Cisco UCS Director Release Notes for Cisco Virtualization Connector Pack, Release 6.7

First Published: 2019-07-04

Last Modified: 2020-11-13

Cisco UCS Director Release Notes for Virtualization Connector Pack

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
6.7.2.1	July 04, 2019	Created for Release 6.7.2.1.
6.7.3.1	November 12, 2019	Updated the release notes for release 6.7.3.1.
6.7.4.1	June 18, 2020 July 16, 2020	Updated the release notes for release 6.7.4.1.
6.7.4.2	November 13, 2020	Updated the release notes for release 6.7.4.2.

Connector Packs

Connector packs help you perform connector level upgrade in Cisco UCS Director without impacting other connectors and without having to upgrade the entire software version. After claiming Cisco UCS Director in Cisco Intersight, as a system administrator, you can view information on new versions of connector packs that are available for upgrade. The top header pane of the user interface displays a Download icon indicating that new connector pack versions are available. You can select and upgrade the connector packs in Cisco UCS Director.

Cisco UCS Director Virtualization Connector Pack

The virtualization connector pack provides features and defect fixes for managing virtual accounts in Cisco UCS Director. You can create a virtual account in Cisco UCS Director for one of the following:

- VMware vSphere
- Microsoft Hyper-V
- RedHat KVM
- PowerShell Agent (required for the Microsoft Hyper-V connector)

Upgrading Connector Packs

Before you begin

- You must have system administrator privileges in Cisco UCS Director.
- Cisco UCS Director has been claimed in Cisco Intersight. For information on claiming a device, see the integrated guided walkthrough titled *Learn How to Claim a Device* available within the **Online Help** menu in the Cisco Intersight user interface.
- Cisco UCS Director is successfully connected to Cisco Intersight.
- Take a snapshot of Cisco UCS Director before you initiate the upgrade.

Procedure

Step 1 On the header, click **New Upgrades Available**.

The **Available System Upgrades** screen appears and will display all available connector packs for upgrade along with version information. Upon login, if you clicked **Yes** to the pop-up message, then the very same upgrade screen appears.

Note The **New Upgrades Available** icon is visible on the header only when new versions of the current running connector packs are available for upgrade.

Step 2 Check the check box of a connector pack from the list.

You can check the check boxes of multiple connector packs.

Step 3 Click **Upgrade**.

Step 4 In the **Confirm Upgrade** dialog box, click **Yes**.

After you confirm that the connector version must be upgraded, the validation process is initiated. If the validation process completes successfully, the upgrade process is initiated and the **System Upgrade Status** screen displays the upgrade status. After the upgrade process is successful, the **Logout** option is enabled.

Step 5 Click **Logout**.

While upgrading a base platform pack that includes changes to all infrastructure components, all Cisco UCS Director services are restarted. As a result, after clicking **Logout**, the screen could appear to be unresponsive

for a few minutes. After all the services are restarted, and the upgrade process is complete, you can login to Cisco UCS Director .

What to do next

You can view the upgrade reports by choosing **Administration** > **System** > **System Updates**. From this screen, you can double-click on a report, and view additional details on the upgrade process. For more information, see Viewing Connector Pack Upgrade Information.

Viewing Connector Pack Upgrade Information

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **System Updates**.
Information such as upgrade request ID, user that initiated the upgrade, upgrade start time and end time, and the upgrade status are displayed.

Step 3 Select a connector pack and choose **View Details** to view details such as connector pack name, upgraded version, and prior version.

Step 4 Click **State History** to view the various states of the connector pack upgrade process. For example, upgrade request received, upgrade process initiated or upgrade process completed.

Step 5 Click **Stages** to view the entire lifecycle of the connector pack upgrade request.

New and Changed Features in Release 6.7.2.1

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 6.7.3.1

Support for Creating and Deleting Recovery Plans for Protection Groups

Starting with this connector pack release, you can now create and delete recovery plans for protection groups. You can use one of the following methods to create and delete recovery plans:

- User Interface—Choose **Virtual** > **Compute** and select an SRM account from the left navigation pane. Choose **SRM sites** and **View Details** > **Recovery Plans**. From this screen, you can create or delete recovery plans. While creating a recovery plan, you can select multiple protection groups.
- Workflow Tasks—This release introduces the following workflow tasks that you can use to create and delete recovery plans.
  - **CreateVMwareSRMRecoveryPlan**
  - **DeleteVMwareSRMRecoveryPlan**
- REST APIs—This release introduces the following REST APIs that you can use to create and delete recovery plans.
  - **CREATE_VMWARE_SRM_RECOVERY_PLAN**
  - **DELETE_VMWARE_SRM_RECOVERY_PLAN**

Defect Fixes

This release includes defect fixes. For more information, see the Resolved Defects in Release 6.7.3.1, on page 8.

Support for Microsoft Windows Server 2019

This release includes support for Microsoft Windows Server 2019 and Microsoft System Center 2019.

New and Changed Features in Release 6.7.4.1

Support for VNC Console

Starting with this release, support for using VNC console to launch a VM client is available.

Support for VMware vSphere vCenter Server 7.0

Starting with this release, VMware vSphere vCenter Server 7.0 is supported. For more information, see the Compatibility Matrix.

Support for Choosing a Boot Option while Provisioning VMs

Starting with this release, while provisioning a VM in UCS Director, you are prompted to choose a boot option. You can choose between BIOS and EFI. When you provision VMs using a system policy, the boot option specified in the system policy and the VM template must be identical. When you provision a VM from the OVF or Content Library, the boot option specified in the template is taken as input.

You can choose this option using user interface, workflow task, or REST API. While provisioning VMs to choose the boot option, you can use the following workflows and REST APIs:

Workflows

- Provision VMware VM
- VMware Provision VM Using ISO Image
- VMware Provision a VM without VDC
- VMware Provision a Blank VM
- VMware OVF Deployment

REST APIs

- VMWARE_VM_PROVISION_WITHOUT_VDC
- VMWARE_BLANK_VM_PROVISION_WITHOUT_VDC
- userAPIProvisionRequest
- userAPISubmitWorkflowServiceRequestWithStartTimeAndDurationHours
- OVF_IMPORT_TO_VMWARE_CLOUD

Enhancement to the Host Node Report

Starting with this release, the Host Details screen and PCI devices screen now display information on the GPUs associated with the VMs. The screen displays the GPU devices and associated VMs after the mapping has been completed. To access the screen, click **Virtual** > **Compute** > **Host Node** > **PCI Devices.**

You can also view the total number of available GPU devices, which are not associated with any VM in the summary report. To view this information, choose **Virtual** > **Compute** > **Host Node** > **Summary** and see the **Resources** grid.

Enhancement to the VMware Guest Operation Task

Starting with this release, the VMware Guest Operation Task has been enhanced for monitoring the progress of task execution for Linux Guest Operating Systems. To enable monitoring, in the workflow task, check the **Trace Logs** check box and enter the values for the following fields:

- **Success Pattern**: Pattern based on which a task execution is considered as succeeded.
- **Failure Pattern**: Pattern based on which a task execution is considered as failed.
- **Log File Name**: The name of the log file with the complete file path. The task execution progress for service requests are retrieved from this log file. This log file is created only when the script you uploaded in the system includes code to generate a log file. You can review the contents of this log file on the guest system to troubleshoot errors when a workflow task results in a failure.
- **Interval Time (seconds)**: Monitoring occurs based on the interval time specified here. The value in this field must be lesser than the value that you specify in the **Wait Time To Complete** field.

Changes to Guest Setup Workflow Task

In prior releases, the Guest Setup workflow task had VM Password specified as the Password input type. Starting with this connector pack release, the Password input type has been modified from VM Password to Password. As a result, after upgrading to this version of the connector pack, validation of this workflow will fail. You must manually edit the workflow and change the Input type from VM Password to Password to ensure successful workflow validation.

New and Changed Features in Release 6.7.4.2

Enhancement to the Import OVF to VMware Cloud Task

Starting with this Connector Pack release, the **Import OVF to VMware Cloud** task has been enhanced to support the deployment of all types of OVFs into Cisco UCS Director. To configure the OVF properties, you can specify the OVF URL and enable the **Fetch OVF Properties** check box in order to automatically fetch the OVF details. You can then add, edit, or delete the OVF properties based on your requirement. The OVF deployment policy details are used as input in the Import OVF to VMware Cloud task.

Support for OVA Deployment Policy

Starting with this Connector Pack release, you can create an OVF deployment policy to support the deployment of all types of OVFs into Cisco UCS Director.

For more information, see Cisco UCS Director VMware vSphere Management Guide, Release 6.7.

Enhancement to the VMRC Console

Starting with this release, the VMRC console is enhanced to support the users who access the Cisco UCS Director appliance through the proxy server.

For more information, see Cisco UCS Director Administration Guide, Release 6.7.

Open Defects in Release 6.7.2.1

The following table lists the open defects in this release.

Defect ID	Headline
CSCvp69849	Top 5 Report: 'Host with Most Disk Usage' not showing details

Open Defects in Release 6.7.3.1

There are no open defects in this release.

Open Defects in Release 6.7.4.1

The following table lists the open defects in this release.

Defect ID	Headline
CSCvt25618	UCSD VDC based VM deployment enables the IPv6 address, by default.

Open Defects in Release 6.7.4.2

There are no open defects in this release.

Resolved Defects in Release 6.7.2.1

The following table lists the resolved defects in this release.

Defect ID	Headline
CSCvp78429	NPE found while executing VM Provisioning using VMware Provision Inputs task(Obselete)
CSCvo79356	Resource Allocation Configuration workflow task deploys IP addresses slowly
CSCva95735	Enhancement for Resize VM Disk task to change a user input type
CSCvk22779	ModifyVMwareVMNetwork task's Network Adapter User input is Generic Text. It should be LOV.
CSCvp23636	vcenter - DVS inventory enhancement requested.
CSCuz45768	Unable use VM Network field with User Input
CSCvq20058	NullPointerException on isDatastoreinMaintenanceMode with VMware 6.5 host with errors.

Resolved Defects in Release 6.7.3.1

The following table lists the resolved defects in this release.

Defect ID	Headline
CSCvq29126	Problems retrieving Custom Fields from VMM in Cisco UCS Director
CSCvq42581	ISO images can't be mapped from datastore when name includes speical character ':'
CSCvq94341	Vmware hardware compatibility matrix csv file found twice : once on filesystem once in jar file.

Defect ID	Headline
CSCvq99951	WinOS 2019 VM deployment fails with Mismatch in the IP Address for the nic(s): : NIC1 error
CSCvr90503	VMWare CD/DVD device should be accessed in a generic way
CSCvr59801	Cisco UCS Director version 6.7 cannot connect to vCenter 6.7 as TLS 1.2 is enforced by VMware
CSCvr56938	Resizing resources failing despite being under the defined resource limit.
CSCvr51965	Cisco UCS Director version 6.7.3.0 does not include HyperV input type for hyper-v accounts.

Resolved Defects in Release 6.7.4.1

The following table lists the resolved defects in this release.

Defect ID	Headline
CSCvt25662	VM Activity report shows deleted VM data as well
CSCvu23727	UCSD 6.7: VM action taking more time to load.
CSCvt99167	VM Actions Request tab content is too slow to retrieve.
CSCvt92426	Remove IPAddress Reservation task does not work when input is passed as user input.
CSCvu03906	VMWare VM snapshots cannot be deleted.
CSCvu35991	Unable to retrieve VDC memory usage details in Cisco UCS Directory with Hyper-V account.
CSCvu17071	Unable to perform actions in virtual machines after upgrading the Cisco UCS Directory from Release 6.7.2.0 to Release 6.7.3.0 or 6.7.4.1.

Resolved Defects in Release 6.7.4.2

The following table lists the resolved defects in this release.

Defect ID	Headline
CSCvv74111	**Modify VM Network** task failed to modify the VM network interface.

Defect ID	Headline
CSCvu81667	Password is not changing while provisioning Ubuntu and CentOS at vSphere.
CSCvv94576	Update **Modify VM Network** task for vwmare cloud to indicate that portgroup was not found.
CSCvt25618	Cisco UCS Director VDC based VM deployment enables the IPv6 address by default.

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.