New Features and Enhancements

New Features and Enhancements

Cisco Data Center Network Manager (DCNM) includes the new features, enhancements, and hardware support that are described in the following section:

New Features and Enhancements in Cisco DCNM, Release 11.4(1)

These following sections include information about the new features, enhancements, and hardware support introduced in the Cisco DCNM Release 11.4(1).

LAN Fabric Deployment Enhancements

The following features are new in Cisco DCNM Release 11.4(1) for the LAN Fabric Deployment.

Software Maintenance Update to use Network Insights for Resources (NIR) Application

To use NIR 2.2.2+ application with DCNM 11.4(1), you must install a maintenance update. Refer to Installing Software Maintenance Update in *Cisco DCNM Installation and Upgrade Guide for LAN Fabric Deployment, Release 11.4(1)* for instructions about how to install the maintenance update.

For more information about Network Insights for Resources, refer to the NIR 2.2.2 Release Notes.

Applications Services Engine

Beginning with Release 11.4(1), along with Computes, you can install Cisco DCNM in Standalone and Native HA mode on Cisco Applications Services Engine. For more information, see Application Services Engine Release Notes for Cisco DCNM.

Support for ASR1K and Cat9K

You can add Cisco IOS XE devices, like ASR1K and Cat9K, to your external fabric in Cisco DCNM. You can use them as edge and core routers. You can also create VRF-Lite external connectivity to them from the border devices that are part of VXLAN EVPN or Routed fabrics.

Enhanced Role-based Access Control

You can see the following role-based access control (RBAC) changes:

- Enhanced Read-only access to the Cisco DCNM Web UI and APIs for the **network-operator** user role
- A new user role called **network-stager**
- Freeze deployment for a particular fabric or all fabrics in DCNM as a user with the **network-admin** role

Note Actions that cannot be performed by a **network-stager** or a **network-operator** role will be grayed out on the DCNM Web UI and appropriately blocked on the corresponding REST APIs.

EPLD Support

Cisco DCNM supports EPLD upgrade for Cisco Nexus 9000 Series Switches and Cisco Nexus 3000 Series Switches. You can upload EPLD images like other images and upgrade them as well.

Multi-Site Domain (MSD) Backup and Restore

You can take a backup of MSD fabrics. When you initiate a backup from the MSD fabric, the backup and restore process is applicable for the member fabrics also.

Golden Backup

You can mark certain fabrics backups as golden in Cisco DCNM. Golden backups of fabrics cannot be deleted. Cisco DCNM archives up to 10 golden backups on a per fabric basis.

IPAM Integration Using Infoblox

You can use the IPAM Integrator application to view the dynamic and static IP allocation in an IPAM server such as Infoblox for the relevant overlay networks defined in DCNM. This application requires read-only access to the IPAM. Currently, this feature is supported for VXLAN EVPN fabrics including MSDs for overlay IPv4 networks for which DHCPv4 has been enabled. You can also choose to sync up records on-demand between the DCNM and Infoblox.

Preprovisioning an Ethernet Interfaces

You can preprovision Ethernet interfaces in the **Interface** window. This preprovisioning feature is supported in Easy, eBGP, and External fabrics. You can add the Ethernet interfaces to only preprovisioned devices before they are discovered in DCNM.

Support for CloudSec in Multi-Site Deployment

CloudSec feature allows secured data center interconnect in a VXLAN EVPN Multi-Site deployment by supporting source-to-destination packet encryption between border gateway devices in different fabrics. Cisco DCNM Release 11.4(1) provides an option to enable CloudSec in an MSD fabric.

The CloudSec feature is supported on Cisco Nexus 9000 Series FX2 platform starting with Cisco NX-OS Release 9.3(5) or later.

Migrating LAN Classic to LAN Fabric

From Cisco DCNM Release 11.4(1), the LAN Classic installation for DCNM is no longer supported. If you're planning to upgrade your LAN Classic deployment to DCNM Release 11.4(1), the only available upgrade option is to the DCNM Release 11.4(1) LAN Fabric deployment, and it's done automatically during the DCNM inline upgrade process.

In the LAN Fabric deployment, there are two fabric templates, namely, **LAN_Classic** and **Fabric_Group**, that you can use to manage your switches in a similar way as it was done in the DCNM Classic LAN, but with an enhanced feature-set.

BGP Peer Template Support

Until Cisco DCNM Release 11.3(1), in VXLAN EVPN Easy Fabric deployments, the same iBGP peer template for iBGP definition was used for the leafs, borders, and BGP RRs. From DCNM Release 11.4(1), the following fields can be used to specify different configurations:

- **iBGP Peer-Template Config** – Specifies the configuration used for BGP RRs on spines.
- **Leaf/Border/Border Gateway iBGP Peer-Template Config** – Specifies the config used for leaf, border, or border gateway. If this field is empty, the peer template defined in **iBGP Peer-Template Config** is used on all BGP enabled devices (RRs, leafs, border, or border gateways).

Viewing Policy Change History

In the DCNM Fabric Builder, you can click the **History** button to view per switch deployment and policy change history.

The newly introduced **Policy Change History** tab provides granular accounting on a per policy basis for each configurable entity in the fabric. This includes information of which users made what changes to what policies capturing all add, update, or delete operations including before and after configuration state comparison.

VMM Workload Automation

VMM workload automation is about the automation of network configuration in Cisco's Nexus switches for workloads spawned in a VMware environment. Note that this is a preview feature in the Cisco DCNM Release 11.4(1). This is an independent daemon that is not packaged with the DCNM. It needs to be downloaded and separately installed either on the DCNM or another Linux system if the pre-requisites are met. In a nutshell, the daemon listens to events from VMware vCenter and appropriate triggers overlay configuration on the corresponding switches below which the workloads are attached.

This feature allows the following functionalities:

- Discover the network objects in the VMware vCenter.
- Discover the connectivity between the servers (vswitches/DVSes) and the Nexus switches imported into DCNM.
- Use DCNM APIs to trigger creation and attachment of the appropriate overlay network configuration on the appropriate switches.

Configuration Compliance (CC) Side-by-side Comparison Enhancements

In prior DCNM 11.x releases, configurations such as boot string, rommon configuration, and other default configurations are ignored during strict CC checks. For such cases, the internal configuration compliance engine ensures that these config changes are not called out as diffs. These diffs are also not displayed in the

Pending Config window. But, the Side-by-side diff utility compares the diff in the two text files and does not leverage the internal logic used in the diff computation. As a result, the diff in default configurations is highlighted in red in the **Side-by-side Comparison** window. Starting from Cisco DCNM Release 11.4(1), such diffs are not highlighted in the **Side-by-side Comparison** window. The auto-generated default configuration that is highlighted in the **Running config** window is not visible in the **Expected config**window.

Programmable Reports

The Programmable Report application enables generation of rich contextual reports using Python scripts. The reports can collect information either directly from the devices or from the DCNM itself. Example reports include Resource tracking in fabrics, top-N top talkers based on VXLAN VNI counters in a fabric etc. Report jobs are run to generate reports. Each report job can generate multiple reports. You can schedule the report to be executed on a per device level or at a fabric level. These reports are then analyzed to obtain detailed information about the devices.

The REPORT template type is used to support the Programmable Reports feature. This template has two template subtypes- UPGRADE and GENERIC. A python SDK is provided to simplify report generation. This SDK is bundled with the DCNM and provides APIs to generate reports.

Layer 4-Layer 7 Services Support for Multi-Site Domain (MSD) Fabrics

The following enhancements are supported from Cisco DCNM Release 11.4(1):

- The service node can now be attached to a vPC border gateway or a vPC leaf or standalone leaf in a member fabric that is part of the MSD..
- RBAC support - the Layer 4-Layer 7 Service supports Role-Based Access Control (RBAC) along with fabric access mode.
- Service node backup and restore
- Fabric Backup and Restore
- Refreshing the Service Policy and Route Peering List
- Attaching a Service Policy or a Route Peering - To attach a specific service policy or route peering to a switch, select the check box next to the required service policy or route peering and click **Attach**.
- Detaching a Service Policy or a Route Peering - To detach a specific service policy or route peering from a switch, select the check box next to the required service policy or route peering and click **Detach**.
- Deployment history - To view deployment history of the switches and networks that are involved in the selected service policy or route peering, click **History** in the **Service Nodes** window.

Adding Authentication Parameters to Outbound Emails

Some SMTP servers may require addition of authentication parameters to emails that are sent from DCNM to the SMTP servers. Starting from Cisco DCNM Release 11.4(1), you can add authentication parameters to the emails that are sent by DCNM to any SMTP server that requires authentication.

Endpoint Locator Enhancements

The following enhancements are supported from Cisco DCNM Release 11.4(1):

- Click the **i** icon in the **Control** > **Endpoint Locator** > **Configure** window to view a template of the configuration that is pushed to the switches while enabling EPL. This configuration can be copied and pushed to RR/Spine devices to enable EPL on external fabrics.

- The name of the network is also displayed in the **Network** drop-down list in the **Monitor > Endpoint Locator > Explore** window. The Network name is obtained from the overlay networks defined in the Networks/VRFs listing.
- Search can be initiated by using the **VM Name** in the **Monitor > Endpoint Locator > Explore** window. The VM information retrieved from VMware vCenter is correlated with the endpoint information in the EPL database to provide a correlated view.
- To display a list of the most recent notifications, click the **Notifications** icon in the **Monitor > Endpoint Locator > Explore** window.
- An alarm is generated if there are any endpoint-related anomalies.

Endpoint Locator and Health Monitor Alarms

Starting from Cisco DCNM Release 11.4(1), alarms are registered and created under the **External** alarm category by the Endpoint Locator (EPL) and Health Monitor applications.

400G Tier Added to Physical Capacity Table

Starting from Cisco DCNM Release 11.4(1), the 400G tier has also been added to the **Physical Capacity** table under the **Capacity** tab. However, the **Physical Capacity** table under the **Capacity** tab will only show information about the physical ports that are present on the switch. For example, if the switch does not have a 400G physical port, the 400G tier is not displayed in the **Physical Capacity** table.

Discovery Support in DCNM Tracker

Typically, with DCNM 11.x, for all imported switches, by default, the discovery engine retrieves relevant inventory, interface, license, feature, module, connectivity etc. information, every 5 minutes. Starting from Cisco DCNM Release 11.4(1), the DCNM tracker has been enhanced to act as a pre-checker for the periodic discovery by comparing and checking the state or configuration outputs and updating the discovery engine if any state or configuration of interest to the discovery engine has changed on the switch. If nothing has changed on the switch, the tracker informs the discovery engine, which then optimizes and skips that periodic discovery cycle for the switch. So, the tracker acts as a discovery helper in this case. In large-scale deployments, the total discovery time is faster when the tracker is installed as unnecessarily polling of discovery-related information on the switch is not performed when there is no change in switch configuration. By default, this feature is turned on when the DCNM tracker is installed.

NX-API Certificate Management for Switches

Cisco NX-OS switches require an SSL certificate to function in NX-API HTTPS mode. SSL certificates are generated by users and signed by their Certificate Authority (CA). You can install the certificates manually using CLI commands on the switch console. From Release 11.4(1), Cisco DCNM provides an easy workflow to upload NX-API certificates to the DCNM, that in turn can be easily installed on the appropriate switches that are managed by DCNM.

Note This feature is supported on switches running on NXOS version 9.2(3) or higher.

Kubernetes Compute Visualization

From Release 11.4(1), Cisco DCNM allows you to import a Kubernetes (K8s) Container Orchestrator in the DCNM. Using standard K8s APIs, DCNM provides a correlated compute and network view of container workloads that are running on compute nodes that are attached to switches imported into the DCNM. The K8s clusters themselves may be running on either bare-metal servers or on virtual machines running in ESXi environments managed by VMware vCenter.

Media Controller Deployment Enhancements

The following features are new in Cisco DCNM Release 11.4(1) for Media Controller Deployment.

Generic Multicast Monitoring

In addition to IP Fabric Non-Blocking Multicast (NBM), IP Fabric Media mode now provides visibility into Generic Multicast traffic. The feature provides end to end flow path visibility, topology, and statistics.

You can use the Generic Multicast feature for monitoring purposes. This feature is applicable for switches with the Cisco NX-OS Release 9.3(5) and later.

Generic Multicast is available with the Media Controller deployment mode. After DCNM installation, you need to decide whether to run DCNM in IP Fabric for Media (IPFM) mode or Generic Multicast mode. You can enable the Generic Multicast mode by using the **pmn.generic-multicast.enabled** server property.

Flow Priority

You can now control priority of migrating flows in case of node or link failures by controlling flow priority through Flow Policy Management.

In the **Add Flow Policy** or **Edit Flow Policy** windows, from the **Flow Priority** drop-down list, you can choose the priority for the flow. You can choose either **Low** or **Critical**. The default value is **Low**.

Any Source Multicast (ASM) Enhancements

You can decide whether to stream sender traffic to spine or not. You can choose to conserve uplink bandwidth at the cost of slight increase in overall flow setup time.

You can check the **Reserve Bandwidth to Receiver Only** check box to push the ASM traffic to spine only if there is a receiver. This feature is applicable for switches with the Cisco NX-OS Release 9.3(5) and later.

You can use the **Deploy** button to deploy only unicast bandwidth configuration or reserve bandwidth configuration.

Real-time Fault and Threshold Notifications

Real-time fault and threshold crossing notifications are available via AMQP. You can create a dedicated queue to get the real-time events. An event is generated when an **interface used bandwidth** reaches to - 60%, 75%, or 90%. A clear event is generated when the usage falls below the 5% threshold.

Copying Switch Running Configuration to Start-up Configuration

Whenever there is any deployment to the switch via DCNM, the switch running configuration is automatically saved to the start-up configuration. In other words, DCNM invokes the **copy r s** command on a switch immediately after a deployment to make sure that the configuration is preserved between the switch reloads. An event with the category ‘CopyRS’ is logged in **Media Controller > Events** when the **copy r s** command is invoked as well as when it’s completed either successfully or with an error.

SAN Deployment Enhancements

The following features are new in Cisco DCNM Release 11.4(1) for SAN Deployment.

Viewing FICON Ports

You can view the Port WWN details by choosing **Settings** > **Columns** and choose the **Port WWN** option from the drop-down list.

You can print, export the data, or customize the columns you want to view.

Zone Migration Tool

You can migrate pWWN-based SAN zones from a Brocade switch to a Cisco MDS switch. This involves the following steps:

1. Generate the Brocade configuration files.
2. Convert the files using the zone migration tool to make them compatible with Cisco MDS switches.
3. Apply the generated zoning output to Cisco MDS switches.

This feature supports migration of Brocade’s fabric switches running Brocade Fabric OS v7.x.x or later in this release.

Removal of LAN Items in Topology

In the DCNM Release 11.4(1) SAN deployment modes, the LAN items have been removed from the Topology window.

The following search options are available for the DEFAULT_LAN scope:

- Quick Search
- VLAN

The following search options are available for the DEFAULT_SAN scope:

- Quick Search
- VLAN
- VSAN ID/Name

Shutdown Interfaces

Click the **No Shutdown** or **Shutdown** toolbar button to enable or disable switch interfaces. After you click a button, a dialog box pops up asking for a confirmation. Click **Yes** to proceed or **No** to cancel the operation.

SAN Insights Enhancements

- The **SAN Insights Flows** dashlet displays donuts depicting flow summary for IT Pairs and ITL Flows when the SCSI protocol is selected from the protocol drop-down list. The **SAN Insights Flows** dashlet displays donuts depicting flow summary for IT Pairs and ITN Flows when the NVMe protocol is selected from the protocol drop-down list. You can display data for Read Completion Time or Write Completion Time by selecting the required option from the dropdown list.
- Top 10 Hosts and the Top 10 Storage charts on the Dashboard now display enclosures/WWPNs/Device Alias in the selected Protocol/Fabric/Switch scope.
- The Flow Summary and the Enclosure Summary donuts are refreshed every 15 minutes.
- From Release 11.4(1), Cisco DCNM allows user to view data for more than two weeks time frame (up to a default maximum of 90 days). You can choose the date using the date picker and view the historical data starting from the selected date at hourly granularity.
- From Release 11.4(1), you can filter ECT Analysis by **Device Alias**, also.
- Starting 11.4 release, the deviation of the ECT less than the baseline is considered as negative deviation. The Web UI screens are expected to display negative values for the computed deviation percentage.
- If ECT is below 10% from Baseline, the color Green implies normal range.

- In Release 11.4(1), the Custom Graphing metrics is enhanced to include the Write IO Failures, Read IO Failures, Write IO Aborts and Read IO Aborts to the drop-down metrics list.
- From Release 11.4(1), the San Insight Pipeline Collector and the SAN Insight Post Processing applications can only be paused and resumed from Cisco DCNM **Web UI** > **Applications** > **Catalog**.

Common Enhancements applicable for all DCNM Install types

Software Maintenance Update to address Log4j2 vulnerability

Cisco DCNM Release 11.4(1) provides Software Maintenance Update (SMU) to address **CVE-2021-45046** and **CVE-2021-44228** issue. Note that CVE-2021-45105 has a lower severity and not used in DCNM with default configuration, therefore it is not addressed here.

For more information, refer to ***Installing Software Maintenance Update for log4j2 Vulnerability*** chapter in Cisco DCNM Installation Guide for your deployment type.

Tetration Agent with DCNM Validation

You can install tetration agent on Cisco DCNM and compute nodes for OVA and ISO installations. After you install the agent, the server nodes will point to the titration cluster and start streaming data to it.

Server Status

From Cisco DCNM Release 11.4(1), you can see the status of the following services as well:

- NTPD server
- DHCP server
- SNMP traps
- Docker Registry
- Syslog Receiver

New Hardware Supported

The following new hardware is supported from Cisco DCNM Release 11.4(1).

- N9K FC/FCoE switch mode support
- N9K FC/FCOE NPV support for N9K-C93360YC-FX2
- N9K-C93180YC-FX3S
- N9K-C93108TC-FX3P

Videos: Cisco DCNM Release 11.4(1)

For videos created for features in Release 11.4(1), see Cisco Data Center Network Manager, Release 11.4(1).