New Features and Enhancements

- New Features and Enhancements in Cisco DCNM, Release 11.3(1), on page 1

New Features and Enhancements in Cisco DCNM, Release 11.3(1)

These following sections include information about the new features, enhancements, and hardware support introduced in the Cisco DCNM Release 11.3(1).

- LAN Fabric Deployment Enhancements, on page 1
- Media Controller Deployment Enhancements, on page 4
- SAN Deployment Enhancements, on page 5
- Common Enhancements applicable for all DCNM Install types, on page 6
- Videos: Cisco DCNM Release 11.3(1)

LAN Fabric Deployment Enhancements

The following features are new in Cisco DCNM Release 11.3(1) for the LAN Fabric Deployment.

Network Provisioning for Layer 4-Layer 7 Services

Automated provisioning and seamless integration of Layer 4-Layer 7 (L4-L7) services, or Elastic services, in a data center is required, due to the growing SLA and security requirements in a cloud environment. Service devices, such as, firewalls and load balancers are typically attached to service leafs with the goal of redirecting appropriate traffic to these nodes where traffic inspection policies can be applied. A simple workflow has been introduced for easy integration of L4-7 services into a VXLAN EVPN fabric. This includes steps for service node attachment, route peering, service policy configuration, and monitoring.

IPv6 Underlay aka VXLANv6

You can create a VXLAN EVPN fabric with IPv6 only underlay, using either IS-IS or OSPFv3 as the IGPs. This support has been added on N9k based NX-OS devices beginning with software version 9.3(1). In such a VXLANv6 fabric deployment, intra-fabric links, routing loopback, vPC peer link SVI, and NVE loopback interface for VTEPs are all configured only with IPv6 addresses. EVPN BGP neighbor peering is also established using IPv6 addressing. VXLANv6 does not support FEX attached to a VXLAN-enabled switch.

Support for POAPv6

Zero-touch Day-0 bring-up of devices is now supported with DCNM using only IPv6. The bootstrap functionality in DCNM has been extended to support either POAPv6. On a per fabric basis, either POAPv4 or POAPv6 can be selected. Coexistence of POAPv4 and POAPv6 across multiple fabrics is supported.

VXLAN EVPN to SR-MPLS and MPLS LDP Interconnection

The following handoff features are supported in DCNM:

- VXLAN to SR-MPLS
- VXLAN to MPLSLDP

These features are supported on the border devices, such as, border leaf, border spine, and border super-spine in VXLAN EVPN fabrics. The devices must be running Cisco NX-OS Release 9.3(1) or later. These DCI handoff approaches are the one box DCI solution where no extra Provider Edge (PE) device is needed on the external fabric.

Support for Non-Nexus devices

You can discover the following non-Nexus devices in an external fabric:

- IOS XE-based devices: Cisco CSR 1000v
- IOS XR-based devices: Cisco ASR 9000 Series Routers and Cisco NCS 5500 Series Routers
- Arista Devices

Hybrid Cloud Connectivity

DCNM 11.3(1) allows seamless integration of your existing Cisco Data Center to the public cloud, not only providing significant investment protection, but also acts as an incremental step for a customer's journey into the cloud. Cisco Multi-Cloud with DCNM version 11.3 supports Microsoft Azure as the first public cloud, with more to come. The integration is achieved employing the Cisco 1000V cloud services router using the same Multi-Site constructs and workflows that are used to extend DCI between multiple on-premise data centers managed by DCNM.

Endpoint Locator 2.0

From Cisco DCNM Release 11.3(1), information about the Endpoint Locator is displayed on a single landing page or dashboard. The dashboard displays a near real-time view (refreshed every 30 seconds) pertaining to all the active endpoints across all fabrics. The data that is displayed on this landing page depends on the scope that you select from the **SCOPE** drop-down list. The following enhancements are made to the Endpoint Locator (EPL) feature on DCNM:

- Support for monitoring and tracking of Dual-attached and Dual-Stack endpoints
- Capability to monitor and display MAC-only endpoints for Layer-2 VXLAN EVPN deployments.
- Multi-Fabric Support: Up to four fabrics are supported. This is supported only in clustered mode.
- Support for Multi-Site Deployments using Multi-Site Domains(MSD)
- EPL for VXLANv6 fabrics
- Supported scale: 100K unique endpoints

Super-Spine Support

Super Spines are supported within the VXLAN EVPN Easy Fabric (aka fabrics created with the Easy_Fabric_11_1 template). Super Spines are devices that allow multiple spine-leaf based VXLAN EVPN PODs to be interconnected in a seamless manner. The same IGP domain extends across the PODs all the way to the Super Spines. Border functionality can optionally be configured on the Super Spines. The following Super-Spine roles are supported in DCNM:

- Super-Spine
- Border Super-Spine
- Border Gateway Super-Spine

Autoprovisioning of ToR Switches

You can add Layer 2 Top-of-Rack (ToR) switches in an external fabric, and they can be connected to the Leaf switches in the Easy Fabric. Typically, the Leaf and ToR devices are connected with back-to-back vPC connection. By enabling an autoprovisioning knob in the Multi-Site Fabric template, appropriate VLAN and interface configuration can be auto-provisioned on the ToR switches, based on the overlay networks that are deployed on the attached leaf switches.

Deploying Networks in Routed Fabrics

From Cisco DCNM Release 11.3(1), you can use the existing Networks & VRFs workflow to create appropriate HSRP or VRRP-based network configuration in a spine-leaf based routed fabric. This is the typical deployment case for MSDs. A routed fabric is run in one VRF, which is the default VRF. Since the fabric is an IPv4 fabric, IPv6 address provisioning for the networks isn't supported. In a routed fabric, a layer-3 network can only be attached to one device or a pair of vPC devices, unless it's a Layer 2 only network.

DCNM Tracker

From Cisco DCNM Release 11.3(1), use the DCNM tracker feature to enable continuous configuration compliance(CC) checks. The DCNM Tracker is targeted for large-scale deployments or for users requiring prompt Out-of-band notifications. The core configuration compliance (CC) engine logic in DCNM is now packaged into a new form factor that can be installed directly on the switch. Installation of a DCNM tracker via the DCNM GUI, leads to the installation of a small utility that runs on the guest shell of the switch and monitors changes in intent, running configuration, and so on. The changes are then relayed back to the parent DCNM instance.

Strict Configuration Compliance

The Strict Configuration Compliance feature performs a strict check on the exact difference between the running configuration on the switch versus the associated intent. Any commands including any defaults generated in the running configuration by the switch, needs to be part of the intent; otherwise an OUT-OF-SYNC status will be reported. In that case, the pending configuration generates **no** commands for the configurations that are present on the switch but aren't present in the associated intent. You can enable the strict configuration compliance feature in the **Fabric Settings** of the easy fabric templates. This feature is disabled by default.

Note If Strict Configuration Compliance is enabled in a fabric, you can't deploy Network Insights for Resources on Cisco DCNM.

Preview Config

Starting from Cisco DCNM Release 11.3(1), you can right-click the switch in the **Fabric Builder** window and click **Preview Config** to view the pending configuration and the side-by-side comparison of the running and expected configuration aka intent.

BFD Underlay

From Cisco DCNM Release 11.3(1), BFD within a fabric is supported natively. The BFD feature is disabled by default in the Fabric Settings. If enabled, BFD can be enabled individually for the underlay protocols, BGP, PIM etc. across the entire fabric. Any custom required BFD configurations must be deployed via the per switch freeform or per interface freeform policies.

Layer 3 Port Channel Support

From Cisco DCNM Release 11.3(1) Layer 3-port channels are natively supported for external connectivity. This includes support for Layer-3 port-channel sub-interfaces. All configuration knobs related to Layer-3 port-channels are available in the default best practice template that is packaged with DCNM.

Symmetric VRF Lite Auto-Provisioning

From Cisco DCNM Release 11.3(1), VRF Lite configuration can be automatically provisioned in a symmetric manner between border devices and external routers connected via VRF Lite.

Operational Support for Easy Fabrics

This feature provides the operational status of a fabric in terms of active monitoring of BGP sessions, IS-IS/OSPF sessions, vPC peer-keep-alive sessions etc. and provides a logical link topology view for easy perusal. In the Fabric Builder, there's a tabular view that lists down this operational status on a per fabric basis.

Pre-ISSU and Post-ISSU Reports for LAN Fabric Deployments

While performing switch image upgrades using DCNM, you can now perform appropriate customized pre-upgrade and post-upgrade checks as part of the enhanced upgrade workflow. This leverages the novel flexible programmable report infrastructure introduced in DCNM 11.3(1). The infrastructure allows a user to generate pre-ISSU and post-ISSU reports when you install the Image Management and Upgrade workflow.

Package [SMU/RPM] in LAN Fabric Deployments

Image Management also helps you to install or uninstall the required packages and patches. All RPM packages and SMU patches of the selected fabric appear in the Package [SMU/ RPM] window. You can now install, uninstall, activate, or deactivate packages using SMU or RPM.

Image Management Policies in LAN Fabric Deployments

The image management policies have the information of intent of NX-OS images along with RPMs or SMUs. The policies can belong to a specific platform or to an umbrella of different types of platforms. An umbrella type policy can have policies for one or more platforms. Regardless of a switch's platform, you can associate an umbrella image management policy with a group of switches. Based on the policy applied on a switch, Cisco DCNM checks if the required NX-OS and RPMs or SMUs are present on the switch. If there is any mismatch between the policy and images on the switch, an appropriate fabric warning is generated.

DCNM on SE appliance

Beginning from Release 11.3(1), for the compute nodes on which NIR/NIA will be hosted, in addition to the OVA/ISO, you can now use the SE-CL-L3 appliance. With the SE, the ISO image is pre-installed in compute mode on the physical appliance. Refer to Application Services Engine Release Notes for Cisco DCNM for more information.

Media Controller Deployment Enhancements

The following features are new in Cisco DCNM Release 11.3(1) for Media Controller Deployment.

RTP Flow Monitor

Cisco DCNM allows you to monitor per flow RTP traffic and receive an alert in case of packet drops. Information about any loss in flow is streamed to the Cisco DCNM controller which then indicates the location in the network where the loss was detected. You can view the flow topology for the active flows.

Scope in Media Controller

The switch groups that you created in the **Administration > DCNM Server > Switch Groups** window are listed under the **SCOPE** drop-down list. Creating switch groups help you to manage switches because they are grouped logically. For example, you can create host or flow policies for switches in a specific switch group instead of creating it for all the switches. Similarly, you can view the flow topology for a specific switch group containing switches.

PMN Read-Only Update

Starting from Cisco DCNM Release 11.3(1), Host Policies, Flow Policies, and Global menu items are displayed in the Media Controller deployment in DCNM Read-only mode. DCNM retrieves information about the host policies, flow policies, and global configuration from each switch in the fabric and displays the retrieved information. The information that is displayed is specific to each switch.

PTP Monitoring Application

The Precision Time Protocol (PTP) is a time synchronization protocol for nodes that are distributed across a network. On a local area network, it achieves clock accuracy in the submicrosecond range, making it suitable for measurement and control systems. In DCNM, PTP Monitoring can be installed as an application.

Discovered Host Enhancement

Starting from Cisco DCNM Release 11.3(1), multiple entries of the same host are grouped as an expandable row

SAN Deployment Enhancements

The following features are new in Cisco DCNM Release 11.3(1) for SAN Deployment.

- From Release 11.3(1), Cisco DCNM allows SAN deployment using OVA/ISO installations. You can also migrate performance data from 10.4(x), 11.1(1), and 11.2(1) releases to the newly installed DCNM 11.3(1).
- From Release 11.3(1), Cisco DCNM SAN Client is shipped with self-signed certificate as trust certificate for the DCNM Server. If the DCNM server certificate is updated to use CA signed certificate, you must modify the trust certificate on the SAN Client.
- You can configure alarms for SAN switches.

SAN Insights Enhancements

- SAN Insights is not supported on Windows from Release 11.3(1).
- From Release 11.3(1), SAN Insights is supported with Cisco DCNM OVA/ISO deployments.
- Top 10 Host and Top 10 Storage analytics is displayed on the SAN Insights Dashboard. Each graph shows Top 10 details based on read/writes for IOPs, throughput, ECT.

  Also, you can also view the data for either Enclosure or WWN.
- Along with the current FC-SCSI endpoints, Cisco DCNM supports flows to the FC-NVMe endpoints also.
  - DCNM Nexus pipeline receives FC-NVMe flow data streaming from Cisco MDS9000 switches.

- Post processing is updated to calculate deviation and other metrics for FC-NVMe flows.
- San Insights Dashboard, Monitoring SAN Insights allow you to choose either FC-SCSI or FC-NMVe analysis.

- Deviation buckets can be configured, based on your requirements, by editing the **san.telemetry.deviation** parameters in the server properties file.

Common Enhancements applicable for all DCNM Install types

Software Maintenance Update to address Log4j2 vulnerability

Cisco DCNM Release 11.3(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.

DCNM Integration with ServiceNow

ServiceNow offers applications for IT Service Management (ITSM) and IT Operations Management (ITOM). There are four primary modules, namely, inventory discovery, incident management, event management, and change management workflows. Starting from Cisco DCNM Release 11.3(1), we provide Cisco DCNM integration with ServiceNow. This enables you to integrate end-user IT data with the ServiceNow platform. The integration provides a default set of ServiceNow custom tables that are populated with configuration data.

REST API Tool

All operations triggered via the DCNM Web UI like discovery, fabric management, monitoring, and so on, result in invocation of a series of HTTP calls to DCNM server to complete the respective task/operation. The REST API tool enables you to examine each of these API calls by viewing the structure of an API call. This tool also provides a corresponding CURL request that can aid in building quick prototypes for northbound integration to DCNM by calling the respective APIs. This tool compliments the Swagger-based REST API definitions that are exposed via the product URL, https://DCNM-IP/api-docs.

Login Image and MOTD

Now you can customize the background image and add a message to the Cisco DCNM Web UI login page. If you have many instances of DCNM, this allows you to identify the correct DCNM instance based on the background image and the message on the login screen.

Licensing Enhancements

From Release 11.3(1), Cisco DCNM Evaluation license validity is extended from 30 days to 60 days. That implies, the evaluation license expires after 60 days. However, Cisco DCNM allows you to use all the licensed features. Switches remain in honor mode until the switch is licensed again or the user manually removes the license.

In addition, the new UI enhancement for bulk license installation, allows you to upload multiple license files at once. It parses the license files, extract serial numbers, and tag them to the respective switches. The appropriate licenses are then applied to the respective switches.

New Hardware Supported

- N9K FC/FCoE switch-mode support for N9K-93180YC-FX

User Access

From Release 11.3(1), Cisco DCNM offers the user access based on your network security requirements. The following user roles are used to access DCNM via SSH or console that is introduced with Release 11.3(1).

- sysadmin
- SSH access by user root

The DCNM GUI root user is no longer created. Alternatively, use the Admin user role to log on to the DCNM Web UI.

Note During Inline upgrade, you must provide a new password for the **sysadmin** user.

Videos: Cisco DCNM Release 11.3(1)

For videos created for features in Release 11.3(1), see Cisco Data Center Network Manager, Release 11.3(1).