Overview

Cisco UCS Director

Cisco UCS Director is a complete, highly secure, end-to-end management, orchestration, and automation solution for a wide array of Cisco and non-Cisco data infrastructure components, and for the industry's leading converged infrastructure solutions based on the Cisco UCS and Cisco Nexus platforms. For a complete list of supported infrastructure components and solutions, see the Cisco UCS Director Compatibility Matrix.

Cisco UCS Director is a 64-bit appliance that uses the following standard templates:

- Open Virtualization Format (OVF) and Open Virtual Appliance (OVA) for VMware vSphere
- Virtual Hard Disk (VHD) for Microsoft Hyper-V

Management through Cisco UCS Director

Cisco UCS Director extends the unification of computing and networking layers through Cisco UCS to provide you with comprehensive visibility and management of your data center infrastructure components. You can use Cisco UCS Director to configure, administer, and monitor supported Cisco and non-Cisco components. The tasks you can perform include the following:

- Create, clone, and deploy service profiles and templates for all Cisco UCS servers and compute applications.
- Monitor organizational usage, trends, and capacity across a converged infrastructure on a continuous basis. For example, you can view heat maps that show virtual machine (VM) utilization across all your data centers.
- Deploy and add capacity to converged infrastructures in a consistent, repeatable manner.
- Manage, monitor, and report on data center components, such as Cisco UCS domains or Cisco Nexus network devices.
- Extend virtual service catalogs to include services for your physical infrastructure.

- Manage secure multi-tenant environments to accommodate virtualized workloads that run with non-virtualized workloads.

Automation and Orchestration with Cisco UCS Director

Cisco UCS Director enables you to build workflows that provide automation services, and to publish the workflows and extend their services to your users on demand. You can collaborate with other experts in your company to quickly and easily create policies. You can build Cisco UCS Director workflows to automate simple or complex provisioning and configuration processes.

Once built and validated, these workflows perform the same way every time, no matter who runs the workflows. An experienced data center administrator can run them, or you can implement role-based access control to enable your users and customers to run the workflows on a self-service basis, as needed.

With Cisco UCS Director, you can automate a wide array of tasks and use cases across a wide variety of supported Cisco and non-Cisco hardware and software data center components. A few examples of the use cases that you can automate include, but are not limited to:

- VM provisioning and lifecycle management
- Network resource configuration and lifecycle management
- Storage resource configuration and lifecycle management
- Tenant onboarding and infrastructure configuration
- Application infrastructure provisioning
- Self-service catalogs and VM provisioning
- Bare metal server provisioning, including installation of an operating system

Features and Benefits

The features and benefits of Cisco UCS Director are as follows:

Feature	Benefit
Central management	• Provides a single interface for administrators to provision, monitor, and manage the system across physical, virtual, and bare metal environments • Provides unified dashboards, reports, and heat maps, which reduce troubleshooting and performance bottlenecks
Self-service catalog	• Allows end users to order and deploy new infrastructure instances conforming to IT-prescribed policies and governance
Adaptive provisioning	• Provides a real-time available capability, internal policies, and application workload requirements to optimize the availability of your resources
Dynamic capacity management	• Provides continuous monitoring of infrastructure resources to improve capacity planning, utilization, and management • Identifies underutilized and overutilized resources

Feature	Benefit
Multiple hypervisor support	• Supports VMware ESX, ESXi, Microsoft Hyper-V, and Red Hat hypervisors
Computing management	• Provisions, monitors, and manages physical, virtual, and bare metal servers, as well as blades • Allows end users to implement virtual machine life-cycle management and business continuance through snapshots • Allows administrators to access server utilization trend analysis
Network management	• Provides policy-based provisioning of physical and virtual switches and dynamic network topologies • Allows administrators to configure VLANs, virtual network interface cards (vNICs), port groups and port profiles, IP and Dynamic Host Control Protocol (DHCP) allocation, and access control lists (ACLs) across network devices
Storage management	• Provides policy-based provisioning and management of filers, virtual filers (vFilers), logical unit numbers (LUNs), and volumes • Provides unified dashboards that allow administrators comprehensive visibility into organizational usage, trends, and capacity analysis details.

Physical and Virtual Management Features

Physical Server Management	Virtual Computing Management
• Discover and collect configurations and changes • Monitor and manage physical servers • Perform policy-based server provisioning • Manage blade power • Manage server life cycle • Perform server use trending and capacity analysis • Perform bare metal provisioning using preboot execution environment (PXE) boot management	• Discover, collect, and monitor virtual computing environments • Perform policy-based provisioning and dynamic resource allocation • Manage the host server load and power • Manage VM life cycle and snapshots • Perform analysis to assess VM capacity, sprawl, and host utilization

Physical Storage Management	Virtual Storage Management
• Discover, collect, and monitor storage filers • Perform policy-based provisioning of vFilers • Provision and map volumes • Create and map Logical Unit Number (LUN) and iGroup instances • Perform SAN zone management • Monitor and manage network-attached storage (NAS) and SAN-based storage • Implement storage best practices and recommendation	• Discover, collect, and monitor storage of vFilers and storage pools • Perform policy-based storage provisioning for thick and thin clients • Create new datastores and map them to virtual device contexts (VDCs) • Add and resize disks to VMs • Monitor and manage organizational storage use • Perform virtual storage trend and capacity analysis
Physical Network Management	**Virtual Network Management**
• Discover, collect, and monitor physical network elements • Provision VLANs across multiple switches • Configure Access Control Lists (ACLs) on network devices • Configure storage network s • Implement dynamic network topologies	• Add networks to VMs • Perform policy-based provisioning with IP and DHCP allocation • Configure and connect Virtual Network Interface Cards (vNICs) to VLANs and private VLANs • Create port groups and port profiles for VMs • Monitor organizational use of virtual networks

Cisco UCS Director Installation Guidelines

Before you install Cisco UCS Director, be aware of the following:

Cisco UCS Director VM Disks

During Cisco UCS Director installation, on either VMware vSphere or Microsoft Hyper-V, the installer creates two hard disks.

- Primary disk—Contains the Cisco UCS Director appliance and operating system. Post-installation, the primary disk is named Hard Disk 1.
- Secondary disk—Contains the Cisco UCS Director database. Post-installation, the secondary disk is named Hard Disk 2.

Both disks are automatically created during the installation with the same disk format and parameters.

Cisco UCS Director OVF and VHD Zip Files

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.

About Licenses

You must obtain a license to use , as follows:

1. Before you install , generate the license key and claim a certificate (Product Access Key).
2. Register the Product Access Key (PAK) on the Cisco software license site, as described in Fulfilling the Product Access Key, on page 5.
3. After you install , update the license in as described in Updating the License.
4. After the license has been validated, you can start to use .

Fulfilling the Product Access Key

Before you begin

You need the PAK number.

Step 1 Navigate to the Cisco Software License website.

Step 2 If you are directed to the Product License Registration page, you can take the training or click **Continue to Product License Registration**.

Step 3 On the Product License Registration page, click **Get New Licenses from a PAK or Token**.

Step 4 In the **Enter a Single PAK or TOKEN to Fulfill** field, enter the PAK number.

Step 5 Click **Fulfill Single PAK/TOKEN**.

Step 6 Complete the additional fields in **License Information** to register your PAK:

Name	Description
Organization Name	The organization name.
Site Contact Name	The site contact name.
Street Address	The street address of the organization.
City or Town	The city or town.
State or Province	The state or province.
Zip or Postal Code	The zip code or postal code.

Name	Description
Country	The country name.

Step 7 Click **Issue Key**.

The features for your license appear, and you receive an email with the Digital License Agreement and a zipped license file.

Digitally Signed Images

images are delivered in digitally signed zip files. These signed zip files are wrapped in a container zip file that includes the following:

- Digitally signed zip file—Contains the installation image
- Verification program—Verifies the certificate chain and signature. During certificate chain validation, the program verifies the authenticity of the end-entity certificate using Cisco's SubCA and root CA certificates. Then, the authenticated end-entity certificate is used to verify the signature.
- Digital signature file—Contains the signature that you can verify before installation.
- Certificate file—Enables you to verify the digital signature. This Cisco-signed x.509 end-entity certificate contains a public key that can be used to verify the signature. This certificate is chained to the Cisco root posted on http://www.cisco.com/security/pki/certs/crcam2.cer.
- ReadMe file—Provides the information and instructions required to verify the digitally signed zip file.

Verify the image offline. Once the image is verified, you can begin the installation of .

Requirements for Verifying Digitally Signed Images

Before you verify a digitally signed image, ensure that you have the following on your local machine:

- Connectivity to https://www.cisco.com during the verification process
- Python 3.4.0 or later
- OpenSSL

Verifying a Digitally Signed Image

Before you begin

Download the image from Cisco.com.

Step 1 Unzip the file you downloaded from Cisco.com and verify that it contains the following files:

- ReadMe file

- Digitally signed zip file, for example `CUCSD_6_8_0_0_68060_VMWARE_GA.zip or CUCSD_6_8_0_0_68060_HYPERV_GA.zip`
- Certificate file, for example `UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer`
- Digital signature generated for the image, for example `CUCSD_6_8_0_0_68060_VMWARE_GA.zip.signature` or `CUCSD_6_8_0_0_68060_HYPERV_GA.zip.signature`
- Signature verification program, for example `cisco_x509_verify_release.py3`

Step 2 Review the instructions in the ReadMe file.

Note If there are any differences between these instructions and those in the ReadMe, follow the ones in the ReadMe.

Step 3 Run the signature verification program from the directory where you have unzipped the downloaded content.

Example: Signature Verification for VMware OVA Installation

```
python cisco_x509_verify_release.py3 -e UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer
-i CUCSD_6_8_0_0_68060_VMWARE_GA.zip -s CUCSD_6_8_0_0_68060_VMWARE_GA.zip.signature -v dgst
-sha512
```

Example: Signature Verification for Hyper-V VHD Installation

```
python cisco_x509_verify_release.py3 -e UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer
-i CUCSD_6_8_0_0_68060_HYPERV_GA.zip -s CUCSD_6_8_0_0_68060_HYPERV_GA.zip.signature -v dgst -sha512
```

Step 4 Review the output and ensure that the verification has succeeded.

Example: Expected Output for VMware OVA Installation

```
Retrieving CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully retrieved and verified crcam2.cer.
Retrieving SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer ...
Successfully retrieved and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully fetched a public key from UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer.
Successfully verified the signature of CUCSD_6_8_0_0_68060_VMWARE_GA.zip using
UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer
```

Example: Expected Output for Hyper-V VHD Installation

```
Retrieving CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully retrieved and verified crcam2.cer.
Retrieving SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer ...
Successfully retrieved and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully fetched a public key from UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer.
Successfully verified the signature of CUCSD_6_8_0_0_68060_HYPERV_GA.zip using
UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer
```

What to do next

Install or upgrade .