



DCNM から ND への移行

- [DCNM から ND への移行の前提条件とガイドライン \(1 ページ\)](#)
- [既存の DCNM 設定の ND への移行 \(4 ページ\)](#)

DCNM から ND への移行の前提条件とガイドライン

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 ND 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. 新しい Nexus Dashboard クラスタを新規に展開します。
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 DCNM 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。
-

ファブリック タイプの互換性

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、ファブリック タイプ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。



(注) SAN ファブリックは、Nexus Dashboard リリース 4.1.1 ではほぼ変更されていません。

4.1.1 より前のファブリック		4.1.1 ファブリック タイプ
ファブリック テクノロジー	ファブリック タイプ	
LAN		
VXLAN EVPN	データセンター VXLAN EVPN	データセンター VXLAN EVPN - iBGP
eBGP VXLAN EVPN	BGP ファブリック	データセンター VXLAN EVPN - eBGP
VXLAN EVPN	キャンパス VXLAN EVPN	キャンパス VXLAN EVPN
eBGP ルーテッド	BGP ファブリック	BGP ファブリック
従来の LAN	拡張クラシック LAN	拡張クラシック LAN
従来の LAN	従来の LAN	レガシークラシック LAN
Custom	外部接続ネットワーク	外部およびファブリック間接続ネットワーク
Custom	カスタム ネットワーク	外部およびファブリック間接続ネットワーク
Custom	マルチサイト外部ネットワーク	外部およびファブリック間接続ネットワーク
LAN モニター	LAN モニター	外部およびファブリック間接続ネットワーク
VXLAN EVPN	VXLAN EVPN マルチサイト	VXLAN (ファブリック グループ)
マルチファブリック ドメイン	ファブリック グループ	クラシック (ファブリック グループ)
IPFM		
IPFM	IPFM	IPFM

4.1.1 より前のファブリック		4.1.1 ファブリック タイプ
ファブリック テクノロジー	ファブリック タイプ	
LAN		
IPFM	IPFM クラシック	IPFM クラシック
ジェネリック マルチキャスト	IPFM クラシック	IPFM クラシック
マルチファブリック ドメイン	ファブリック グループ	IPFM (ファブリック グループ)

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。

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	11.5(4)から繰り越し
コンテナオーケストレータ (K8s) ビジュアライザ	11.5(4)から繰り越し
vCenter による VMM の可視性	11.5(4)から繰り越し
構成された Nexus Dashboard Orchestrator	11.5(4)から繰り越されません
設定されたプレビュー フィーチャー	11.5(4)から繰り越されません
SAN インストールの LAN スイッチ	11.5(4)から繰り越されません
IPAMの統合	11.5(4)から繰り越されません
カスタマー トポロジ	11.5(4)から繰り越されません。再作成して保存する必要があります
DCNM トラッカー	11.5(4)から繰り越されません
ファブリックのバックアップ	11.5(4)から繰り越されません
レポート定義とレポート	11.5(4)から繰り越されません
スイッチのイメージとイメージ管理ポリシー	11.5(4)から繰り越されません
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

DCNM 11.5 (4) の機能	アップグレードのサポート
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。ファブリックで再度有効にする必要があります。
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 ND 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) [Nexus Dashboard] ダウンロード ページに移動します。
<https://software.cisco.com/download/home/286327743/type/286328258/>
- 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。

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_4.1.1_Upgrade_Tool_OVA_ISO.zip
Linux または Windows	DCNM_To_NDFC_4.1.1_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。

```
# unzip DCNM_To_NDFC_4.1.1_Upgrade_Tool_LIN_WIN.zip
Archive: DCNM_To_NDFC_4.1.1_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。

```
# ./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/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_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 DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip
Archive: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip
creating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/log4j2.properties
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/DCNMBBackup.sh
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/DCNMBBackup.bat
creating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/jarchivelib-0.7.1-jar-with-dependencies.jar
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/bcprov-jdk15on-1.68.jar
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/not-going-to-be-commons-ssl-0.3.20.jar
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/jnm.jar
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/slf4j-simple-1.7.21.jar
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/log4j.properties
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/dcnmbbackup.jar
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/sequences.info.oracle
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/tables.info.postgres
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/sequences.info.postgres
inflating: DCNM_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。

```
# unzip DCNM_To_NDFC_4.1.1_Upgrade_Tool_OVA_ISO.zip
Archive: DCNM_To_NDFC_4.1.1_Upgrade_Tool_OVA_ISO.zip
inflating: DCNM_To_NDFC_Upgrade_Tool_OVA_ISO_4.1.1
extracting: DCNM_To_NDFC_Upgrade_Tool_OVA_ISO_4.1.1.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
DCNM_To_NDFC_Upgrade_Tool_OVA_ISO_4.1.1 -s DCNM_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。

- 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_4.1.1
```

- 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 4.1.1 の場合は、次のようになります：

```
C:\DCNM_To_NDFC_Upgrade_Tool_LIN_WIN>DCNMBackup.bat
Enter DCNM root directory [C:\Program Files\Cisco Systems\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
4.1.1 or not.
If upgrade to Nexus Dashboard 4.1.1 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 DCNMBackup - Total number of Json data entries in
backup/es/pmdb_sanportratedata_daily.data ==> 145
2024-07-25 22:35:35,036 [main] INFO DCNMBackup - ##### Total time to export Daily data: 7
seconds.
2024-07-25 22:35:35,036 [main] INFO DCNMBackup - ##### Total time to export PM data: 36
seconds.
2024-07-25 22:35:35,169 [main] INFO DCNMBackup - Creating data file...
2024-07-25 22:35:38,083 [main] INFO DCNMBackup - Creating metadata file...
2024-07-25 22:35:38,085 [main] INFO DCNMBackup - Creating final backup archive...
2024-07-25 22:35:38,267 [main] INFO DCNMBackup - Done

```

- たとえば、Linux用のリリース 4.1.1 の場合は、次のようになります：

```

# ./DCNMBackup.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
4.1.1 or not.
If upgrade to Nexus Dashboard 4.1.1 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 DCNMBackup - Total number of Json data entries in
backup/es/pmdb_sanportratedata_daily.data ==> 92
2024-07-26 04:04:46,543 [main] INFO DCNMBackup - ##### Total time to export Daily data: 3
seconds.
2024-07-26 04:04:46,543 [main] INFO DCNMBackup - ##### Total time to export PM data: 11
seconds.
2024-07-26 04:04:46,958 [main] INFO DCNMBackup - Creating data file...
2024-07-26 04:04:47,456 [main] INFO DCNMBackup - Creating metadata file...

```

```
2024-07-26 04:04:47,467 [main] INFO DCNMBackup - Creating final backup archive...
2024-07-26 04:04:47,478 [main] INFO DCNMBackup - Done.
```

- たとえば、OVAのリリース 4.1.1 の場合は、次のようになります：

```
# ./DCNM_To_NDFC_Upgrade_Tool_OVA_ISO_4.1.1
*****
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 4.1.1 or not.
If upgrade to Nexus Dashboard 4.1.1 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 4.1.1
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)

- DCNM 設定の復元に進む前に、Nexus Dashboard GUI 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)] > [全般 (General)] > [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 nslookup を実行します。次の例をご覧ください。

```
$ nslookup smartreceiver.cisco.com
Server:          24.233.18.143
Address:         24.233.18.143#53

Name:   smartreceiver.cisco.com
Address: 146.112.59.81
Name:   smartreceiver.cisco.com
Address: 2a04:e4c7:ffff::f
```

Nexus Dashboard のデプロイメントに基づいて、IPv4 アドレスまたは IPv6 アドレスのいずれかを使用できます。

さらに、Nexus Dashboard 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 新しいクラスタで設定のバックアップを復元します。

詳細については、「[Nexus Dashboard のバックアップと復元](#)」を参照してください。

- a) 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。

- b) [復元 (Restore)] スライド ページにアクセスするには、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。

- c) 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。

- 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 のバックアップと復元](#)」の「リモート ストレージ ロケーションの作成」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とは異なるクラスタにいる場合、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。

- d) [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。
- e) [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。
- f) 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。
- g) DCNM から ND/NDFC にアップグレードする場合、ND/NDFC は常に **外部IP の無視** 設定を無視し、可能な場合は常にバックアップの既存の IP を使用しようとします。それ以外の場合は、新しい IP を使用します。

次の表は、システムが IP アドレスをどのように扱うかについての詳細を示しています。

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。[管理 (Manage)]>[ファブリック (Fabrics)] で、[Fabric]をダブルクリックして、[ファブリックの概要 (Fabric Overview)] を表示します。[アクション (Actions)] ドロップダウンリストから、[再計算と展開 (Recalculate and Deploy)] 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	<p>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</p> <p>構成の違いが作成されます。に</p> <p>[管理 (Manage)] > [ファブリック (Fabrics)] で、ファブリックをダブルクリックして [ファブリックの概要 (Fabric Overview)] を表示します。 [アクション (Actions)] ドロップダウンリストから、[再計算と展開 (Recalculate and Deploy)] を選択します。 [構成の展開 (Deploy Config)] をクリックします。</p>

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 – <ul style="list-style-type: none"> • 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 – <ul style="list-style-type: none"> • 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

- h) [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。

- i) 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。

- j) 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 ND ファブリックの状態が、ND 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。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) ND リリース 4.1.1 に SAN デプロイメントがある場合：

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 [管理 (Admin)] > [ライセンス (Licensing)] > [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) ND リリース 4.1.1 で LAN デプロイメントがある場合：

DCNM 11.5(4) からアップグレードする場合、一部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。詳細については、[アップグレード後の機能の互換性 \(3 ページ\)](#) を参照してください。

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。