



CloudCenter Suite 5.0 Documentation

First Published: February 16, 2019

Last Modified: June 10, 2019

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive San Jose, CA 95134-1706 USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387) Fax: 408 527-0883

1. CloudCenter Suite 5.0	2
1.1 The CloudCenter Suite	3
1.2 Release Notes	5
1.2.1 CloudCenter Suite 5.0 Release Notes	6
1.2.2 Latest Suite Admin Release Notes	8
1.2.3 Latest Workload Manager Release Notes	9
1.2.4 Latest Action Orchestrator Release Notes	10
1.2.5 Latest Cost Optimizer Release Notes	11
1.3 Browser Compatibility	12
1.4 Support Information	13
1.4.1 Documentation Website	14
1.4.2 Documentation Accessibility	15
1.4.3 OpenSource Version Matrix	16
1.4.4 End of Support Notices	17
1.5 Security Considerations	19
1.6 Module Versions	21

CloudCenter Suite 5.0

Welcome to CloudCenter Suite 5.0 Documentation

The following cards allow you to progress with each module. To begin, click the *Suite Installer* card to view the documentation for that module. Once installed, click the *Suite Administrator* card.



Suite Installer

Installs Suite Admin using the virtual appliance installers



Suite Admin

Central location to manage all your Cisco CloudCenter Suite modules



Workload Manager

Model, deploy, and manage applications



Action Orchestrator

Orchestration and automation solution



Cost Optimizer

Cloud cost management and optimization solution

The CloudCenter Suite

Suite Architecture

- [Overview](#)
- [The Suite Architecture](#)
- [Port Requirements](#)
- [The Suite Administrator](#)
- [The Modules](#)

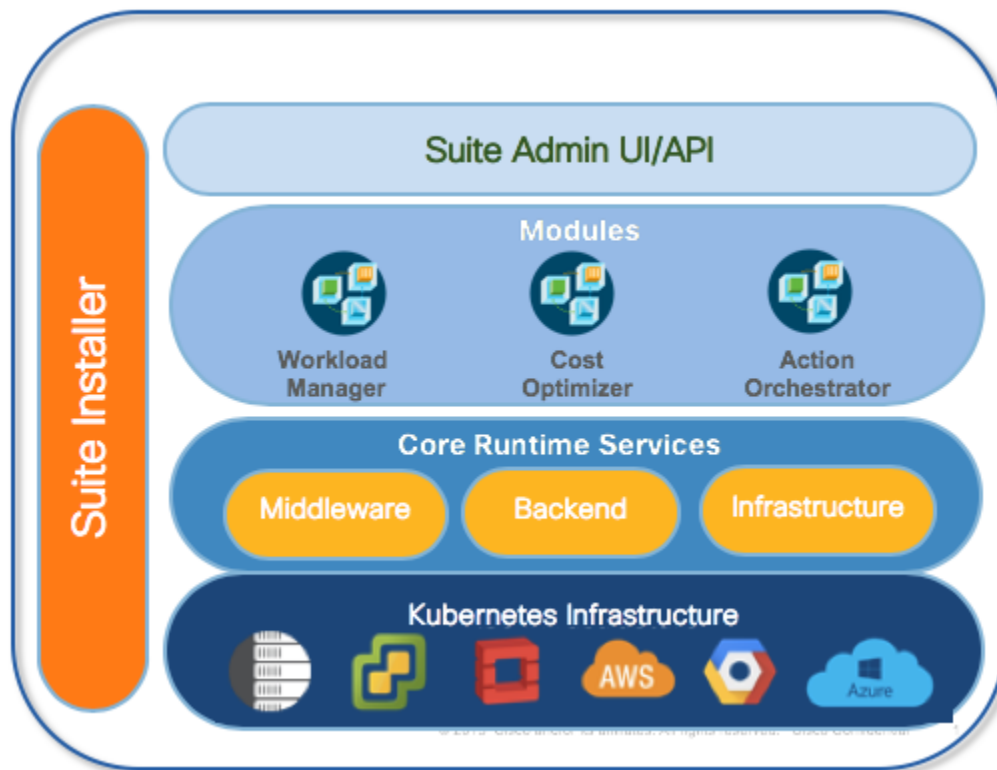
The CloudCenter Suite is Cisco's hybrid cloud deployment platform. This platform takes a unique approach to install, configure, and maintain hybrid cloud environments that are often encountered by Information Technology (IT) departments to adopt business agility and improve time-to-market solutions within an enterprise. As a cloud-based organization, your enterprise can choose from multiple cloud (*multicloud*) providers depending on your location, policies, permissions, security requirements, and governance regulations for both traditional and modern IT requirements.

The CloudCenter Suite provides a solution that is cloud agnostic, works with diverse workloads, provides cross-domain orchestration, supports cost-optimization, and integrates easily in an agile world.

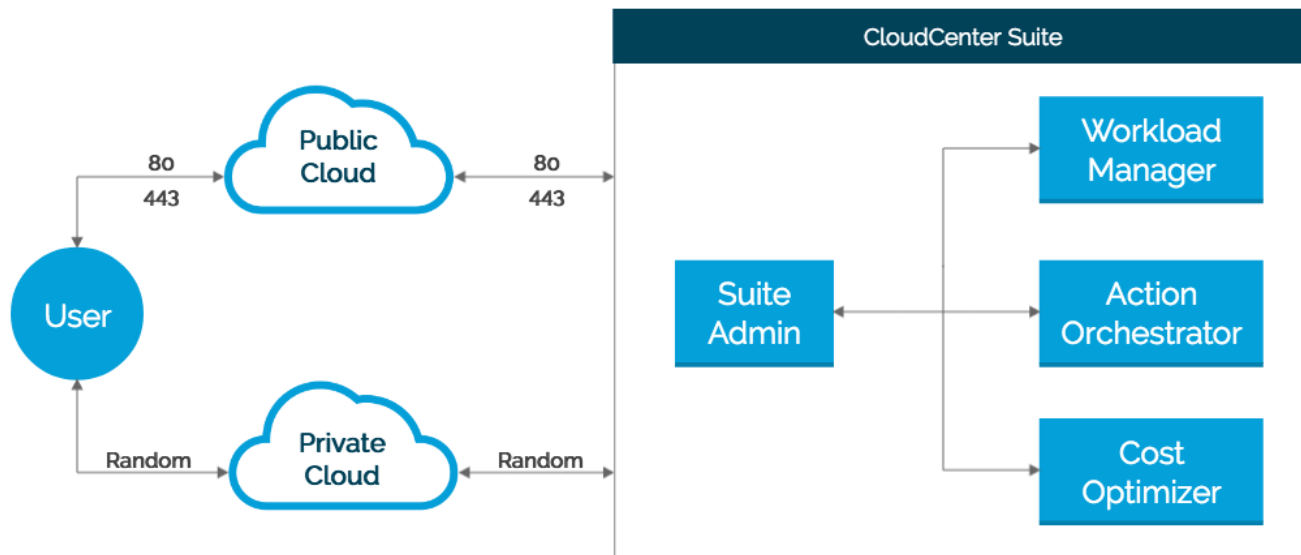
The CloudCenter Suite is made up of the following components:

- **Suite Installer** – Installs the Suite Admin. See [Suite Installer](#) for additional details.
- **Suite Admin** – Installs and launches a suite of modules. See [The Suite Admin](#) section below for additional details.
- **Modules** – The Workload Manager, the Cost Optimizer, and the Action Orchestrator. See [The Modules](#) section below for additional details.
- **Core Runtime Platform and Kubernetes Infrastructure** – A Kubernetes-based platform that allows you to launch each module on a new or existing Kubernetes cluster.

The following image displays the Suite Admin architecture.



The following image identifies the ports that must be open for the CloudCenter Suite to function as designed.



When you download and install the Suite Admin using the [Suite Installer](#), the Suite Admin is **already installed** and you have the option to install additional modules through the Suite Admin UI. You can:

- Install additional modules that are available of your choice based on the list available in the Dashboard.
- Upgrade the Suite Admin or installed module each time a new version becomes available.

The Suite Admin facilitates the installation of the following modules:

- **Workload Manager:** This module allows IT organizations to provide management for clouds (public/private/container), applications, VMs/pods, governance policies with centralized visibility and permission control for enterprise environments. See [Workload Manager](#) for additional details.
- **Action Orchestrator:** This module allows IT organizations to use cross-domain orchestration to automate a process that has multiple, complex steps with a specific order and implemented across different technical domains. See [Action Orchestrator](#) for additional details.
- **Cost Optimizer:** This module allows IT organizations to use cost optimization in a pay-per-use environment to avoid consumption that does not add value. See [Cost Optimizer](#) for additional details.

Each module in the CloudCenter Suite is independent and allows access to additional gateways or endpoints so you can add on module-specific components on supported clouds.

Back to: [CloudCenter Suite Home](#)

Release Notes

Release Notes for the CloudCenter Suite

- [CloudCenter Suite 5.0 Release Notes](#)
- [Latest Suite Admin Release Notes](#)
- [Latest Workload Manager Release Notes](#)
- [Latest Action Orchestrator Release Notes](#)
- [Latest Cost Optimizer Release Notes](#)

CloudCenter Suite 5.0 Release Notes

CloudCenter Suite 5.0 Release Notes

- [Release Date](#)
- [Architecture](#)
- [Release Cadence](#)
- [Installation](#)
- [Upgrade Path](#)
- [Clouds](#)
- [Security](#)
- [Limitations](#)
- [End of Life Notices](#)
- [Documentation](#)
- [Known Issues](#)

CloudCenter Suite 5.0.0 Release Date: February 16, 2019

Updated:

- June 10, 2019: Added a *Release Cadence* section.
- CloudCenter Suite 5.0 is a Cisco solution that includes multiple modules. Click the required module to view the documentation and release notes for each module.
 - [Suite Admin](#)
 - [Workload Manager](#)
 - [Action Orchestrator](#)
 - [Cost Optimizer](#)
- Install the CloudCenter Suite using a common installer (called the *Suite Installer*). See [Installer Overview](#) for additional details.
- Once installed, the UI facilitates the installation and version updates of all modules within the CloudCenter Suite.
- Each module in the CloudCenter Suite can have access to additional gateways or endpoints that allow enterprises to add module-specific *components*.

The CloudCenter Suite release model includes major, minor, and maintenance releases.

Each release has the following characteristics:

- **Major** releases are characterized as follows:
 - Significant architectural updates, feature additions, and/or UI changes.
 - A major release version is CloudCenter Suite 5.0.0.
 - When a major release becomes available, all modules also become available with corresponding versions.
- **Minor** releases are characterized as follows:
 - Includes multiple feature additions or updates.
 - A minor release version is CloudCenter Suite 5.1.0.
 - When a minor release becomes available, all modules also become available with corresponding versions.
- **Maintenance** releases are characterized as follows:
 - Includes fixes for specific issues.
 - A maintenance release version is CloudCenter Suite 5.0.1.
 - Each module can have its own release train and need not all have the same minor release.
 - Each minor release version is tracked with module-level release notes for each module.
 - When you update one module to a particular release, we recommend you update all other modules available for that release (if installed) to the same release.
 - See [Module Lifecycle Management](#) for additional details.

CloudCenter Suite 5.0.0 is available as installer files for ALL components for all supported clouds. See [Installer Overview](#) for additional details.

You can only install the CloudCenter Suite as a fresh installation.

The backup and restore functionality is currently not available in the CloudCenter Suite. Contact the [CloudCenter Suite Support team](#) for additional details.

You can launch the CloudCenter Suite using one of the following options:

- **Private Clouds:**
 - [VMware vSphere](#)
 - [OpenStack](#)
- **Public Clouds:**
 - [Amazon Elastic Container Service for Kubernetes \(Amazon EKS\)](#)
 - [Google Google Kubernetes Engine \(GKE\)](#)
 - [Azure Container Service \(AKS\)](#)

See [Security Considerations](#) for details.

This section identifies the areas which were previously available in [CloudCenter 4.10](#) and which are not supported by the CloudCenter Suite.

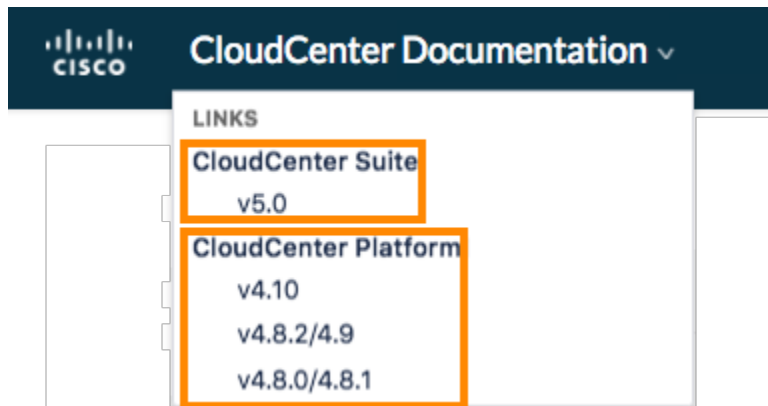
- CloudCenter Suite 5.0.0 is only available in the English language.
- Cloud support is limited to the listed clouds for each module.
- Batch, Parallel, and Desktop execution options are not available.
- Capacity manager and Federation Management are not supported.
- The concept of high availability is available in the backend and not an explicit configuration.
- The backup and restore functionality is not available

See [End of Support Notices](#) for additional details.

The <https://docs.cloudcenter.cisco.com> website is the home of the following products:

- CloudCenter Suite 5.0 and later releases (includes documentation for all modules that are part of the CloudCenter Suite Suite, including the [Workload Manager](#), which is the new name for the legacy CloudCenter platform).
- The **CloudCenter Platform** 4.x releases (the legacy versions of the current Workload Manager).

You can access one of the releases listed above from the dropdown list in the left header bar as displayed in the following screenshot. From any page, you can navigate to your release of choice by selecting the release from this dropdown list!



CloudCenter Suite 5.0.0 has no known issues.

Back to: [CloudCenter Suite Home](#)

Latest Suite Admin Release Notes

Suite Admin 5.0.3 Release Notes

- [Release Date](#)
- [New Installation](#)
- [Updating Existing Installations](#)
- [Clouds](#)
- [API](#)
- [Documentation](#)
- [Known Issues](#)
- [Resolved Issues](#)

First Published: June 24, 2019

Updated:

- December 7, 2020: Updated the *Documentation* section to include a list of pages that were updated.


New CloudCenter Suite 5.0.3 installers are available for all supported clouds. You can download these files from software.cisco.com.

See the [Installer](#) section for procedural details.

You can update any module that is available in CloudCenter Suite 5.0.3.

 You cannot upgrade the Kubernetes cluster for this release.

You can only update a module from CloudCenter Suite 5.0.0 or 5.0.1 or 5.0.2 to CloudCenter Suite 5.0.3:

 Updating the Suite Admin takes approximately 5-10 minutes. During this time you will:

- See an interruption in the CCS service until the pods restart and regain the *Running* status.
- See a few error messages being displayed, they are temporary.
- Be logged out – try logging in after a few minutes.

- Verify if an update is required/available. See [CloudCenter Suite 5.0 Release Notes > Release Cadence](#) for additional details.
- When a module update becomes available, the module card displays an **Update** button.
 - First update the Suite Admin module.
 - Update each remaining module individually. See [Update Module](#) for additional details.

No updates

No updates

The following documentation changes were implemented in CloudCenter Suite 5.0.3:

- [Existing Cluster Installation](#) (updated the cluster version from v1.11.0 to v1.11.3)
- [VMware vSphere Appliance Setup](#) (added an optional step to assign a Unique ID in Step 10)
- [Prepare Infrastructure](#) (added root disk storage details)
- [VMware vSphere Appliance Setup](#) (added a tip in Step 4g and a note to Step 10)
- [VMware vSphere Installation](#) (added a note to the allowed list tip)
- [End of Support Notices](#) (updated the page to reflect the latest information for the EOL and EOS for Cisco CloudCenter products)

When updating from Suite Admin 5.0.2 to 5.0.3, connectivity to your SMTP server will fail. This is not an issue when updating from Suite Admin 5.0.1 to 5.0.3.

Workaround: Go to your [Email Settings](#) page. Confirm all of the setting are as expected. Re-enter the password. Save the settings. The management cluster should now be able to communicate with your SMTP server.

No updates

Back to: [CloudCenter Suite Home](#)

Back to: [Suite Admin Release Notes](#)

Latest Workload Manager Release Notes

Workload Manager 5.0.3 Release Notes

- [Release Date](#)
- [Installation and Update](#)
- [Clouds](#)
- [API](#)
- [Documentation](#)
- [Known Issues](#)
- [Resolved Issues](#)

First Published: June 24, 2019

Updated:

- July 22, 2019: Added support for Cisco APIC, Release 4.0, as part of the [ACI Extensions](#) support.
- August 7, 2020: Updated the *Documentation* section to include a list of pages that were updated.

See the [Suite Admin 5.0.3](#) release notes to install or update the Workload Manager module.

Updating Workload Manager to 5.0.3 is required when you update Cost Optimizer to 5.0.3.

See also [CloudCenter Suite 5.0 Release Notes > Release Cadence](#).

No updates

No updates

The following documentation changes were implemented in Workload Manager 5.0.3:

- [Understand Application Tier Properties](#) (updated for technical accuracy)
- [ACI Extensions](#) (updated for technical accuracy)
- [Deployment, VM, and Container States](#) (updated for technical accuracy)
- [Permission Control](#) (updated for technical accuracy)
- [Application Tasks](#) (updated for technical accuracy)
- [OOB Services](#) (updated for technical accuracy)
- [Specify SSH Options](#) (updated for technical accuracy)
- [Artifact Repository](#) (updated for technical accuracy)
- [Service Administration](#) (updated for technical accuracy)
- [Benchmark Applications](#) (updated for technical accuracy)
- Removed pages on NFS and CephFS services as they were deprecated
- [Financial Overview](#) (removed management fee and cost-related items as they were deprecated)
- [ServiceNow Extensions](#) (added Madrid to the list of supported ServiceNow versions)
- [Specify SSH Options](#) (added a note to the Default option in the table)
- [Deploy an Application](#) (clarified the SSH/RDP usage)
- [Worker \(Conditional\)](#) (renamed this page to ensure continuity over releases)
- [Management Agent](#) (added details on the AgentLite option and realigned the page)
- [Options to Install the Worker](#) (added this page)
- [Install Worker on a Linux Image](#) (updated for technical accuracy and flow)
- [Conditional Component Appliance Images](#) (updated for technical accuracy)
- [Cloud Overview > Minimum Permissions for Public Clouds](#) (updated for technical accuracy)
- [Actions Library](#) (updated reboot action response for each cloud)
- [Deployment Parameters](#) (added the *Understanding Service and Deployment Parameters* section)
- [List VMs](#) (restricted to CloudCenter 4.x)
- [Guidance for Callout Scripts](#) (updated details for the *hwClockUTC* parameter)
- [VM Management API Calls](#) (updated the URI to reflect Managed VMs)

None

CSCvq27037: In Workload Manager 5.0.2, for an AWS cloud with a China region, attempting to add a cloud account would fail.

Resolution: Workload Manager 5.0.3 includes a fix to allow cloud accounts to be added to AWS clouds with a China region.

Back to: [CloudCenter Suite Home](#)

Back to: [Workload Manager Release Notes](#)

Latest Action Orchestrator Release Notes

Action Orchestrator 5.0.3 Release Notes

- [Release Date](#)
- [Installation and Upgrade](#)
- [Clouds](#)
- [API](#)
- [Documentation](#)
- [Known Issues](#)
- [Resolved Issues](#)

First Published: June 24, 2019

Updated:

- February 3, 2020: Updated the *Documentation* section to include the updated page.

See the [Suite Admin 5.0.3](#) release notes to install or update the Action Orchestrator module.

See also [CloudCenter Suite 5.0 Release Notes](#) > Release Cadence.

No updates

No updates

The following documentation changes were implemented in Action Orchestrator 5.0.3:

- [Execute Python Script](#) (updated description for Script to Execute on Target, Script Variable, and Property Name)
- [Execute Python Script Activity For Python 2.7 \(Obsolete\)](#) (updated description for Script to Execute on Target, Script Variable, and Property Name)
- [Data Schema](#) (updated links)

No updates

No updates

Back to: [CloudCenter Suite Home](#)

Back to: [Action Orchestrator Release Notes](#)

Latest Cost Optimizer Release Notes

Cost Optimizer 5.0.3 Release Notes

- [Release Date](#)
- [Installation and Update](#)
- [Clouds](#)
- [API](#)
- [Documentation](#)
- [Known Issues](#)
- [Resolved Issues](#)

First Published: June 24, 2019

Updated:

- December 11, 2019: Updated the *Documentation* section to include a list of pages that were modified.

See the [Suite Admin 5.0.3](#) release notes to install or update the Cost Optimizer module. Updating Cost Optimizer to 5.0.3 is required when you update Workload Manager to 5.0.3.

See also [CloudCenter Suite 5.0 Release Notes > Release Cadence](#).

No updates

No updates

The following documentation changes were implemented in Cost Optimizer 5.0.0:

- [Cost Optimizer Troubleshooting](#) (added a new section for Kubernetes Troubleshooting)
- [Cloud Overview > Minimum Permissions for Public Clouds](#) (updated for technical accuracy)

No updates

The following issues were resolved/addressed in Cost Optimizer 5.0.3:

- **CSCvp99890:** Cost Optimizer fails to display dashlets when logged in as a Financial Expert user.
Resolution: Cost Optimizer includes a fix to display dashlets for a Financial Expert user.
- **CSCvq09515:** Cost Optimizer RI Opportunities are not listed.
Resolution: Cost Optimizer 5.0.3 includes a fix to renew RI Opportunities that are due for expiry.
- **CSCvq27037:** In Cost Optimizer 5.0.2, for an AWS cloud with a China region, attempting to add a cloud account would fail.
Resolution: Cost Optimizer 5.0.3 includes a fix to allow cloud accounts to be added to AWS clouds with a China region.

Back to: [CloudCenter Suite Home](#)

Back to: [Cost Optimizer Release Notes](#)

Browser Compatibility

Browser Compatibility and Resolution

- [Browser Compatibility](#)
- [Resolution Requirements](#)
- [Language Option](#)

For CloudCenter Suite 5.0, Cisco supports the browser versions listed in the following table.

Browser	Version
Microsoft Edge	Version 16 and later
Firefox	Version 64.0 and later
Chrome	Version 71.0.3578.98 and later
Safari	Version 12.0.1 and later

* Internet Explorer is not supported.

Optimize your browser resolution by setting your monitor display to at least 1828 x 762 px to view the screen without scrolling.

Cisco provides English as the language option for the CloudCenter Suite.

Back to: [CloudCenter Suite Home](#)

Support Information

Support Information

- [Documentation Website](#)
- [Documentation Accessibility](#)
- [OpenSource Version Matrix](#)
- [End of Support Notices](#)

Back to: [CloudCenter Suite Home](#)

Documentation Website

Documentation Website

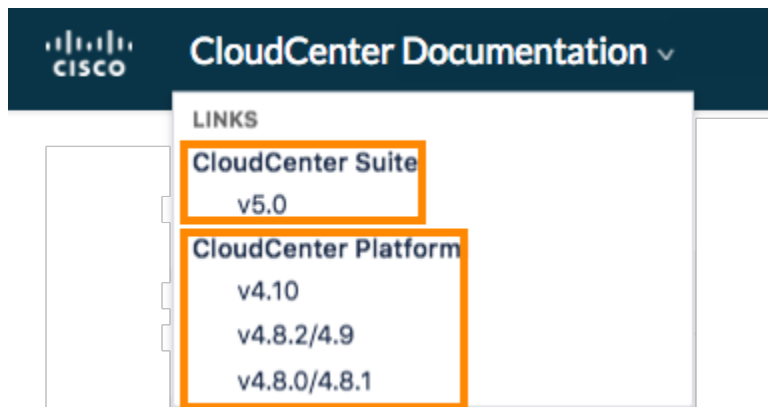
- [Website Compatibility](#)
- [Website Navigation](#)

For security and compliance reasons, CloudCenter Suite documentation (<https://docs.cloudcenter.cisco.com>) is accessible on browsers that support the Transport Layer Security (TLS) 1.2 protocol defined in RFC 5246. See your browser documentation for compliance details.

The <https://docs.cloudcenter.cisco.com> website is the home of the following products:

- The CloudCenter Suite 5.0 and later releases (includes documentation for all modules that are part of the CloudCenter Suite, including the [Workload Manager](#) module).
- The **CloudCenter Platform** 4.x releases (the older versions of the current [Workload Manager](#) module).

You can access one of the releases listed above from the dropdown list in the left header bar as displayed in the following screenshot.



From any page, you can navigate to your release of choice by selecting the release from this dropdown list!

Back to: [CloudCenter Suite Home](#)

Documentation Accessibility

Documentation Accessibility

- [Overview](#)
- [Accessibility Features](#)
- [Keyboard Shortcuts](#)

The information in this section applies to CloudCenter Suite Suite 5.0 releases.

For a list of accessibility features in CloudCenter Suite Suite 5.0, see [Voluntary Product Accessibility Template \(VPAT\)](#) on the Cisco website, or contact accessibility@cisco.com.

To expand the tree pane, follow this procedure:

1. Press the **return** key when the item is in focus.
2. Press the **tab** key to view the children for each item.

Back to: [CloudCenter Suite Home](#)

OpenSource Version Matrix

OpenSource Version Matrix

For a complete list of application versions for each module in the CloudCenter Suite, refer to the *CloudCenter OpenSource documentation* at software.cisco.com for the appropriate CloudCenter Suite *version*.

See the following image for additional details on finding this file: software.cisco.com > **CloudCenter** > *version* > **CloudCenter Suite OpenSource documentation**.

Software Download

[Downloads Home](#) / [Cloud and Systems Management](#) / [Cloud Management](#) / [CloudCenter Suite](#) / [CloudCenter- 5.0\(0\)](#)

Expand All Collapse All

Latest Release ▼

5.0(1)

All Release ▼

5 ▼

5.0(1)

5.0(0)

CloudCenter Suite

Release 5.0(0)

[▲ My Notifications](#)

Related Links and Documentation

- No related links or documentation -

File Information	Release Date	Size	
AzureRM CloudCenter Suite Installer ccs-azurermsuiteinstaller-cloudcenter-5.0.0-20190308.zip	25-Mar-2019	5188.45 MB	↓ 🛒 📄
Google CloudCenter Suite Installer ccs-google-suiteinstaller-cloudcenter-5.0.0-20190308.tar.gz	25-Mar-2019	5364.97 MB	↓ 🛒 📄
OpenStack CloudCenter Suite Installer ccs-openstack-suiteinstaller-cloudcenter-5.0.0-20190308.qcow2	25-Mar-2019	13678.44 MB	↓ 🛒 📄
VMware CloudCenter Suite Installer ccs-vmware-suiteinstaller-cloudcenter-5.0.0-20190308.ova	25-Mar-2019	5214.54 MB	↓ 🛒 📄
SNOW This optional Update Set adds a CloudCenter category in ServiceNow's Service Portal and enables the iframe integration so users can access CloudCenter from ServiceNow ccs-ServiceNow_UI_UpdateSet_v3.0-5.0.0.zip	22-Mar-2019	0.07 MB	↓ 🛒 📄
The README describes the images required for installing CloudCenter Suite README_download_Cisco_CloudCenter-Suite-release-5.0.0	22-Feb-2019	0.00 MB	↓ 🛒 📄
AzureRM CloudCenter Cloud Remote ccs-azurerm-cloudremote-5.0.0-20190215.zip	22-Feb-2019	2715.71 MB	↓ 🛒 📄
AzureRM CloudCenter Repo Virtual Appliance ccs-azurerm-repo-appliance-5.0.0-20190215.zip	22-Feb-2019	11887.16 MB	↓ 🛒 📄
Jenkins Client Plugin ccs-JenkinsClient-5.0.0-20190215.hpi	15-Feb-2019	11.74 MB	↓ 🛒 📄
Installers and artifacts needed to build Virtual Appliances using your operating system image ccs-installer-artifacts-5.0.0-20190215.tar	15-Feb-2019	121.49 MB	↓ 🛒 📄
CloudCenter Suite OpenSource library documentation ccs-opensource-documentation-5.0.0-20190215.zip	15-Feb-2019	20.86 MB	↓ 🛒 📄
OpenStack CloudCenter Cloud Remote ccs-openstack-cloudremote-5.0.0-20190215.qcow2	15-Feb-2019	4960.00 MB	↓ 🛒 📄
OpenStack CloudCenter Repo Virtual Appliance ccs-openstack-repo-appliance-5.0.0-20190215.qcow2	15-Feb-2019	15982.94 MB	↓ 🛒 📄
VMware CloudCenter Cloud Remote ccs-vmware-cloudremote-5.0.0-20190215.ova	15-Feb-2019	2789.89 MB	↓ 🛒 📄

Back to: [CloudCenter Suite Home](#)

End of Support Notices

End-of-Sale and End-of-Life Announcements for Cisco CloudCenter Products

- Cisco CloudCenter Suite
 - Cisco CloudCenter Suite (On-Prem / Self-Hosted)
 - Suite Installer
 - Suite Admin
 - Workload Manager/Cost Optimizer
 - Action Orchestrator
 - Cisco CloudCenter Suite SaaS
- Cisco CloudCenter Platform (Legacy)
 - Cisco CloudCenter Platform 4.10.x
 - Cisco CloudCenter Platform 4.9.x and prior



This bulletin provides the consolidated information for all Cisco CloudCenter products and replaces previously provided information.

Cisco CloudCenter Suite releases are supported for up to 18 months. However, Cisco reserves the right to change and defer support timelines as required. The Last Date of Support (LDOS) marks the last date for customers to receive applicable service and support as entitled by active service contracts for covered products. After this date, the service is no longer available.

Cisco CloudCenter Suite (On-Prem / Self-Hosted)

Suite Installer

CloudCenter Release	Kubernetes Version	CCP Tenant Image	Release Date	LDOS
Suite Installer 5.1.1	1.13.5	ccp-tenant-image-1.13.5.ova	September 26, 2019	March 26, 2021
Suite Installer 5.2.0	1.16.3	ccp-tenant-image-1.16.3-ubuntu18-6.1.0.ova	May 9, 2020	November 9, 2021
Suite Installer 5.2.3	1.16.3	ccp-tenant-image-1.16.3-ubuntu18-6.1.1.ova	October 13, 2020	April 13, 2022

Cisco announces the End-of-life and End-of-Support for Kubernetes clusters deployed by **5.0(x) Cisco CloudCenter Suite Installers**. No patches or maintenance releases will be provided. Support for modules running on older Kubernetes clusters will be *best effort* as determined by Cisco TAC. Customers are always encouraged to use the latest Suite Installer to backup and restore their existing CloudCenter Suite application to a supported Kubernetes cluster version.

Suite Admin

CloudCenter Release	Release Date	LDOS
Suite Admin 5.0	February 16, 2019	August 16, 2020
Suite Admin 5.1	August 19, 2019	February 19, 2021
Suite Admin 5.2	May 9, 2020	November 9, 2021

Workload Manager/Cost Optimizer

CloudCenter Release	Release Date	LDOS
Workload Manager 5.0/Cost Optimizer 5.0	February 16, 2019	August 16, 2020
Workload Manager 5.1/Cost Optimizer 5.1	August 19, 2019	February 19, 2021
Workload Manager 5.2/Cost Optimizer 5.2	March 31, 2020	September 30, 2021
Workload Manager 5.3/Cost Optimizer 5.3	May 7, 2020	November 7, 2021
Workload Manager 5.4/Cost Optimizer 5.4	July 30, 2020	January 30, 2022

Action Orchestrator

CloudCenter Release	Release Date	LDOS
Action Orchestrator 5.0	February 16, 2019	August 16, 2020

Action Orchestrator 5.1	August 19, 2019	February 19, 2021
Action Orchestrator 5.2	May 29, 2020	November 29, 2021

Cisco CloudCenter Suite SaaS

Cisco [announces](#) the end-of-sale and end-of-life dates for **Cisco CloudCenter Suite SaaS**. Customers with active service contracts will continue to receive support from the Cisco Technical Assistance Center (TAC) as shown below. The following table describes the end-of-life milestones, definitions, and dates for the affected product(s).

End-of-Life Milestones		
Milestone	Definition	Date
End-of-Life Announcement Date	The date the document that announces the end-of-sale and end-of-life of a product is distributed to the general public.	November 6, 2020
Last Date of Support (LDOS)	The last date to receive applicable service and support as entitled by active service contracts for covered products. After this date, the service is no longer available.	TBD <i>Target - Feb 2021</i>

For additional information please review [Cisco's End-of-Life Policy](#) and the [End-of-Life and End-of-Sale Notices for CloudCenter Suite](#).

Cisco CloudCenter Platform 4.10.x

Cisco [announces](#) the end-of-sale and end-of-life dates for the **Cisco CloudCenter Platform (Legacy/4.x)**. The last day to order the affected product(s) is **May 7, 2021**. Customers with active service contracts will continue to receive support from the Cisco Technical Assistance Center (TAC) as shown below. The following table describes the end-of-life milestones, definitions, and dates for the affected product(s).

End-of-Life Milestones		
Milestone	Definition	Date
End-of-Life Announcement Date	The date the document that announces the end-of-sale and end-of-life of a product is distributed to the general public.	November 6, 2020
End-of-Sale Date	The last date to order the product through Cisco point-of-sale mechanisms. The product is no longer for sale after this date.	May 7, 2021
Last Date of Support (LDOS)	The last date to receive applicable service and support as entitled by active service contracts for covered products. After this date, the service is no longer available.	May 7, 2024

For additional information please review [Cisco's End-of-Life Policy](#) and the [End-of-Life and End-of-Sale Notices for CloudCenter Platform \(Legacy\)](#).

Cisco CloudCenter Platform 4.9.x and prior

Cisco [announces](#) the End-of-life and End-of-Support for versions of **Cisco CloudCenter Platform 4.9.1 and earlier**. Software maintenance support for all versions listed above ended on **October 31, 2020**. No patches or maintenance releases will be provided. Customers are encouraged to migrate to Cisco CloudCenter Platform 4.10.0.10 or to Cisco CloudCenter Suite 5.2.3 or later.

Back to: [CloudCenter Suite Home](#)

Security Considerations

Security Considerations

- [Overview](#)
- [Product Overview](#)
- [CloudCenter Suite Architecture](#)
- [User Authentication](#)
- [Cloud Authentication](#)
- [REST API Calls](#)
- [UI Authentication](#)
- [Module Security](#)
- [Role-Based Access Control](#)

This section provides design specification details related to the security of the CloudCenter Suite.

This section DOES NOT provide on operational policies such as key rotation, incident management and business continuity policies are not covered in this document.

CloudCenter Suite is an enterprise-class solution that offers a secure, scalable, extendable, and multi-tenant solution that can scale to meet the needs of the most demanding IT organizations and cloud service providers.

CloudCenter Suite uses various types of metadata, authentication information (such as *customer credentials and keys*), cloud usage metrics, and users associated with cloud applications to deploy and manage applications on cloud infrastructures.

The CloudCenter Suite does not store *customer application data* (data that is created, used, or managed by the user's cloud applications).

- Customer application data is only stored on customer premises or on cloud infrastructures.
- Customer application data is not stored or accessed by CloudCenter Suite at any point.

CloudCenter Suite provides end-to-end security with:

- A comprehensive key management mechanism
- Full application and application tier network isolation (micro-segmentation)
- Data encryption for data both in transit and at rest
- User identity management and authentication control
- User, application, and object-level access control

The CloudCenter Suite architecture is deployed as a distributed architecture and is composed of several key architectural components as described in [The CloudCenter Suite Architecture](#).

CloudCenter Suite supports user password, hash-based authentication, and SAML 2.0-based Single Sign-On (SSO) authentication. CloudCenter Suite also provides authentication for REST API endpoint access.

CloudCenter Suite authenticates users through a unique username and password. The password is not stored in clear-text, but is converted using a secure one-way hash algorithm (SHA256) with a random salt. If different users use the same password, this will not result in the same password hash. This hash code is generated and stored when the user creates the password for the first time or changes the password at a later time. Upon login, the hash code is regenerated using the specified password and matched against the stored hash code to authenticate the user. Since this is a one-way hash algorithm, no Cisco employee or third-parties can discover the user password. The password is neither reverse recoverable, nor subject to brute force dictionary attack.

CloudCenter Suite leverages SAML (2.0) to integrate with customer identity platforms such as Active Directory (AD) and LDAP. For SAML-based SSO authentication, the user directory, password, and authentication mechanism are controlled by the customer. Customers may further choose to enable multi-factor authentication on their user login page through well-known identity provider platforms such as ADFS, Ping Identity, Okta, and so forth. The CloudCenter Suite only uses the user's email address as the user identity in SSO mode. Customers can configure unique SAML Identity Providers (IdP) properties on a per tenant basis. The CloudCenter Suite tenant admin can optionally set additional mapping rules to automatically sync user groups and user group membership based on custom properties provide by IdP

The CloudCenter Suite authenticates to public, private, and hybrid clouds using cloud account credentials provided to CloudCenter Suite when a user configures cloud environments. These cloud account credentials are stored securely in the CloudCenter Suite database using AES-256 encryption.

Configuring and registering clouds and cloud accounts in CloudCenter Suite is limited to CloudCenter Suite administrators. The CloudCenter Suite administrator can decide if additional tenant administrators and end-users can configure their own cloud account information. See [Initial Administrator Setup](#) for details.



Effective [Suite Admin 5.0.1](#), Cisco provides CSRF protection for all API calls. See [CSRF Token Protection](#) for additional details.

Access to the REST API interface is limited to configured user accounts. To authenticate API requests, all CloudCenter Suite REST APIs require basic authentication using an API key as the password. For example:

```
curl -H "Accept:application/json" -H "Content-Type:application/json" -u <user_accountNumber>:<api_key> -X GET https://<HOST>:<PORT>/api/v1/suite-idm/currentUser/userInfo
```

In addition to the user's *accountNumber.apikey* combination, all CloudCenter Suite REST APIs can also accept the *JSON Web Token (JWT)*. For example:

```
curl -H "Accept:application/json" -H "Content-Type:application/json" -H "Authorization: Bearer <JWT>" -X GET https://<HOST>:<PORT>/api/v1/suite-idm/currentUser/userInfo
```

A REST API key is a 36-character, randomly generated, case-sensitive, hexadecimal UUID string. This key, combined with the user's unique Account Number (*accountNumber*), is used for REST API authentication. During authentication, the REST API key specified in the HTTPS request is matched with the REST API key stored in the CloudCenter Suite database. This prevents the user from revealing the real user password in any automation script, and also allows REST API authentication to work with either user/password hash-based or SAML SSO-based authentication.

To provide data security, all REST API requests must be issued over a secure, encrypted, HTTPS connection.

The REST API key for each user is stored securely in CloudCenter Suite database using SHA256 one-way hash. The [API Key](#) section provides additional details about secure key storage and key operations. See [Suite Admin API](#) for details on CloudCenter Suite REST APIs and how to use them.

All users can generate their own API keys – the Suite Admin has no control over this function.

The CloudCenter Suite UI requires user authentication. Each authenticated user will have a unique Session ID to track activities and a JWT to ensure API access. The JWT expires in 15 minutes and the UI auto-refreshes the JWT token if it detects the user actively using the UI. If the user is logged off or if the user is disabled or deleted, the user's active JWT is no longer valid.

The CloudCenter Suite connects to a Cisco hosted Helm repository and a Docker registry to check for available modules and updates. These repositories are fully compliant with export control and requires authentication for each user connecting to the repository. All CloudCenter Suite module are packaged as Helm Chart and Docker images. The Helm Chart refers to Docker images via the image's SHA256 hash. The Helm Chart itself is signed and verified by the CloudCenter Suite upon installation or upgrade. This way the integrity of the Helm Chart and Docker images are guaranteed.

The CloudCenter Suite offers granular control of access to each CloudCenter Suite resource through role-based, module-level access control. Access to resources like services, clouds, application profiles, deployment environments, and other CloudCenter Suite resources can be managed based on roles associated with users or user groups. See [Understand Roles](#) for details.

Back to: [CloudCenter Suite Home](#)

Module Versions

Unable to render {include} The included page could not be found.

Back to: [CloudCenter Suite Home](#)

1. Installer 5.0 Home	2
1.1 Installer Overview	3
1.2 Installer Virtual Appliances	4
1.2.1 Virtual Appliance Overview	5
1.2.2 Amazon Appliance Setup	7
1.2.3 Azure Appliance Setup	8
1.2.4 GCP Appliance Setup	10
1.2.5 OpenStack Appliance Setup	14
1.2.6 VMware vSphere Appliance Setup	17
1.3 Installation Approach	22
1.3.1 Prepare Infrastructure	23
1.3.2 New Cluster Installation	25
1.3.2.1 Amazon EKS Installation	26
1.3.2.2 Azure Installation	29
1.3.2.3 Google GKE Installation	33
1.3.2.4 OpenStack Installation	37
1.3.2.5 VMware vSphere Installation	41
1.3.3 Existing Cluster Installation	47
1.3.4 Offline Repository	51
1.4 Troubleshooting	54

Installer 5.0 Home

CloudCenter Suite Installer 5.0 Documentation

Saturday, February 16, 2019: Cisco released [CloudCenter Suite 5.0 Release Notes](#)

- [Suite Admin 5.0.0](#) released on February 16, 2019
- [Suite Admin 5.0.1](#) released on April 6, 2019
- [Suite Admin 5.0.2](#) released on May 17, 2019
- [Suite Admin 5.0.3](#) released on June 24, 2019

Search

[VMware vSphere Installation](#)

updated Sep 24, 2020

[view change](#)

[VMware vSphere Appliance Setup](#)

updated Sep 24, 2020

[view change](#)

[Troubleshooting](#)

updated Jun 19, 2020

[view change](#)

Installer Overview

Installer Overview

- [Overview](#)
- [Supported Clouds](#)
- [Installer Appliance Download Location](#)

The CloudCenter Suite provides a new way to install, configure, and maintain multiple modules that jointly make up the suite. The CloudCenter Suite has a common installer to install, upgrade, and integrate all modules included in the suite.

You can install the CloudCenter Suite by using installer appliance images provided by Cisco. As part of the installation process, the CloudCenter Suite installs the Suite Admin. Once authenticated, each user can access the Suite Admin using valid credentials created by the Suite Administrator.



Installers are already incorporated in the CloudCenter Suite SaaS offer, see [SaaS Information](#) for additional details.

Cisco supports the corresponding Kubernetes engine (or managed services) for the following public clouds for the CloudCenter Suite:

- [Amazon Elastic Container Service for Kubernetes \(Amazon EKS\)](#)
- [Google Kubernetes Engine \(GKE\)](#)
- [Azure Kubernetes Service \(AKS\)](#)

Cisco supports the following private clouds for the CloudCenter Suite:

- [VMware vSphere](#)
- [OpenStack](#)

Major releases include installer appliances for the following components and cloud providers.

You can download these files from software.cisco.com.

The [Virtual Appliance Overview](#) section provides more details on these files.

Installer Virtual Appliances

Installer Virtual Appliances

- [Virtual Appliance Overview](#)
- [Amazon Appliance Setup](#)
- [Azure Appliance Setup](#)
- [GCP Appliance Setup](#)
- [OpenStack Appliance Setup](#)
- [VMware vSphere Appliance Setup](#)

Virtual Appliance Overview

Virtual Appliance Overview

- [Virtual Appliance Overview](#)
- [General Virtual Appliance Approach](#)
- [Port Architecture](#)
- [Cloud-Specific Setup](#)

The only way to install the Suite is to use the Virtual Appliance Installer method. Cisco builds these appliances on CentOS 7.x base images.





Installers are already incorporated in the CloudCenter Suite SaaS offer, see [SaaS Information](#) for additional details.

To prepare infrastructure for the appliance approach, follow this process.

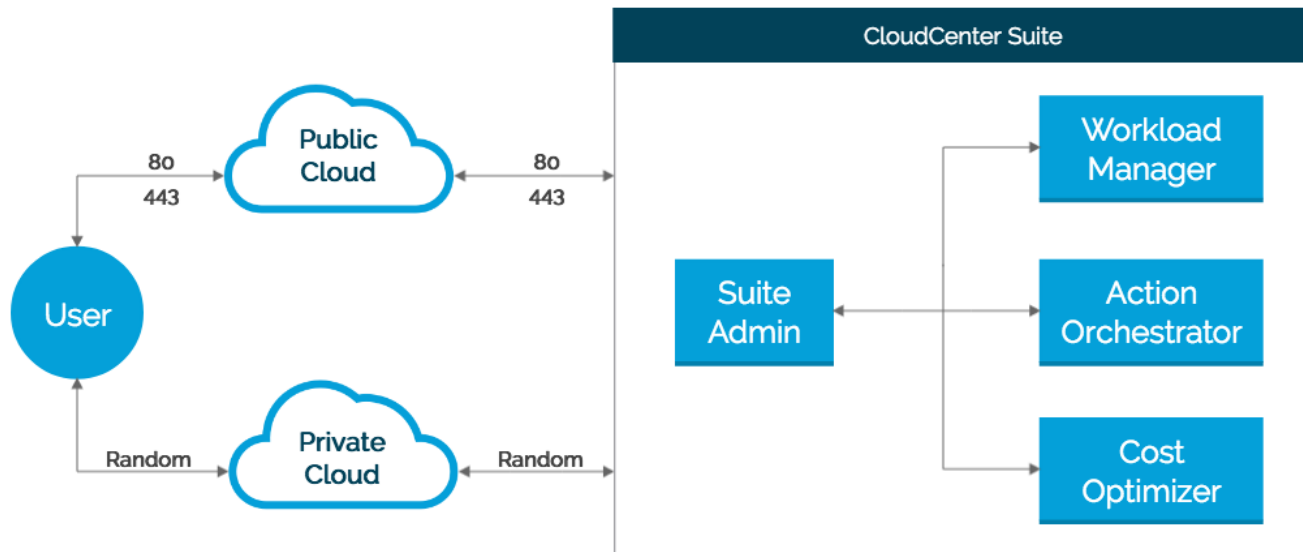
1. Review and ensure that you have met the requirements to [Prepare Infrastructure](#) before installing the CloudCenter Suite.
2. Review the list of [Supported Suite Installers](#) to verify the supported Virtual Appliances.
3. Navigate to software.cisco.com to download virtual appliances for each supported cloud.
4. Follow directions as specified in the table below to obtain and import each image.


Cloud	Image Type	Description
AWS	Shared image (AMI)	Obtain launch permissions for the AWS account. Refer to the AWS documentation for additional context. Request image sharing for the AWS account by opening a CloudCenter Support case (https://mycase.cloudapps.cisco.com/case or http://www.cisco.com/c/en/us/support/index.html). In your request, specify the following details: <ol style="list-style-type: none"> a. Your AWS account number b. Your CloudCenter Suite version c. Your Customer ID (CID) d. Your customer name e. Specify if your setup is in production or for a POC f. Your Contact Email address
Azure	Downloaded Virtual Appliance (VHD from the ZIP folder)	Create a new Azure image using the provided VHD file provided by Cisco and launch a VM using that image. Refer to the Azure documentation for additional context.
GCP	Shared image	Create a new GCP image using the provided VHD provided by Cisco and launch a VM using that image. Refer to the GCP documentation for additional context
OpenStack	Downloaded Virtual Appliance (QCOW2)	Import the QCOW2 image file using the OpenStack client. Refer to the OpenStack Documentation for additional context.

VMware vSphere	Downloaded Virtual Appliance (OVA)	<p>Follow this procedure:</p> <ol style="list-style-type: none"> Download the OVA image. Import the OVA to your vSphere environment by using the vSphere client <ol style="list-style-type: none"> When you import the OVA as a VM, ensure that it is powered off on vSphere. If your environment requires a static IP, use a VMware Customization Spec to manually configure the static IP for the installer VM. A default password is required to ensure access to the VM using the console (in case the SSH has issues). <div data-bbox="521 363 1482 562" style="border: 1px solid green; padding: 5px; margin: 5px 0;"> <p> If you provide a default password or public-key, be aware of the following requirements:</p> <ul style="list-style-type: none"> The login user is the cloud-user. If you configure a default password or public key in the VM, you must also configure the default instance ID and hostname fields as they are dependent and required fields. Use this password to access the VM via vSphere console. You cannot use this password to SSH into the launched VMs. </div> Select the required Network for the interface to be connected. Convert the VM to a template. <div data-bbox="521 648 1482 758" style="border: 1px solid orange; padding: 5px; margin: 5px 0;"> <p> You <i>must</i> convert the VM to template and then create a VM from this template, so that the template can be used when installing a VMware data center. If you do not provide the template name when installing a VMware data center, your installation will fail.</p> </div> Select the template created in the previous step and <i>clone to Virtual Machine</i>, to launch the installer VM. This template will also be used as the value for the <i>vSphere Template Name</i> cloud setting, in the installer UI. After the VM is created from the template, power it on. To access the UI, go to the newly created VM's IP using HTTPS protocol in a supported browser (see Browser Compatibility).
----------------	------------------------------------	--

5. Launch the installer instance using the image.

The following image identifies the ports that must be open for the CloudCenter Suite to function as designed.



 The per-cloud setup procedures are only listed below to serve as sample setup scenarios.

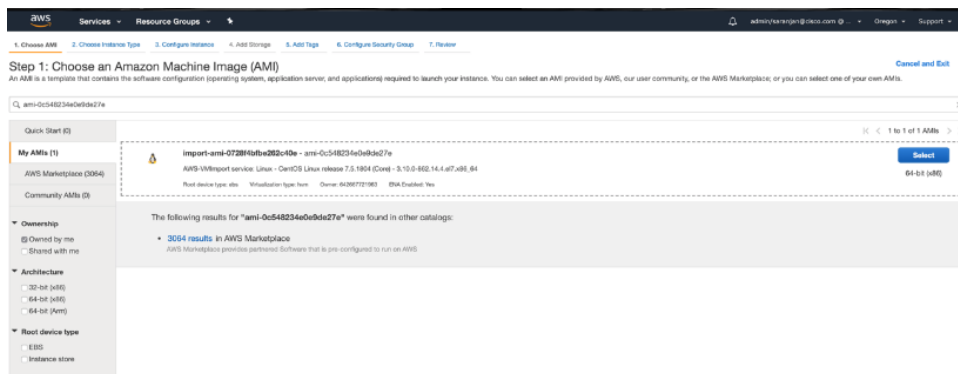
- [Amazon Appliance Setup](#)
- [GCP Appliance Setup](#)
- [Azure Appliance Setup](#)
- [OpenStack Appliance Setup](#)
- [VMware vSphere Appliance Setup](#)

Amazon Appliance Setup

Amazon Appliance Setup

To setup infrastructure for Amazon, follow this process.

1. Request image sharing for the AWS account by opening a [CloudCenter Support case](#). In your request, specify the following details:
 - a. Your AWS account number
 - b. Your CloudCenter Suite version
 - c. Your Customer ID (CID)
 - d. Your customer name
 - e. Specify if your setup is in production or for a POC
 - f. Your Contact Email
2. After you open a case, your support case is updated with the share AMI IDs. **Proceed to the next step only after your support case is updated with the AMI IDs.**
3. Navigate to the EC2 dashboard and search for the AMI ID name provided in the [CloudCenter Support case](#) (from Step 2 above)
4. Launch the EC2 instance using the AMI.
 - a. Navigate to the EC2 dashboard.




- b. Create EC2 instance in desired Region, VPC, subnet.
 - i. Choose an Instance Type.
 - ii. Configure the instance details for your environment.
 - iii. Review the instance launch details.
 - iv. Select an existing key-pair or create a new pair as required.
 - v. Create a security group with Ports 443, 80 (and optionally, 22) to be open.
 - vi. Launch the instance with the security group and key pair created in the previous two steps.
 - vii. Access the installer using the IP of the launched instance via HTTPS from your favorite browser.

Azure Appliance Setup

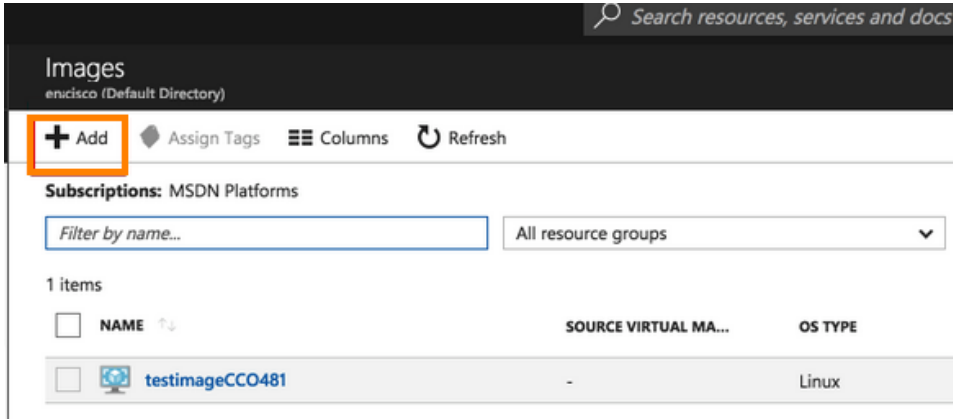
Azure Appliance Setup

To setup infrastructure for Azure clouds, follow this process.

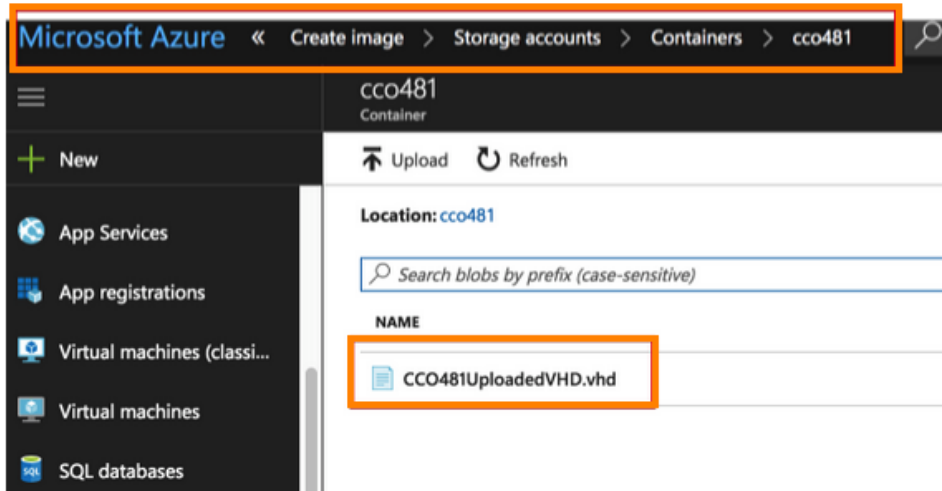
1. Upload the Cisco-provided VHD to the desired Azure Storage account/Region. See <https://docs.microsoft.com/en-us/azure/virtual-machines/linux/upload-vhd#option-1-upload-a-vhd> for detailed instructions.

 You must use the Azure CLI to perform this upload.

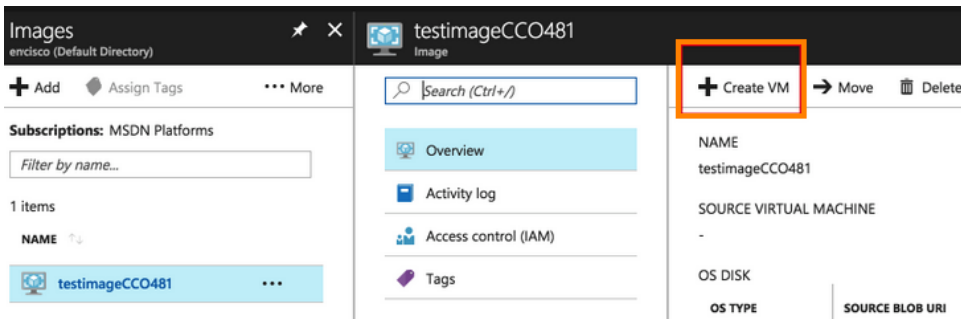
2. Create a Linux image from the uploaded .vhd file.



3. Select the disk name that you created in Step 2. In this example, it is CCO4100UploadedVHD.vhd.



1. Spin up a VM using the created image from Azure console.



You have now setup the installer for an Azure cloud.

GCP Appliance Setup

GCP Appliance Setup

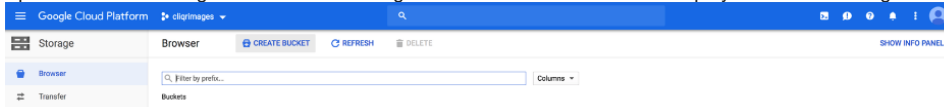
- [Overview](#)
- [Cloud Storage Bucket](#)
- [Create the Image](#)
- [Create the Instance](#)

Setting up the GCP appliance, is a multi-step process:

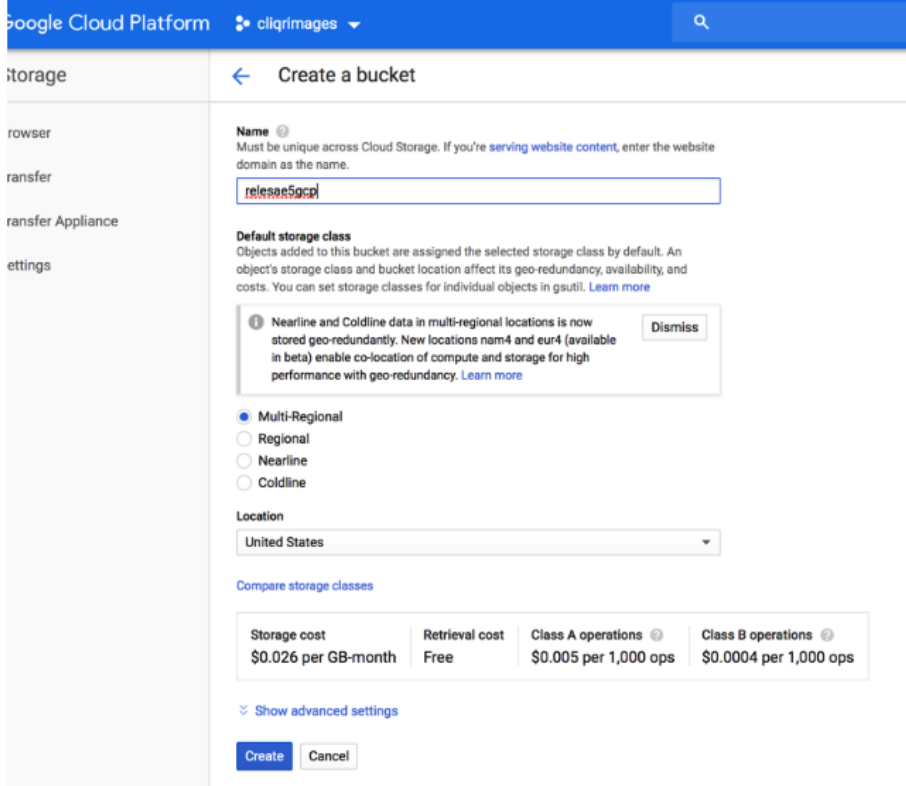
- Address the prerequisite permissions
- Create a storage [bucket](#) using the tar.gz file provided by Cisco
- Create the image
- Create the instance

To upload Cisco's tar.gz file to the GCP bucket, follow this process.

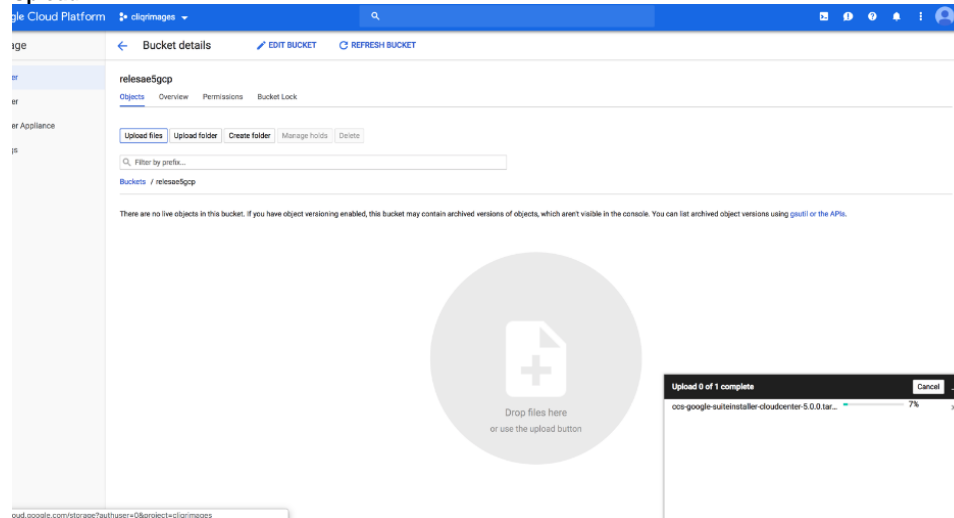
1. Open the Cloud Storage browser in the Google Cloud Platform Console as displayed in the following screenshot.



2. Click **Create bucket** and complete the required information for your environment. The following screenshot provides a sample setup.



- Upload the the tar.gz file provided by Cisco by dragging and dropping the file to the main pane as visible in the following screenshot or by clicking **Upload**.

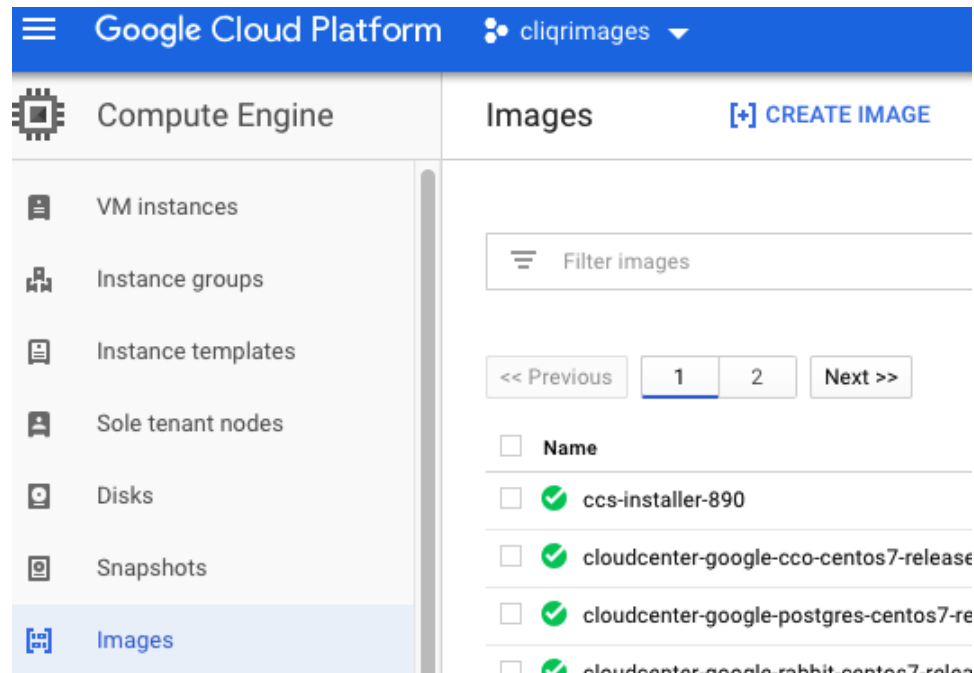


Uploading the file might take some time based on your network speed.

- After the upload is complete, use the same bucket to create the image as described in the next section.

To create an image, follow this process.

- Login to Google Cloud Platform.
- Create a Service Account with the following permissions:
 - Kubernetes Engine (Admin)
 - Compute Engine (Admin)
 - Service Account (User)
- Select **Compute Engine**.
- Click on **Images**.
- Click on **Create Image**.



6. Provide a **Name** for the new instance, select *Cloud Storage File* as the **Source**, browse and select the *image* file from the cloud storage bucket (uploaded in Step 2 above) for your environment and click **Create**.

The screenshot shows the 'Create an image' page in the Google Cloud Platform console. The left sidebar lists various Compute Engine resources, with 'Images' selected. The main content area contains the following fields and options:

- Name:** cloudcentersuite-v1
- Family (Optional):** (empty)
- Description (Optional):** (empty)
- Labels (Optional):** + Add label
- Encryption:** Data is encrypted automatically. Select an encryption key management solution.
 - Google-managed key** (No configuration required)
 - Customer-managed key** (Manage via Google Cloud Key Management Service)
 - Customer-supplied key** (Manage outside of Google Cloud)
- Source:** Cloud Storage file
- Cloud Storage file:** Your image source must use the .tar.gz extension and the file inside the archive must be named disk.raw. [Learn more](#). Path: bucket/folder/file. **Browse**
- Footer:** You will be billed for this image. [Compute Engine pricing](#)

Buttons: **Create** and **Cancel**

7. Select the bucket where you uploaded the Cisco provided tar.gz file.

The screenshot shows the 'Images' page in the Google Cloud Platform console. The left sidebar lists various Compute Engine resources, with 'Images' selected. The main content area displays the details for an image named 'suite-950':

- Labels:** None
- Creation time:** Dec 15, 2018, 4:27:39 AM
- Encryption type:** Google managed
- Equivalent REST:** [Equivalent REST](#)

Buttons: **EDIT**, **DELETE**, and **CREATE INSTANCE**

1. Navigate to the GCP > Compute Engine > VM Instances section and click **Create Instance**.
2. Select appropriate values for the new instance and click **Create**.



- Check the button to Allow HTTP or HTTPS access
- Change ports should list 443, 5671

Google Cloud Platform cliqimages

Create an instance

To create a VM instance, select one of the options:

- New VM instance**
Create a single VM instance from scratch
- New VM instance from template**
Create a single VM instance from an existing template
- Marketplace**
Deploy a ready-to-go solution onto a VM instance

Name
instance-1

Region us-west1 (Oregon) **Zone** us-west1-a

Machine type
Customize to select cores, memory and GPUs.
1 vCPU 3.75 GB memory [Customize](#)

Container
 Deploy a container image to this VM instance. [Learn more](#)

Boot disk
New 20 GB standard persistent disk
Image: suite-950 [Change](#)

Identity and API access
Service account
Compute Engine default service account

Access scopes
 Allow default access
 Allow full access to all Cloud APIs
 Set access for each API

Firewall
Add tags and firewall rules to allow specific network traffic from the Internet
 Allow HTTP traffic
 Allow HTTPS traffic
[Management, security, disks, networking, sole tenancy](#)

You will be billed for this instance. [Compute Engine pricing](#)

[Create](#) [Cancel](#)

3. Once the instance is created use the assigned public IP for this instance to access the suite installer UI.

You have now setup the installer for an GCP cloud.

OpenStack Appliance Setup

OpenStack Appliance Setup

To setup infrastructure for OpenStack clouds, follow this process.



The exact VM size really depends on the instance type configuration in your environment! However, a suggested size can be 4 CPU with 16 GB memory.

1. Download the CloudCenter Suite QCOW2 file to your local machine.
2. Login into your OpenStack datacenter to perform this task.
 - a. Click **Images**.
 - b. Click the **Create Image** button.
 - c. Enter a valid name.
 - d. Click the **File Browse** button.
 - e. Select the QCOW2 file stored in your local machine.

The screenshot shows a file selection dialog box with the search results for "suite-v0.0.978.qcow2" in the "Downloads" folder. Below the dialog, the "Format" dropdown is set to "QCOW2". The "Image Requirements" section includes "Kernel" (Choose an image), "Ramdisk" (Choose an image), "Architecture" (empty), "Minimum Disk (GB)" (0), and "Minimum RAM (MB)" (0). At the bottom, there are "< Back", "Next >", and "Create Image" buttons.

3. In the **Format** dropdown, select QCOW2.
4. To share this image with other users, select **Public** in the **Image Sharing Visibility** field.

- Click **Next** and then click the **Create Image** button.



The image import will take some time depending on the network speed. During this time, do not close the browser/application/tab.

- Create the instance for each component using the imported images:
 - Follow the standard OpenStack procedure to create the instance from an image.
 - Create the security group(s) with Port 80 and 443 (optionally 22 if you need SSH access) open for Ingress and Outbound communication.
 - You may need to assign floating IP to your VM after you create the VM is created.
- Select a new or existing key pair to log into each instance – if multiple key pairs are available, you must *select one* to be used for the CloudCenter instance.



If you do not select a key pair, you will not be able to log into the component VM!

You have now setup the installer for an OpenStack cloud.

VMware vSphere Appliance Setup

VMware vSphere Appliance Setup

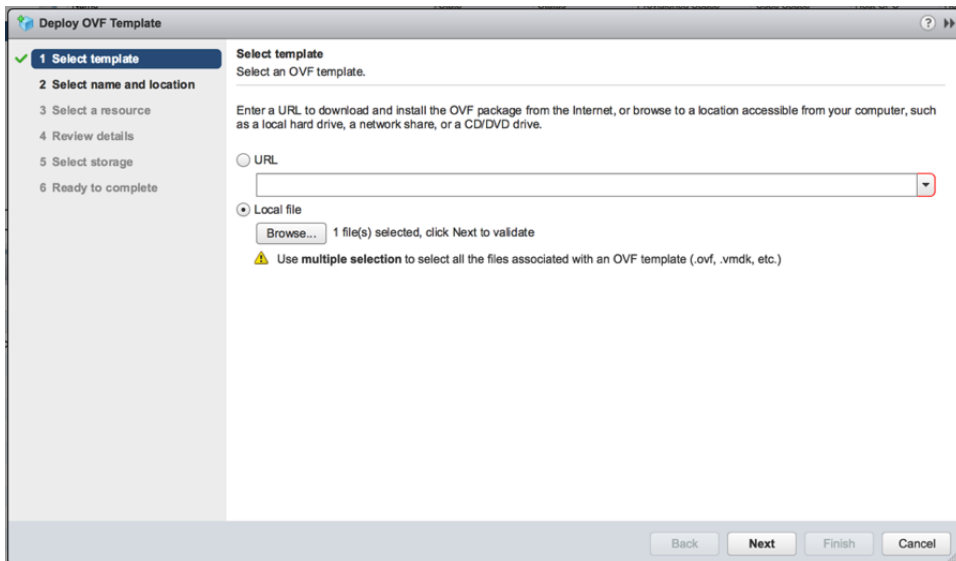
To setup infrastructure using CloudCenter appliances for VMware vSphere clouds, follow this process.

1. **Configure Network Time Protocol (NTP) on the VMware ESXi hosts – this is important as the CloudCenter Suite installation can fail, if NTP is not configured or if it is wrongly configured.**

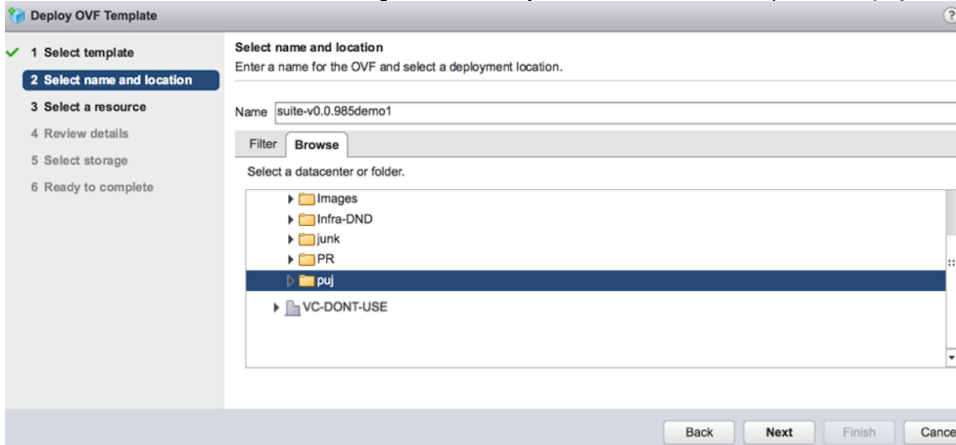
See https://kb.vmware.com/s/article/57147?lang=en_US for additional details.

2. Download the OVA image file from software.cisco.com to your local machine.
3. Log into the VMware Datacenter console and click on the **VMs and Templates** section.
4. Deploy an OVA template (right-click and select Deploy OVA Template option).

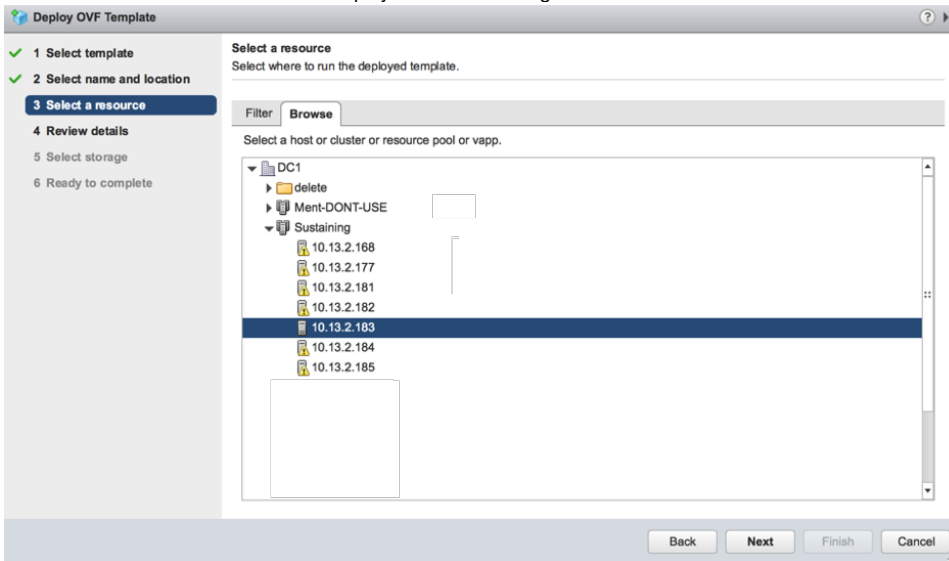
- a. Click the **Local file** option, click **Browse** to provide the location for the downloaded OVA file, ensure the file is selected, and then click **Next** as displayed in the following screenshot.



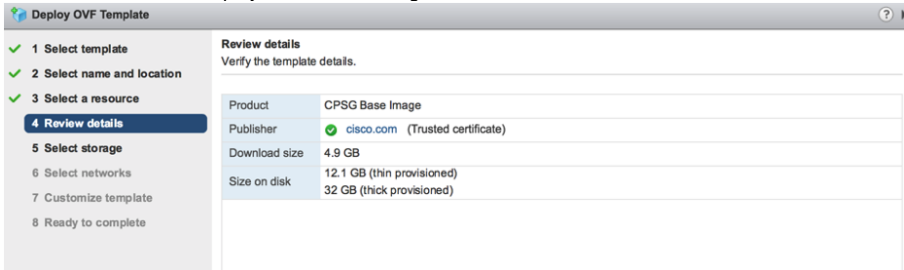
- b. Provide a suitable name and select the target folder where you need to create the Template as displayed in the following screenshot.



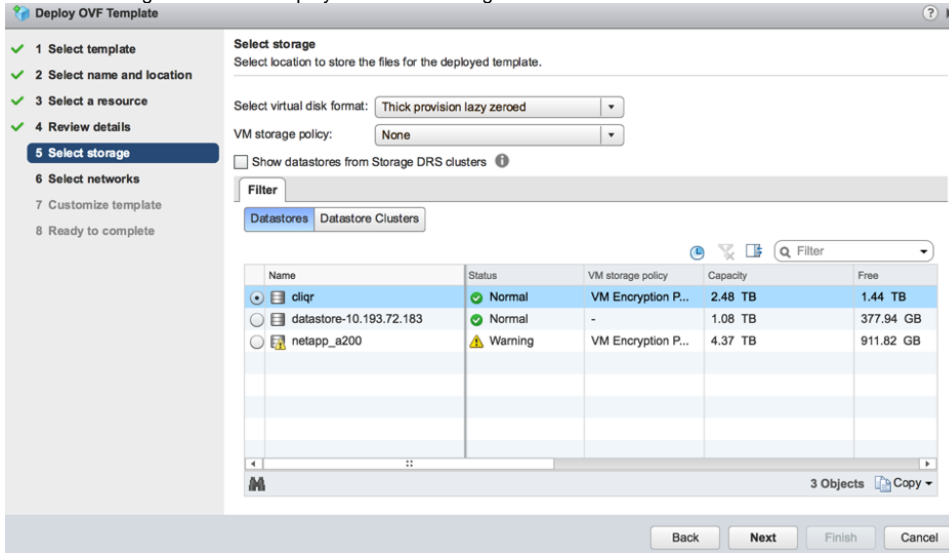
c. Select a suitable host and cluster as displayed in the following screenshot.



d. Review the details as displayed in the following screenshot.



e. Select the storage location as displayed in the following screenshot.



- f. Select a destination network as displayed in the following screenshot.

Deploy OVF Template

- ✓ 1 Select template
- ✓ 2 Select name and location
- ✓ 3 Select a resource
- ✓ 4 Review details
- ✓ 5 Select storage
- 6 Select networks**
- 7 Customize template
- 8 Ready to complete

Select networks
Select a destination network for each source network.

Source Network	Destination Network
mgmt	VM Network

IP Allocation Settings
IP protocol: IPv4 IP allocation: Static - Manual ⓘ

Back Next Finish Cancel

- g. Customize the template as required for your environment and review the completed information as displayed in the following screenshot.



Do not customize your setup credentials at this point or any other point during the installation. You can do so after you complete the installation process.

Deploy OVF Template

- ✓ 1 Select template
- ✓ 2 Select name and location
- ✓ 3 Select a resource
- ✓ 4 Review details
- ✓ 5 Select storage
- ✓ 6 Select networks
- ✓ 7 Customize template
- 8 Ready to complete**

Ready to complete
Review configuration data.

Name	suite-v0.0.985demo
Source VM name	suite-v0.0.985
Download size	4.9 GB
Size on disk	32 GB
Folder	puj
Resource	10.13.72.183
Storage mapping	1
Network mapping	1
IP allocation settings	IPv4, Static - Manual
Properties	A unique ID for this VM instance = default-instance-id Default user's password = Encoded user-data = Hostname = default-hostname SSH public keys = URL to seed instance data from =

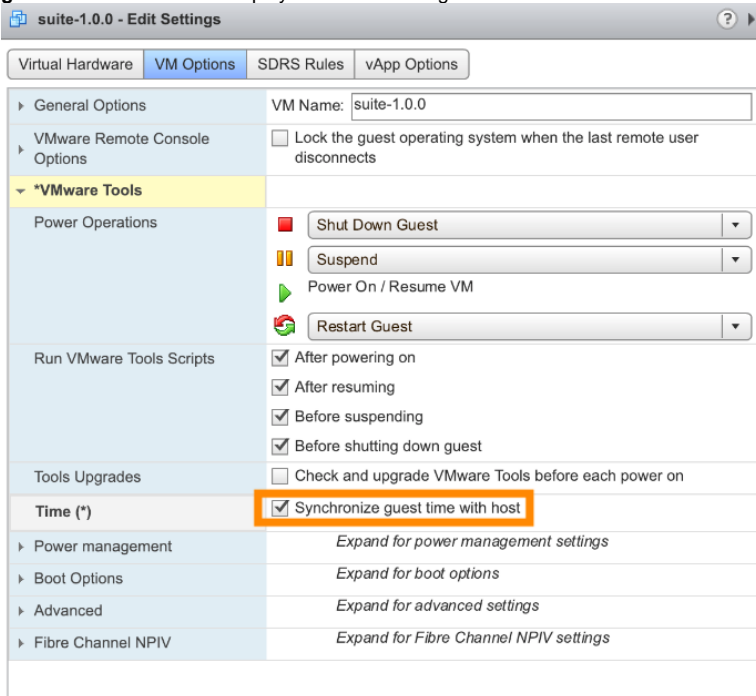
Back Next Finish Cancel

- h. Click **Finish** to start deploying the VM from the template inside the target folder.
5. Wait for some time so the VM is cloned and created, then refresh the VM page to view the powered off VM – The OVA is imported as a VM (powered off) on vSphere.

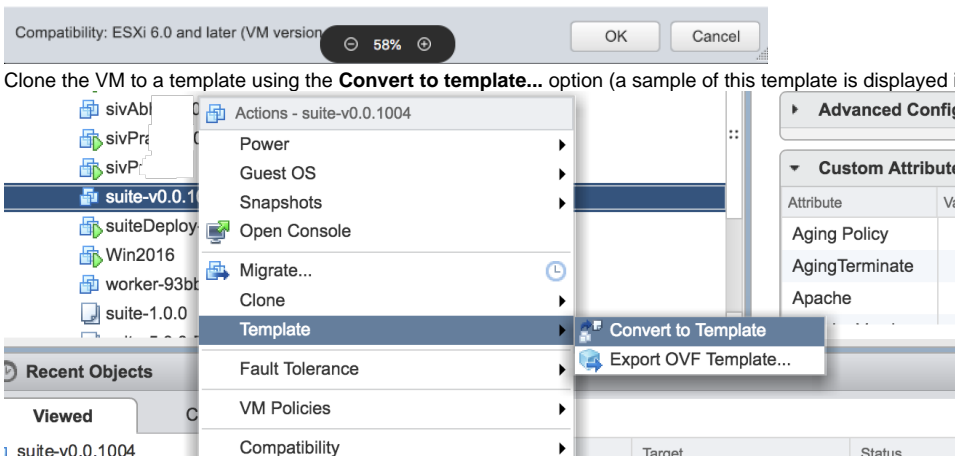


When you import the OVA as a VM, ensure that it is powered **off** on vSphere.

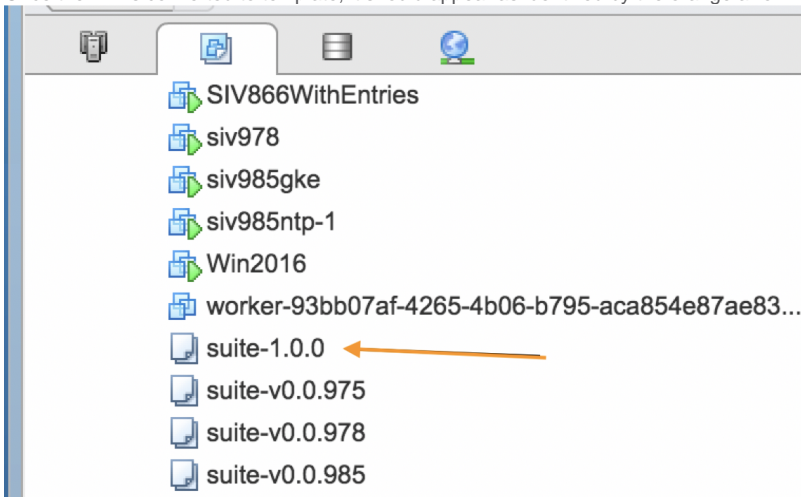
- Right-click to edit the VM Settings for the powered off VM. Click the *VM Options* tab. Under *VMware Tools*, select the checkbox to **Synchronize guest time with host** as displayed in the following screenshot.



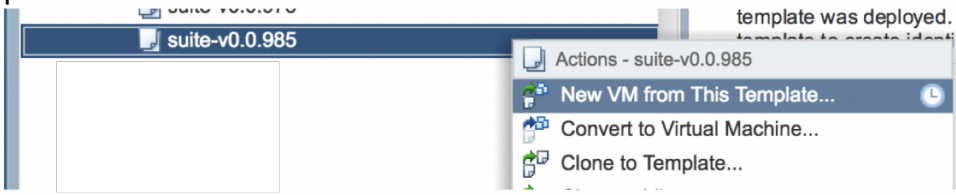
- Clone the VM to a template using the **Convert to template...** option (a sample of this template is displayed in the following screenshot).




- Once the VM is converted to template, it should appear as identified by the orange arrow in the following screenshot.

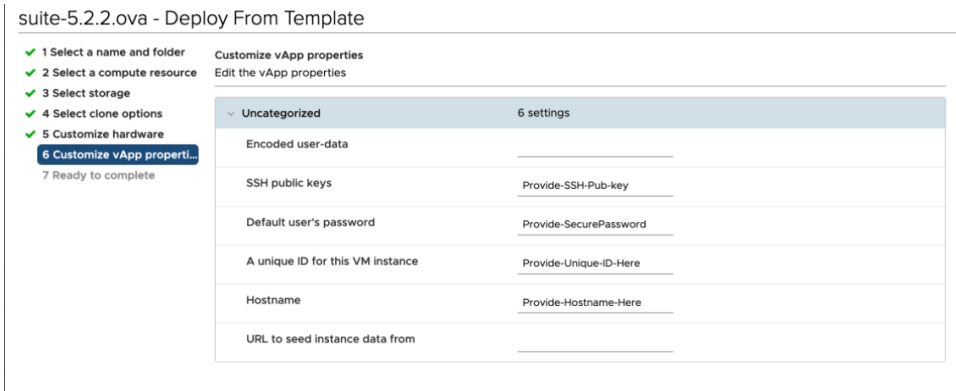


- Right click this template name and select the **New VM from This Template** option as displayed in the following image – This template will also be used as the value for the *vSphere Template Name* cloud setting, when you provide the details to install the Suite Admin.

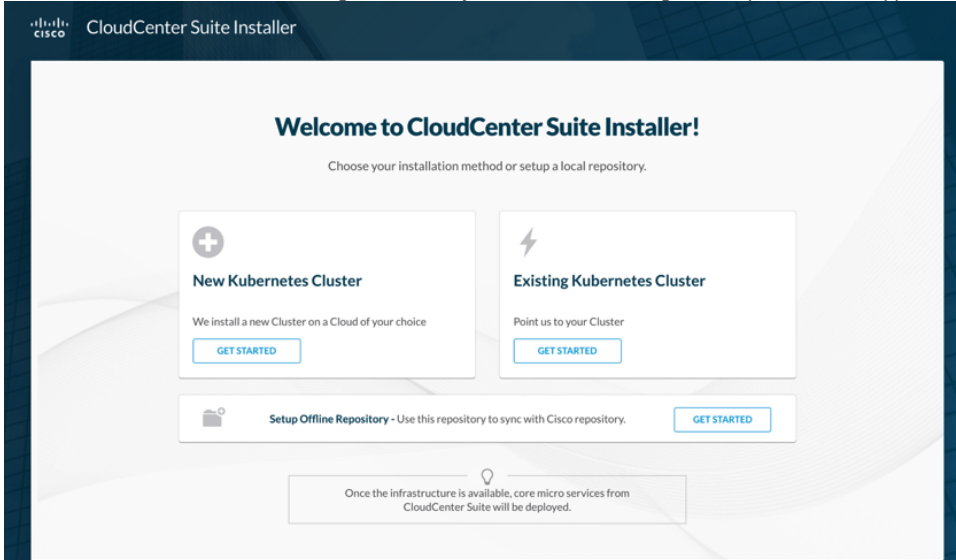


- Edit the **1e Customize vApp properties** to ensure that the VM has unique values for **A unique ID for this VM instance**, **Hostname**, **Default user's password**, and **SSH public keys** for this VM instance.

 For the password and/or the public key to take effect when deploying the VMware OVA for the. CloudCenter Suite installer, you **must** change the *default-instance-id* to something else than *default-instance-id* or *the hostname*!



- After the VM is created from the template, power it on.
- Use this IP address to access the UI, go to the newly created VM's IP using HTTPS protocol in a supported browser (see [Browser Compatibility](#)).



You have now setup the installer for a VMWare cloud.

Installation Approach

Installation Approach

- [Prepare Infrastructure](#)
- [New Cluster Installation](#)
- [Existing Cluster Installation](#)
- [Offline Repository](#)

Prepare Infrastructure

Prepare Infrastructure

- [General Compatibility](#)
- [Resource Requirements for CloudCenter Suite Modules](#)
- [Number of VMs](#)
- [IP Pool Requirements](#)
- [NTP Requirements](#)
- [The Suite Installer Dashboard](#)
- [Without Internet Access](#)

See [Browser Compatibility](#) for additional details.

The CloudCenter Suite requires Tiller v2.10.0 to be installed. Refer to the [Helm documentation](#) for additional details.



Installers are already incorporated in the CloudCenter Suite SaaS offer, see [SaaS Information](#) for additional details.

The following table lists the minimum resource requirements assuming that you install all available modules.

Module ^{1,2}	Public Cloud			Private Cloud ³		
	vCPU	Memory (GB)	Storage (GB)	vCPU	Memory (GB)	Storage (GB)
Suite Admin	15	35	300	15	35	300
Workload Manager ⁴ and Cost Optimizer	13	59	120	13	59	120
Action Orchestrator	5	6	60	5	6	60
Kubernetes Cluster (3 primary servers and 1 load balancer)	na	na	na	14	56	140
Total	33	100	480	47	156	620

¹ Update only one module at a time. If you simultaneously update more than one module, your update process may fail due to limited resource availability.

² Before updating any module, verify that you have un-allocated CPU/Memory in your cluster to ensure that your environment has free CPU/Memory – a module-update scenario requires additional resources for the old pod to continue running until the new pod initializes and takes over. This additional resource requirement is temporary and only required while a module update is in Progress. After the module is updated, the additional resources are no longer needed.

³ On private clouds (vSphere and OpenStack), each of the 3 primary server instances require 4 vCPU, 16 GB memory and 40 GB storage (root disk), the load balancer instance requires an additional 2 vCPU, 8 GB memory, and 20 GB storage, hence the difference in the additional requirement of 14 vCPU and 56 GB memory, and 140 GB storage (root disk). See the *Number of VMs* section below for additional details.

⁴ Workload Manager numbers include considerations for 4 Cloud Regions in the same instance. To support additional cloud regions, you must scale your cluster by adding Kubernetes worker nodes. You will need 1 CPU and 3 GB memory for each additional region.

A CloudCenter Suite installation launches a highly available Kubernetes cluster which consists of primary server(s), worker(s), and an API load balancer instances.



The number of worker nodes (for both private and public cloud) vary based on the instance type selected during the installation process.

For private clouds, a redundant cluster requires a minimum of 2 out of 3 primary server nodes to be running at any point, so the cluster can function as designed.



If you plan to scale up at a later date, be aware that the worker instance type selected at installation time will also be used for the scaled nodes.

The CloudCenter Suite requires that the underlying disks for Kubernetes disk attachments be redundant and available. Most public clouds already provide built-in redundancy for their block disks (AWS EBS, GCP Persistent Disks, and so forth). Be sure to verify that the Datastores/Datastore Clusters are also on redundant, non-local storage (NFS, NetApp) before you begin the installation process.

You must select IP address to ensure that each IP endpoints is available, accessible, and not used by any other resource.

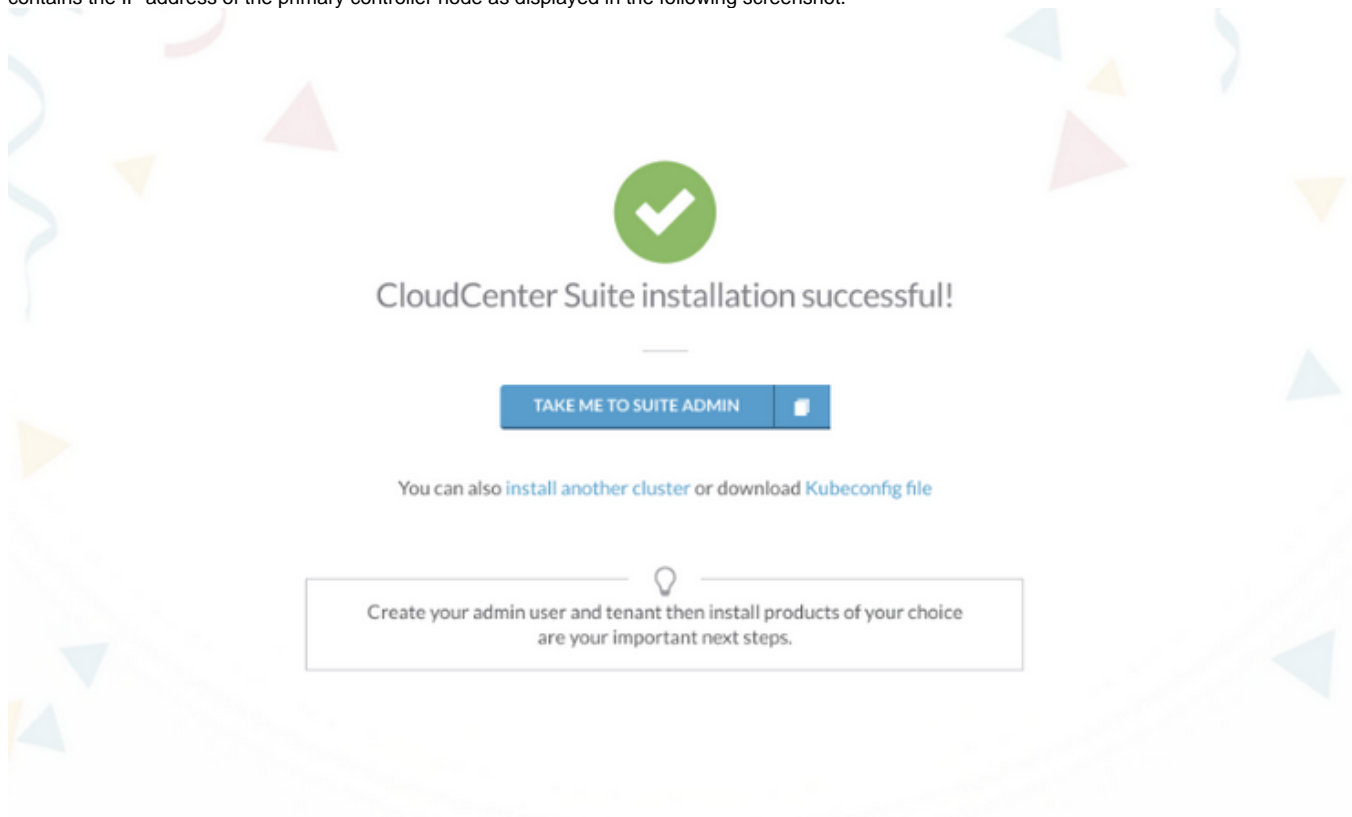
When configuring or modifying you pool of IP addresses, be aware of the following requirements:

- Verify if the IP pool can accommodate additional workloads.
- Select your instance type according to the following dependencies – based on your instance type selection, the installer displays the error or success information in the UI.
 - The CloudCenter Suite setup requires 3 primary servers and 1 load balancer.
 - The CloudCenter Suite dynamically calculates the number of application VMs (workers).
- Do not use 172.18.0.1/16 for the installer instance as this IP address is used by the Docker/Kubernetes setup.

You must either set the Network Time Protocol (NTP) time at the datacenter level or at the time of installation.

If set at installation time, then verify that the network can access the NTP server.

Effective CloudCenter Suite 5.0.1, the time for all worker and primary server nodes is synced with the *primary* controller node. The *primary* controller node is the instance used to launch the CloudCenter Suite – identified by the link that takes you to the Suite Admin UI (Take Me to Suite Admin). This link contains the IP address of the primary controller node as displayed in the following screenshot.



After launching the installer, navigate to the IP address of your VM in a supported browser. This presents the Suite Installer Dashboard. The Suite Installer Dashboard has the following options:

- [New Cluster Installation](#)
- [Existing Cluster Installation](#)

The Cisco Repository is used to host Cisco-related files and packages for various purposes. You may need to install the CloudCenter Suite in an environment that does not have internet access. If so, you need to set up the offline repository. See [Offline Repository](#) to sync your offline repository with the Cisco repository.

As you will be shutting down the installer VM after the installation, you can reuse that VM to set up the offline repository.

New Cluster Installation

Install the CloudCenter Suite on a New Kubernetes Cluster

Once you access the Suite Installer Dashboard (see [Prepare Infrastructure](#)), you can install a new cluster and launch nodes for the new Kubernetes cluster

- [Amazon EKS Installation](#)
- [Azure Installation](#)
- [Google GKE Installation](#)
- [OpenStack Installation](#)
- [VMware vSphere Installation](#)

Amazon EKS Installation

Amazon EKS Installation

- [Amazon Nuances](#)
- [Installation Process](#)

Amazon creates the following resources for the AWS account:

- An EKS Cluster with user-provided specifications
- Two Cloud formation stacks for VPC and Workers nodes (Prefixed with -VPC and -WORKERS)
- Two IAM Roles
- Volumes for storage class



You cannot trigger a Delete call by deleting the Amazon cluster from either the AWS console or the AWS CLI. Instead, use the Delete API.

- Additionally, refer to your module documentation for module-specific dependencies:

Module	Documentation
Workload Manager	Cloud Overview
Action Orchestrator	Add Cloud Account
Cost Optimizer	Cloud Overview

To install the CloudCenter Suite on a new Amazon cluster, perform the following procedure.

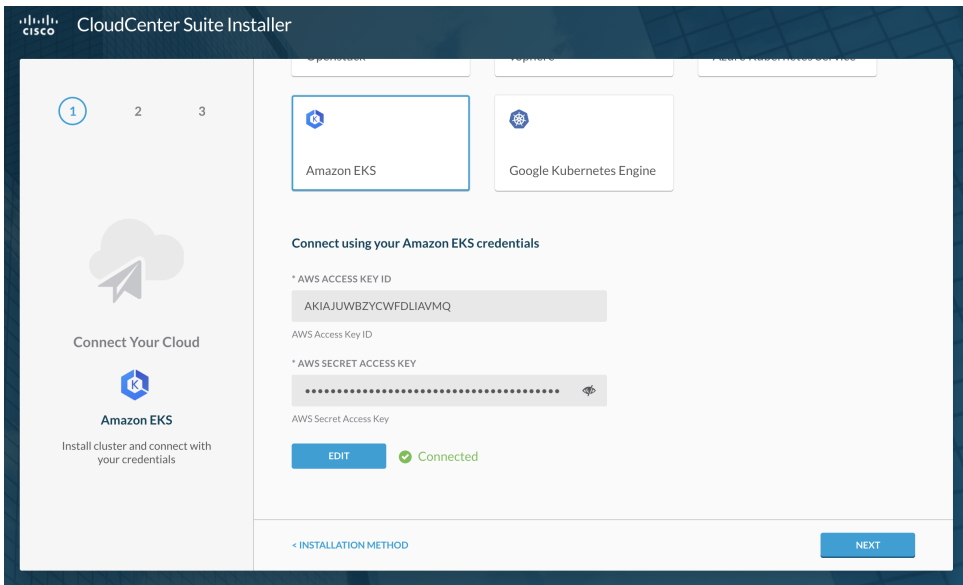
1. Verify that you have prepared your environment as listed in the *Amazon Nuances* section above.
2. Navigate to the Suite Installer Dashboard.
3. Click **New Kubernetes Cluster**.
4. Select **Amazon EKS**.
5. To connect using Amazon cloud credentials, enter the following details.

EKS Details	Description
AWS Access Key ID	AWS access key ID for the account
EKS Secret Access Key	AWS secret access key

6. Click **Connect**.

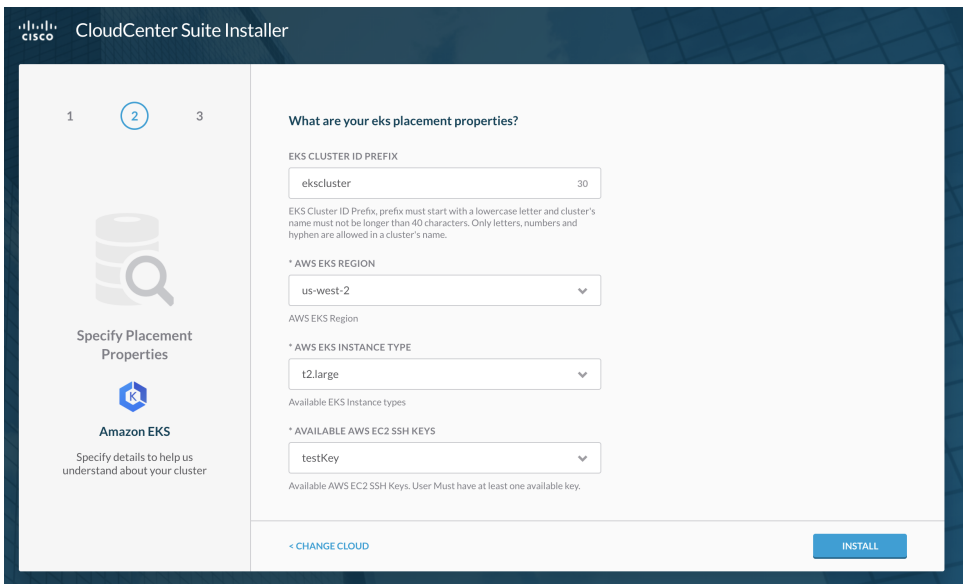
The screenshot shows the 'CloudCenter Suite Installer' interface. On the left, there are three numbered steps: 1 (selected), 2, and 3. Below the steps is a 'Connect Your Cloud' section with an 'Amazon EKS' icon and the text 'Install cluster and connect with your credentials'. On the right, there are three installation method options: 'Openstack', 'vSphere', and 'Azure Kubernetes Service'. Below these are two options for the Kubernetes engine: 'Amazon EKS' (selected) and 'Google Kubernetes Engine'. Underneath, there is a section titled 'Connect using your Amazon EKS credentials' with two input fields: '* AWS ACCESS KEY ID' (containing 'AKIAIJS4EFW3BNGDLYWA') and '* AWS SECRET ACCESS KEY' (containing 'hAPsIvI8vAwXfA6EUnXyzzgukUezdIX+QeJ7EK13'). A 'CONNECT' button is located below the input fields. At the bottom, there is a '< INSTALLATION METHOD' button on the left and a 'NEXT' button on the right.

7. Once the connection is validated, click **Next**.

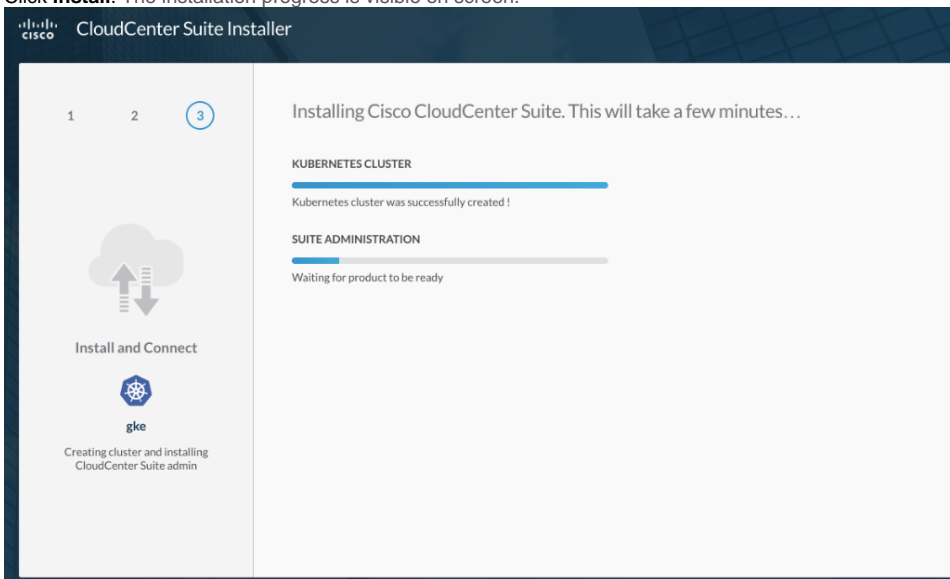


8. To specify the cloud properties, enter the following details.

EKS Details	Description
EKS Cluster ID Prefix	EKS Cluster ID Prefix, the prefix must start with a lowercase letter and cluster's name must not be longer than 40 characters. Only letters, numbers and hyphen are allowed in a cluster's name.
AWS EKS Region	Select region to launch the cluster.
EKS Instance Type	Select the type of instance of worker nodes.
Available EC2 SSH Keys	Select the SSH key, account must have at least one key.



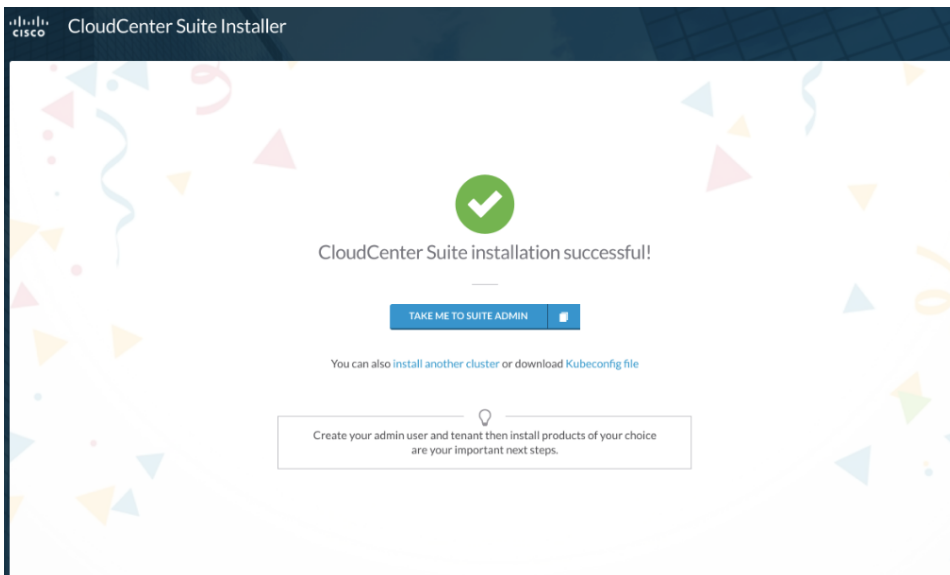
9. Click **Install**. The installation progress is visible on screen.



If the Suite Admin is installed in EKS, you cannot use the config file immediately after downloading it from the Suite installer success page. To access the Kubernetes cluster, access your command window to install AWS-IAM-AUTHENTICATOR and execute the following commands:

```
brew install kubernetes-cli
curl -Lo aws-iam-authenticator https://github.com/kubernetes-sigs/aws-iam-authenticator/releases/download/v0.3.0/heptio-authenticator-aws_0.3.0_darwin_amd64
chmod +x aws-iam-authenticator
sudo mv aws-iam-authenticator /usr/local/bin
```

10. Once successful, you see the following message.



11. You have the following options at this point:
- Click **Take Me To Suite Admin** to launch and set up the [Suite Admin](#).
 - Click **Install Another Cluster** to start another installation and go back to the homepage (Installer Dashboard).
 - Download **Kubeconfig file** to connect to the launched cluster using the [kubectl](#) tool.
12. Be sure to switch off the installer VM. You can reuse this VM for any other purpose, for example, as an Offline Repository.

Azure Installation

Azure AKS Installation

- [Azure Nuances](#)
- [Installation Process](#)

Verify the following Azure nuances:

- Your valid Azure account is valid and allows you to use sufficient resource quota. See <https://docs.microsoft.com/en-us/azure/aks/container-service-quotas> for additional details.
- Create the resource group in a cloud region that supports Azure.
- Additionally, refer to your module documentation for module-specific dependencies:

Module	Documentation
Workload Manager	Cloud Overview
Action Orchestrator	Add Cloud Account
Cost Optimizer	Cloud Overview

To install the CloudCenter Suite on a new Azure AKS cluster, perform the following procedure.

1. Verify that you have prepared your environment as listed in the *Azure Nuances* section above.
2. Navigate to the Suite Installer Dashboard.
3. Click **New Kubernetes Cluster**.
4. Select **Azure Kubernetes Service**.

The screenshot shows a multi-step installation wizard. Step 1 is active, showing a 'Connect Your Cloud' section with the 'Azure Kubernetes Service' option selected. The main area displays five cloud options: Openstack, vSphere, Amazon EKS, Google Kubernetes Engine, and Azure Kubernetes Service. The 'Azure Kubernetes Service' option is highlighted with a blue border. Below the options, there is a section for 'Connect using your Azure Kubernetes Service credentials' with input fields for 'AKS TENANT ID' and 'AKS CLIENT ID'. A 'NEXT' button is visible at the bottom right.

5. To connect using Azure Kubernetes Service cloud credentials, enter the following details, and click **Connect**.

AKS TENANT ID	The AKS account tenant ID.
AKS CLIENT ID	The AKS account client ID.
AKS CLIENT SECRET	The AKS account client secret.
AKS SUBSCRIPTION ID	The AKS subscription ID.



Refer to <https://docs.microsoft.com/en-us/azure/aks/kubernetes-service-principal> to learn about how to setup service principles with Azure Kubernetes Service (AKS), and use the credentials to populate the above fields.

6. Once the connection is validated, click **Next**.

7. To specify the placement properties, enter the following details.

AKS Placement Property	Description
Resource Group	The AKS resource group to launch the cluster
VM Size	The VM size of the cluster node
AKS Cluster ID Prefix	<ul style="list-style-type: none"> The prefix must begin with a lowercase letter. The entire name that you enter for this cluster must not be longer than 12 characters. Only letters, numbers and hyphens are allowed in this field.

1 2 3

Specify Placement Properties

Azure Kubernetes Service

Specify details to help us understand about your cluster

What are your aks placement properties?

* RESOURCE GROUP
Installer-West-3

List of supported resource groups in AKS

* VM SIZE
Standard_DS4_v2

List of supported VM sizes in AKS

AKS CLUSTER ID PREFIX
mycluster01

AKS cluster ID prefix. prefix must start with a lowercase letter and cluster's name must not be longer than 12 characters. Only letters, numbers are allowed in a cluster's name.

< CHANGE CLOUD

INSTALL

8. Click **Install**. The installation progress is visible on screen.

CloudCenter Suite Installer

1 2 3

Installing Cisco CloudCenter Suite. This will take a few minutes...

KUBERNETES CLUSTER

Kubernetes cluster was successfully created!

SUITE ADMINISTRATION

Waiting for product to be ready

Install and Connect

gke

Creating cluster and installing CloudCenter Suite admin

9. Once successful, you see the following message.

CloudCenter Suite Installer

CloudCenter Suite installation successful!

TAKE ME TO SUITE ADMIN

You can also install another cluster or download Kubeconfig file

Create your admin user and tenant then install products of your choice are your important next steps.

10. You have the following options at this point:

- a. Click **Take Me To Suite Admin** to launch and set up the [Suite Admin](#).

- b. Click **Install Another Cluster** to start another installation and go back to the homepage (Installer Dashboard).
 - c. Download **Kubeconfig file** to connect to the launched cluster using the [kubectl](#) tool.
11. Be sure to switch off the installer VM. You can reuse this VM for any other purpose, for example, as an Offline Repository.

Google GKE Installation

Google GKE Installation

- [Google Nuances](#)
- [Installation Process](#)

Verify that the following minimum permissions (roles) are set up:

- Service Account User
- Kubernetes Engine Admin
- Compute Engine Admin

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMS, App Engine apps, or systems running outside Google.

Service account name


ad

Display name for this service account

Service account ID

ad-581

@wakanda-214819.iam.gserviceaccount.com  

Project role 

Role

Service Account User ▼ 


Create VMs and other GCP tasks with a service account. Users cannot impersonate the account directly as they can with Service Account Actor role.

Role

Kubernetes Engine Admin ▼ 

Full management of Kubernetes Clusters and their Kubernetes API objects.

Role

Compute Admin ▼ 

Full control of all Compute Engine resources.

[+ ADD ANOTHER ROLE](#)

Furnish a new private key

Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.

Enable G Suite Domain-wide Delegation

Allows this service account to be authorized to access all users' data on a G Suite domain without manual authorization on their parts. [Learn more](#)

- Additionally, refer to your module documentation for module-specific dependencies:

Module	Documentation
Workload Manager	Cloud Overview
Action Orchestrator	Add Cloud Account

Cost Optimizer

Cloud Overview

To install the CloudCenter Suite on a new GKE Kubernetes cluster, perform the following procedure.

1. Verify that you have prepared your environment as listed in the *Google Nuances* section above.
2. Navigate to the Suite Installer Dashboard.
3. Click **New Kubernetes Cluster**.
4. Select the cloud of your choice (GKE in this case).
5. Generate a service account JSON file with the following minimum required permissions in the GKE console – be sure to check the "Furnish a new private key" checkbox for the JSON file to generate the key.



If you check the **Furnish a new private key** checkbox the resulting JSON file from the service account automatically contains a key when you download the file.

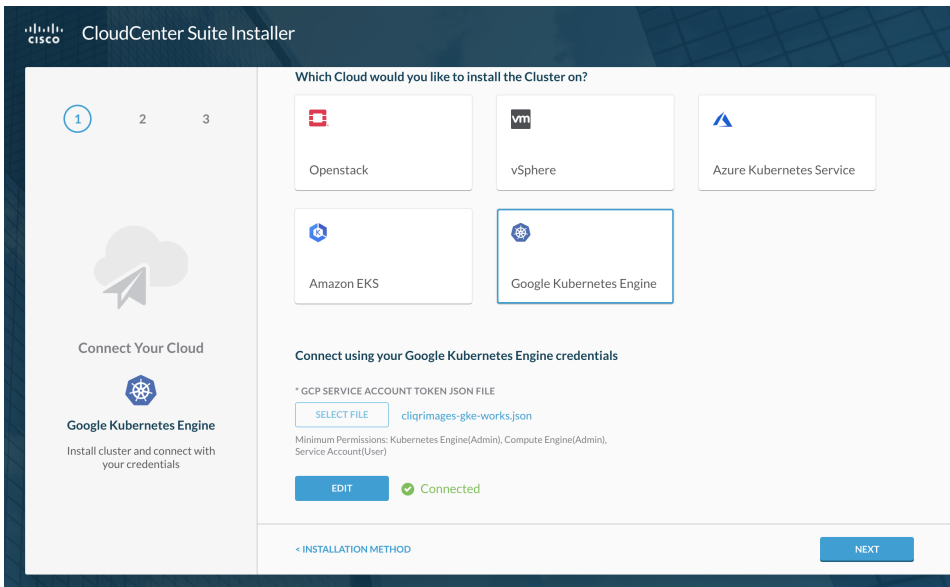
- a. Kubernetes Engine (Admin)
- b. Compute Engine (Admin)
- c. Service Account (User)

The screenshot shows the Google Cloud Platform IAM & admin console for project 'wakanda'. On the left, a list of service accounts is displayed with columns for Name, Email, and Key ID. On the right, the 'Create service account' dialog is open. The 'Service account name' is 'test'. The 'Project role' is set to 'Compute Admin'. The 'Role' is 'Service Account User'. The 'Key type' is 'JSON' (Recommended). The 'Furnish a new private key' checkbox is checked. The 'Enable G Suite Domain-wide Delegation' checkbox is unchecked. The 'CANCEL' button is visible at the bottom of the dialog.

6. To connect using Google cloud credentials, download the Google **service account token in JSON** format that you created in the previous step.
7. Upload the JSON file mentioned in the previous step and click **Connect** to validate the credentials.

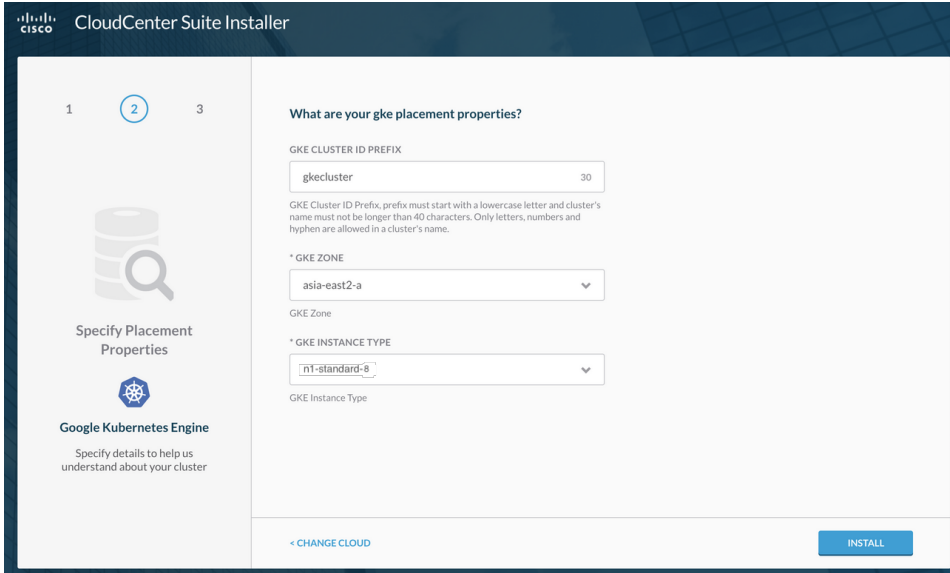
The screenshot shows the CloudCenter Suite Installer dashboard. The 'Which Cloud would you like to install the Cluster on?' screen is displayed. The 'Google Kubernetes Engine' option is selected and highlighted with a blue border. Below the selection, the 'Connect using your Google Kubernetes Engine credentials' section is visible, including a 'SELECT FILE' button and a 'CONNECT' button. The 'NEXT' button is also visible at the bottom right of the screen.

8. Once the connection is validated, click **Next**.

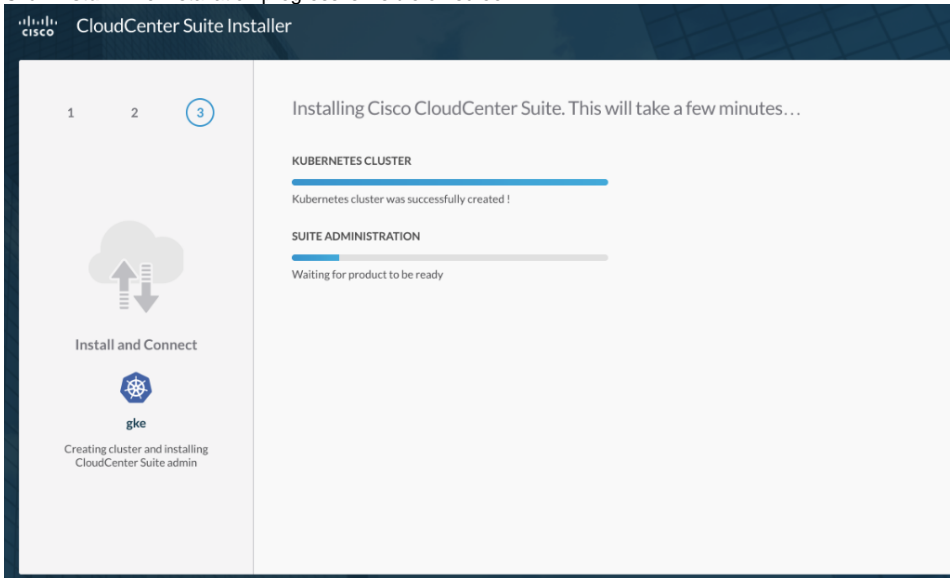


9. Enter the following details to specify the cloud properties.

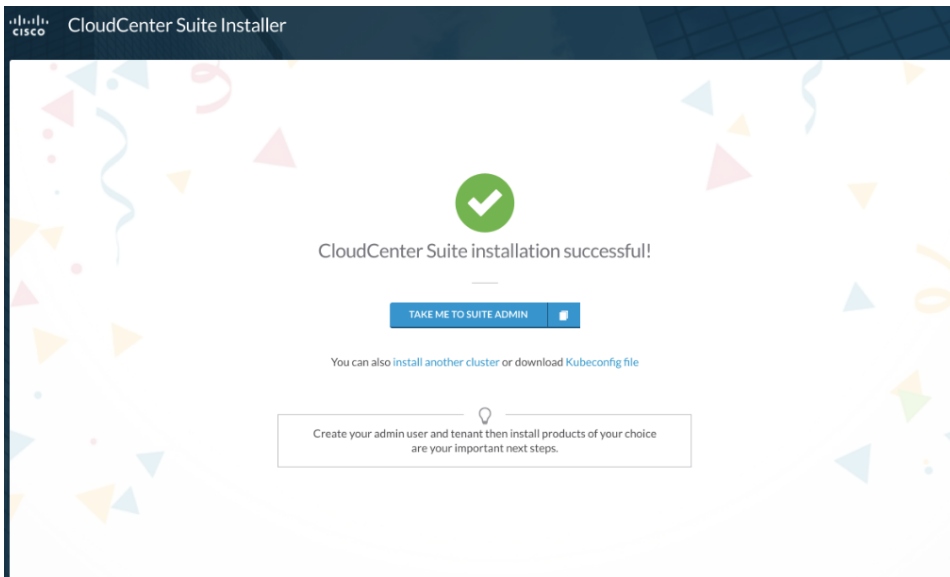
GKE Details	Description
GKE Cluster ID Prefix	<ul style="list-style-type: none"> The prefix must begin with a lowercase letter. The entire name for this cluster must not be longer than 40 characters. Only letters, numbers and hyphens are allowed in this field.
GKE Zone	The Google cloud zone to launch the cluster.
GKE Instance Type	Select the minimum resource requirements based on your environment setup.



10. Click **Install**. The installation progress is visible on screen.



11. Once successful, you see the following message.



12. You have the following options at this point:
- Click **Take Me To Suite Admin** to launch and set up the [Suite Admin](#).
 - Click **Install Another Cluster** to start another installation and go back to the homepage (Installer Dashboard).
 - Download **Kubeconfig file** to connect to the launched cluster using the [kubectl](#) tool.
13. Be sure to switch off the installer VM. You can reuse this VM for any other purpose, for example, as an Offline Repository.

OpenStack Installation

OpenStack Installation

- [OpenStack Nuances](#)
- [Installation Process](#)

Verify the following OpenStack nuances:

- OpenStack newton release with at least the following service versions:
 - Cinder V2
 - Keystone V3
 - OpenStack Nova V2
 - OpenStack Networking V2
 - OpenStack Glance V2
- The tenant and project requirements for OpenStack Cloud are as follows:
 - One Subnet with DNS servers set on the subnet
 - Minimum Quota
 - 11 Volumes
 - 7 VMs
 - 200 GB Volume Quota
 - Flavor with at least two vCPUs and 8 GB RAM
- **Network Time Protocol (NTP) must be configured – this is important as the CloudCenter Suite installation can fail, if NTP is not configured or if it is wrongly configured.**



If you setup CloudCenter Suite in offline mode, you must provide valid NTP server details before you save your configuration.

- Additionally, refer to your module documentation for module-specific dependencies:

Module	Documentation
Workload Manager	Cloud Overview
Action Orchestrator	Add Cloud Account
Cost Optimizer	Cloud Overview

To install the CloudCenter Suite on a new OpenStack cluster, perform the following procedure.

1. Verify that you have prepared your environment as listed in the *OpenStack Nuances* section above.
2. Navigate to the Suite Installer Dashboard.
3. Click **New Kubernetes Cluster**.
4. Select the cloud of your choice.
5. To connect using OpenStack cloud credentials, enter the following details.

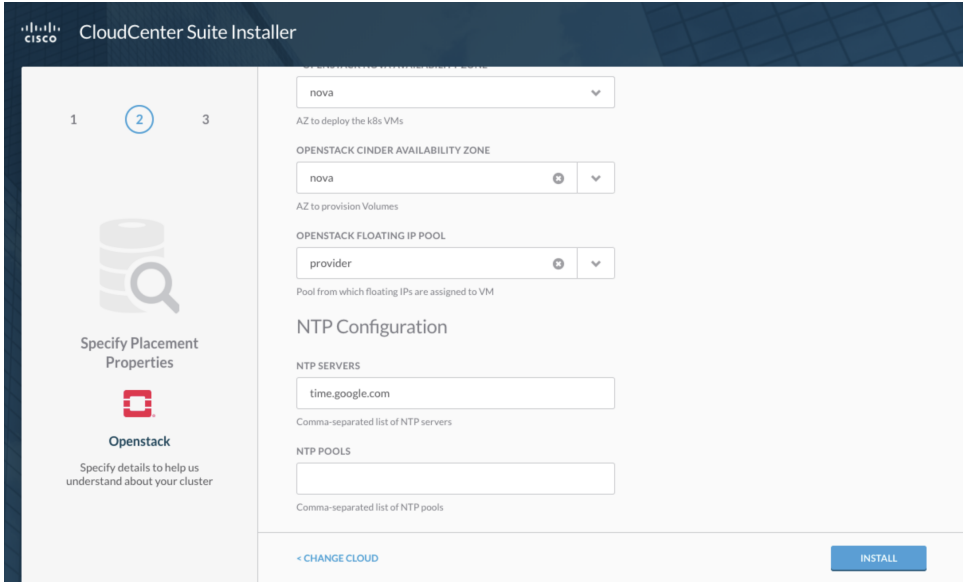
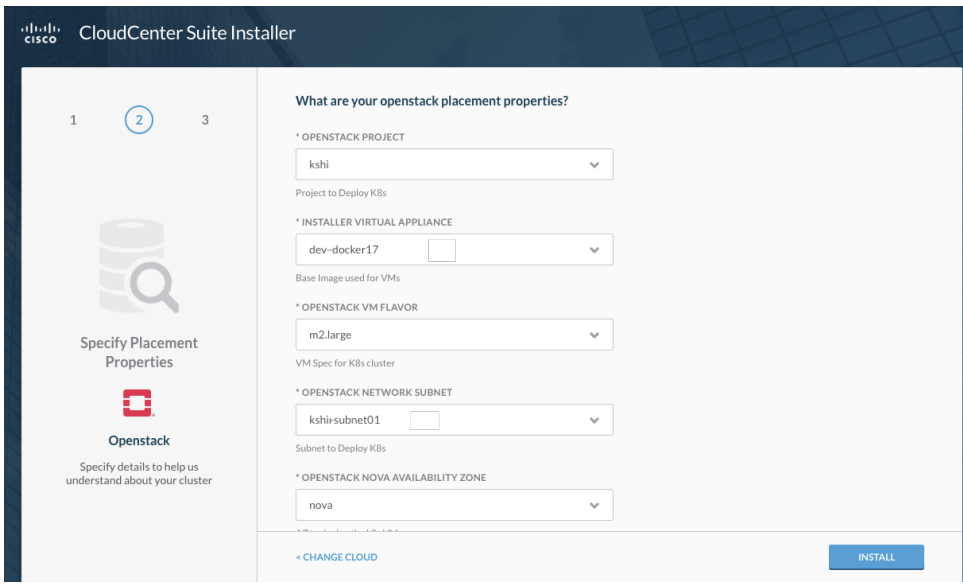
OpenStack Details	Description
Identity Username	The OpenStack account username.
Identity Password	The OpenStack account password.
OpenStack Domain Name	The OpenStack account domain name.
OpenStack Identity URL	The OpenStack authentication service URL.

6. Click **Connect**.
7. Once the connection is validated, click **Next**.
8. To specify the placement properties, enter the following details.

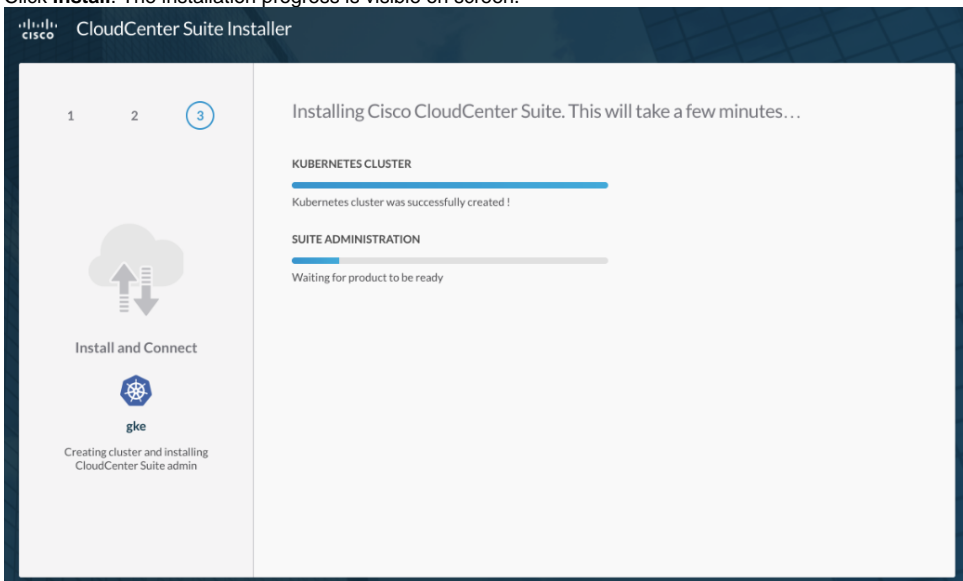


If you setup CloudCenter Suite in offline mode, you must provide valid NTP server details before you save your configuration.

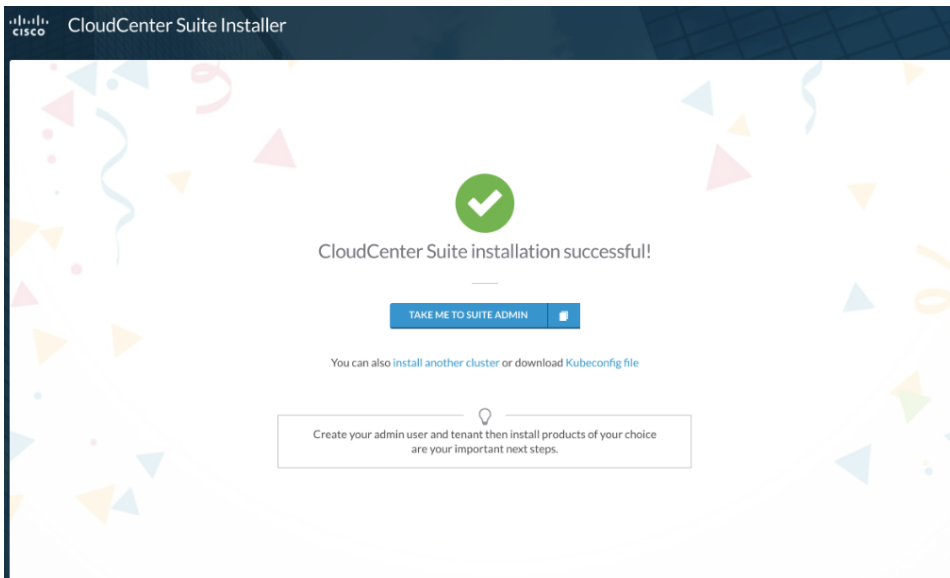
OpenStack Details	Description
OpenStack Project	The OpenStack project to which the Kubernetes cluster is deployed.
Installer Virtual Appliance	The base image for the OpenStack installer – this must be the same image as the CloudCenter Suite virtual appliance.
OpenStack VM Flavor	The VM specification for the Kubernetes cluster.
OpenStack Network Subnet	The network where the VMs will be deployed.
OpenStack Nova Availability Zone	The compute availability zone.
OpenStack Cinder Availability Zone	The OpenStack volume availability zone. This field is required if the Nova availability zone is different from the Cinder Availability Zone.
OpenStack Floating IP Pool	Floating IP pool from which IP addresses are assigned to VMs.
NTP Servers	The list of IP addresses or FQDNs of your NTP server(s) – to be used to sync VM clocks.



9. Click **Install**. The installation progress is visible on screen.



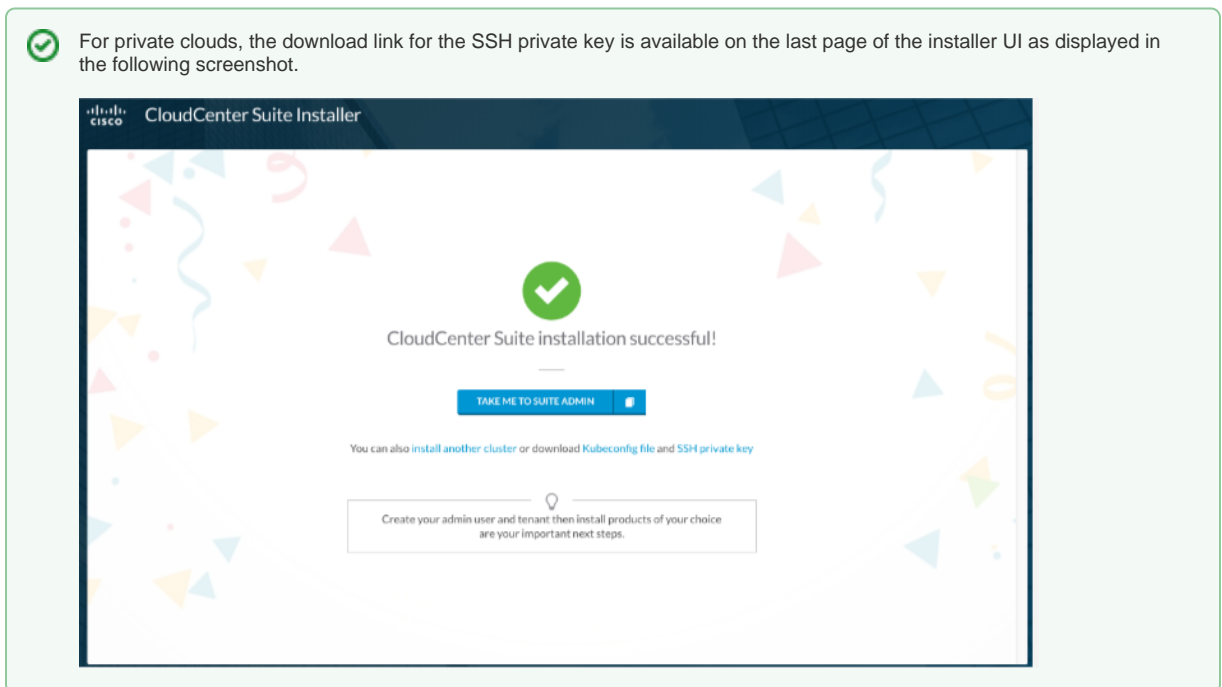
10. Once successful, you see the following message.



11. You have the following options at this point:

- Click **Take Me To Suite Admin** to launch and set up the [Suite Admin](#).
- Click **Install Another Cluster** to start another installation and go back to the homepage (Installer Dashboard).
- Download **Kubeconfig file** to connect to the launched cluster using the [kubectl](#) tool.
- Download **SSH private key** to SSH into your cluster node on private clouds – each time you launch a new cluster using the installer, the CloudCenter Suite generates a new key-pair for that cluster.

✔ For private clouds, the download link for the SSH private key is available on the last page of the installer UI as displayed in the following screenshot.



12. Be sure to switch off the installer VM. You can reuse this VM for any other purpose, for example, as an Offline Repository.

VMware vSphere Installation

VMware vSphere Installation

- [VMware Nuances](#)
- [Installation Process](#)

Verify the following VMware nuances:

- Ensure to use Version 6.0 and higher.
- Verify that you have sufficient shared storage between hosts.
- You must have privileges to launch a VM and access the selected DC/Datastore.
- Your datacenter must exist at the root level.



Be aware that CloudCenter Suite does not support folders at the root level.

- **Network Time Protocol (NTP) must be configured – this is important as the CloudCenter Suite installation can fail, if NTP is not configured or if it is wrongly configured.**



If you setup CloudCenter Suite in offline mode, you must provide valid NTP server details before you save your configuration.

- In CloudCenter Suite 5.1 and earlier, if your environment has strict URL rules that redirects (for example, using a shorter URL that redirects to <https://storage.googleapis.com>) the configured URL, you may not be able to complete the installation as these kind of redirects may not be allowed if you have installed the repository in an offline cluster. As the offline solution is not completely air gapped in CloudCenter Suite 5.0 and 5.1, you must add these URLs to your allowed lists behind the firewall so you can access these sites.

- ✔ The installation process assumes internet connectivity to certain domains. When installing CloudCenter Suite into environments residing behind a proxy, please ensure the following domains are entirely accessible. Remember the proxy information - this will be used during the installation of CloudCenter Suite.

Note: The Installer VM supports HTTP and HTTPS proxies, with or without username and password. The proxy must support TLS 1.2.

Warning: Several of the following links might perform redirects. Please ensure your proxy and firewall are configured to allow redirects of the following URLs.

Proxy URL	Description
https://devhub.cisco.com http://devhub.cisco.com https://devhub-docker.cisco.com http://devhub-docker.cisco.com	Repository for Cisco CloudCenter Suite Docker Charts
https://gcr.io http://gcr.io	Repository for Cisco CloudCenter Suite Helm Charts
https://storage.googleapis.com http://storage.googleapis.com	Repository for Cisco CloudCenter Suite Tiller Image
Other	The Suite Installer may require additional connections to the installation environment (for example, vCenter, Hyperflex Data Platform, AWS Console, and so forth) Please ensure your cloud target is reachable via the proxy!

- For CloudCenter Suite to use a particular user account in VMware, that account must have the permissions identified in the table below.

vCenter Object	Required Permission	Reason
Network	Assign Network	If the default network in a template/snapshot must be changed
Datastore	Allocate space	For persistent disk operation
	Browse datastore	
	Low level file operations	
	Remove file	
Folder	Create folder	For user folder creation
Resource	Apply recommendation	For datastore cluster support
	Assign VM to resource pool	For resource pool selection
Tasks	Create task	For VM operation
	Update task	
Virtual Machine	All permissions	
Global Role	Set Custom Attributes	To add custom attributes on virtual machines
	Manage Custom Attributes	

- Additionally, refer to your module documentation for module-specific dependencies:

Module	Documentation
Workload Manager	Cloud Overview
Action Orchestrator	Add Cloud Account
Cost Optimizer	Cloud Overview

To install the CloudCenter Suite on a new vSphere cluster, perform the following procedure.

1. Verify that you have prepared your environment as listed in the *VMware Nuances* section above.
2. Navigate to the Suite Installer Dashboard.
3. Click **Get Started** in the New Kubernetes Cluster tile to create a new Kubernetes cluster and install the Suite Admin on it.
4. Click vSphere and enter your vSphere credentials and click **Connect**.

vCenter Details	Description
vCenter Host	The IP address or hostname of the vSphere setup
vCenter Username	The username to be used for the vSphere setup
vCenter Password	The password to be used for the vSphere setup

The screenshot displays a web-based configuration interface for connecting to a vSphere environment. On the left, there is a sidebar with a 'Connect Your Cloud' section featuring the VMware logo and the text 'Install cluster and connect with your credentials'. The main content area is titled 'Connect using your vSphere credentials' and includes three input fields: 'vCenter Host' with the value '10.13.2.11', 'vCenter Username' with the value 'admin@vsphere.local', and 'vCenter Password' which is masked with dots. Below these fields, there is an 'EDIT' button and a green checkmark followed by the text 'Connected'. At the bottom of the form, there are two buttons: '< INSTALLATION METHOD' and 'NEXT'.

5. Once the connection is validated, click **Next**.
6. To specify the placement properties, enter the following details.

vCenter Details	Description
Cluster	The cluster to deploy the node in the above datacenter.
Resource Pool	The resource pool used to deploy the node.
Datastore	The datastore cluster to associate with the node.
Network	The network cluster to associate with the node.
Folder	The folder from which the cluster node is selected.
Node Prefix	Any user-defined prefix.
Virtual Appliance Template Folder	The folder containing the template to launch the Kubernetes cluster nodes.

Virtual Appliance Template Name	The name of the installer VM Template that you created earlier and from where you launched the Suite Installer – use this same template to create worker VMs. See VMware vSphere Appliance Setup for dependent details on creating the Suite Installer Virtual Appliance.
IP Allocation Mode	This switch allows you to select the mode: <ul style="list-style-type: none"> • DHCP: This strategy allows the IP to be allocated by the DHCP server to the instance on server boot up. This IP address is not known prior to server boot up. • Static IP: This strategy allows the customer to provide the IP address. As this IP address may or may not be available to the server (based on the availability), you must perform adequate checks to ensure IP availability before using this strategy.
Instance Type	Select the minimum Hardware Requirements based on your setup requirements. Based on your selection, the system automatically calculates the required instance type.

7. Specify the NTP Configuration details:

If you setup CloudCenter Suite in offline mode, you must provide valid NTP server details before you save your configuration.

NTP details	Description
NTP Servers	The list of IP addresses or FQDNs of your NTP server(s) – to be used to sync VM clocks.

NTP Pools

The list of IP addresses or FQDNs of your NTP pools.

CloudCenter Suite Installer

1 2 3

Specify Placement Properties

vm
vSphere
Specify details to help us understand about your cluster

* VIRTUAL APPLIANCE TEMPLATE NAME
suite-5.0.0-RC2.5
Name of the virtual appliance template - alphanumeric characters, '-', or '.'

NODE PREFIX
12
Optional prefix for node names - lower case alphanumeric characters, '-' or '.' start with an alphabetic character, and end with an alphanumeric character

* IP ALLOCATION MODE
 DHCP Static IP
vSphere IP allocation - DHCP or static IP

* WORKER INSTANCE TYPE
8CPU_32GBMem
4 workers will be launched

NTP Configuration
NTP SERVERS
Comma-separated list of NTP servers/pools - hostname or IP Address

< CHANGE CLOUD INSTALL

8. Conditional if using Static IP.

a. The *Start IP* and *End IP* for the Static IP Pool range should be large enough to cover the following VMs:

- i. 3 primary servers
- ii. 1 Load Balancer
- iii. *Number of Worker VMs* used in your environment

The *Number of Worker VMs* depends on the selected instance type. For example:

- If the instance type is large (8 CPU, 32GB memory), then 4 workers are created and the total static IPs required for this environment are 8 IPs (4 worker VMs, 3 primary servers, and 1 load balancer).
- If the instance type is large (8 CPU, 24GB memory), then 5 workers are created and the total static IPs required for this environment are 9 IPs (5 worker VMs, 3 primary servers, and 1 load balancer).
- If the instance type is large (8 CPU, 16GB memory), then 7 workers are created and the total static IPs required for this environment are 10 IPs (6 worker VMs, 3 primary servers, and 1 load balancer).
- If the instance type is smaller (4 CPU, 16GB memory), then 8 workers are created, so the static IPs required for this environment are 12 IPs (8 worker VMs, 3 primary servers, and 1 load balancer).

Accordingly, select the IP range by taking into consideration the *Number of Worker VMs* that will be created based on instance type.

This is just an example, be aware that different datacenters will have different instance types configurations and dependencies.

To determine the number of workers select the instance type in the CloudCenter Suite installer, the *Number of Worker VMs* are calculated and displayed at the bottom of the instance field as displayed in the following screenshot.

1 2 3

Specify Placement Properties

vm
vSphere
Specify details to help us understand about your cluster

* VIRTUAL APPLIANCE TEMPLATE NAME
suite-5.0.0-RC2.5
Name of the virtual appliance template - alphanumeric characters, '-', or '.'

NODE PREFIX
12
Optional prefix for node names - lower case alphanumeric characters, '-' or '.' start with an alphabetic character, and end with an alphanumeric character

* IP ALLOCATION MODE
 DHCP Static IP
vSphere IP allocation - DHCP or static IP

* STATIC IP POOL END IP
10.1.1.24
End IP of the static IP range

* SUBNET MASK
255.255.248.0
Netmask corresponding to the IP range specified

* DNS SERVER LIST
:
Comma-separated list of DNS server IPs to be used

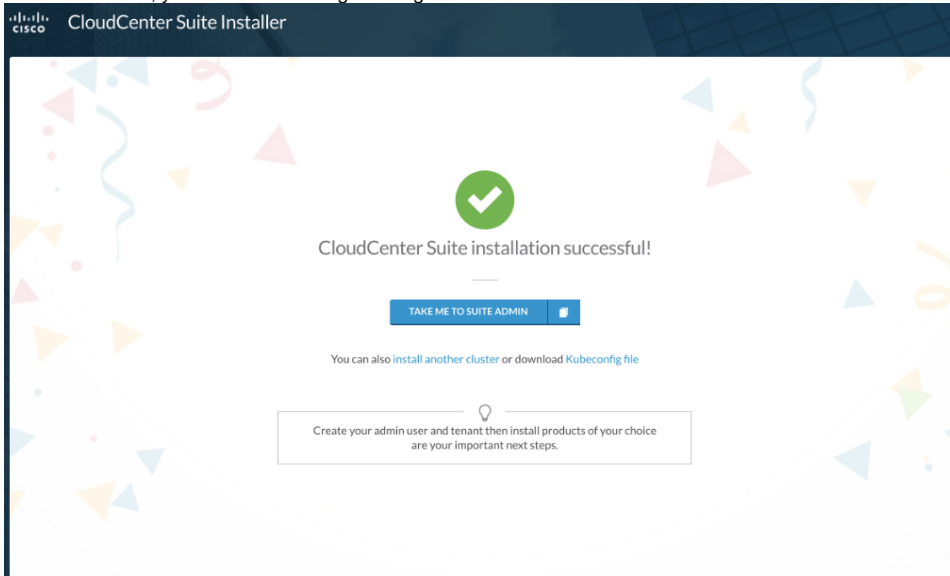
* GATEWAY LIST
10.1.1.1
Comma-separated list of gateway IPs to be used

* WORKER INSTANCE TYPE
4CPU_16GBMem
8 workers will be launched

- b. If you need to scale up nodes after setting up the Suite Admin, then you must ensure a wider range:
 - i. If you plan to scale up by one node and you have already selected the instance type such that 8 worker VMs are created, then the valid static IP range must be 10.0.0.12 to 10.0.0.24 (or higher, depending on the scale up number).
 - ii. In this example:
 - 1. The worker VMs will consume 8 IPs, the primary server VMs will consume 3 IPs, and the load balancer will consume 1 IP.
 - 2. Additionally, you need to scale up by one node which will consume 1 more IP, making taking the total to 13 IPs.
 - 3. These IPs should be available for allocation – they should not have been allocated to any other VM or resource.

9. Click **Install**. The installation progress is visible on screen.

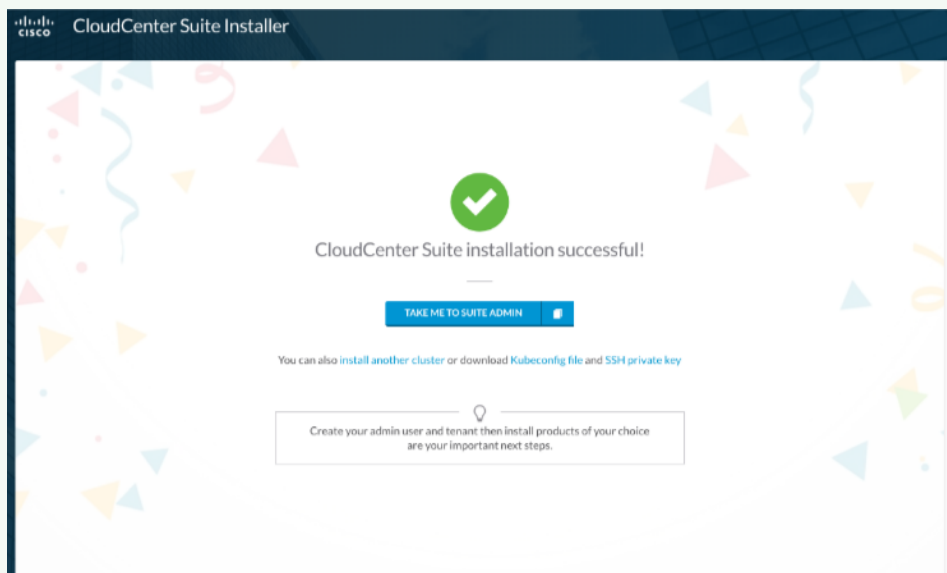
10. Once successful, you see the following message.



11. You have the following options at this point:

- a. Click **Take Me To Suite Admin** to launch and set up the [Suite Admin](#).
- b. Click **Install Another Cluster** to start another installation and go back to the homepage (Installer Dashboard).
- c. Download **Kubeconfig file** to connect to the launched cluster using the [kubectl](#) tool.
- d. Download **SSH private key** to SSH into your cluster node on private clouds – each time you launch a new cluster using the installer, the CloudCenter Suite generates a new key-pair for that cluster.

✔ For private clouds, the download link for the SSH private key is available on the last page of the installer UI as displayed in the following screenshot.



12. Be sure to switch off the installer VM. You can reuse this VM for any other purpose, for example, as an Offline Repository.

Existing Cluster Installation

Install the CloudCenter Suite on an Existing Kubernetes Cluster

- [Overview](#)
- [Restrictions](#)
- [Prerequisites](#)
- [Procedure](#)

Once you access the Suite Installer Dashboard (see [Prepare Infrastructure](#)), you can choose to install the Suite Admin on an existing cluster.

Before proceeding with section, adhere to the following restrictions:

- AWS: The CloudCenter Suite does not currently support a Suite Admin installation on an existing AWS cluster.
- Permission: Admin-level permissions for the cluster are mandatory for a user to install the Suite Admin in an existing cluster.

Verify that the cluster adheres to the following requirements:

- Kubernetes Version: The existing Kubernetes cluster must be of Version v1.11.3.
- Kubernetes Add ons: Install Cert-manager version v0.5.2 (required) using the following command (refer to <https://cert-manager.readthedocs.io/en/latest/> for details):

```
kubect1 apply -f https://raw.githubusercontent.com/jetstack/cert-manager/release-0.5/contrib/manifests/cert-manager/with-rbac.yaml
```

- StorageClass: The default storageClass must be configured.
- Kubeconfig: The kubeconfig user must have cluster-admin permission in the kubeconfig namespace.
 - If the cluster does not support Load Balancer.
 - GCP: You must remove auth provider and use the admin user password.
- Pod Priority: Define the PriorityClass for suite-high/suite-medium/suite-low.
 - Refer to <https://kubernetes.io/docs/concepts/configuration/pod-priority-preemption/> for details.
 - The commands to define PriorityClass are listed in the following code block.

```
# create pod priority class: suite-high/suite-medium/suite-low
##### begin create pod priority

cat <<EOF | kubectl apply -f -

apiVersion: scheduling.k8s.io/v1beta1

kind: PriorityClass

metadata:
  name: suite-high

value: 1000000

globalDefault: false

description: "High priority"

---

apiVersion: scheduling.k8s.io/v1beta1

kind: PriorityClass

metadata:
  name: suite-medium

value: 10000

globalDefault: false

description: "Medium priority"

---

apiVersion: scheduling.k8s.io/v1beta1

kind: PriorityClass

metadata:
  name: suite-low

value: 100

globalDefault: false

description: "Low priority"

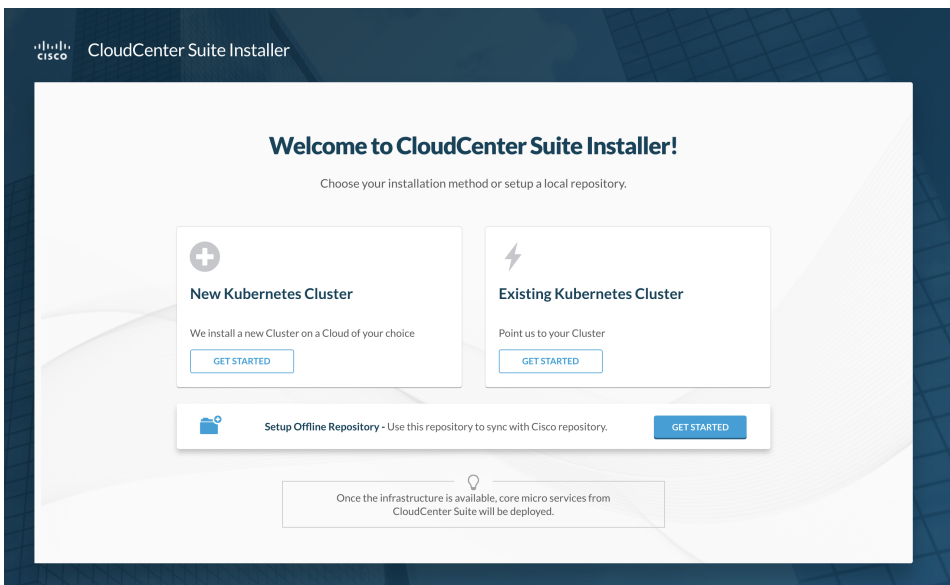
EOF

##### end create pod priority
```

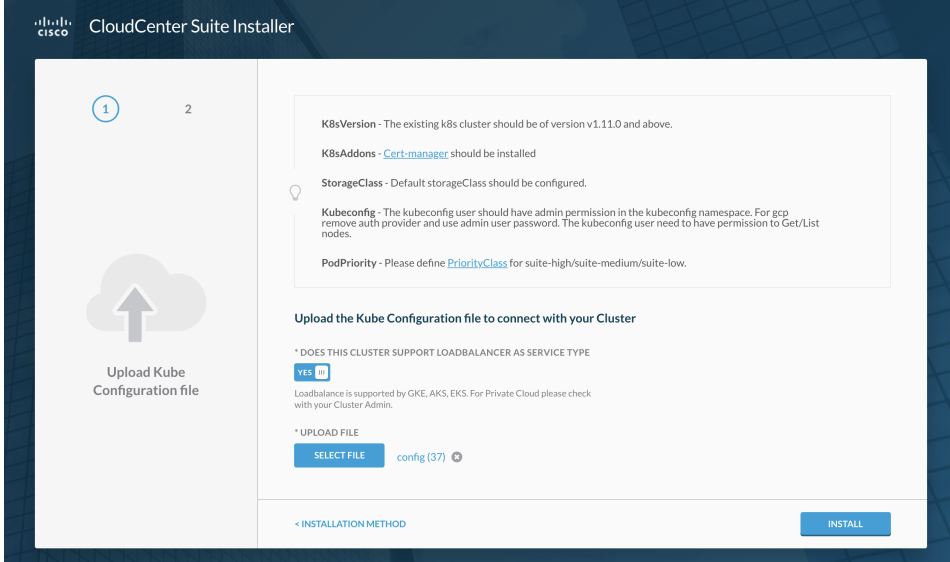
- RBAC - Must be enabled.

To install the CloudCenter Suite on an existing cluster, perform the following procedure.

1. Navigate to the Suite Installer Dashboard.
2. Click **Existing Kubernetes Cluster** to get started as displayed in the following screenshot.

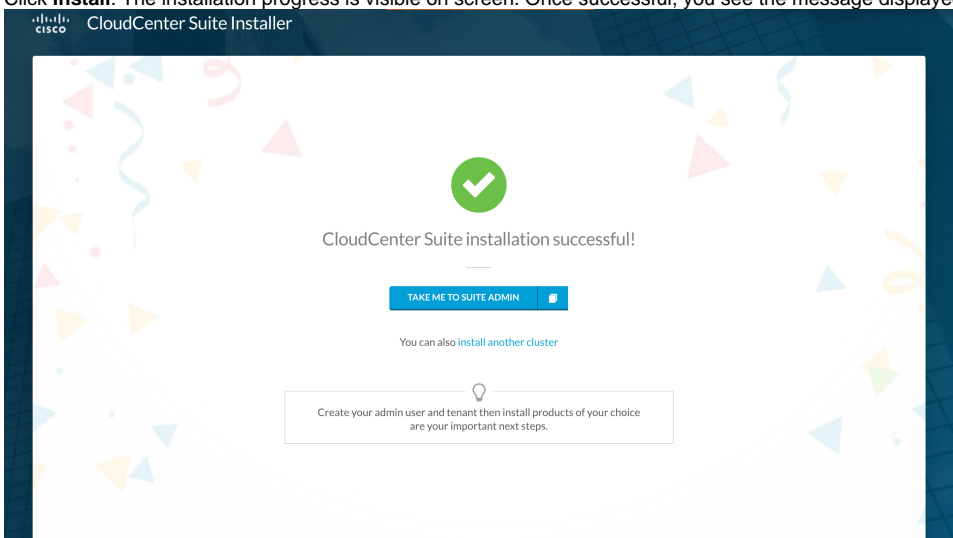


3. Verify that you have met the items identified in the *Prerequisites* section above. The following screenshot displays these tips as well.



4. Identify if you cluster supports **load balancer as the *service type*** – accordingly, turn this toggle
- YES** – Toggle ON if supported (public clouds generally support load balancers)
 - NO** – Toggle OFF if not supported (private clouds generally do not support load balancers)
5. Upload the Kubeconfig file.

6. Click **Install**. The installation progress is visible on screen. Once successful, you see the message displayed in the following screenshot.



7. You have the following options at this point:
- Click **Take Me To Suite Admin** to launch and set up the [Suite Admin](#).
 - Click **Install Another Cluster** to start another installation on the same cluster.

You have now installed the Suite Admin on an existing cluster.

Offline Repository

Offline Repository

- [Introduction](#)
- [Prerequisites for Offline Repository](#)
- [Setup the Offline Repository](#)

A repository connection enables access from one of the CloudCenter Suite VMs to the default **Cisco Products Repository**. This default repository is only accessible if you have **direct internet access**.

The CloudCenter Suite will try to connect to the Cisco Products Repository to install and upgrade the product modules.

! The default Cisco Products Repository is only accessible if your underlying Kubernetes cluster has direct internet access.

If you are behind a proxy, you may have internet access but will not be able to move forward with installing modules without the offline repository.

If you do not have internet access, you must:

- Install the Cisco Products Repository in your environment.
- Connect the CloudCenter Suite to the offline repository (see [Offline Repository Configuration](#)).

After you create a VM from the OVA, you have the option to use the VM as an offline repository server.

The offline repository connects to the default Cisco Products Repository and allows you to install or upgrade within the Suite Administration.

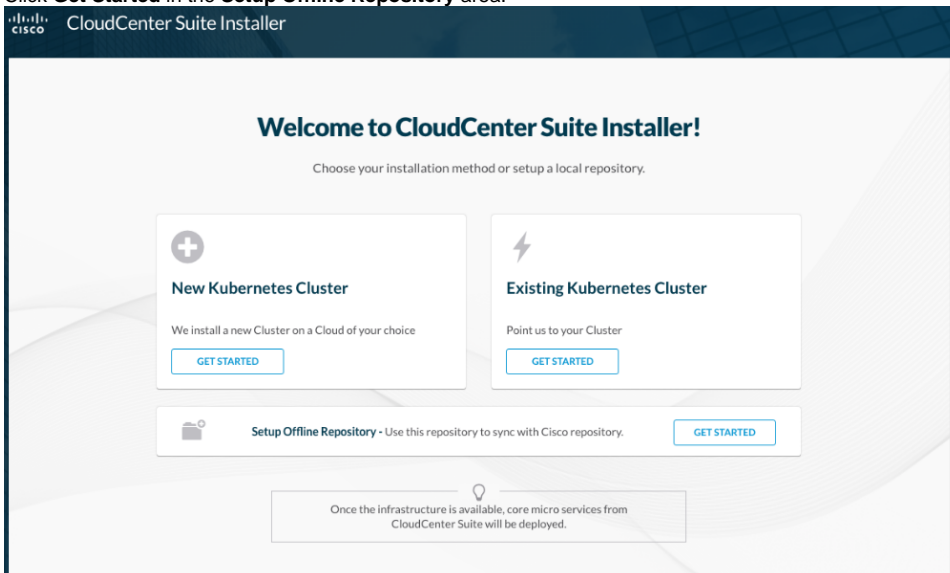
! The offline repository is the same for all supported clouds – and is only supported for OpenStack and VMware clouds.

- The offline repository VM must have access to the Cisco repository at devhub-docker.cisco.com and devhub.cisco.com.
- You must manually set up a valid DNS name for the repository VM.
- You must get a valid certificate and a private key pair for the DNS name (self-signed certificates are *not* acceptable, you must get a [Certificate Authority](#) to sign the certificate)
- The repository VM must be accessible from the Kubernetes cluster through the domain name.
- *Optional.* If your offline repository server requires a proxy to connect to the Internet, you must have the proxy configuration ready.
- A VM that was used for the installation can also be used as an offline repository after the installation completes.


i Once converted to an offline repository, this VM can no longer be used as the installer VM.

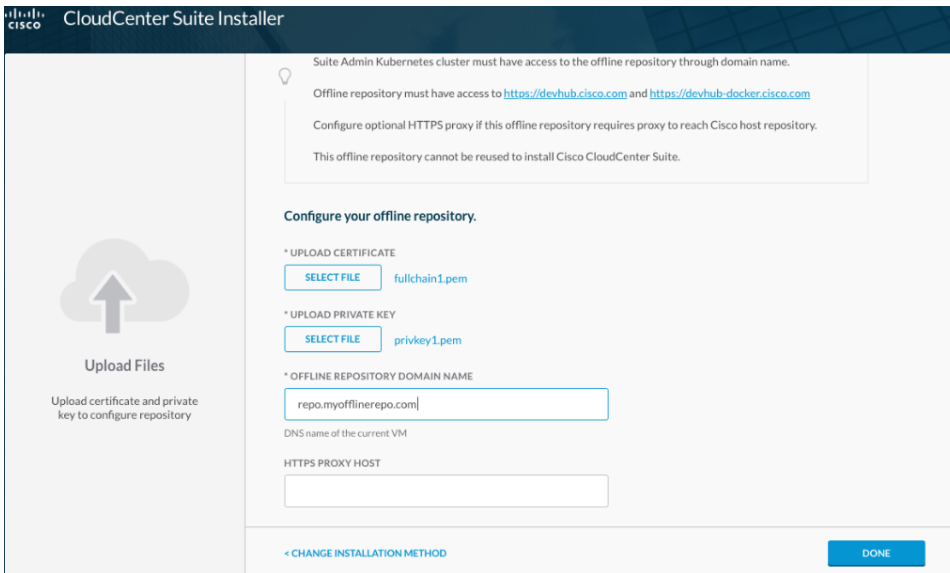
To setup an offline repository, follow this procedure.

1. Click **Get Started** in the **Setup Offline Repository** area.



2. Click Select File to upload the certificate and the private key.

-  Verify that the certificate and private key files have been assigned 755 permissions (full permissions for the owner, and read/execute permission for others).



CloudCenter Suite Installer

Suite Admin Kubernetes cluster must have access to the offline repository through domain name.

Offline repository must have access to <https://devhub.cisco.com> and <https://devhub-docker.cisco.com>

Configure optional HTTPS proxy if this offline repository requires proxy to reach Cisco host repository.

This offline repository cannot be reused to install Cisco CloudCenter Suite.

Configure your offline repository.

* UPLOAD CERTIFICATE
 fullchain1.pem

* UPLOAD PRIVATE KEY
 privkey1.pem


* OFFLINE REPOSITORY DOMAIN NAME

DNS name of the current VM


HTTPS PROXY HOST

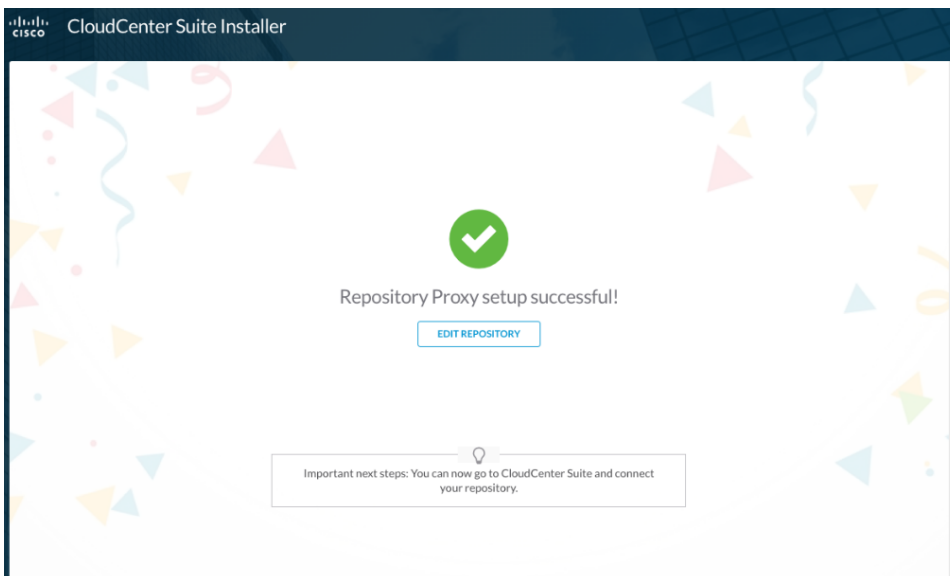
[< CHANGE INSTALLATION METHOD](#)

3. Enter the DNS name in the **Offline Repository Domain Name** field.
4. (Optional) Enter the proxy IP or DNS name in the HTTPS Proxy Host field..


-  This step is required only if you connect to the Internet via a proxy.

5. Click **Done** to complete the installation.
6. Navigate back to CloudCenter Suite to connect to the repository and perform further actions in CloudCenter Suite.


-  Once you setup offline repository, note its DNS name so you can re-launch the CloudCenter Suite Installer Repository Proxy success page so you can edit the repository details at a later date.



CloudCenter Suite Installer




Repository Proxy setup successful!

 Important next steps: You can now go to CloudCenter Suite and connect your repository.

Edit Offline Repository

Once you have set up the repository, you can click the **Edit Repository** link to change the certificates, DNS name, and proxy settings.

If you are editing the repository at a later time, use the DNS address (that you noted down after you *Setup the Offline Directory* as described in the previous section) to re-launch the CloudCenter Suite Installer Repository Proxy success page and click the **Edit Repository** link.



Upload Files

Upload certificate and private key to configure repository

Configure your offline repository.

* UPLOAD CERTIFICATE

* UPLOAD PRIVATE KEY

* OFFLINE REPOSITORY DOMAIN NAME

valid domain name matching the provided certificate

HTTPS PROXY HOST

proxy host IP address or DNS name, e.g. myproxy.com


PORT

proxy port, allowed value range is from 1 to 65535

PROXY REQUIRES PASSWORD
 YES



If you change the proxy password in the proxy instance, wait for at least 30 seconds for the new password to take effect, before updating the new password in the **Edit Repository** page.



Upload Files

Upload certificate and private key to configure repository

valid domain name matching the provided certificate

HTTPS PROXY HOST

proxy host IP address or DNS name, e.g. myproxy.com

PORT

proxy port, allowed value range is from 1 to 65535

PROXY REQUIRES PASSWORD
 YES

* USER NAME

username to be used to authenticate to proxy

* PASSWORD

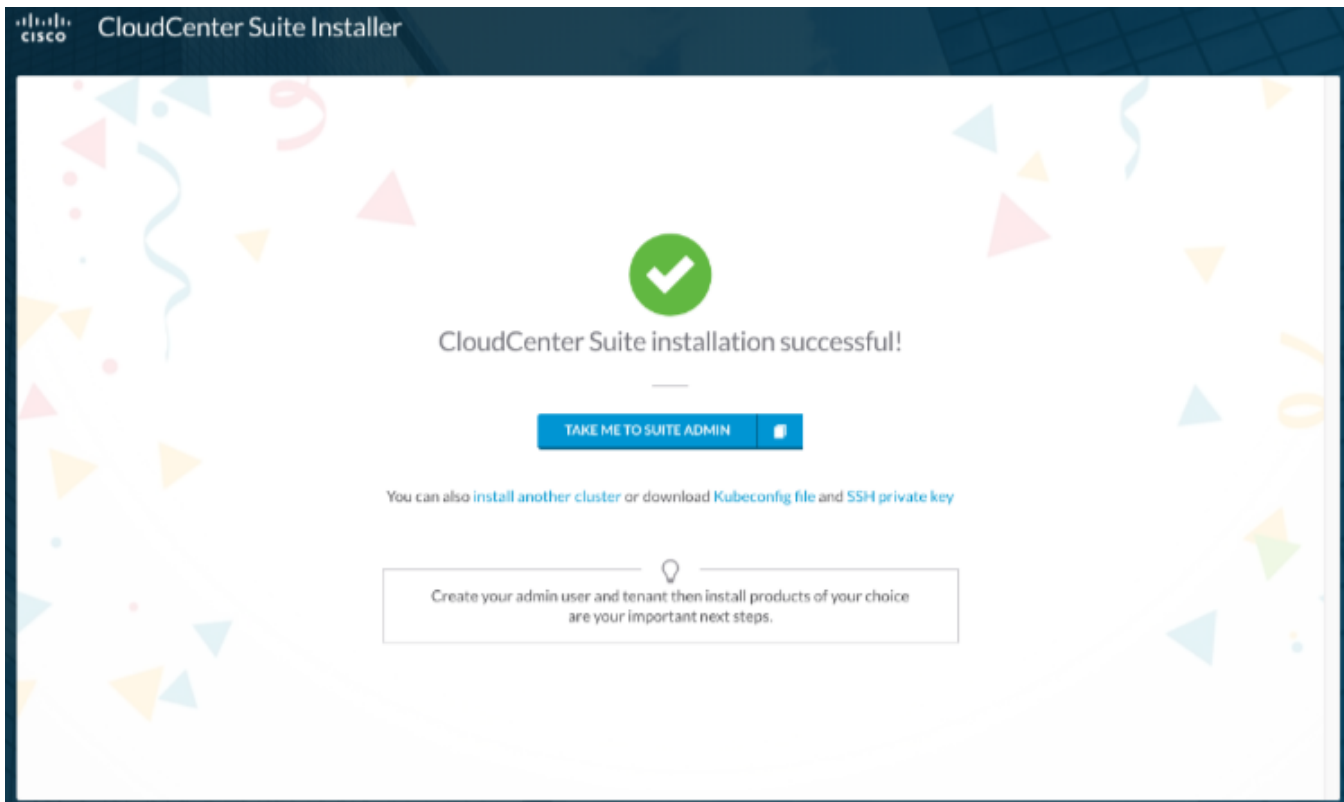
password to be used to authenticate to proxy

Troubleshooting

Troubleshooting

- Finding Kubernetes Resources
- Error during the Suite Installation Process (Lack of Resources)
- The Progress bar for a Kubernetes Cluster is Stuck at Launching cluster nodes on the cloud or Configuring the primary cluster
- Installation Failed: Failed to copy <script-name.sh> to remote host or any error related to SSH connection failure
- A Pod has Unbound PersistentVolumeClaims
- The Kubernetes Cluster Is Installed Successfully, but the Progress Bar for Suite Administration is Stuck at Waiting for product to be ready
- After Using Suite Admin for a While, Users Cannot Login to Suite Admin if Any Cluster Node is in a NotReady State
- Installation Failed: Failed to copy <script-name.sh> to remote host or any error related to SSH connection failure
- Error in Creating a Cluster
- Download Logs

For private clouds, the download link for the **Kubeconfig file** is available on the last page of the installer UI as displayed in the following screenshot.



While you may see this file for successful installations in the above screen, you will not be able to access this file if your installation was not successful. This file is required to issue any command listed in the <https://kubernetes.io/docs/reference/kubectl/cheatsheet/> section of the Kubernetes documentation.

By default, the **kubectl** command looks for the Kubeconfig file in the **\$HOME/.kube** folder.

- **Successful installation:** Copy the downloaded Kubeconfig file to your **\$HOME/.kube** folder and then issue any of the **kubectl** commands listed in the Kubernetes cheatsheet link above.
- **Stalled Installation:**
 - Private clouds and most public clouds: SSH into one of the primary server nodes and copy the Kubeconfig file from **/etc/kubernetes/admin.conf** to the **/root/.kube** folder.
 - GCP: Login to GCP, access the Kubernetes Engine, locate your cluster, click **Connect** to Connect to the cluster, and click the **copy** icon as displayed in the following screenshot. You should have already installed **gcloud** in order to view this icon.

Connect to the cluster

You can connect to your cluster via command-line or using a dashboard.

Command-line access

Configure `kubectl` command line access by running the following command:

```
$ gcloud container clusters get-credentials pujanrc221-7220e62e-ca6f-4f08-963c-9e49b --zone us-east1-b --project
```

[Run in Cloud Shell](#)

Cloud Console dashboard

You can view the workloads running in your cluster in the Cloud Console [Workloads dashboard](#).

[Open Workloads dashboard](#)

OK

At any time, if your installation stalls due to a lack of resources, perform this procedure to analyze the error logs.

To fetch the logs for this pod run :

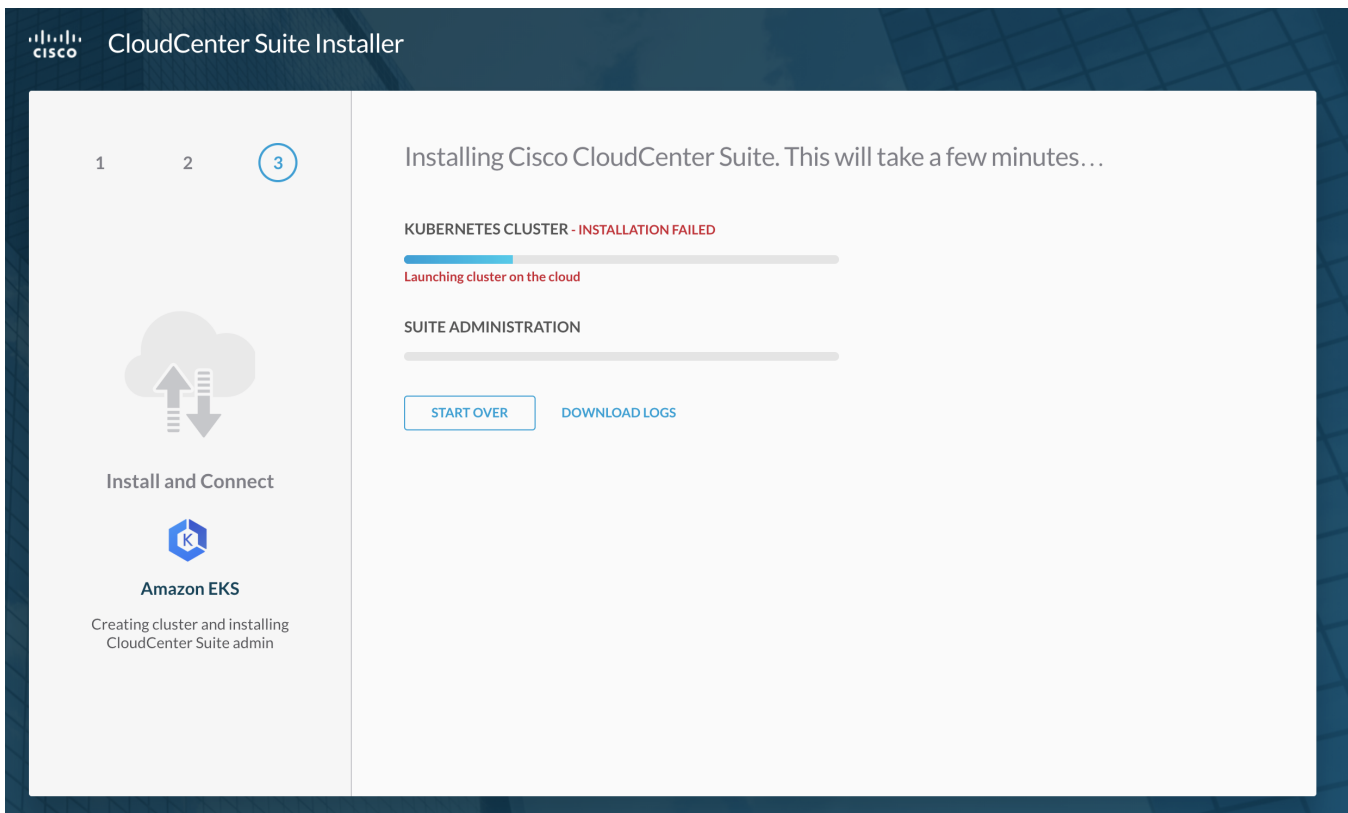
1. Locate the actual name of the container by running the following command:

```
kubectl get pods -all-namespaces | grep common-framework-suite-prod-mgmt-xxxx
```

2. Click the **Download Logs Download** link to download the installation logs for the failed service in case of an installation failure.
3. **View the** Logs for the container: common-framework-suite-prod-mgmt ...
4. Run the following command to view the error:

```
kubectl logs -f common-framework-suite-prod-mgmt-xxxx -n cisco
```

The issue displayed in the following screenshot could be an issue with the cloud environment. Refer to your cloud documentation for possible issues.

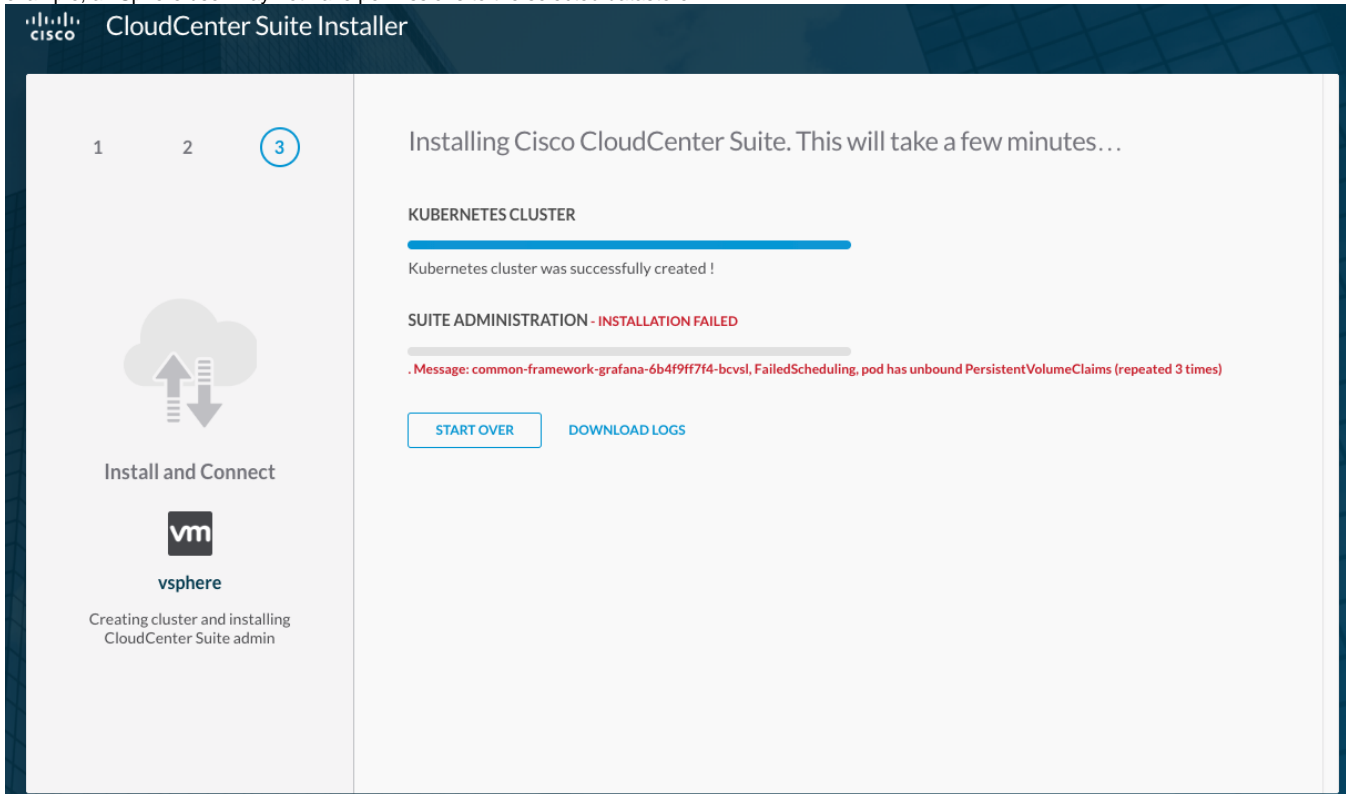


Other examples:

- If the target cloud is vSphere, check if the cloud account being used has permissions to launch a VM and if the VM is configured with a valid IPv4 address.
- If the cluster nodes are configured to use static IP, verify if the IP pool used is valid and if all the launched nodes have a unique IP from the pool.

This issue can occur when the installer node cannot SSH/SCP into launched cluster nodes. Verify if all the launched nodes have a valid IPv4 address and if the installer network can communicate with the Kubernetes cluster network (if they are on different networks). Also verify that the cluster nodes are able to connect to vSphere.

The problem displayed in the following screenshot is usually caused when the cloud user does not have permissions to the configured storage. For example, a vSphere user may not have permissions to the selected datastore.



This issue indicates that the CloudCenter Suite installation has some issue. Use the downloaded SSH key to SSH into one of the primary server nodes. To check the status of the pods, run **kubectl get pods --all-namespaces** for each pod. If the status does not display **Running**, run the following commands to debug further:

```
kubectl describe pod <pod-name> -n cisco
```

or

```
kubectl logs -f <pod-name> -n cisco
```

Use the downloaded SSH key to SSH into each cluster node and check if the system clock is synchronized on all nodes. Even if the NTP servers were initially synchronized verify if they are still active by using the following command.

```
ntpdate <ntp_server>
```

This issue may be the result of any of the following situations:

- Are all the cluster nodes up and running with a valid IP address?
- If the nodes are running, then use the downloaded SSH key to SSH into one of the primary server nodes.
- Run the following command on the primary server to verify if all the nodes are in the **Ready** state.

```
kubectl get nodes
```

If any of the nodes are **Not Ready** state, then run the following command on the node:

```
kubectl describe node <node-name>
```

If none of the above methods work, retry the installation or contact your CloudCenter Suite admin.

In case of failure (due to a quota availability issue) during the installation process, an error message similar to the one displayed in the following screenshot appears.

The screenshot shows the 'CloudCenter Suite Installer' interface. On the left, a sidebar indicates the current step is 'Specify Placement Properties' for 'Google Kubernetes Engine'. The main area is titled 'What are your gke placement properties?' and contains three input fields: 'GKE CLUSTER ID PREFIX' (value: gkecluster), '* GKE ZONE' (value: asia-east2-a), and '* GKE INSTANCE TYPE' (value: n1-standard-2). A dark blue error box is overlaid on the bottom right, displaying the following text: 'Error in Creating Cluster! rpc error: code = PermissionDenied desc = Insufficient project quota to satisfy request: resource "/ROUTES": request requires '3.0' and is short '2.0', project has a quota of '300.0' with '1.0' available.' At the bottom of the main area, there are three buttons: '< CHANGE CLOUD' (disabled), 'ERROR IN CREATING CLUSTER! RPC ERROR: CODE...' (highlighted in red), and 'INSTALL'.

Click the **Download Logs Download** link to download the installation logs for the failed service in case of an installation failure. See [Monitor Modules > Download Logs](#) for additional information.