Guidelines and Limitations

Guidelines and Limitations

This section lists guidelines and limitations that are related to the Cisco DCNM Release 11.3(1).

- The icons or fonts on Cisco DCNM GUI may not appear correctly on Microsoft Windows 10 browsers. This problem can occur if your Windows 10 is set to block untrusted fonts or some security or mitigation options. Microsoft's Internet Explorer Browser Support team has provided with the following steps to address this issue.

  Configure the *Allow Font Downloads* Internet Explorer Setting on the Internet Zone and Restricted Sites Zone (enabled by default). Perform the following steps:

  1. Search for **Group Policy Editor** in Control Panel.
  2. Choose **Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Internet Zone > Allow Font Downloads**.
  3. Double click and choose the **Enabled** radio button.
  4. Click **OK**.
  5. Choose **Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Restricted Sites Zone > Allow Font Downloads**.
  6. Double click and choose the **Enabled** radio button.
  7. Click **OK**.
  8. Restart the computer so that the new setting takes effect.

- You must apply patch for any changes that happen on switch side (Nexus 3000 and/or Nexus 9000), to enable Cisco DCNM to support those features. To apply that patch to your Cisco DCNM Native HA setup, follow the steps below:

  1. Stop the services on the Active node using the **/etc/init.d/FMServer** stop command.

2. Run **patch.sh** on the Active node.
3. Run **patch.sh** on Standby node.

Note Services are not stopped on Standby node.

4. Start services on the Active node using the **/etc/init.d/FMServer start** command.
5. Stop the services on Active node using the **/etc/init.d/FMServer stop** command, and roll back the patch.
6. Roll back the patch on the Standby node.
7. Start services on the Active node using **/etc/init.d/FMServer start** command.

- 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.
- **POAP Dynamic Breakout**—From Cisco NX-OS Release 7.0(3)I4(1), POAP dynamically breaks out ports to detect a DHCP server behind one of the broken-out ports. Previously, the DHCP server that is used for POAP was directly connected to a normal cable as the breakout cables were not supported. POAP determines which breakout map (for example, 10gx4, 50gx2, 25gx4, or 10gx2) brings up the link that is connected to the DHCP server. If breakout is not supported on any of the ports, POAP skips the dynamic breakout process. After the breakout loop completes, POAP proceeds with the DHCP discovery phase as normal.

  Cisco DCNM leverages the dynamic breakout to simplify the fabric setup by retaining successful breakout configuration. Since dynamic breakout requires the other side of the link to be active, there are circumstances where you must manually breakout interfaces, or may notice breakout in places which are not desired. In those situations, you must adjust the ports on the Interfaces page before performing Save and Deploy in the Fabric Builder.
- Before using the licensed features, install a Cisco DCNM license for each Nexus-managed platform. For information about licensing, see the Cisco DCNM Licensing Guide, Release 11.x.
- Depending on how a switch handles the **cdp enable** CLI command (enabled or disabled by default), Cisco DCNM shows this as config difference, although the Save and Deploy operation is performed to correct it. This depends on the default behavior of the switch image (that is, whether the **show running-config** shows the CLI or not). To address this issue, the respective policy template that is applied on the interfaces must be updated, so that the CLI is ignored during the configuration compliance check.
- Create a free-form configuration on all the white box switches that are managed by Cisco DCNM as shown below, and deploy them on all the switches before the final Save and Deploy operation.

```
line console
speed 115200
stopbits 2
```

  This is only applicable to the Cisco DCNM LAN Fabric mode.
- On Microsoft Windows 2016 Standard server, run the Cisco DCNM installation EXE file as an administrator. Cisco DCNM installation will not start on Microsoft Windows 2016 Standard server unless

you set the EXE file as an administrator. To start the installation EXE file, you can right-click on the EXE file, and choose **Run as administrator**.

- When the Cisco Nexus 9000v Virtual Switches are cloned, they may use the same serial number. Since Cisco DCNM discovers them using the same serial number, the device discovery operation fails.
- You cannot access the Cisco DCNM Web UI, when the user system is configured with the same IP address range as that of internal subnet used by the Application Framework in DCNM. For more information, see *Cisco DCNM Troubleshooting Guide*.
- The VXLAN OAM feature in Cisco DCNM is only supported on a single fabric or site.
- You cannot configure ICAM on the Cisco Nexus 9000 Series Switches Release 7.0(3)I7(6), and therefore, the telemetry will fail until the switch issue is resolved.
- Though you can delete PMN hosts, we recommended that you use this option with extreme caution, understanding that manual effort is needed to bring the solution back in sync.
- Cisco DCNM in Media Controller Deployment Release 11.x does not support non-default VRFs for Cisco Nexus 9000 Release 9.3(x).
- From Cisco DCNM Release 11.2(1), the Device Connector allows you to change the access mode via the Web UI at **Administration > DCNM Server > Device Connector > Settings > General**. The Cisco Intersight will not configure its device connector, and therefore, the Read-Only and Allow Control access mode in the Device Connector are not operational.
- Cisco DCNM does not support hot snapshots. While taking snapshots, we recommend that you power off the VM. Otherwise, ensure that you uncheck the **Snapshot the virtual machine's memory** option.
- Cisco DCNM does not support suspending or unsuspending of the VMs.
- Do not install NIR on standalone DCNM
- If NIR was installed and stopped, it does not stop service containers running on DCNM compute nodes.

  If the NIR application is deleted from DCNM, a few service containers continues to run DCNM compute nodes and must be stopped manually using **afw service** commands.
- When DCNM Tracker is enabled, the NIR LAN Telemetry feature in Managed mode and the EPL feature with the **Configure my Fabric** option selected, will not work. As a workaround, disable the DCNM tracker on the switches that are configured during the EPL or NIR LAN Telemetry configuration. For EPL, disable the DCNM tracker on the Spines/Route Reflectors (both RR1 and RR2). For NIR LAN Telemetry, disable the DCNM tracker on all the switches selected for telemetry configuration.
- The DCNM installer creates a _deviceImage-0.iso in the DCNM VM folder and mounts the ISO permanently to the VM. If this ISO is removed or the CD/DVD is disconnected, the VM will not boot. The VM will enter Emergency Mode and prompt you with the message:Give root password for maintenance. If the VM is down, CD/DVD drive can be disconnected. However, after you power it up again, the VM will enter Emergency Mode and provide a prompt.
- For leaf-leaf ports in non-VPC cases, DCNM will always push the **shutdown** command. If you want to bring up the port, add the **no cdp enable** command to the interface freeform policy on one of the ports.
- Two-factor authentication is not supported in DCNM.
- In Cisco DCNM SAN deployment, if the DCNM server streaming the SAN analytics is over-utilized, the Elasticsearch database service goes down. This results in performance issues. The Pipeline service

may be consuming all the CPU and system resources on the Cisco DCNM server. To troubleshoot this, do the following task:

1. Stop the Pipeline service.
2. Reduce the streaming load from the MDS fabric.
3. Start Elasticsearch service.
4. Start the Pipeline service.

- In Cisco DCNM SAN deployment, when you enable or disable alarms on a Primary node, it will not be applied to all the nodes in the Federation. You must manually enable or disable alarms on all nodes on all servers in the Federation setup. You must restart the DCNM Server to apply the changes.
- In Cisco DCNM SAN deployment, when you add or delete alarm policies on a Primary node, it will not be applied to all the nodes in the Federation. You must restart all the DCNM servers to apply this change on all servers in the Federation setup.
- In Cisco DCNM SAN deployment, when you modify the server properties on Cisco DCNM **Web UI > Administration > DCNM Server > Server Properties** on a Primary node, it will not be applied to all the nodes in the Federation. You must manually make the changes to the server properties on all nodes on all servers in the Federation setup. You must restart the DCNM Server to apply the changes.
- SAN Insights is not recommended on Windows Deployments, and is no longer supported from Release 11.3(1).
- SAN Insights is best supported on Linux from Release 11.0(1), and on Cisco DCNM OVA/ISO deployments from Release 11.3(1).
- From Cisco DCNM Release 11.3(1), you cannot download the SAN Client package from the Software Downloads page. You must install Cisco DCNM, launch Web UI to download the SAN Client and Device Manager. For more information, Cisco DCNM Installation and Upgrade Guide for SAN Deployment.
- In Releases prior to 11.3(1), if you have installed a preview feature, perform the following before you upgrade to Release 11.3(1):
  - Remove the configuration from older release setup.
  - Reset the property to enable the preview feature. On the Cisco DCNM Web UI, choose **Administration > DCNM Server > Server Properties**. Reset the **enable preview feature** property.
- We recommend that you do not upgrade any underlying third-party software separately. All the necessary software components will be DCNM upgrade will cause performance issues.

Certain commands must not be executed on Cisco DCNM, as they may harm the functionality of various components on the network. The following table shows the commands and specifies the reason why they must not be executed.

Table 1: List of Commands that must not be executed on Cisco DCNM

Command	Reason
systemctl restart network	This is a common Linux command that the network administrators use when editing the interface properties. The command has shown to render the DCNM useless when converting to the cluster mode. Use the equivalent **appmgr** commands for changing any IP addresses for eth0, eth1, or eth2 interfaces.

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 11.3(1) 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:

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.