Cisco UCS Director Release Notes, Release 6.7

First Published: 2019-01-09

Last Modified: 2020-11-20

Cisco UCS Director Release Notes

Cisco UCS Director

Cisco UCS Director delivers unified, highly secure management for supported compute, network, storage, and virtualization platforms and for the industry's leading converged infrastructure solutions, which are based on the Cisco Unified Computing System (Cisco UCS) and Cisco Nexus platforms. Cisco UCS Director extends the unification of computing and network layers through Cisco UCS to provide data center administrators with comprehensive visibility and management capabilities for compute, network, storage, and virtualization. For more information, see Cisco UCS Director on Cisco.com.

Revision History

Release	Date	Description
6.7	January 9, 2019	Created for Release 6.7.
6.7(1.0)	April 9, 2019	Updated to include information on Release 6.7(1.0). See the following sections: • New and Changed Features in Release 6.7(1.0), on page 18 • Open Bugs in Release 6.7(1.0), on page 34 • Resolved Bugs in Release 6.7(1.0), on page 36
6.7(2.0)	June 14, 2019	Updated the document to include information on Release 6.7(2.0). See the following sections: • New and Changed Features in Release 6.7(2.0), on page 18 • Open Bugs in Release 6.7(2.0), on page 35 • Resolved Bugs in Release 6.7(2.0), on page 36

Release	Date	Description
6.7(3.0)	August 19, 2019	Updated the document to include information on Release 6.7(3.0). See the following sections: • Supported Upgrade Paths to Cisco UCS Director, Release 6.7(3.0), on page 6 • New and Changed Features in Release 6.7(3.0), on page 19 • Open Bugs in Release 6.7(3.0), on page 35 • Resolved Bugs in Release 6.7(3.0), on page 37
6.7(4.0)	March 9, 2020	Updated the document to include information on Release 6.7(4.0). See the following sections: • Supported Upgrade Paths to Cisco UCS Director, Release 6.7(4.0), on page 7 • Supported Upgrade Paths for Bare Metal Agent Patch Release 6.7(4.0), on page 8 • New and Changed Features in Release 6.7(4.0), on page 25 • Open Bugs in Release 6.7(4.0), on page 35 • Resolved Bugs in Release 6.7(4.0), on page 37

System Requirements

The system requirements for this release are available in the Cisco UCS Director installation and upgrade guides for the following:

- VMware vSphere
- Microsoft Hyper-V

Supported Browser Versions

Cisco UCS Director supports the following browsers:

- Internet Explorer 8 or higher

- Firefox 12 or higher (PC and Apple MAC)
- Safari 6 or higher
- Google Chrome 18 or higher
- Opera 12 or higher (PC and Apple MAC)

Minimum System Requirements for a Single-Node Setup

The following tables detail the minimum resource requirements for a single-node setup of Cisco UCS Director. Cisco recommends a single-node setup for installations of up to 5000 VMs.

For optimal performance, the entire memory and CPU allocations specified in the table below should be reserved. Failure to follow these specifications could affect performance. For example, 4 vCPU cores with 3000 MHz and 16G of memory must be reserved for the Cisco UCS Director VM.

The minimum memory required for the **inframgr** service is automatically set during deployment. To enable the **inframgr** service to use more than the minimum required memory, edit the `inframgr.env` file available in the following location:

`/opt/infra/bin/`

In this file, update the MEMORY_MAX parameter to the value you want. To activate the changes, restart the **inframgr** service.

The default memory settings are MEMORY_MIN=8192m and MEMORY_MAX=8192m.

For information about minimum system requirements for a multi-node setup, see the Cisco UCS Director Multi-Node Installation and Configuration Guide.

Table 1: Minimum system requirements for a single-node installation (up to 5,000 VMs)

Element	Minimum Supported Requirement
vCPU	4
Allocated Memory	16 GB
Reserved Memory	16 GB
Disk Space	100 GB
Disk Write I/O Bandwidth	4 MBps
Disk Read I/O Bandwidth	4 MBps
Memory Allocated for **inframgr**	8 GB

Restart the Cisco UCS Director database and all Cisco UCS Director services after making these changes to the `/etc/my.cnf`.

Minimum System Requirements for a Multi-Node Setup

System Requirements for the Primary Node

Number of VMs	vCPU Allocation	Memory Allocation (GB)	Memory Reservation (GB)	Disk Size (GB)	Inframgr Memory Allocation (GB)
1 - 5000	4	16	16	100	8
5001 - 10000	4	22	22	100	12
10001 - 15000	4	28	28	100	12
15001 - 20000	4	34	34	100	16
20001 - 25000	8	40	40	100	16
25001 - 30000	8	46	46	100	24
30001 - 35000	8	52	52	100	24
35001 - 40000	8	58	58	100	28
40001 - 45000	8	64	64	100	28
45001 - 50000	8	64	64	100	32

You can configure the Inframgr memory allocation in the `/opt/infra/bin/inframgr.env` file.

System Requirements for the Database Node

Number of VMs	vCPU Allocation	Memory Allocation (GB)	Memory Reservation (GB)	Disk Read I/O Bandwidth (MBps)	Disk Write I/O Bandwidth (MBps)	Disk Size (GB)	MySQL InnoDB Buffer Pool (GB)
1 - 5000	4	12	12	4	4	100	8
5001 - 10000	4	16	16	6	6	100	12
10001 - 15000	4	28	28	8	8	100	24
15001 - 20000	4	40	40	10	10	200	36
20001 - 25000	8	52	52	12	12	200	48
25001 - 30000	8	64	64	14	14	200	60

Number of VMs	vCPU Allocation	Memory Allocation (GB)	Memory Reservation (GB)	Disk Read I/O Bandwidth (MBps)	Disk Write I/O Bandwidth (MBps)	Disk Size (GB)	MySQL InnoDB Buffer Pool (GB)
30001 - 35000	8	76	76	16	16	300	72
35001 - 40000	16	90	90	18	18	600	84
40001 - 45000	16	90	90	20	20	600	84
45001 - 50000	16	90	90	22	22	600	84

You can configure the MySQL InnoDB Buffer Pool parameter in the `/etc/my.cnf` file.

Note To determine the currently configured disk read I/O bandwidth and disk write I/O bandwidth, use the **Collect Diagnostics** option from the Cisco UCS Director Shell Admin menu.

MySQL Parameters

VMs	Thread Cache Size	Maximum Connections	innodb lock wait timeout	Query Cache Size (MB)	Maximum Connection Errors	Connection Timeout	innodb read I/O Threads	innodb write I/O Threads
1 - 5000	1000	1000	100	128	10000	20	64	64
5001 - 10000	1000	1000	100	128	10000	20	64	64
10001 - 15000	1000	1000	100	128	10000	20	64	64
15001 - 20000	1000	1000	100	128	10000	20	64	64
20001 - 25000	2000	2000	100	128	10000	20	64	64
25001 - 30000	2000	2000	100	128	10000	20	64	64
30001 - 35000	4000	2000	100	128	10000	20	64	64
35001 - 40000	4000	4000	100	128	10000	20	64	64

VMs	Thread Cache Size	Maximum Connections	innodb lock wait timeout	Query Cache Size (MB)	Maximum Connection Errors	Connection Timeout	innodb read I/O Threads	innodb write I/O Threads
40001 - 45000	4000	4000	100	128	10000	20	64	64
45001 - 50000	4000	4000	100	128	10000	20	64	64

Configure these parameters in the `/etc/my.cnf` file.

Installation and Upgrade Notes

Cisco UCS Director uses a standard virtual machine that is delivered in OVF format for VMware, and in VHD format for Microsoft Hyper-V. It can be hosted on VMware vSphere or vCenter, or on Microsoft Hyper-V Manager. For installation instructions, see the appropriate Cisco UCS Director installation guide.

Cisco UCS Director, Release 6.7 is installed on two disks in the virtual machine (VM). The primary disk (Hard Disk 1) hosts the operating system and the Cisco UCS Director application. The secondary disk (Hard Disk 2) hosts the Cisco UCS Director database. For information on the system requirements for both these disks, see the Cisco UCS Director installation guide or the *Cisco UCS Director Upgrade Guide*.

Note Cisco UCS Director OVF and VHD zip files are created using zip 3.x in CentOS 6.x. For Linux systems, you can extract the zip files with unzip 6.x or higher or with the latest version of the 7-Zip archiving tool. For Windows systems, you can extract the zip files with the native Extract All in Windows Explorer for Windows 10 and Windows Server 2012 or with the latest versions of archiving tools such as 7-Zip or WinRAR.

Note After you apply the upgrade patch and complete that installation, choose the **Start Services** option of ShellAdmin to start/restart the Cisco UCS Director services and complete the patch process. The patch process is not complete until the services have started, the login screen is displayed, and the admin user can sign in.

All Cisco UCS Director services must be stopped before you perform other ShellAdmin procedures, such as apply additional patches, take a database backup, or restore a database from a backup.

Installing Cisco UCS Director Powershell Agent and the Powershell Console

Installing a newer version of the PowerShell Agent requires that you uninstall the older version first. To remove the older version of PowerShell Agent, stop the Cisco PSA Service first and then uninstall the agent. For instructions on installing, see Cisco UCS Director PowerShell Agent Installation and Configuration Guide, Release 6.7.

Before installing Cisco UCS Director Powershell Console 6.7, you must uninstall the earlier version of the Powershell Console from the system. To install the latest version, download and double-click the `UCSDirector_PSC_6.7.2.0.exe` file.

Supported Upgrade Paths to Cisco UCS Director, Release 6.7(3.0)

The following are the supported upgrade paths for Cisco UCS Director, Release 6.7(3.0).

See the Cisco UCS Director Upgrade Guide for detailed steps on how to upgrade to Release 6.7 from your current release.

Important Cisco UCS Director Release 6.7, Release 6.7(1.0), and Release 6.7(2.0) are no longer available for download. It is recommended that you upgrade immediately to release 6.7(3.0).

Upgrade Paths from Release 6.7(x.x)

- From Release 6.7(2.0) to Release 6.7(3.0)
- From Release 6.7(1.0) to Release 6.7(3.0)
- From Release 6.7 to Release 6.7(3.0)

Upgrade Paths from Release 6.6(x.x)

- From Release 6.6(2.0) to Release 6.7(3.0)
- From Release 6.6(1.0) to Release 6.7(3.0)
- From Release 6.6 to Release 6.7(3.0)

Upgrading from Versions Prior to Release 6.6

If you have a version prior to Release 6.6(0.0) installed, you cannot upgrade directly to Release 6.7(3.0). You must first upgrade to Release 6.6(0.0) or Release 6.6(1.0) and then upgrade to Release 6.7(3.0).

With release 6.7(x.x), the multi-node configuration in Cisco UCS Director was modified to support only one database node and one primary node. So when you upgrade from release 6.6 to release 6.7(3.0), the upgrade process will make the following changes in your environment:

- Migrates existing data from the inventory database node to the monitoring database node, and converts the monitoring database node to the database node.
- Upgrades the primary node to the current release.

For more information, see the *Cisco UCS Director Multi-Node Installation and Configuration Guide, Release 6.7*.

Supported Upgrade Paths to Cisco UCS Director, Release 6.7(4.0)

Following are the supported upgrade paths for Cisco UCS Director, Release 6.7(4.0):

Upgrade Paths from Release 6.7(x.x)

- From Release 6.7(3.0) to Release 6.7(4.0)
- From Cisco UCS Director Connector Packs version 6.7(3.2) to Release 6.7(4.0)
- From Cisco UCS Director Connector Packs version 6.7(3.1) to Connector Packs version 6.7(3.2) to Release 6.7(4.0)

Upgrade Paths from Release 6.6(x.x)

- From Release 6.6(2.0) to Release 6.7(3.0) to Release 6.7(4.0)
- From Release 6.6(1.0) to Release 6.7(3.0) to Release 6.7(4.0)
- From Release 6.6 to Release 6.7(3.0) to Release 6.7(4.0)

Upgrading from Versions Prior to Release 6.6

If you have a version prior to Release 6.6(0.0) installed, you cannot upgrade directly to Release 6.7(4.0). You must first upgrade to Release 6.6(0.0) or Release 6.6(1.0), then upgrade to Release 6.7(3.0) and finally upgrade to Release 6.7(4.0).

With release 6.7(x.x), the multi-node configuration in Cisco UCS Director was modified to support only one database node and one primary node. So when you upgrade from release 6.6 to release 6.7(3.0), the upgrade process will make the following changes in your environment:

- Migrates existing data from the inventory database node to the monitoring database node, and converts the monitoring database node to the database node.
- Upgrades the primary node to the current release.

For more information, see the *Cisco UCS Director Multi-Node Installation and Configuration Guide, Release 6.7*.

Supported Upgrade Paths for Bare Metal Agent Patch Release 6.7(4.0)

The following are the supported upgrade paths for the Bare Metal Agent Patch Release 6.7(4.0):

- From Release 6.7(2.0) to Patch Release 6.7(4.0)
- From Release 6.7(3.1) to Patch Release 6.7(4.0)

Note To apply a Bare Metal Agent 6.7(4.0) patch, you must only choose **Apply Patch** option in the shelladmin.

Upgrading Optimized Multi-Node Setup to Release 6.7(3.0) or Later Versions

Before you begin

Login to the primary node and from the Shell Admin console, choose **Stop Services** to halt all services running on the primary node.

Procedure

Step 1 Login to the database node.

Step 2 From the Shell Admin console, choose **Apply Signed Patch** to upgrade the node to Release 6.7(3.0) or the later version.

Step 3 Login to the primary node, and from the Shell Admin console, choose **Apply Signed Patch** to upgrade the node to Release 6.7(3.0) or the later version.

Step 4 Choose **Start Services** to start all the services on the primary node.

New and Changed Features

This section provides an overview of the significant new and changed features in this release. This section does not provide an exhaustive list of all enhancements included in this release.

Note For information about the physical and virtual devices and software supported by Cisco UCS Director in this release, see the Compatibility Matrix for this release.

New and Changed Features in Release 6.7

Introduction of Base Platform Pack and System Update Manager

This release introduces the capability to update the following components of the Cisco UCS Director software:

- Base Platform Pack—Includes basic infrastructure components such as the user interface, Shell admin console changes, and critical defect fixes.
- System Update Manager—Includes the framework that helps you upgrade all connector packs and the base platform pack.

Documented in the Cisco UCS Director Administration Guide, Release 6.7.

Introduction of Optimized Multi-Node Configuration

Earlier versions of Cisco UCS Director allowed you to configure the following nodes in a multi-node configuration:

- One primary node
- One or more service nodes
- One monitoring database node
- One inventory database node

Starting with this release, the multi-node configuration in Cisco UCS Director has been modified to support only the following nodes:

- One database node
- One primary node

As a result, when you upgrade to Cisco UCS Director Release 6.7, the upgrade process will make the following changes in your environment:

- Migrates existing data from the inventory database node to the monitoring database node, and converts the monitoring database node to the database node.
- Upgrades the primary node to the current release.

Documented in the Cisco UCS Director Multi-Node Installation and Configuration Guide, Release 6.7.

Enhancement to SSL Certificates

Starting with this release, Cisco UCS Director requires a self-signed SSL certificate. When you install Cisco UCS Director Release 6.7, the system checks if there is a self-signed certificate available or not. If there is no certificate available, when the administrator user logs in to the user interface, the systems prompts the user to generate the self-signed certificate.

Documented in the Cisco UCS Director Administration Guide, Release 6.7, and Cisco UCS Director Shell Guide, Release 6.7.

Introduction of Read-Only Access for Orchestration Workflow Tasks

Starting with this release, administrators with read-only privileges in the system, (users such as network administrators or storage administrators), have read-only privileges to workflow information in the user interface. The **Orchestration** page in the administrator user interface includes new options, **View** and **Workflow Designer**. Using these options, you can view workflow task information either in a textual summary format or in a graphical representation.

All workflow task information that is displayed is read-only.

Documented in the Cisco UCS Director Administration Guide, Release 6.7.

Introduction of the Service Request Quick View Panel

The header pane of the administrator user interface has a new icon that launches the **Service Request Quick View** panel. It displays 25 of the most recent service requests that are in the following states:

- In-Progress
- Completed Successfully
- Failed

Note This feature is not available in Cisco UCS Director instances that have been cross-launched from Cisco Intersight.

Documented in the Cisco UCS Director Administration Guide, Release 6.7.

Input and Global Variable Scoping

In cases where a task or workflow input variable has the same name as a global variable, the value of the local variable is displayed. The global value is "hidden" for the duration of the workflow. This applies also to any level of nested variable substitution.

Documented in the Cisco UCS Director Orchestration Guide.

Clone a Workflow Task in the Workflow Designer

In the Workflow Designer, you can clone a task to create another instance of the task in the workflow. In contrast to a task instance created by dragging and dropping, the new task is populated with the cloned task's parameter values (except its name).

Documented in the Cisco UCS Director Orchestration Guide.

Improved Looping in Workflows

When incrementing by count, you can specify a starting index and a step increment (or decrement, if negative) in the **Start Loop** task.

Documented in the Cisco UCS Director Orchestration Guide.

Nested Variable Evaluation in Workflows

You can nest variable references in Orchestration workflows. References are evaluated starting with the innermost reference and evaluating outward to any number of levels.

Documented in the Cisco UCS Director Orchestration Guide.

Customize an Existing Guest VM in RHEV

You can change the host name, DNS domain, DNS server list, and NIC configuration, and use of VDC policy configuration of an existing VM under Red Hat Enterprise Virtualization (RHEV). To customize an existing VM, create an orchestration workflow containing the **RHEV KVM - Guest Customization** task and make the desired changes in the admin inputs, or in the user inputs when running the service request.

Documented in the Cisco UCS Director Task Library Reference 6.7.

Mount and Unmount ISO images in HyperV

You can mount and unmount ISO images on VM CD drives using the **HyperV VM Mount ISO As CD ROM** and **HyperV VM UnMount ISO From CD ROM** tasks in an orchestration workflow.

Enhancements to Tenant Management

This release introduces a provision to define globally unique identifier (GUID) for SCVMM provider, and define an alias name for the tenant. While the tenant name cannot be changed after creation, the alias name of the tenant can be changed as required.

Documented in the Cisco UCS Director APIC Management Guide, Release 6.7.

Introduction of ACI Data Plane Policing, FHS Trust Policy, ND RA Prefix Policy, and IGMP Snoop Static Group

This release introduces the following polices:

- ACI Data plane policing (DPP)—This policy allows you to manage bandwidth consumption on ACI fabric access interfaces. DPP monitors the data rates for a particular interface. When the data rate exceeds user-configured values, marking or dropping of packets occurs immediately.
- First-Hop Security (FHS) trust policy—This policy allows you to closely control address assignment and derived operations, such as address resolution (AR), to enable a better IPv4 and IPv6 link security and management.

- Neighbor discovery router advertisement (ND RA) prefix policy—This policy allows you to configure the prefix carried in RA messages sent by the router.
- IGMP snoop static group—You can configure IGMP static group range support to specify group ranges in class maps and attach the class maps to an interface.

Documented in the Cisco UCS Director APIC Management Guide, Release 6.7.

Extension of support for APIC account

You can perform the following tasks in an APIC account:

- Adding an EPG
- Adding a Domain to an EPG
- Adding a Static Node to EPG
- Adding a Static Path to EPG

Documented in the Cisco UCS Director APIC Management Guide, Release 6.7.

Support for EPG Contract Master

This release introduces a provision to define an endpoint group (EPG) as a contract master for another EPG in the same tenant. To streamline associating contracts to new EPGs, you can enable EPG to inherit all the (provided and consumed) contracts from master EPG.

Documented in the Cisco UCS Director APIC Management Guide, Release 6.7.

Enhancements to APIC Contracts

Cisco UCS Director introduces fields to define alias name, DSCP target, and tag for a contract subject during creation.

When a contract is applied to both inbound and outbound traffic while creating a contract subject, the user gets the additional fields to define the service graph, QoS prioirty, and target DSCP for the in-term and out-term properties. If the selected contract does not apply to both directions, the filter chain must be configured for consumer to provider and provider to consumer separately. Cisco UCS Director has the provision to define the filter chain for consumer to provider and provider to consumer.

Documented in the Cisco UCS Director APIC Management Guide, Release 6.7.

Enhancements to External EPG

This release of Cisco UCS Director has the provision to associate one or multiple sites to EPG when you add an external EPG to the template.

Documented in the Cisco UCS Director APIC Management Guide, Release 6.7.

Support to set AS Path to the Action Rule Profile

This release introduces support to set autonomous system (AS) path to the action rule profile. You can also append the specified AS number to the AS path of the route that is matched by the route map.

Documented in the Cisco UCS Director APIC Management Guide, Release 6.7.

Support for IP SLA Monitoring Policy

This release has the provision to create an IP SLA monitoring policy. You can set the SLA frequency to define the interval probe time to track a packet.

Documented in the Cisco UCS Director APIC Management Guide, Release 6.7.

Enhancements to Routed Outside

To support protocol and QoS in an external routed network, this release introduces additional fields in the following actions:

- Create a routed outside
- Add a route map or profile to an external routed network
- Add a logical node profile to an external routed network
- Add a logical node to a logical node profile of an external routed network
- Add a static route to a logical node
- Add an external network to an external routed network

Documented in the Cisco UCS Director APIC Management Guide, Release 6.7.

Extension of support for APIC L3out tasks changes

New fields have been added to the following tasks to extend the support of L3out in the APIC account:

- Adding an external routed network in APIC account
- Adding a logical node profile to external routed network
- Adding an external network to APIC external routed network
- Adding a static route to a logical node in APIC account
- Adding a routed profile to an external routed network
- Adding a logical node to a logical node profile of an external routed network

Documented in the Cisco UCS Director APIC Management Guide, Release 6.7.

Introduction of Logical NetFlow Monitoring Policy

This release introduces a provision to deploy and enable NetFlow policies on a per-interface basis, depending on the traffic-type or address family to be monitored (IPv4, IPv6, or Layer 2 (CE type)).

Documented in the Cisco UCS Director APIC Management Guide, Release 6.7.

Support for IGMP interface policy and route map

Cisco UCS Director has the provision to add an IGMP interface policy and create route map policy for route redistribution or policy-based routing.

Documented in the Cisco UCS Director APIC Management Guide, Release 6.7.

Support for route control context

This release introduces a provision to define match action rules and set action rules for a route map. Also, you can create an action rule profile which is used to define the route-map set clauses for the L3out.

Documented in the Cisco UCS Director APIC Management Guide, Release 6.7.

Support for static route and route control profile

Cisco UCS Director has the provision to add a next hop address to a static route and to add a route control profile to a subnet and external network.

Documented in the Cisco UCS Director APIC Management Guide, Release 6.7.

ACI Policy-Based Redirect

You can provision service appliances, such as firewalls and load balancers, as managed or unmanaged nodes without requiring a Layer 4 to Layer 7 package. Cisco Application Centric Infrastructure (ACI) policy-based redirect (PBR) simplifies the provisioning of service appliances by enabling the consumer and provider endpoint groups to be in the same virtual redirect and forwarding (VRF) instance.

Documented in the Cisco UCS Director APIC Management Guide, Release 6.7.

Support for vzAny

The vzAny managed object provides a convenient way of associating all endpoint groups (EPGs) in a Virtual Routing and Forwarding (VRF) instance to one or more contracts, instead of creating a separate contract relation for each EPG. Cisco UCS Director has introduced actions to create and update vzAny provided and consumed contracts. Also, users can create vzAny contract interface which is used to associate an EPG from the destination tenant with the imported contract.

Documented in the Cisco UCS Director APIC Management Guide, Release 6.7.

Support for Subject Label and Provider/Consumer Label

This release introduces a provision to define labels that determine which EPG consumers and EPG providers can communicate with one another. Label matching determines which subjects of a contract are used with a given EPG provider or EPG consumer of that contract. Users can define:

- vzAny provided subject label to VRF
- vzAny consumed subject label to VRF
- vzAny EPG provided any labels
- vzAny EPG consumed any labels

Documented in the Cisco UCS Director APIC Management Guide, Release 6.7.

Enhancements to EPG

Cisco UCS Director has extended the support for EPG to define data plane policy, forwarding control, preferred group member, flood on encapsulation, and FHS trust control policy during creation of EPG. The following ehnacements were done while adding an object to an EPG:

- Add Domain to EPG—When the VMM type domain profile is chosen, user is provided with additional fields to:

- Define delimiter for the domain name.
- Allow micro-segmentation which enables automatic assignment of endpoints to EPGs.
- Enter port encapsulation for static VLAN.
- Enable netflow to monitor IP packets that are passing through the ports.

- Add Static Node to EPG—The new fields are enabled to enter a VLAN value that is part of one of the static VLAN blocks associated with the domain, and to choose Trunk, Access (802.1p), or Access (untagged) as the traffic mode for the EPG.
- Add Static Path to EPG—While adding a static path to an EPG, users are provided with options to define the path type, encapsulation, and primary VLAN for micro-segmentation.

Documented in the Cisco UCS Director APIC Management Guide, Release 6.7.

Support for Loopback interface on Layer 3 Device

From this release, you can configure loopback interface on the following Cisco network devices:

- Cisco Nexus 3000 Series switches
- Cisco Nexus 5000 Series switches
- Cisco Nexus 6000 Series switches
- Cisco Nexus 7000 Series switches
- Cisco Nexus 9000 Series switches

Documented in the Cisco UCS Director Network Devices Management Guide, Release 6.7.

Enhancements to HSRP

This release introduces support to enable the latest version (version 2) of HSRP in the interface. You can enable pre-empt and set the minimum pre-empt delay time for the local router to postpone taking over the active role. Optionally, you can set the upper and lower threshold values used by vPC to determine when to fail over to the vPC trunk.

Documented in the Cisco UCS Director Network Devices Management Guide, Release 6.7.

Enhacements to SVI

This release introduces support to choose VRF for SVI, set the ICMP redirect to notify the hosts on the data link that a better route is available for a particular destination, and to enable and configure OSPF for SVI.

Documented in the Cisco UCS Director Network Devices Management Guide, Release 6.7.

Enhancements to Port Profile

This release provides support to set maximum ports for the port profile when Vethernet is chosen as the port profile type.

Documented in the Cisco UCS Director Network Devices Management Guide, Release 6.7.

Enhancements to Maintenance Policy

This release introduces support to schedule server shutdown and to deploy storage configuration.

Documented in the Cisco UCS Director Management Guide for Cisco UCS Manager, Release 6.7.

Support for Managing QOS Policy Groups

This release introduces support to create,delete, and modify Netapp QOS policy groups.

This release introduces support to create, delete, and modify NetApp QOS policy groups. The QOS policy group allows you to control the resources that can be consumed by storage objects (such as volumes, LUNs, VMDKs, or SVMs) to manage network performance. Also, provides support to associate and configure QOS policy groups with LUNs and Volumes within the same SVM.

Documented in the Cisco UCS Director NetApp Management Guide, Release 6.7.

Support for Cisco UCS Director Express for Big Data in Cisco UCS Director

The enhancements to Cisco UCS Director Express for Big Data in Cisco UCS Director include the following:

- Support for Cloudera 6.0
- Support for Splunk 7.1.3 and Splunk 7.2
- Support for MapR 6.1
- Support for SmartSense service in Hortonworks cluster
- Support for S3260 M5 Storage Server for Hadoop and Splunk distributions

Documented in the Cisco UCS Director Express for Big Data Deployment and Management Guide, Release 3.7.

Create Cisco UCS and UCS Central Policies in Orchestration

This release introduces orchestration tasks to create and delete maintenance policies and quality of service (QoS) policies for both Cisco UCS Manager Manager and Cisco UCS Central . The tasks are:

- Create UCS Maintenance Policy
- Delete UCS Maintenance Policy
- Create UCS QoS Policy
- Delete UCS QoS Policy
- Create UCS Central Maintenance Policy
- Delete UCS Central Maintenance Policy
- Create UCS Central QoS Policy
- Delete UCS Central QoS Policy

Documented in the Cisco UCS Director Task Library Reference 6.7.

Manage Cisco UCS Firmware in Orchestration

This release introduces tasks to upgrade the infrastructure components in a Cisco UCS Manager account, such as the fabric interconnects, the I/O modules, and Cisco UCS Manager . The new tasks are:

- Get UCS Server Firmware Upgrade Status
- Get UCS Infra Firmware Upgrade Status
- Prepare for UCS Firmware Install
- Install UCS Infra Firmware

Documented in the Cisco UCS Director Task Library Reference 6.7.

Support for Upgrading Firmware from MicroSD cards or FlexFlash cards on Rack Mount Servers

Starting with this release, you can upgrade firmware on rack servers using ISO images from MicroSD cards (for M5 servers) or FlexFlash cards (for M4 servers).

This feature is only supported on Cisco UCS M5 or higher servers running Cisco IMC version 3.1(3a) or higher and on Cisco UCS M4 servers running Cisco IMC version 4.0(2) or higher.

Documented in the Cisco UCS Director Rack Server Management Guide, Release 6.7.

Support for Scheduling Upgrades Using Host Image Mapping Profiles on Rack Mount Servers

Starting with this release, new scheduling options have been introduced in the **Run Upgrade** and **Apply Profile** screens for host image profile procedures. Using these options, you can schedule these processes to run at a later point in time.

Documented in the Cisco UCS Director Rack Server Management Guide, Release 6.7.

Introduction of Power Restore Policy for Cisco UCS C-series Servers

Starting with this release, you can configure a power restore policy for Cisco UCS C-series servers. You cannot create this policy on ENCS servers.

Documented in the Cisco UCS Director Rack Server Management Guide, Release 6.7.

Enhancements to Email Alerts on Faults

Starting with this release, you can configure the system to send email alerts for all open faults on Cisco UCS C-series servers, based on the configured email alert rule, irrespective of whether you have been notified previously for a fault or not. A new option **Send alert for all faults every 24 hours** has been introduced in the **Add Email Alert Rule** screen. If you select this option, the system will send email alerts every 24 hours for all open faults that match the specified alert rule.

Documented in the Cisco UCS Director Rack Server Management Guide, Release 6.7.

Important Cisco UCS Director Release 6.7 is no longer available for download. It is recommended that you must upgrade immediately to release 6.7(2.0).

New and Changed Features in Release 6.7(1.0)

Introduced Support for New Hardware and Software Versions

This release introduces support for the following:

- EMC PowerMax
- ONTAP version 9.5

For more information, see the *Cisco UCS Director Compatibility Matrix, Release 6.7*.

Deprecated REST API

The `userAPIHypervVMProvisioningWithVMNetwork` REST API used for provisioning a Hyper-V VM that is associated with a network group, is deprecated. All features related to hosts and cluster selection for VM provisioning are not supported. We recommend you use the `HYPERV_VM_PROVISION` REST API for Hyper-V VM provisioning after you upgrade from Cisco UCS Director version 6.6 or a prior version to version 6.7 or later.

Support for Cisco UCS Director Express for Big Data in Cisco UCS Director

The Local Disk Configuration policy is enhanced to support the OS disk partition value to be greater than 50 GB. We recommend that you allocate the OS disk partition value based on the available actual disk size.

Important Cisco UCS Director Release 6.7(1.0) is no longer available for download. It is recommended that you must upgrade immediately to release 6.7(2.0).

New and Changed Features in Release 6.7(2.0)

Visual Representation of Device Claim Status

The administrator interface of Cisco UCS Director now includes an icon on the menu bar to indicate the claim status of the device in Cisco Intersight. The cloud icon with a red cross mark indicates that the Cisco UCS Director device is not claimed, and the cloud icon with a green check indicates that the device is claimed.

Documented in the Cisco UCS Director Administration Guide, Release 6.7.

Support for Big Data Cluster Version

This release introduces support for Cloudera 6.1.

Documented in the Cisco UCS Director Express for Big Data Deployment and Management Guide, Release 3.7.

Support for vSphere/ESXi 6.7

This release introduces support for vSphere/ESXi 6.7 Baremetal OS installation.

Documented in the Cisco UCS Director Bare Metal Agent Installation and Configuration Guide, Release 6.7.

Important Cisco UCS Director Release 6.7 and Release 6.7(1.0) are no longer available for download. It is recommended that you must upgrade immediately to release 6.7(2.0).

New and Changed Features in Release 6.7(3.0)

Support for Netflow Monitor Policy and End Point Retention Policy

This release of Cisco UCS Director introduces:

- Logical NetFlow monitoring policy—You can create a logical NetFlow monitoring policy to associate a flow record with the monitoring policy. The monitor policy identifies packet flows for ingress IP packets and provides statistics based on these packet flows.
- Endpoint retention policy—You can create an endpoint retention policy to set the hold interval, bounce entry aging interval, local endpoint aging interval, remote endpoint aging interval, and move frequency for endpoints. You can associate an endpoint retention policy to a bridge domain during bridge domain creation.

Enhancements to Bidirectional Forwarding Detection

You can use Bidirectional Forwarding Detection (BFD) to detect the number of times a sub-second failure occurs in the forwarding path between the ACI fabric border leaf switches configured to support peering router connections. This release of Cisco UCS Director introduces the following policy and profile to support BFD:

- BFD Interface Policy—In Cisco UCS Director, you can enable or disable the admin, control, and echo admin state for the BFD interface policy. You can set the detection multiplier, minimum transmit interval, minimum receive interval, and echo receive interval for the BFD interface policy.
- BFD Interface Profile—In the profile, you can set if authentication is required or not for accessing the profile and choose a BFD interface policy for the profile.

Enhancements to Hot Standby Router Protocol

This release of Cisco UCS Director introduces the following policies and profiles to support Hot Standby Router Protocol (HSRP) in Cisco APIC account. The HSRP protocol acts as the gateway for the endpoints behind the Layer 2 switches.

- HSRP Interface Policy—While defining the HSRP interface policy, you can enable or disable BFD and control sourcing of hellos from the burned-in MAC address (BIA) to identify devices. You can set the minimum time to delay HSRP group initialization after an interface comes up, and set the time period to delay HSRP group initialization after the router has reloaded.
- HSRP Group Policy—In the HSRP group policy, you can enable or disable preemption for a group, set the priority for HSRP to define the active and standby routers, and choose MD5 or simple authentication method. Also, you can set the hello interval, hold interval, minimum preemption delay, the delay time for resuming the preemptive action after reloading the active HSRP leaf, the maximum amount of time allowed for the HSRP client to prevent preemption, and the timeout value for authentication.
- HSRP Interface Profile—In Cisco UCS Director, you can choose a specific version of HSRP interface policy for the logical interface profile.

- HSRP Interface Group to Interface Profile—You can define the ID, name, and type of the HSRP interface group along with the mode in which the IP address can be obtained for the group. You can provide a virtual Media Access Control (MAC) address and an IP address that is shared among a group of configured routers. You can also provide comma separated multiple IPv4 or IPv6 addresses that can be used as secondary virtual IP addresses.

Support for Dynamic Host Configuration Protocol

This release of Cisco UCS Director provides support for creating a DHCP relay policy with a unique name. A DHCP relay policy is used to dynamically assign IP address when the DHCP client and server are in different subnets. The DHCP relay profile contains one or more providers. Starting with this release, you can add providers to the DHCP relay policy at the tenant level and at the infrastructure level.

You can add a DHCP relay label to logical interface profile by assigning a DHCP policy to an infra or a tenant.

CoPP Leaf/Spine Policy Support for APIC Fabric Switch

Starting with this release, you can create and manage the APIC control plane policing (CoPP) leaf and spine policy to be applied on Cisco ACI leaf/spine switches. While creating a CoPP leaf/spine policy, choose **CoPP has custom values** as the type of profile if you wish to set policy for each protocol separately.

Enhancements to Routed Interface

From this release, you can configure the secondary IP address and BGP peer connectivity profile for the routed interface, routed sub-interface interface, and SVI interface.

Introduction of New REST APIs

This release introduces REST APIs for the following features:

- NetFlow Monitor Policy
  - CREATE_APIC_NETFLOW_MONITOR_POLICY
  - UPDATE_APIC_NETFLOW_MONITOR_POLICY
  - DELETE_APIC_NETFLOW_MONITOR_POLICY
- End Point Retention Policy
  - ADD_APIC_TENANT_BRIDGE_DOMAIN
  - MODIFY_APIC_TENANT_BRIDGE_DOMAIN
  - ADD_APIC_ENDPOINT_RETENTION_POLICY
  - UPDATE_APIC_ENDPOINT_RETENTION_POLICY
  - REMOVE_APIC_ENDPOINT_RETENTION_POLICY
- BFD Interface Policy
  - CREATE_APIC_BFD_INTERFACE_POLICY
  - DELETE_APIC_ BFD_INTERFACE _POLICY
  - UPDATE_APIC_ BFD_INTERFACE _POLICY

- BFD Interface Profile
  - CREATE_APIC_BFD_INTERFACE_PROFILE
  - DELETE_APIC_ BFD_INTERFACE _PROFILE
  - UPDATE_APIC_ BFD_INTERFACE _PROFILE
- HSRP Interface Policy
  - CREATE_APIC_HSRP_INTERFACE_POLICY
  - DELETE_APIC_HSRP_INTERFACE_POLICY
  - UPDATE_APIC_HSRP_INTERFACE_POLICY
- HSRP Group Policy
  - CREATE_HSRP_GROUP_POLICY
  - DELETE_HSRP_GROUP_POLICY
  - UPDATE_HSRP_GROUP_POLICY
- HSRP Interface Profile
  - CREATE_APIC_HSRP_INTERFACE_PROFILE
  - DELETE_APIC_HSRP_INTERFACE _PROFILE
  - UPDATE_APIC_HSRP_INTERFACE _PROFILE
- HSRP Interface Group to Interface Profile
  - CREATE_APIC_HSRP_INTERFACE_GROUP
  - UPDATE_APIC_HSRP_INTERFACE_GROUP
  - DELETE_APIC_HSRP_INTERFACE_GROUP
- DHCP Relay Policy
  - CREATE_DHCP_RELAY_POLICY
  - DELETE_DHCP_RELAY_POLICY
- DHCP Relay Policy Providers
  - ADD_PROVIDERS_TO_DHCP_RELAY_POLICY
  - DELETE_PROVIDERS_FROM_DHCP_RELAY_POLICY
- DHCP Relay Label
  - ADD_APIC_TENANT_DHCP_RELAY_LABEL_TO_INTERFACE_PROFILE
  - DELETE_APIC_TENANT_DHCP_RELAY_LABEL_FROM_INTERFACE_PROFILE
- CoPP Leaf Policy

- APIC CoPP Leaf Policy
  - CREATE_APIC_FABRIC_COPP_LEAF_POLICY
  - DELETE_APIC_FABRIC_COPP_ LEAF_POLICY
  - UPDATE_APIC_FABRIC_COPP_ LEAF_POLICY
- Associate Custom Values to Copp Leaf Policy
  - ASSOCIATE_CUSTOM_VALUES_TO_APIC_COPP_LEAF_POLICY
- CoPP Spine Policy
  - CREATE_APIC_FABRIC_COPP_SPINE_POLICY
  - DELETE_APIC_FABRIC_COPP_SPINE_POLICY
  - UPDATE_APIC_FABRIC_COPP_SPINE_POLICY

- Routed Interface
  - APIC_TENANT_INTERFACE_TO_LOGICAL_INTERFACE_PROFILE_CREATE
  - APIC_TENANT_INTERFACE_TO_LOGICAL_INTERFACE_PROFILE_DELETE
- Routed Interface—BGP Peer Connectivity
  - ADD_BGP_PEER_CONNECTIVITY_PROFILE_TO_INTERFACE_OF_LOGICAL_INTERFACE_PROFILE
  - REMOVE_BGP_PEER_CONNECTIVITY_PROFILE_FROM_INTERFACE_OF_LOGICAL_INTERFACE_PROFILE
  - UPDATE_BGP_PEER_CONNECTIVITY_PROFILE_FROM_INTERFACE_OF_LOGICAL_INTERFACE_PROFILE
- Routed Interface—Secondary IP Address
  - Add_APIC_TENANT_SECONDARY_ADDRESS_TO_INTERFACE
  - DELETE_APIC_TENANT_SECONDARY_ADDRESS_TO_INTERFACE

Rename UCS Central Global Service Profile

This release introduces support for renaming the existing UCS central global service profiles using workflow task and REST API. You can use the orchestration task **Rename UCS Central Global Service Profile** to rename the existing UCS central global service profiles. Also, you can rename the selected global service profile name in the related workflows and service request. You can view the list of renamed task by choosing **UCS Central Account** under **Multi-Domain Managers** and clicking **Renamed Global Service Profiles**.

Note To view descriptions of these workflow tasks, see the Task Library that you can launch in the following ways:

- Choose **Orchestration** > **Workflows** in the user interface.
- Go to `http://IP_address/app/cloudmgr/onlinedocs/cloupiaTaskLib.html` where *IP_address* is the IP address of Cisco UCS Director.

Workflow to Upgrade Firmware for Cisco UCS Manager Using Cisco UCS Director

This release introduces support for upgrading firmware for Cisco UCS Manager using the **Upgrading Firmware on Cisco UCS Infra** workflow. You can execute the following tasks to upgrade the firmware.

- Download UCS Firmware
- Install UCS Infra Firmware
- Wait for UCS Infra Firmware to Upgrade
- Cisco UCS Director Administrator Approval for Fabric Interconnect (FI) Reboot

Note The Cisco UCS Director administrator should approve the fabric interconnect reboot request for the Cisco UCS Manager account by choosing **Organizations** > **My Approvals**. Upon approval, the pending activities in the Cisco UCS Manager will be approved.

- Wait for Cisco UCS Infra Firmware to Upgrade after Primary FI Reboot
- Get Cisco UCS Infra Firmware Upgrade Status

Enhancements to the Download UCS Firmware Workflow Task

Starting with this release, the **Download UCS Firmware** workflow task has been enhanced to display the percentage of the firmware download in the workflow log.

Enhancements to the Prepare for Firmware Install Workflow Task

Starting with this release, the **Prepare for Firmware Install** workflow task has been enhanced to display the list of affected and not affected components for the chosen host firmware package in the workflow log.

Support for Cisco Hyperflex in Cisco UCS Director

The enhancements to Cisco Hyperflex in Cisco UCS Director include the following:

- Support for Cisco HX-Series Server version 3.5.2a
- Support for Cisco HX Data Platform software version 4.0.
- Support for Connection Timeout (Seconds) and Socket Read Timeout (Seconds) while adding Hyperflex accounts.

Documented in the Cisco UCS Director HyperFlex Systems Management Guide, Release 6.7.

Enhancement to Enable Services while Creating Logical Interface

Creating logical interface (LIF) allows you to enable services, such as Network File System (NFS), Common Internet File System (CIFS), Fibre Channel Protocol (FCP), and Internet Small Computer System Interface (iSCSI). You can perform this using user interface, workflow task, and REST API.

Documented in the Cisco UCS Director NetApp Management Guide, Release 6.7.

Support for VLAN Trunking for the DVPortGroup Task and API

Prior to this release, while using the Create DVPort Group workflow task or the API, you could only specify VLANs for the **VLAN Type** field and specify a VLAN ID. Starting with this release,you can specify **VLAN Trunking** as a value for the **VLAN Type** field and specify a Trunk VLAN range. You can enter either a range of VLAN IDs or list of comma separated IDs. These changes are available for the **Modify VMWare DV Port Group** workflow task and API as well.

The report on all DV port groups configured in the system now displays the following information:

- VLAN type for the group—VLAN or VLAN Trunking
- VLAN Trunk Range—Displays the VLAN Trunk Range that you had specified.

Enhancements to the Provision VM Workflow Task

Starting with this release, the output of the Provisioning VM workflow task for all VM types has been enhanced to include the following information:

- Disk size of the boot volume
- Image path of the template
- UUID of the VM instance
- BIOS UUID
- vCenter UUID
- VM folder name

Enhancements to Create VM Disk Workflow Task

Starting with this release, the **Create VM Disk** workflow task has been enhanced to display the following information in the workflow task output:

- Disk UUID
- Disk Label

This enhancement is available in the Create VM Disk API as well. In addition, the **Disks** page for the VM now includes additional columns to display the Disk UUID.

Introduction of the Select Host Task

This release introduces a new workflow task called **Select Host**, using which you can retrieve information such as CPU usage and memory for the host. For this workflow task, as an input, you can specify the host name of a standalone host name or a host within a cluster. The output of this workflow task displays the following information:

- Host Name
- Host UUID
- Cluster Name —if applicable
- Product Version

- Hardware Vendor and Hardware Model
- Total number of VMs and active VMs on the host
- Memory, Power and Storage Capacity information

Enhanced Reporting for DV Switches Objects

Starting with this release, the following reports have been introduced for DV Switches:

- Distributed Port Groups

  Choose **Network** > **Cloud** > **DVSwitch** > **Distributed Port Groups**

- Uplink Port Groups

  Choose **Network** > **Cloud** > **DVSwitch** > **Uplink Port Groups**

- Ports

  Choose **Network** > **Cloud** > **DV Port Groups** > **Ports**

New and Changed Features in Release 6.7(4.0)

Enhancements to the Approval Task

An approval task requires the intervention of a Cisco UCS Director user to allow a workflow to run to completion. This user is typically an administrator who has go-or-no-go authority over the workflow process.

In releases earlier than Cisco UCS Director 6.7(4.0), when an approval task is used within a workflow loop, the approval request will be initiated to the mapped user only for the first iteration and the approval request will be skipped in the subsequent iterations. Starting with the release 6.7(4.0), when an approval task is used within a loop task of a workflow, the approval request will be initiated to the respective mapped user for each iteration. The progress of the approval task can be seen under the **Show Details Status** tab of the **Service Request Submit Status** screen. The approval task behaviour remains same during rollback of the workflow.

Documented in the Cisco UCS Director Orchestration Guide, Release 6.7.

Support for Cisco UCS C480 ML M5 Servers

Starting with this release, VM hosts list PCI devices and displays a summary of GPU devices (supported by Cisco UCS C480 ML M5 servers). The administrator portal displays information in the following screens for these hosts:

- **PCI Devices**—displays the list of PCI devices on the server.
- **Summary**—includes new fields such as **Number of PCI devices**, **Number of GPU devices**, **Number of passthrough-enabled devices**, and **Number of passthrough-disabled devices**.

In addition, to manage these GPU devices on the Cisco UCS C480 ML M5 servers, the following workflows and tasks have been introduced:

- VMware VM Tasks
  - Map GPU Devices to VMware VM
  - Unmap GPU Devices from VMware VM

- VMware Host Tasks
  - Disable PCIe Passthrough for GPU Devices on Host
  - Enable PCIe Passthrough for GPU Devices on Host
- ESXi Provisioning and GPU Discovery—To install ESXi on Cisco UCS C480ML M5 servers, register the host with vCenter and enable PCIe passthrough on GPU devices.

Deprecation of Support for VNC Console

Starting with this release, support for using VNC console to launch a VM client is no longer available. You must launch the VM client using the VMware Remote Console (VMRC). To reconfigure existing VMs that have been configured with VNC to use VMRC, use the **Unconfigure VNC** option and **Disable VNC** task.

For more information on using VMRC, see *Cisco UCS Director VMware vSphere Management Guide, Release 6.7*.

Support for Enforcing Default Password Reset

Starting with this release, you are prompted to reset the default SSH root user and shelladmin user passwords before logging into the Cisco UCS Director administrator interface. You are prompted to reset these passwords in the following scenarios:

- If you have not reset the passwords prior to upgrading to release 6.7(4.0)
- If you are installing a new version of Cisco UCS Director using the OVA and have not reset the passwords.

In an optimized multi-node environment, you must reset the password for these user accounts on the application node and the database node.

This feature works in the optimized multi-node environment only if you have set up passwordless authentication between the application node and the database node. For information on setting up passwordless authentication, see the *Cisco UCS Director Multi-Node Installation and Configuration Guide, Release 6.7*.

Support for Upgrading the Bare Metal Agent (BMA) using a Connector Pack

This release introduces support for upgrading the Bare Metal Agent (BMA) with a connector pack. A new screen titled **BMA System Updates**, accessible from **Administration** > **System** menu, has been introduced. This screen displays the status of the recent updates made to the BMA. Also, a new system task called **BMA Update System Task** has been introduced. This system task is disabled by default. This system task is enabled only after you install the BMA connector pack, and it is set to run every 4 hours. In addition, a new workflow task called **Monitoring Task** has been introduced in the task library.

Support for Syncronizing Users from Cisco Identity Services Engine (Cisco ISE)

Starting with this release, you can sychronize and retrieve user accounts created in Cisco Identity Services Engine (Cisco ISE) by integrating a Cisco ISE server with Cisco UCS Director.

Following are the prerequisites to configuring a Cisco ISE server in Cisco UCS Director:

- Add Cisco UCS Director as a network device in Cisco ISE and enable TACACS authentication.

  The shared secret key that you enter in Cisco ISE is required to configure the server in Cisco UCS Director.

- Specify an authentication protocol in Cisco ISE.

  It can either be Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). The authentication protocol that you select in Cisco ISE must be selected in Cisco UCS Director when you add the Cisco ISE server.

- Enable the External RESTful Services (ERS) APIs in Cisco ISE.

  In a cluster-setup, you must enable ERS for the primary administration node and for all the other nodes.

For information on supported Cisco ISE versions, see the *Cisco UCS Director Compatibility Matrix, Release 6.7*.

Introduction of Email Notification for Rollback Service Requests

Starting with this release, when you initiate a rollback of a service request, an email notification is sent to the users configured as recipients in the email notification policy for the initial service request. In earlier releases, email notifications were sent to users configured in the email notification policy only for the initial service request.

Introduction of Additional Options for Rollback on Failure of Service Requests

Starting with this release, while creating a workflow, you can configure rollback options for the workflow. The user interface includes the following new options:

- **Rollback Workflow on Failure**
- **Abort Rollback on Failure** (displayed only if you check the **Rollback Workflow on Failure**)

Selecting the **Rollback Workflow on Failure** option ensures that the service request is automatically rolled back when the service request fails. In this scenario, a rollback service request is initiated. Selecting the **Abort Rollback on Failure** check box terminates the rollback of a service request if the execution of any task within the rollback service request fails.

Support for Auto-populating User Input Details for Workflows

Starting with this release, while mapping a user input for a workflow task, the **Input Label** field and the **Input Description** field are automatically populated, based on the input type. You can edit these values as well. However, you cannot create multiple user input names with the same value.

Introduction of a new API to Halt a Rollback SR on Task Failure

This release introduces a new API **userAPIRollbackServiceRequest**. You can use this API to rollback a service request and set it to continue with the rollback in the event of a failure of a task execution. To use this API, you must provide the service request ID as a value for the API. If any task in the rollback service request fails, by default, the service request skips the task and continues to execute. If you set the value of the API to false, then if any task fails, the rollback service request halts.

Support for New Actions in Tabular Reports for Orchestration Workflows

Starting with this release, while working with tabular forms with orchestration workflows, you can now choose multiple entries and perform actions such as deleting entries, or reordering entries within the table.

Workflow Optimization

Starting with this release, the switching time between tasks is optimized such that the entire workflow completes faster.

Introduction of Quick Export for Workflows

This release introduces a new option called **Quick Export** on the **Workflows** page, using which you can select workflows and export them to your machine. After you select workflows and choose **Quick Export**, the subsequent screen lists the following information for the selected workflows:

- Script modules
- Workflow
- Custom tasks
- Activities
- Open APIs

You must provide a file name and choose **Export Workflow**.

Note The **Quick Export** option is also available from the right-click menu.

Support for Processing Header Response

Generic API task allows you to fetch specific values from the output of header response when the value of **Header Response** is set as **True** in the **Output Definition** table of a Generic API task. If the value of **Header Response** is set as **False** in the **Output Definition** table, you can fetch the output response values using JSON or XML.

For more information on processing header response, refer Working with Generic API Task of Cisco UCS Director.

Support for Generating a Task Using an OpenAPI Specification File

The OpenAPI specification file from connectors such as NetApp, VMware, defines all APIs of connectors in the JSON or YAML format. Starting with this connector pack release, Cisco UCS Director has the provision to upload the OpenAPI specification file to Cisco UCS Director and make use of the connector specific API for creating a task. You can use the task created based on a OpenAPI specification file, in Cisco UCS Director workflow to perform a specific operation on the connector account.

You can also reset an API to their original form by clicking **Reset** after choosing the API that needs to be reset. Before initiating the reset process, ensure that the task created based on the API are deleted and workflows that use the API task are deleted from Workflow designer.

For more information on generating a task using an OpenAPI specification file, refer Cisco UCS Director Orchestration Guide.

Changes to Cisco UCS Director SDK Bundle

Starting with this release, the Cisco UCS Director SDK bundle uses the `http-client-4.4.jar` files. The SDK bundles of prior releases of Cisco UCS Director used the `commons-httpclient-3.1.jar`

files. As a result of this change, if your customized programs use classes from the `commons-httpclient-3.1.jar`, you must update your code to use the new http-client classes.

Introduction of New Generic Tasks

Generic tasks allow you to automate certain operations on input parameter and deliver the processed output to next task. In the **Workflow Designer**, you can find the generic tasks under the **Cloupia Tasks** > **General Tasks** folder.

This release introduces the following generic tasks:

- **Process Text**

  You can add the **Process Text** task to any workflow to manipulate the defined inputs as per the operations and deliver the manipulated text as an output to next task. In the **Process Text** task, you must define the following parameters:

  1. Input List—You can add a list of input names as task inputs that can be mapped with values on which the operation must be performed.
  2. Operations—You can provide a name for the operation, and then choose an operation type and input parameter on which the operation has to be performed.
  3. Output List—You can define an output name and associate the output name with one of the operation outputs displayed based on defined operation names. These outputs can be mapped as inputs for other task.
  4. Check this option for script mode—You can enable this check box to enter the script for manipulating the text.

  For more information on the **Process Text** task, refer the Generic Tasks of Cisco UCS Director Base Platform Connector Pack.

- **Convert Type**

  You can use the **Convert Type** task to convert the given input value to any desired output type as required for a task. For example, you can convert the generic text into an email ID format and input the email ID as input for another task.

  You can define multiple input labels and an output type for each input label. So that, the **Convert Type** task converts each input value into defined output type.

- **Register LOV**

  The **Register LOV** task registers given key value pairs as an LOV in the workflow task input, which can be used by other tasks or workflows after registration. During LOV registration, you can define LOV name and LOV pairs in the JSON format as text or upload as a file:

  ```
  {"LOVName1" : {"LOVLabel":"LOVValue","LOVLabel":"LOVValue","LOVLabel":"LOVValue"},
  "LOVName2": {"LOVLabel":"LOVValue","LOVLabel":"LOVValue","LOVLabel":"LOVValue"}}
  ```

  You can also define the type of variables that you want to regsiter. You have the provision to enable overriding of LOV pairs when there is an LOV with the same name.

- **Get Data From Tabular Report**

  You can use the **Get Data From Tabular Report** task to retrieve specific data from a tabular report. To retrieve a report data, you have to provide report name, choose columns that you need in the output, and specify filter criteria to filter the data in the report.

- **Process Time**

  You can use the **Process Time** task to perform action such as converting time format, get system time and so on. To process time, define the input in a specific time format or define normal time value without following any format. Then, choose one or more operations such as **Convert Time Format**, to be performed on input time, and define the output format in which the processed time has to be output for each operation.

  The supported operations are: **Convert Time Format**, **Get System Time**, **Get Time Difference**, **Get Time Component**, **Get Prior or After Time**, and **Get Time from NTP server**.

  For the **Get Prior or After Time** operation type, you have to input two values: Date in any format and a generic number. Based on set prior or after action and time component, the output will be processed. For example, if you have set input as **16/07/2019** and **2**, chosen **Before** and **Date** in the **Select Prior or After** and **Select Time Component** drop-down lists, then the processed time output is **14**.

  For **Get Time from NTP server** operation type, you have to provide the IP address of the NTP server or DNS name.

- **Read File**

  Starting this connector pack release, you can use the **Read File** task to read the content of a specific file and generate an output with either the entire content of the file or the content in a specific line.

  You can also provide a regular expression pattern to read the lines matching the given pattern.

Support for PC/vPC Leaf Policy

Starting with this release, you can create a port channel interface leaf policy and virtual port channel leaf policy. The port channel (PC) and virtual port channel (vPC) leaf policy is a template to dictate port behavior and is associated to an Access Entity Profiles (AEP). After creating the policy, you can associate the following to it :

- Netflow monitor policy
- Virtual destination groups
- Virtual source groups
- Override policy group

Documented in Cisco UCS Director APIC Management Guide, Release 6.7.

Support for Route Tag Policy

This release of Cisco UCS Director provides support for creating a route tag policy with a tag value which is used to prevent routing loops.

When a transit route is redistributed into Open Shortest Path First (OSPF) or Enhanced Interior Gateway Routing Protocol (EIGRP), the route is tagged with the tag value specified in the route tag policy to prevent routing loops. If a route is received on an OSPF or EIGRP L3Out with this tag value, the route is dropped.

Documented in Cisco UCS Director APIC Management Guide, Release 6.7.

Support for Creating VRF in APIC

Starting with this release, you can define IPv4 unicast address family or IPv6 unicast address family as the EIGRP address family type, to configure an EIGRP routing instance. You can then add an APIC EIGRP to a Virtual routing and forwarding (VRF) object (called as private network in the APIC GUI).

Documented in Cisco UCS Director APIC Management Guide, Release 6.7.

Support for Access Port Selector

From this release, you can add an access port selector to a fabric interface profile. In Cisco UCS Director, choose **Physical** > **Network** > **Multi-Domain Managers** > **<APIC Account>** and click the **Fabric Interface Profiles** tab. Choose a profile and click **View Details** to view the access port selectors of the fabric interface profile. To add an access port selector to the fabric interface profile, click **Add** and complete the fields in the **Create Access Port Selector** screen.

Documented in Cisco UCS Director APIC Management Guide, Release 6.7.

Support for VMM Domain

This release of Cisco UCS Director provides support for creating a virtual machine manager (VMM) domain to integrate APIC with a third-party VMM (for example, VMware vCenter) to extend the benefits of ACI to the virtualized infrastructure. You can create VMM domains with one of the following virtual switches:

- VMware vSphere distributed switch (VDS)
- Cisco AVS
- Cisco AVE

Documented in Cisco UCS Director APIC Management Guide, Release 6.7.

Enhancements to add Domain to an EPG

Starting with this release, you can configure a default port binding type for all new vEthernet port profiles. For VMM type domain profiles, you can choose either **AVE** or **native** as the switching mode. You can choose **auto**, **VLAN**, or **VXLAN** as the encapsulation node for VMM type domain profiles.

Documented in Cisco UCS Director APIC Management Guide, Release 6.7.

Introduction of New REST APIs

This release introduces REST APIs for the following features:

- Route Tag Policy
  - CREATE_APIC_ROUTE_TAG_POLICY
  - DELETE_APIC ROUTE_TAG _POLICY
  - UPDATE_APIC ROUTE_TAG _POLICY
- Netflow Monitor Policy
  - CREATE_APIC_NETFLOW_MONITOR_POLICY_TO_PC_VPC_INTERFACE_POLICY_GROUP
  - DELETE_APIC_NETFLOW_MONITOR_POLICY_FROM_PC_VPC_INTERFACE_POLICY_GROUP

- Override Policy Group
  - CREATE_OVERRIDE_POLICY_GROUP_TO_INTERFACE_POLICY_GROUP
  - UPDATE_OVERRIDE_POLICY_GROUP_TO_INTERFACE_POLICY_GROUP
  - DELETE_OVERRIDE_POLICY_GROUP_FROM_INTERFACE_POLICY_GROUP
- VDestination Groups
  - ADD_FABRIC_VDESTINATION_GROUP_TO_APIC_PC_VPC_INTERFACE_POLICY
  - REMOVE_FABRIC_VDESTINATION_GROUP_FROM_APIC_PC_VPC_INTERFACE_POLICY
- VSource Groups
  - ADD_FABRIC_VSOURCE_GROUP_TO_APIC_PC_VPC_INTERFACE_POLICY
  - REMOVE_FABRIC_ VSOURCE _GROUP_FROM_APIC_PC_VPC_INTERFACE_POLICY

Support for newer Versions of Cisco Application Centric Infrastructure Controllers and Cisco Application Centric Infrastructure Multi-Site Controllers

This release introduces support for the following:

- Cisco Application Centric Infrastructure Controllers 4.1(x) and 4.2(x)
- Cisco Application Centric Infrastructure Multi-Site Controllers 2.1(x) and 2.2(x)

Documented in Cisco UCS Director Compatibility Matrix, Release 6.7.

Support for RHEL 8.0

This release introduces support for RHEL 8.0 Baremetal OS installation.

Documented in the Cisco UCS Director Bare Metal Agent Installation and Configuration Guide, Release 6.7.

Monitoring the Big Data Statistics for MapR Account

In earlier releases, statistical data generation for MapR account was part of inventory collection. Starting with this release, a new system task (monitor) is created within the MapR account to generate the statistical data for MapR accounts based on your requirement. Thereby, increasing the speed of inventory collection. You can navigate to the Big Data Tasks folder here: **Administration** > **System** > **System Tasks**.

Documented in the Cisco UCS Director Express for Big Data Deployment and Management Guide.

Connector Pack Releases

This section lists all the connector pack releases that are currently available through Cisco Intersight for Cisco UCS Director, Release 6.7.

For information on upgrading connector packs, see the Cisco UCS Director Administration Guide, Release 6.7.

Name	Latest Version Available	Release Notes
Cisco ACI and APIC Connector Pack	6.7.4.2 6.7.4.1 6.7.3.2 6.7.3.1 6.7.2.1	Release Notes
Base Platform Pack and System Update Manager Connector Pack	6.7.4.3 6.7.4.2 6.7.4.1 6.7.3.2 6.7.3.1	Release Notes
Bare Metal Agent Connector Pack	6.7.4.2 6.7.3.1	Release Notes
Cisco BigData Express Connector Pack	6.7.3.1	Release Notes
Cisco HyperFlex Connector Pack	6.7.4.2 6.7.4.1. 6.7.3.1	Release Notes
Cisco IMC Connector Pack	6.7.4.1 6.7.3.1	Release Notes
Cisco UCS Director Virtualization Connector Pack for: • VMware vSphere • Microsoft Hyper-V • RedHat KVM • PowerShell Agent (required for the Microsoft Hyper-V connector)	6.7.4.2 6.7.4.1 6.7.3.1 6.7.2.1	Release Notes
Cisco UCS Director F5 BIG-IP Connector Pack	6.7.4.1	Release Notes
Powershell Connector Pack	6.7.3.1	Release Notes
Cisco UCS Connector Pack	6.7.2.1	Release Notes

Name	Latest Version Available	Release Notes
EMC Connector Pack	6.7.4.1 6.7.2.1	Release Notes
IBM Connector Pack	6.7.2.1	Release Notes
NetApp ONTAP Connector Pack	6.7.2.1	Release Notes
Network Devices Connector Pack	6.7.4.1	Release Notes

Open and Resolved Bugs

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products.

Note You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, you can register for an account.

For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ.

Open Bugs in Release 6.7

You can find detailed information about all open bugs in Release 6.7 through the open bug search for Release 6.7. This search uses the following parameters:

Important Cisco UCS Director Release 6.7 is no longer available for download.

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco UCS Director.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 6.7(0.0).
Filter	Choose **Open** from the Status drop-down list.

Open Bugs in Release 6.7(1.0)

You can find detailed information about all open bugs in Release 6.7(1.0) through the open bug search for Release 6.7(1.0). This search uses the following parameters:

Important Cisco UCS Director Release 6.7(1.0) is no longer available for download.

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco UCS Director.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 6.7(1.0).
Filter	Choose **Open** from the Status drop-down list.

Open Bugs in Release 6.7(2.0)

You can find detailed information about all open bugs in Release 6.7(2.0) through the open bug search for Release 6.7(2.0). This search uses the following parameters:

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco UCS Director.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 6.7(2.0)
Filter	Choose **Open** from the Status drop-down list.

Open Bugs in Release 6.7(3.0)

You can find detailed information about all open bugs in Release 6.7(3.0) through the open bug search for Release 6.7(3.0). This search uses the following parameters:

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco UCS Director.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 6.7(3.0)
Filter	Choose **Open** from the Status drop-down list.

Open Bugs in Release 6.7(4.0)

You can find detailed information about all open bugs in Release 6.7(4.0) through the open bug search for Release 6.7(4.0). This search uses the following parameters:

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco UCS Director.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 6.7(4.0)
Filter	Choose **Open** from the Status drop-down list.

Resolved Bugs in Release 6.7

You can find detailed information about all resolved bugs in Release 6.7 through the resolved bug search query for Release 6.7. This search uses the following parameters:

Important Cisco UCS Director Release 6.7 is no longer available for download.

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco UCS Director.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 6.7(0.0).
Filter	Choose **Fixed** from the Status drop-down list.

Resolved Bugs in Release 6.7(1.0)

You can find detailed information about all resolved bugs in Release 6.7(1.0) through the resolved bug search for Release 6.7(1.0). This search uses the following parameters:

Important Cisco UCS Director Release 6.7(1.0) is no longer available for download.

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco UCS Director.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 6.7(1.0).
Filter	Choose **Fixed** from the Status drop-down list.

Resolved Bugs in Release 6.7(2.0)

You can find detailed information about all resolved bugs in Release 6.7(2.0) through the resolved bug search for Release 6.7(2.0). This search uses the following parameters:

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco UCS Director.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 6.7(2.0)
Filter	Choose **Fixed** from the Status drop-down list.

Resolved Bugs in Release 6.7(3.0)

You can find detailed information about all resolved bugs in Release 6.7(3.0) through the resolved bug search for Release 6.7(3.0). This search uses the following parameters:

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco UCS Director.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 6.7(3.0)
Filter	Choose **Fixed** from the Status drop-down list.

Resolved Bugs in Release 6.7(4.0)

You can find detailed information about all resolved bugs in Release 6.7(4.0) through the resolved bug search for Release 6.7(4.0). This search uses the following parameters:

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco UCS Director.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 6.7(4.0)
Filter	Choose **Fixed** from the Status drop-down list.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.