



DCNM から NDFC への移行

- [DCNM から NDFC への移行の前提条件と注意事項 \(1 ページ\)](#)
- [既存の DCNM 設定の NDFC への移行 \(4 ページ\)](#)

DCNM から NDFC への移行の前提条件と注意事項



- (注) ファブリック コントローラ サービスで Nexus Dashboard をすでに実行している場合は、このセクションをスキップし、代わりに [既存の ND クラスタをこのリリースへアップグレード](#) の説明に従ってアップグレードしてください。

DCNM 11.5(4) からのアップグレードは、次のワークフローで構成されます。

1. このセクションに記載されている前提条件とガイドラインが満たされていることを確認します。
2. ターゲット NDFC リリースに固有の移行ツールを使用して、既存の設定をバックアップします。
3. ファブリック コントローラ (NDFC) サービスを使用して、新しい Nexus Dashboard クラスタを展開します。



- (注)
- 以前のリリースでは、クラスタがすでに展開された後にサービスをインストールし、有効にする必要がありましたが、このリリースでは、統合インストールの導入により、クラスタの初期展開時にサービスを有効にすることに注意してください。
 - Nexus Dashboard クラスタをファブリック コントローラ (NDFC) サービスでのみ展開します。他のサービス (ファブリック コントローラ + Insights など) で展開しないでください。これを行うと、次の手順で構成バックアップを復元する際に、「バックアップファイルはこの展開モードと互換性がありません」というメッセージで移行が失敗します。

4. ステップ 1 で作成した設定のバックアップを復元します。



(注) アップグレードを実行する前に：

- 各ファブリックのクレデンシャルの検証
 - LAN ファブリックの場合、[Web UI] > [管理 (Administration)] > [クレデンシャルの管理 (Credentials Manage)] > [LAN のクレデンシャル (LAN Credentials)] ページで、各ファブリックを選択し、[検証 (Validate)] を選択して行います。
 - SAN ファブリックの場合、[Web UI] > [管理 (Administration)] > [クレデンシャルの管理 (Credentials Manage)] > [SAN のクレデンシャル (SAN Credentials)] ページで、各ファブリックを選択し、[検証 (Validate)] を選択して行います。
- Thousand Eyes 統合アプリケーションなどのアプリケーションを DCMN で実行している場合は、移行手順を進める前にそのアプリケーションを無効化にします。

ペルソナ互換性

適切なアップグレードツールを使用することで、次の表に示すように、ペルソナのために新しく展開された Nexus Dashboard Fabric Controller に、DCNM リリース 11.5(4) からバックアップされたデータを復元できます。

DCNM 11.5 (4) からのバックアップ	アップグレード後の NDFC でのペルソナの有効化
OVA/ISO/SE での DCNM 11.5 (4) ローカルエリアネットワーク (LAN) ファブリックの展開	ファブリック コントローラ + ファブリック ビルダー
OVA/ISO/SE での DCNM 11.5 (4) PMN の展開	ファブリック コントローラ + メディアの IP ファブリック (IPFM)
OVA/ISO/SE での DCNM 11.5 (4) SAN の展開	SAN コントローラ
Linux での DCNM 11.5 (4) SAN の展開	SAN コントローラ
Windows での DCNM 11.5 (4) SAN の展開	SAN コントローラ

アップグレード後の機能の互換性

次の表に、アップグレード後に DCNM 11.5(4) のバックアップから復元される機能に関連する注意点を示します。



(注) SAN Insights および VMM Visualizer 機能は、復元後に有効になりません。Nexus Dashboard ファブリック コントローラ UI の [設定 (Settings)] > [機能管理 (Feature Management)] ページで有効にするように選択できます。

DCNM 11.5 (4) の機能	アップグレードのサポート
構成された Nexus Dashboard Insights 詳細については、 Cisco Nexus Dashboard ユーザー ガイド を参照してください。	サポート対象
コンテナオーケストレータ (K8s) ビジュアライザ	サポート対象
vCenter による VMM の可視性	サポート対象
構成された Nexus Dashboard Orchestrator	未サポート
設定されたプレビュー フィーチャー	サポート対象外
SAN インストールの LAN スイッチ	サポート対象外
IPv6 で検出されたスイッチ	サポート対象外
DCNM トラッカー	サポート対象外
ファブリックのバックアップ	未サポート
レポート定義とレポート	未サポート
スイッチのイメージとイメージ管理ポリシー	サポート対象外
SAN CLI テンプレート	11.5(4)から繰り越されません
イメージ/イメージ管理データの切り替え	11.5(4)から繰り越されません
低速ドレイン データ	11.5(4)から繰り越されません
Infoblox 設定	11.5(4)から繰り越されません
エンドポイント ロケーションの設定	アップグレード後に、エンドポイント ロケータ (EPL) を再構成する必要があります。ただし、履歴データは最大 500 MB まで保持されます。
アラーム ポリシーの設定	11.5(4)から繰り越されません
パフォーマンス管理データ	アップグレード後、最大 90 日間の CPU/メモリ/インターフェイス統計情報が復元されます。
温度データ	温度データはバックアップに保存されないため、移行後に復元されません。移行後に温度データ収集を再度有効にする必要があります。

既存の DCNM 設定の NDFC への移行

このセクションでは、既存の DCNM 11.5(4) 設定をバックアップし、新しい Nexus Dashboard クラスタを展開し、設定を復元して移行を完了する方法について説明します。

手順

ステップ 1 アップグレードツールをダウンロードします。

- a) NDFC ダウンロードページに移動します。

<https://software.cisco.com/download/home/281722751/type/282088134/>

- b) **[最新のリリース (Latest Releases)]** リストで、ターゲットとするリリースを選択します。
c) 展開タイプに適したアップグレードツールをダウンロードします。

- NDFC リリース 12.2.2 の場合 :

DCNM 11.5(4) 展開タイプ	アップグレードツールのファイル名
ISO/OVA	DCNM_To_NDFC_12_2_2_Upgrade_Tool_OVA_ISO.zip
Linux または Windows	DCNM_To_NDFC_12_2_2_Upgrade_Tool_LIN_WIN.zip

- NDFC リリース 12.2.3 の場合 :

DCNM 11.5(4) 展開タイプ	アップグレードツールのファイル名
ISO/OVA	DCNM_To_NDFC_12_2_3_Upgrade_Tool_OVA_ISO.zip
Linux または Windows	DCNM_To_NDFC_12_2_3_Upgrade_Tool_LIN_WIN.zip

- d) **sysadmin** アカウントを使用して、アップグレードツール イメージを既存の DCNM 11.5(4) サーバーにコピーします。

ステップ 2 アーカイブを抽出し、Linux/Windows 展開の署名を検証します。

(注)

ISO/OVA アーカイブを使用している場合は、次の手順へスキップします。

- a) Python 3 がインストールされていることを確認します。

```
$ python3 --version
Python 3.9.6
```

- b) ダウンロードしたアーカイブを解凍します。

- NDFC リリース 12.2.2 の場合 :

```
# unzip DCNM_To_NDFC_12_2_2_Upgrade_Tool_LIN_WIN.zip
Archive: DCNM_To_NDFC_12_2_2_Upgrade_Tool_LIN_WIN.zip
```

```
extracting: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip
extracting: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip.signature
inflating: ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
inflating: cisco_x509_verify_release.py3
```

- NDFC リリース 12.2.3 の場合 :

```
# unzip DCNM_To_NDFC_12_2_3_Upgrade_Tool_LIN_WIN.zip
Archive: DCNM_To_NDFC_12_2_3_Upgrade_Tool_LIN_WIN.zip
extracting: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip
extracting: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip.signature
inflating: ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
inflating: cisco_x509_verify_release.py3
```

- c) 署名を検証します。

ZIP アーカイブ内にはアップグレードツールと署名ファイルがあります。アップグレードツールを検証するには、次のコマンドを使用します。

- NDFC リリース 12.2.2 の場合 :

```
# ls -l
-rwxr-xr-x. 1 root root 16788 Apr 20 2023 cisco_x509_verify_release.py3
-rw-r--r--. 1 root root 1422 Aug 12 2023 ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
-rw-r--r--. 1 root root 9541673 Jul 25 03:09 DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip
-rw-r--r--. 1 root root 256 Jul 25 03:09 DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip.signature
-rw-r--r--. 1 root root 9548328 Jul 26 06:11 DCNM_To_NDFC_12_2_2_Upgrade_Tool_LIN_WIN.zip

# ./cisco_x509_verify_release.py3 -e ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM -i
DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip -s DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip.signature -v
dgst -sha512

Retrieving CA certificate from https://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully retrieved and verified crcam2.cer.
Retrieving SubCA certificate from https://www.cisco.com/security/pki/certs/innespace.cer
...
Successfully retrieved and verified innespace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully fetched a public key from ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM.
Successfully verified the signature of DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip using
ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
```

- NDFC リリース 12.2.3 の場合 :

```
# ls -l
-rwxr-xr-x. 1 root root 16788 Apr 20 2023 cisco_x509_verify_release.py3
-rw-r--r--. 1 root root 1422 Aug 12 2023 ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
-rw-r--r--. 1 root root 9541673 Jul 25 03:09 DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip
-rw-r--r--. 1 root root 256 Jul 25 03:09 DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip.signature
-rw-r--r--. 1 root root 9548328 Jul 26 06:11 DCNM_To_NDFC_12_2_3_Upgrade_Tool_LIN_WIN.zip

# ./cisco_x509_verify_release.py3 -e ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM -i
DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip -s DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip.signature -v
dgst -sha512

Retrieving CA certificate from https://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully retrieved and verified crcam2.cer.
Retrieving SubCA certificate from https://www.cisco.com/security/pki/certs/innespace.cer
...
Successfully retrieved and verified innespace.cer.
Successfully verified root, subca and end-entity certificate chain.
```

```
Successfully fetched a public key from ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM.
Successfully verified the signature of DCMN_To_NDFC_Upgrade_Tool_LIN_WIN.zip using
ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
```

- d) 検証スクリプト署名を確認したら、スクリプト自体を抽出します。

```
# unzip DCMN_To_NDFC_Upgrade_Tool_LIN_WIN.zip
Archive: DCMN_To_NDFC_Upgrade_Tool_LIN_WIN.zip
creating: DCMN_To_NDFC_Upgrade_Tool_LIN_WIN/
inflating: DCMN_To_NDFC_Upgrade_Tool_LIN_WIN/log4j2.properties
inflating: DCMN_To_NDFC_Upgrade_Tool_LIN_WIN/DCNMBackup.sh
inflating: DCMN_To_NDFC_Upgrade_Tool_LIN_WIN/DCNMBackup.bat
creating: DCMN_To_NDFC_Upgrade_Tool_LIN_WIN/jar/
inflating: DCMN_To_NDFC_Upgrade_Tool_LIN_WIN/jar/jarchivelib-0.7.1-jar-with-dependencies.jar
inflating: DCMN_To_NDFC_Upgrade_Tool_LIN_WIN/jar/bcprov-jdk15on-1.68.jar
inflating: DCMN_To_NDFC_Upgrade_Tool_LIN_WIN/jar/not-going-to-be-commons-ssl-0.3.20.jar
inflating: DCMN_To_NDFC_Upgrade_Tool_LIN_WIN/jar/jnm.jar
inflating: DCMN_To_NDFC_Upgrade_Tool_LIN_WIN/jar/slf4j-simple-1.7.21.jar
inflating: DCMN_To_NDFC_Upgrade_Tool_LIN_WIN/jar/log4j.properties
inflating: DCMN_To_NDFC_Upgrade_Tool_LIN_WIN/jar/dcnmbackup.jar
inflating: DCMN_To_NDFC_Upgrade_Tool_LIN_WIN/jar/sequences.info.oracle
inflating: DCMN_To_NDFC_Upgrade_Tool_LIN_WIN/jar/tables.info.postgres
inflating: DCMN_To_NDFC_Upgrade_Tool_LIN_WIN/jar/sequences.info.postgres
inflating: DCMN_To_NDFC_Upgrade_Tool_LIN_WIN/jar/tables.info.oracle
```

ステップ3 アーカイブを抽出し、ISO/OVA 展開の署名を検証します。

(注)

Linux/Windows アーカイブを使用している場合は、次の手順にスキップします。

- a) ダウンロードしたアーカイブを解凍します。

- NDFC リリース 12.2.2 の場合：

```
# unzip DCMN_To_NDFC_12_2_2_Upgrade_Tool_OVA_ISO.zip
Archive: DCMN_To_NDFC_12_2_2_Upgrade_Tool_OVA_ISO.zip
inflating: DCMN_To_NDFC_Upgrade_Tool_OVA_ISO
extracting: DCMN_To_NDFC_Upgrade_Tool_OVA_ISO.signature
inflating: cisco_x509_verify_release.py3
inflating: ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
```

- NDFC リリース 12.2.3 の場合：

```
# unzip DCMN_To_NDFC_12_2_3_Upgrade_Tool_OVA_ISO.zip
Archive: DCMN_To_NDFC_12_2_3_Upgrade_Tool_OVA_ISO.zip
inflating: DCMN_To_NDFC_Upgrade_Tool_OVA_ISO
extracting: DCMN_To_NDFC_Upgrade_Tool_OVA_ISO.signature
inflating: cisco_x509_verify_release.py3
inflating: ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
```

- b) 署名を検証します。

ZIP アーカイブ内にはアップグレードツールと署名ファイルがあります。アップグレードツールを検証するには、次のコマンドを使用します。

```
# ./cisco_x509_verify_release.py3 -e ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM -i
DCMN_To_NDFC_Upgrade_Tool_OVA_ISO -s DCMN_To_NDFC_Upgrade_Tool_OVA_ISO.signature -v dgst -sha512
Retrieving CA certificate from https://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully retrieved and verified crcam2.cer.
Retrieving SubCA certificate from https://www.cisco.com/security/pki/certs/innerspace.cer ...
Successfully retrieved and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
```

```
Successfully fetched a public key from ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.pem.
Successfully verified the signature of DCNM_To_NDFC_Upgrade_Tool_OVA_ISO using
ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.pem
```

ステップ 4 既存の設定をバックアップします。

バックアップ ツールは、過去 90 日間の Performance Management データを収集します。

- a) DCNM リリース 11.5(4) アプライアンス コンソールにログインします。
- b) スクリーン セッションを作成します。

次のコマンドは、追加のコマンドを実行するためのセッションを作成します。

```
dcnm# screen
```

このコマンドは、ウィンドウが表示されていない場合、または切断された場合でも実行を続けることに注意してください。

- c) スーパー ユーザー (root) アクセス権を取得します。

```
dcnm# su
Enter password: <root-password>
[root@dcnm]#
```

- d) OVA および ISO の場合は、アップグレード ツールの実行権限を有効にします。

```
[root@dcnm]# chmod +x ./DCNM_To_NDFC_Upgrade_Tool_OVA_ISO
```

- e) 前の手順でダウンロードしたアップグレード ツールを実行します。

- たとえば、Windows の リリース 3.2.1 の場合 :

```
C:\DCNM_To_NDFC_Upgrade_Tool_LIN_WIN>DCNMBackup.bat
Enter DCNM root directory [C:\Program Files\Cisco Systems\dcnm]:
Initializing, please wait...
*****
Welcome to DCNM-to-NexusDashboard Upgrade Tool for Linux/Windows.
This tool will analyze this system and determine whether you can move to Nexus Dashboard
3.2.1 or not.
If upgrade to Nexus Dashboard 3.2.1 is possible, this tool will create files to be used for
performing the upgrade.
Thank you!
*****
This tool will backup config data. Exporting Operational data like Performance(PM) might
take some time.
Do you want to export operational data also? [y/N]: y
*****
Sensitive information will be encrypted using an encryption key.
This encryption key will have to be provided when restoring
the backup file generated by this tool.
Please enter the encryption key:
Enter it again for verification:
....
2024-07-25 22:35:34,944 [main] DEBUG
org.apache.http.impl.conn.PoolingHttpClientConnectionManager - Connection [id: 0][route:
{s}->https://127.0.0.1:9200] can be kept alive indefinitely
2024-07-25 22:35:34,944 [main] DEBUG
org.apache.http.impl.conn.DefaultManagedHttpClientConnection - http-outgoing-0: set socket
timeout to 0
2024-07-25 22:35:34,944 [main] DEBUG
org.apache.http.impl.conn.PoolingHttpClientConnectionManager - Connection released: [id:
0][route: {s}->https://127.0.0.1:9200][total kept alive: 1; route allocated: 1 of 20; total
allocated: 1 of 20]
```

```

2024-07-25 22:35:34,969 [main] INFO DCNMBBackup - Total number of Json data entries in
backup/es/pmdb_sanportratedata_daily.data ==> 145
2024-07-25 22:35:35,036 [main] INFO DCNMBBackup - ##### Total time to export Daily data: 7
seconds.
2024-07-25 22:35:35,036 [main] INFO DCNMBBackup - ##### Total time to export PM data: 36
seconds.
2024-07-25 22:35:35,169 [main] INFO DCNMBBackup - Creating data file...
2024-07-25 22:35:38,083 [main] INFO DCNMBBackup - Creating metadata file...
2024-07-25 22:35:38,085 [main] INFO DCNMBBackup - Creating final backup archive...
2024-07-25 22:35:38,267 [main] INFO DCNMBBackup - Done

```

- たとえば、Linuxの3.2.1リリースの場合：

```

# ./DCNMBBackup.sh
Enter DCNM root directory [/usr/local/cisco/dcm]:
Initializing, please wait...
*****
Welcome to DCNM-to-NexusDashboard Upgrade Tool for Linux/Windows.
This tool will analyze this system and determine whether you can move to Nexus Dashboard
3.2.1 or not.
If upgrade to Nexus Dashboard 3.2.1 is possible, this tool will create files to be used for
performing the upgrade.
Thank you!

*****

This tool will backup config data. Exporting Operational data like Performance(PM) might
take some time.
Do you want to export operational data also? [y/N]: y
*****
Sensitive information will be encrypted using an encryption key.
This encryption key will have to be provided when restoring
the backup file generated by this tool.

Please enter the encryption key:
Enter it again for verification:
.....
2024-07-26 04:04:46,540 [main] INFO DCNMBBackup - Total number of Json data entries in
backup/es/pmdb_sanportratedata_daily.data ==> 92
2024-07-26 04:04:46,543 [main] INFO DCNMBBackup - ##### Total time to export Daily data: 3
seconds.
2024-07-26 04:04:46,543 [main] INFO DCNMBBackup - ##### Total time to export PM data: 11
seconds.
2024-07-26 04:04:46,958 [main] INFO DCNMBBackup - Creating data file...
2024-07-26 04:04:47,456 [main] INFO DCNMBBackup - Creating metadata file...
2024-07-26 04:04:47,467 [main] INFO DCNMBBackup - Creating final backup archive...
2024-07-26 04:04:47,478 [main] INFO DCNMBBackup - Done.

```

- たとえば、OVAのリリース3.2.1の場合：

```

# ./DCNM_To_NDFC_Upgrade_Tool_OVA_ISO
*****
Welcome to DCNM-to-NexusDashboard Upgrade Tool for OVA/ISO.
This tool will analyze this system and determine whether you can move to
Nexus Dashboard 3.2.1 or not.
If upgrade to Nexus Dashboard 3.2.1 is possible, this tool will create files
to be used for performing the upgrade.
NOTE:
Only backup files created by this tool can be used for upgrading,
older backup files created with 'appmgr backup' CAN NOT be used
for upgrading to Nexus Dashboard 3.2.1
Thank you!

*****
Continue? [y/n]: y

```

```

Collect operational data (e.g. PM, EPL)? [y/n]: y
Does this DCNM 11.5(4) have DCNM Tracker feature enabled on any switch on any fabric? [y/n]:
n

Sensitive information will be encrypted using an encryption key.
This encryption key will have to be provided when restoring
the backup file generated by this tool.

Please enter the encryption key:
Enter it again for verification:
.....
Adding backup header
Collecting DB table data
Collecting DB sequence data
Collecting stored credentials
Collecting Custom Templates
Collecting CC files
Collecting L4-7-service data
Collecting CVisualizer data
Collecting EPL data
Collecting PM data - WARNING: this will take a while!
Collecting AFW app info
Decrypting stored credentials
Adjusting DB tables
Creating dcnm backup file
Creating final backup file
Done.
Backup file: backup11_sandcnm_20240726-113054.tar.gz

```

ステップ 5 このドキュメントの前の章のいずれかの説明に従って、新規に Nexus Dashboard クラスタを展開します。

Nexus Dashboard プラットフォーム、ファブリック コントローラ サービス、および上記の導入の章に記載されている特定のフォーム ファクタのすべてのガイドラインと前提条件を満たしていることを確認します。

(注)

- Nexus Dashboard クラスタをファブリック コントローラ (NDFC) サービスでのみ展開します。他のサービス (ファブリック コントローラ + Insights など) で展開しないでください。これを行うと、次の手順で構成バックアップを復元する際に、「バックアップファイルはこの展開モードと互換性がありません」というメッセージで移行が失敗します。
- DCNM 設定の復元に進む前に、Nexus Dashboard ファブリック コントローラ UI で、必要な数の永続 IP アドレスを指定する必要があります。
- 既存の設定で Cisco Smart Software Management (CSSM) に直接接続するスマート ライセンスを使用している場合は、新しい Nexus Dashboard に CSSM Web サイトに到達するために必要なルートがあることを確認する必要があります。

smartreceiver.cisco.com の IP アドレスのサブネットが、Nexus Dashboard 管理ネットワーク用に、Nexus Dashboard の **[管理 (Admin)] > [システム設定 (System Settings)] > [ルート (Routes)]** ページのルート テーブルに追加されていることを確認します。

最新のサブネットを見つけるには、smartreceiver.cisco.com に ping を実行します。次の例をご覧ください。

```

$ ping smartreceiver.cisco.com
PING smartreceiver.cisco.com (146.112.59.81): 56 data bytes
64 bytes from 146.112.59.81: icmp_seq=0 ttl=52 time=48.661 ms

```

```
64 bytes from 146.112.59.81: icmp_seq=1 ttl=52 time=44.730 ms
64 bytes from 146.112.59.81: icmp_seq=2 ttl=52 time=48.188 ms
```

さらに、NDFC は新しい製品インスタンスと見なされるため、信頼を再確立する必要があります。期限切れの信頼トークンを使用してバックアップを作成した場合は、アップグレード後にスマートライセンス設定ウィザードを手動で実行し、有効なトークンを入力する必要があります。

ステップ 6 Nexus Dashboard リリース 3.2.1 で導入された統合バックアップおよび復元機能を使用して、新しいクラスターに構成のバックアップを復元します。

詳細については、「[Nexus Dashboard とサービスの統合バックアップおよび復元](#)」を参照してください。

- a) バックアップから復元する前に、NDFC ファブリックを導入準備します。
これらの手順では、以前に作成したバックアップから復元します。バックアップが作成されたときに NDFC サービスが ND の一部であった場合は、この復元プロセスを開始する前に NDFC ファブリックを導入準備する必要があります。
- b) 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 & 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。
- c) 次のいずれかの方法を使用して、[復元 (Restore)] スライド 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 (Restore)] 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。

- d) 該当する場合、[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。

(注)

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。

- 構成バックアップ テーブルのアップロード : [バックアップ ファイル (Backup File)] エリアが表示され、復元するローカル バックアップ ファイルをドラッグアンドドロップするか、システム上のローカルエリアに移動して復元するバックアップ ファイルを選択できます。

- リモート ロケーション :

1. [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、「[Nexus Dashboard とサービスの統合バックアップおよび復元](#)」の「リモート ロケーションの構成」の手順に従ってから、ここに戻ります。リモート バックアップ プロセスの一部としてリモート ロケーションを構成しますが、リモート バックアップ を構成したクラスターとは異なるク

ラストにいる場合、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、他のクラスターで構成したリモート バックアップを検出できるようになります。

2. **[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。

- e) **[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。
- f) **[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。
- g) 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。**[次へ (Next)]** をクリックします。
- h) (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 設定を無視する (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 設定は無視されます。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。

- i) **[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。
- j) 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。
- k) 復元プロセスが成功すると、**[進行状況 (Progress)]** に 100% と表示され、**[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。

(注)

新しい ND 統合バックアップおよび復元機能を使用してバックアップされた構成を復元した後、ND レベルで表示される NDFC ファブリックの状態が、NDFC ファブリックの実際の状態と同期していない可能性があります。NDFC ファブリックのステータスを同期中に戻すには、**[ファブリック概要 (Fabric Overview)]** ページで、ページ上部の **[アクション (Actions)]** をクリックし、**[再計算と展開 (Recalculate and Deploy)]** を選択します。

ステップ 7 アップグレード後のタスクを完了します。

- a) SAN コントローラ ペルソナを使用している場合：

バックアップからデータを復元すると、すべての server-smart ライセンスが **OutofCompliance** になります。

UI の **[操作 (Operations)] > [ライセンス管理 (License Management)] > [スマート (Smart)]** ページから、ポリシーを使用したスマート ライセンシングに移行し、SLP を使用して CCSM との信頼を確立できます。

b) ファブリック コントローラ ペルソナを使用している場合：

DCNM 11.5(4) からアップグレードする場合、次の機能については引き継がれないため、再設定が必要です。

- エンドポイント ロケータを再設定する必要があります
- IPAM 統合を再設定する必要があります
- アラーム ポリシーを再設定する必要があります
- カスタム トポロジを再作成して保存する必要があります
- ファブリックで PM 収集を再度有効にする必要があります
- データの収集を開始するには、温度データ収集を再度有効にする必要があります
- スイッチ イメージをアップロードする必要があります

リリース 11.5(4) の展開タイプ	11.5(4) では、トラップ IP アドレスは以下から収集されます：	LAN デバイス管理の接続性	アップグレード後のトラップ IP アドレス	結果
LAN ファブリック メディア コントローラ	eth1 (または HA システムの場合 vip1)	管理	管理サブネットに属する	Honored 構成の違いは、ありません。対応不要です。

リリース 11.5(4) の展開タイプ	11.5(4) では、トラップ IP アドレスは以下から収集されます：	LAN デバイス管理の接続性	アップグレード後のトラップ IP アドレス	結果
LAN ファブリック メディア コントローラ	eth0（または HA システムの場合 vip0）	管理	管理サブネットに属していない	無視されます。管理プールの別の IP がトラップ IP として使用されます。 構成の違いが作成されます。Web UI の [LAN][Fabrics][Fabrics] で、[Fabric]をダブルクリックして [Fabric Overview] を表示します。 [ファブリックアクション (Fabrics Actions)] ドロップダウンリストから、 [設定の再計算 (Recalculate Config)] を選択します。 [構成の展開 (Deploy Config)] をクリックします。
LAN ファブリック メディア コントローラ	eth0（または HA システムの場合 vip0）	データ	データサブネットに属する	Honored 構成の違いは、ありません。対応不要です。

リリース 11.5(4) の展開タイプ	11.5(4) では、トラップ IP アドレスは以下から収集されます：	LAN デバイス管理の接続性	アップグレード後のトラップ IP アドレス	結果
LAN ファブリック メディア コントローラ	eth0（または HA システムの場合 vip0）	データ	データ サブネットに属していない	無視されます。 データ プールの別の IP がトラップ IP として使用されます 構成の違いが作成されます。Web UI の [LAN][Fabrics][Fabrics] で、[Fabric] をダブルクリックして [Fabric Overview] を表示します。 [ファブリックアクション (Fabrics Actions)] ドロップダウンリストから、 [設定の再計算 (Recalculate Config)] を選択します。 [構成の展開 (Deploy Config)] をクリックします。

リリース 11.5(4) の展開タイプ	11.5(4) では、トラップ IP アドレスは以下から収集されます：	LAN デバイス管理の接続性	アップグレード後のトラップ IP アドレス	結果
SAN 管理	OVA/ISO – • trap.registaddress (設定されている場合) • eth0 (trap.registaddress が設定されていない場合) Windows/Linux – • trap.registaddress (設定されている場合) • イベントマネージャ アルゴリズムに基づくインターフェイス (trap.registaddress が設定されていない場合)	N/A	データ サブネットに属する	Honored 構成の違いは、ありません。対応不要です。
		N/A	データ サブネットに属していない	無視されます。 データ プールの別の IP がトラップ IP として使用されます

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。