New and Changed Information

This chapter contains the following section:

New and Changed Information

The following table provides an overview of the significant changes to this guide for this current release. The table does not provide an exhaustive list of all changes made to the guide or of the new features in this release.

Table 1: New and Changed Behavior in Cisco DCNM, Release 11.4(1)

Feature	Description	Where Documented
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 borders. You can also create VRF-Lite external connectivity using them as borders.	Configuring IOS-XE Devices for Discovery
Enhanced Role-based Access Control	A new role called network-stager is added to Cisco DCNM. As a network stager, you can make changes or create intents, but not deploy them on the fabric. A network stager cannot view the administrator options.	Enhanced Role-based Access Control in Cisco DCNM • Video on Cisco.com • Video on YouTube
EPLD Support	Cisco DCNM supports EPLD upgrade for Cisco Nexus 9000 Series Switches. You can upload EPLD images like other images and upgrade them as well.	EPLD Installation
Multi-Site Domain Backup and Restore	You can take a backup of MSD fabrics. When you initiate a backup from the parent fabric, the backup process is applicable for the member fabrics as well.	• Backing Up Fabrics • Restoring MSD Fabrics • Video on Cisco.com • Video on YouTube

Golden Backup	You can initiate golden backups for all fabrics in Cisco DCNM. Golden backups of fabrics cannot be deleted. Cisco DCNM archives up to 10 golden backups.	Golden Backup
Support for IPAM Integration Using Infoblox	You can use the IPAM Integrator application to view the IP allocation in IPAM server and relevant networks defined in DCNM. This application allows read-only access to the IPAM and DCNM servers.	IPAM Integrator • Video on Cisco.com • Video on YouTube
Preprovisioning an Ethernet Interface	You can preprovision Ethernet interfaces in the Interface window. This preprovisioning feature is supported in Easy, eBGP, and External fabrics.	Pre-provisioning an Ethernet Interface
CloudSec in Multi-Site Deployment	CloudSec feature allows secured data center interconnect in a multi-site deployment by supporting source-to-destination packet encryption between border gateway devices in different fabrics.	Support for CloudSec in Multi-Site Deployment • Video on Cisco.com • Video on YouTube
Managing LAN Classic Templates	When you upgrade your LAN Classic deployment to DCNM Release 11.4(1), it's automatically upgraded to the LAN Fabric deployment 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.	Managing Switches Using LAN Classic Templates
BGP Peer Template Support	You can use the following fields to specify different configurations: • **iBGP Peer-Template Config** – Specifies the config used for RR and spines with border role. • **Leaf/Border/Border Gateway iBGP Peer-Template Config** – Specifies the config used for leaf, border, or border gateway.	Creating a New VXLAN BGP EVPN Fabric
Viewing Policy Accounting History	You can click the **History** button to view per switch deployment and policy change history.	• Fabric Multi Switch Operations • Viewing Policy Change History
Workload Automation for VMware vSphere	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).	VMM Workload Automation • Video on Cisco.com • Video on YouTube

Side-by-side Comparison	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 are 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.	Configuration Compliance in DCNM
Programmable Report	The Programmable Report application enables generation of reports using Python 2.7 scripts. Report jobs are run to generate reports. Each report job can generate multiple reports. You can schedule the report to run for a specific device or fabric.	Programmable Report • Video on Cisco.com • Video on YouTube

Layer 4-Layer 7 Service	The following enhancements are supported from Cisco DCNM Release 11.4(1): • The service node can now be attached to a vPC border gateway. • Support for Multi-Site Domains (MSD) • RBAC support - Starting from Cisco DCNM Release 11.4(1), 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 checkbox 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 checkbox 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.	Layer 4-Layer 7 Service
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.	Adding Notification Forwarding
ServiceNow	Starting from Cisco DCNM Application version 1.1, multiple MID servers can be added in the **Cisco DCNM > Properties** table. This means that data can be retrieved from multiple DCNM setups at the same time. In the ServiceNow GUI, data from each DCNM is distinguished by the DCNM IP address. You can also specify the categories for which incidents have to be created.	DCNM Integration with ServiceNow

Endpoint Locator	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 spines or border gateway 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. • Search can be initiated by using the **VM Name** in the **Monitor > Endpoint Locator > Explore** window. • Tp 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
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.	Endpoint Locator Alarms Health Monitor Alarms
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.	More Details

Discovery Tracker	Starting from Cisco DCNM Release 11.4(1), the discovery tracker acts 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. In the absence of the DCNM tracker or if there is a tracker malfunction, the discovery engine performs as before by initiating a query every 5 minutes to discover all the data on the switches on which the tracker is missing or unresponsive. By default, this feature is turned on when the DCNM tracker is installed.	Discovery Tracker
NX-API Certificate Management for Switches	Cisco DCNM provides a Web UI framework to upload NX-API certificates to DCNM. Later, you can install the certificates on the switches that are managed by DCNM. **Note** This feature is supported on switches running on NXOS version 9.2(3) or higher.	NX-API Certificate Management for Switches • Video on Cisco.com • Video on YouTube
Container Visualization	Release 11.3(1) allows you to visualize Container Orchestrator in Lab set up. From Release 11.4(1), Cisco DCNM allows you to configure Container Orchestrator. This feature allows you to visualize Kubernetes cluster as Container Orchestrator with the Cisco DCNM.	• Container Orchestrator • Using the UI Controls on Container Orchestrator Visualization