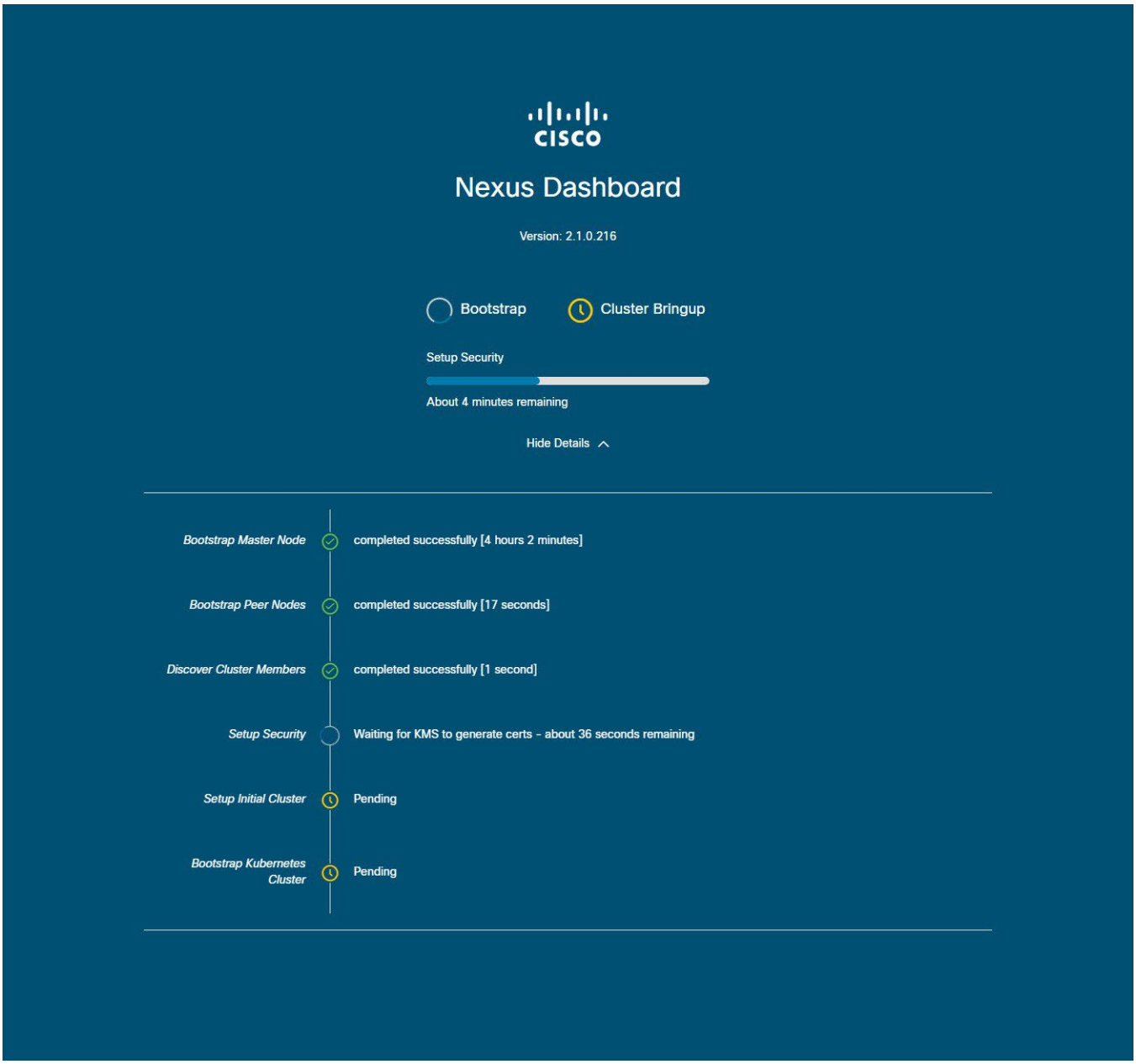
6. 「セカンダリ ノードの管理」または「スタンバイ ノードの管理」の説明に従い、新しいノードの電源をオンにして、新しいセカンダリノードまたはスタンバイノードとしてクラスタに追加します。

   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。



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. グループにクラスタを再度追加します。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 Dashboard 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構成手順は、「 xref:https://www.cisco.com/c/en/us/td/docs/dcn/nd/3x/articles-321/nexus- dashboard-admin-321.html#_securitySecurity] 」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）

秘密キーと自己署名証明書の生成

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、「CRS の作成、および CA 署名付き証明書の取得」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構成手順は、「 xref:https://www.cisco.com/c/en/us/td/docs/dcn/nd/3x/articles-321/nexus- dashboard-admin-321.html#_securitySecurity] 」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（**Infrastructure**）**] > [**ファブリック接続（**Fabric Connectivity**）**]** 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、そのファブリック/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 リストからファブリックを選択します。
   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（**Infrastructure**）**] > [**ファブリック接続（**Fabric Connectivity**）**]** に移動します。
5. BGW が存在するファブリックで **[**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、そのファブリック/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 リストからファブリックを選択します。
   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。

シスコが採用している 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：2024 年 3 月 1 日
最終更新日：2024 年 3 月 1 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