Guidelines and Limitations

Guidelines and Limitations

The guidelines and limitations for installing and upgrading Cisco DCNM Release 11.2(1) 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.

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 11.2(1).
- 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.
- ElasticSearch was used to store the Performance monitoring stats, End point locator (EPL) data. If the compute cluster was deployed in the Cisco DCNM Release 11.1(1), and you must retain the ElasticSearch data intact, ensure that you take a backup of the compute nodes. You can restore the nodes after you upgrade. To backup, a compute node, you need to execute the backup script on each of the compute node separately. After you deploy the new compute, you can restore the backup on that compute node.
- 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.