Guidelines and Limitations

Guidelines and Limitations

The guidelines and limitations for installing and upgrading Cisco DCNM are as follows:

General Guidelines and Limitations

- Adhere to the following password requirements. If you do not comply with the requirements, the DCNM application might not function properly:
  - It must be at least 8 characters long and contain at least one alphabet and one numeral.
  - It can contain a combination of alphabets, numerals, and special characters.
  - Do not use any of these special characters in the DCNM password: <SPACE> " & $ % ' ^ = < > ; : ` \ | / , .*
  - From Cisco DCNM Release 11.0(1), the characters that are allowed in the Administrative password is restricted for OVA and ISO installations. Therefore while upgrading, the old password used in DCNM 11.0(1) or 11.1(1) is not valid. However, different passwords are allowed during Upgrade.

    The new Administrative password that is entered is used in the following scenarios.

    —accessing the DCNM appliance via its console.

    —accessing the appliance via SSH

    —for applications running on the appliance, e.g. Postgres DBMS

    However, after the upgrade, since Postgres DBMS is restored from the backup that is taken on DCNM 10.4(2), you must logon to the Cisco DCNM Web UI using the password used on DCNM Release 10.4(2) appliance.
- Do not interrupt the boot process (such as pressing the Ctrl+ALT + DELETE keys) when installing DCNM. If you interrupt, you must restart the installation process.
- Ensure that you configure the timezone after installation or upgrade, before performing any other operations on the Cisco DCNM Appliance. Use the NTP server for configuring timezones.

- To check the status of the running Postgres database in Native HA setup, use **pg_ctl** command. Do not use the **systemctl** command.
- Do not begin the password with Hash (#) symbol. Cisco DCNM considers the password as an encrypted text if it begins with # symbol.
- We recommend that you do not upgrade any underlying third-party software separately. All the necessary software components will be updated during the inline upgrade procedure. Upgrading the components outside of DCNM upgrade will cause performance issues.

Fresh Installation

- For Virtual Appliances (OVA/ISO), the installer installs the Operating system and Cisco DCNM components.
- The DCNM OVA cannot be deployed by connecting the vSphere client directly to the ESXi server.

Upgrade

- Ensure that you do not perform inline upgrade from an SSH session. The session may timeout and result in an incomplete upgrade.
- Disable Telemetry in the earlier release before you upgrade to Cisco DCNM Release .
- Disable Telemetry before you deploy Compute Nodes. You can enable Telemetry after deploying compute nodes.

  For DCNM in Native HA mode, Telemetry is supported with 3 compute nodes only.
- If you need to run Network Insights applications, you must install 3 compute nodes.
- Disable Telemetry before modifying Interface settings. You can enable Telemetry after modifying the settings.
- During a backup and restore process, the compute nodes are also included in the backup. After you deploy the new compute, you can restore the backup on the compute node.

  If there was no backup, disconnect the 3 compute nodes, and erase the data on all the compute nodes. On the Cisco DCNM Web Client UI, navigate to **Application** > **Compute**. Select the **+** icon to join the compute nodes.
- To erase data on the compute node, logon to the compute node through an SSH session and erase the data using the **rm -rf /var/afw/vols/data** command.

Note You must run the above command separately on all compute nodes to erase data.

- Before starting NIR application after upgrade, on the DCNM Web UI, choose **Application** > **Preferences**. Modify the network settings as required. If you do not modify the network settings after upgrade before you enable the Telemetry on the Fabrics, the configuration will not complete. You must stop the NIR app, modify the network settings and start the app again, to resolve the issue.

Checking TPM Partition before Converting DCNM-SE to Nexus Dashboard

A few Cisco Application Services Engine (SE) nodes that was factory pre-installed with DCNM 11.5(1) or earlier may have a corrupted TPM partition. This causes the installation of Cisco Nexus Dashboard software to fail. You must check the TPM Partition before upgrading from Cisco DCNM-SE to Cisco Nexus Dashboard.

Note TPM is not a requirement for DCNM 11.x releases. Therefore, this issue does not affect existing DCNM 11.x functionality of the device, even if the device is affected by this issue. No further action is required until you decide to upgrade to Cisco Nexus Dashboard.

To identify if your Cisco DCNM-SE is affected by this issue, perform the following steps:

Procedure

Step 1 SSH to Cisco Application Services Engine using **sysadmin** user.

Step 2 Run the following command to view the list of models and their vendors.

lsblk-S

```
[root@dcnm-se-active sysadmin]$ lsblk -S
NAME   HCTL       TYPE     VENDOR   MODEL             REV TRAN
...
sdc    0:2:2:0    disk     Cisco    UCSC-RAID12G-2GB  5.10
sdd    0:2:3:0    disk     Cisco    UCSC-RAID12G-2GB  5.10
sde    0:2:4:0    disk     Cisco    UCSC-RAID12G-2GB  5.10
sdf    7:0:0:0    disk     UNIGEN   PQT8000           1100 usb  /*identiifying device from
 UNIGEN Vendor*/
sdg    8:0:0:0    disk     UNIGEN   PHF16H0CM1-ETG    PMAP usb
sdl    1:0:0:0    disk     ATA      Micron_5100_MTFD  H072 sata
...
```

Applications Services Engine from **UNIGEN** vendor is detected with device name **sdf**.

Step 3 Run the following command to view the partitions in the disk.

lsblk -s or **lsblk**

- **Example1**

  The following example shows functioning TPM disk with two partitions sdf1 and sdf2. This can be installed with Cisco Nexus Dashboard software with no issues.

```
[root@dcnm-se-active sysadmin]$ lsblk
NAME                 MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
...
sdc                    8:32   0   2.2T  0 disk
sdd                    8:48   0   2.2T  0 disk
sde                    8:64   0   371.6G  0 disk
sdf                    8:80   1   7.7G  0 disk  /*functioning TPM with partition*/
 |--sdf1                 8:81   1    60M  0 part
 |--sdf2                 8:82   1   3.7G  0 part
nvme0n1              259:0    0   1.5T  0 disk
```

```
 |--nvme0n1p1          259:1    0   1.5T  0 part
   |--flashvg-flashvol 253:3    0   1.5T  0 lvm  /var/afw/vols/data/flash
...
```

- **Example2**

  The following example shows defective or corrupted TPM disk with no partitions defined on device **sdf**. This unit cannot be used to install Cisco Nexus Dashboard software, and must be replaced.

```
[root@dcnm-se-active sysadmin]$ lsblk
NAME                  MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
...
sdc                     8:32   0   2.2T  0 disk
sdd                     8:48   0   2.2T  0 disk
sde                     8:64   0   371.6G  0 disk
sdf                     8:80   1   16G  0 disk  /*corrupted TPM without partition*/
nvme0n1               259:0    0   1.5T  0 disk
 |--nvme0n1p1          259:1    0   1.5T  0 part
   |--flashvg-flashvol 253:3    0   1.5T  0 lvm  /var/afw/vols/data/flash
...
```

Step 4 If your device has a TPM disk with no partitions, contact Cisco Technical Assistance Center (TAC) to initiate RMA and replace the device.

No further action is required if your TPM has partitions.