VMware Cloud Foundation Operations and Administration Guide

VMware Cloud Foundation 3.0

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About the VMware Cloud Foundation Operations and Administration Guide

The *VMware Cloud Foundation Operations and Administration Guide* provides information about managing a VMware Cloud Foundation™ system, including managing the system's virtual infrastructure, managing users, configuring and deploying service offerings, and upgrading and monitoring the system.

Intended Audience

The *VMware Cloud Foundation Operations and Administration Guide* is intended for cloud architects, infrastructure administrators, and cloud administrators who are familiar with and want to use VMware software to quickly deploy and manage an SDDC. The information in this document is written for experienced data center system administrators who are familiar with:

- Concepts of virtualization, software-defined data centers, virtual infrastructure (VI), and virtual desktop infrastructure (VDI)
- VMware virtualization technologies, such as VMware ESXi™, the hypervisor
- Software-defined networking using VMware NSX®
- Software-defined storage using VMware vSAN™
- IP networks

Additionally, you should be familiar with these VMware software products, software components, and their features:

- VMware vSphere®
- VMware vCenter Server® and VMware vCenter Server® Appliance™
- VMware Platform Services Controller™
- VMware vRealize® Log Insight™
- VMware Horizon®
- VMware App Volumes™

Related Publications

The *VMware Cloud Foundation Planning and Preparation Guide* provides detailed information about the software, tools, and external services that are required for Cloud Foundation.

The *VMware Cloud Foundation Architecture and Deployment Guide* contains detailed information about a Cloud Foundation system, its components, and the network topology of a deployed system.

Administering Cloud Foundation Systems 1

As an SDDC administrator, you use the information in the *VMware Cloud Foundation Operations and Administration* document to understand how to administer and operate your installed Cloud Foundation system.

An administrator of an Cloud Foundation system performs tasks such as:

- Manage certificates.
- Add capacity to your system.
- Configure and provision the systems and the workload domains that are used to provide service offerings.
- Manage provisioned workload domains.
- Monitor alerts and the health of the system.
- Troubleshoot issues and prevent problems across the physical and virtual infrastructure.
- Perform life cycle management on the Cloud Foundation software components.

See the *VMware Cloud Foundation Overview and Deployment* document for an introduction to the overview and architecture of a Cloud Foundation system, and detailed descriptions of the software that is deployed in the environment.

This chapter includes the following topics:

VMware Software Components Deployed in a Typical Cloud Foundation System

In a typical Cloud Foundation system, you will encounter specific VMware software that SDDC Manager deploys in the system.

Note For information about which specific editions of each VMware product are licensed for use with the Cloud Foundation license, use the information resources at the Cloud Foundation product information page at http://www.vmware.com/products/cloud-foundation.html.

For the exact version numbers of the VMware products that you might see in your Cloud Foundation system after the initial bring-up process, see the *Release Notes* document for your Cloud Foundation version. If the system has been updated after the initial bring-up process using the Life Cycle Management features, see GUID-E27D3021-A821-41CC-B68E-60297D71F109#GUID-E27D3021-A821-41CC-B68E-60297D71F109 for details on how to view the versions of the VMware software components that are within your system.

Caution Do not manually change any of the settings that SDDC Manager sets automatically. If you change the generated settings, like names of VMs, unpredictable results might occur. Do not change settings for the resources that are automatically created and deployed during workflows, the workload domain processes, assigned IP addresses or names, and so on.

You can find the documentation for the following VMware software products and components at docs.vmware.com:

- vSphere (vCenter Server, Platform Services Controller, and ESXi)
- vSAN
- NSX for vSphere
- vRealize Log Insight
- vRealize Operations
- vRealize Automation

Web Interfaces Used When Administering Your Cloud Foundation System

You use SDDC Manager loaded in a browser for the single-point-of-control management of your Cloud Foundation system. This user interface provides centralized access to and an integrated view of the physical and virtual infrastructure of your system.

In addition to using the SDDC Manager Dashboard, you can use the following user interfaces for administration tasks involving their associated VMware software components that are part of a VMware SDDC. All these interfaces run in a browser, and you can launch them from within the SDDC Manager Dashboard.

Launch links are typically identified in the user interface by the launch icon: ↗.

VMware SDDC Web Interfaces	Description	Launch Link Location in SDDC Manager Dashboard
vSphere Web interface	This interface provides direct management of resources managed by the vCenter Server instances, for identity management, and for management of the NSX resources that provide the software-defined networking capabilities of the SDDC. You can also manage object level storage policies for distributed software-defined storage provided by vSAN.	1 On the SDDC Manager Dashboard, click **Inventory > Workload Domains.** 2 In the Name column, click a workload domain name. 3 Click the **Services** tab. 4 Click the appropriate launch link.
vRealize Log Insight Web interface	When the vRealize Log Insight instance is licensed for use in the system, this interface provides direct access to the logs and event data collected and aggregated in vRealize Log Insight for troubleshooting, trend analysis, and reporting.	1 On the SDDC Manager Dashboard, click **Inventory > Workload Domains.** 2 In the Name column, click a workload domain name. 3 Click the **Services** tab. 4 Click the appropriate launch link.

Getting Started with SDDC Manager

2

You use SDDC Manager to perform administration tasks on your Cloud Foundation system. This user interface provides an integrated view of the physical and virtual infrastructure and centralized access to manage the physical and logical resources.

You work with the SDDC Manager Dashboard by loading it in a web browser. For the list of supported browsers and versions, see the *Release Notes*.

Note When performing out-of-band (OOB) troubleshooting of hardware, some vendors may use Java-based consoles. Refer to the vendor documentation for supported browsers.

This chapter includes the following topics:

Log In to the SDDC Manager Dashboard

You access SDDC Manager through the SDDC Manager Dashboard in a supported browser.

Prerequisites

To log in, you need the SDDC Manager IP address or FQDN and the password for the `vcf` user. You had added this information to the deployment parameter worksheet before bring-up.

Procedure

1 In a browser, type one of the following:

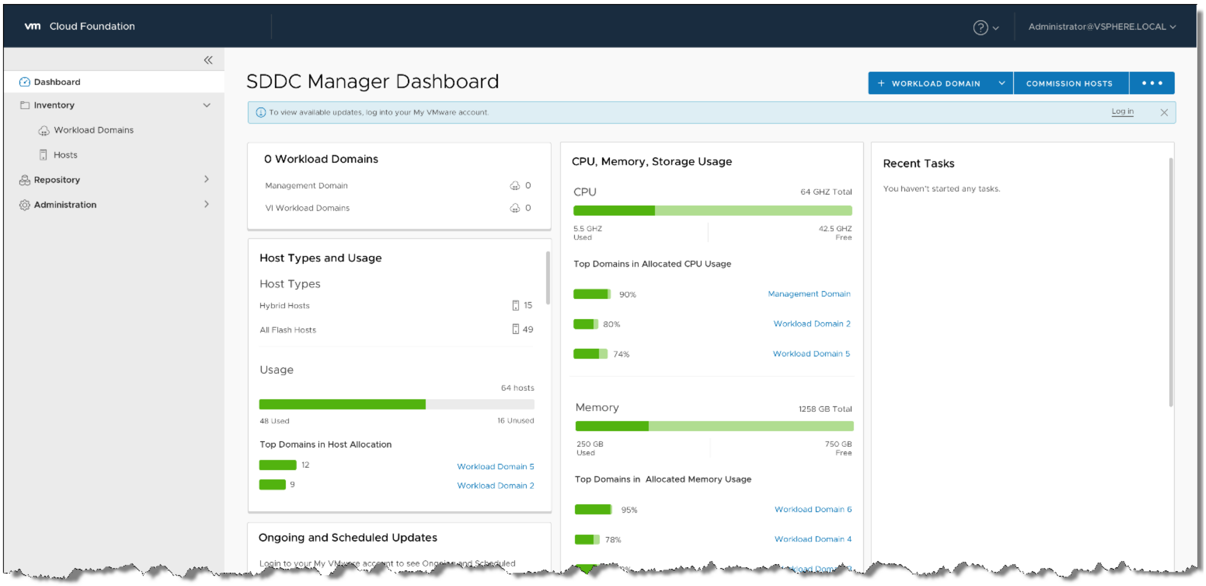
   - `https://`*FQDN* where *FQDN* is the host name of the SDDC Manager.
   - `https://`*IP_address* where *IP_address* is the IP address of the SDDC Manager.

2 Log in with the following credentials:

   User name: `vcf`

   Password you provided on the deployment parameter worksheet before bring-up

You are logged in to SDDC Manager and the Dashboard page appears in the browser.



To view available updates, log into your My VMware account.

You haven't started any tasks.

Login to your My VMware account to see Ongoing and Scheduled

Tour of the SDDC Manager User Interface

SDDC Manager provides the user interface for your single point of control for managing and monitoring your Cloud Foundation system and for provisioning virtual environments.

You use the Navigation bar to move between the main areas of the user interface.

Navigation Bar

On the left side of the interface is the Navigation bar. The Navigation bar provides a hierarchy for navigating to the corresponding pages.

Category	Functional Areas
Dashboard	The Dashboard provides the high-level administrative view for SDDC Manager features and functions in the form of widgets, including: Workload Domains; CPU, Memory, Storage Usage; Host Types and Usage; Recent Tasks; Ongoing and Scheduled Updates; Update History; and more. You can control which widgets display and how they are arranged on dashboard. ■ To rearrange the widgets, click the heading of the widget and drag it into the desired position. ■ To hide a widget, hover the mouse anywhere over the widget to reveal the **X** in the upper-right corner, and click the **X**. ■ To add a widget to the dashboard, click the three dots adjacent to the Commission Hosts button in the upper right corner of the page and select **Add New Widgets**. This displays all hidden widgets and enables you to select them.
Inventory	The Inventory category directs you to the following destinations: ■ Click **Workload Domains** to go directly to the Workload Domains page, which displays and provides access to all current workload domains and controls for managing workload domains. This page includes detailed status and information about all existing workload domains, including IP addresses, health status, owner, number of hosts, update status, and more. It also displays CPU, memory, and storage utilization for each workload domain, and collectively across all domains. ■ Click **Hosts** to go directly to the Hosts page, which displays and provides access to all current hosts and controls for managing hosts. This page includes detailed status and information about all existing hosts, including IP addresses, network pool, health status, domain and cluster assignment, and storage type. It also displays CPU, memory, and storage utilization for each host, and collectively across all hosts.

Category	Functional Areas
Repository	The Repository category directs you to the following destinations: ■ Click **Bundles** to view the Cloud Foundation product bundles in your current deployment. ■ Click **Download History** to view the history of update bundle downloads, including version number, date, and other release details. If a bundle is available but has not yet been downloaded, controls for immediate or scheduled downloading appear next to the bundle. **Note** To access patches and bundles, you must be logged in to your myvware account through the **Administration > Update Management** page.
Administration	The Administration category directs you to the following destinations: ■ Click **Network Settings** to view and manage network pool settings, including network pool configuration. You can create new pools, and view and modify existing pools. A network pool is a collection of network information with an IP inclusion range reserved for Cloud Foundation. See About Network Pools for more information. ■ Click **Licensing** to manage VMware product licenses. Add the licenses for the component products that comprise your Cloud Foundation deployment. See Select Licenses for more information. ■ Click **Users** to manage Cloud Foundation users and groups, including creating users and groups, setting privileges, assigning roles, and so on. ■ Click **Update Management** to log in to your myvmware account, and gain access to patch and update bundles. ■ Click **vRealize Suite** to deploy and manage vRealize Automation, vRealize Operations, and vRealize Log Insight as components of Cloud Foundation. See Chapter 8 Adding vRealize Components to Cloud Foundation for details. ■ Click **Security** to configure your certificate authorities. See Configure Certificate Authority. ■ Click **VMware CEIP** to enroll in the VMware Customer Improvement Plan. This plan provides VMware with information that enables VMware to improve its products and services, to fix problems, and to advise you on how best to deploy and use our products. As part of the CEIP, VMware collects technical information about your organization's use of VMware products and services on a regular basis in association with your organization's VMware license key(s).

Log out of the SDDC Manager Dashboard

Log out of SDDC Manager when you have completed your tasks.

Procedure

1 In the SDDC Manager Dashboard, open the logged-in account menu by clicking the down arrow next to the account name in the upper right corner.

2 Click the menu choice to log out.

Managing Users and Groups

3

You can allow the users and groups in your Microsoft Active Directory (AD) domain to use their credentials to log in to the SDDC Manager Dashboard as well as the vCenter Server instances that are deployed in your Cloud Foundation system.

You had provided a password for the superuser account (user name `vcf`) in the deployment parameter sheet before bring-up. After Cloud Foundation is deployed, you can log in with the superuser credentials and then add vCenter Server or AD users or groups to Cloud Foundation. Authentication to the SDDC Manager Dashboard uses the VMware vCenter® Single Sign-On authentication service that is installed with the Platform Services Controller feature during the bring-up process for your Cloud Foundation system.

This chapter includes the following topics:

Assign Cloud Foundation Role to AD Users or Groups

You can assign the Cloud Admin role to AD users or groups so that they can log in to SDDC Manager with their AD credentials.

Procedure

1 Log in to the SDDC Manager Dashboard with your superuser credentials.

2 Click **Administration > Users**.

3 Click **+ User or Group**.

4 Select one or more user or group by clicking the check box next to the user or group.

You can either search for a user or group by name, or filter by user type or domain.

5 Scroll down to the bottom of the page and click **Add**.

The Cloud Admin role is assigned to the selected user or group.

View Role Details

The Cloud Admin role has read, write, and delete privileges.

Procedure

1 On the SDDC Manager, click **Administration > Users**.

2 In the Role column, click Cloud Admin.

The Role Details page displays privilege for the Cloud Admin role.

Remove Cloud Foundation Role for a User or Group

You can remove the Cloud Admin role from an AD user or group. The removed user or group will not be able to log in to the SDDC Manager Dashboard.

Procedure

1 On the SDDC Manager Dashboard, click **Administration > Users**.

2 Hover your mouse in the user or group row that you want to remove.

Three dots appear to the left of the user/group name column.

3 Click the dots and click **Remove User**.

The Cloud Admin role is removed for the specified user.

Managing Certificates for Cloud Foundation Components

4

You can manage certificates for all external-facing Cloud Foundation component resources, including configuring a certificate authority, generating and downloading CSRs, and installing them. This section provides instructions for using both Microsoft and non-Microsoft certificate authorities.

You can manage the certificates for the following components.

- Platform Services Controllers
- vCenter Server
- NSX Manager
- SDDC Manager
- vRealize Automation
- vRealize Log Insight
- vRealize Operations

Note You cannot manage certificates for NSX-T in the SDDC Manager.

You replace certificates for the following reasons:

- Certificate has expired or is close to expiring.
- Certificate has been revoked.
- You do not want to use the default VMCA certificate.
- Optionally, when you create a new workload domain.

However, it is recommended that you replace all certificates right after deploying Cloud Foundation. After you create new workload domains, you can replace certificates for the appropriate components as needed.

1 Before Replacing Certificates

Before replacing certificates, keep in mind the following recommendations and notes.

2 View Certificate Information

You can view details of a currently active certificate for a component resource directly in the SDDC Manager Dashboard.

3 Configure Certificate Authority

   Before you can generate and install certificates, you must configure a certificate authority (CA).

4 Install Certificates with the Microsoft Certificate Authority

   You can generate a CSR and signed certificates, and install them for selected resource components directly in the SDDC Manager Dashboard.

5 Install Certificates with Non-Microsoft Certificate Authority

   If you intend to generate and install non-Microsoft CA certificates, you must download the certificate signing request (CSR) from the SDDC Manager Dashboard and have it manually signed by a third-party CA. You can then use the controls in the SDDC Manager Dashboard to install the certificate.

6 Clean Out Old or Unused Certificates

   Old or unused certificates are stored in a trust store in SDDC Manager. You can delete old certificates through the SDDC Manager VM.

Before Replacing Certificates

Before replacing certificates, keep in mind the following recommendations and notes.

- Do not replace certificate if any update operations are in progress. Wait until updates complete before proceeding.
- At the beginning of the certificate replacement workflow, the SDDC Manager Dashboard automatically takes a snapshot (`pre-replace-certificate`) of the component resources, except for the vRealize Suite components.

  This enables you to roll back if the certificate replacement process fails. If the process succeeds, this snapshot is automatically deleted.
- When replacing the default VMCA certificates with external CA-signed certificates, the Common Name (CN) defined in the external CA-signed certificate must contain the Fully Qualified Domain Name (FQDN) of the Cloud Foundation component.

  If the CN does not contain the FQDN, the certificate replacement operation will fail pre-validation.

  Note Wildcard certificates are not supported.
- Cloud Foundation must use the default **`vmca`** certificate management mode in vSphere.

  This value is configured in vSphere by the `vpxd.certmgmt.mode` parameter in the Advanced Settings for the vCenter Server for your Cloud Foundation deployment (**vSphere Web Client > [vCenter identifier] > Configure tab > Settings > Advanced Settings**).

  This property must be set to the default **`vmca`** value. Do not modify this property when replacing the default VMCA certificates with external CA-signed certificates. Do not change this parameter to **`custom`**. Cloud Foundation uses VMCA for internal certificates when externally facing certificates are replaced with external CA-signed certificates.

- If you need to replace the certificate for the Virtual Appliance Management Interface (VAMI) on the vRealize Automation virtual appliances, see Replace the vRealize Automation Appliance Management Site Certificate in the vRealize Automation product documentation.

View Certificate Information

You can view details of a currently active certificate for a component resource directly in the SDDC Manager Dashboard.

Procedure

1 In the SDDC Manager Dashboard, click **Inventory > Workload Domains**.

   The Workload Domains page displays information for all workload domains.

2 In the list of domains, click the name of the workload domain to open the details page for that domain.

   The workload domain details page displays CPU, memory, and storage allocated to the domain.

3 Select the **Security Tab**.

   This tab lists the certificates for each Cloud Foundation resource component, including the following details:

   - Issuer, such as Certificate Authority.
   - Start and finish dates for certificate validity.
   - Current certificate status: `Active`, `Expiring` (will expire within 15 days), or `Expired`.
   - Certificate operation status.

4 To view certificate details, expand the resource to view the certificate details In the Resource Type column.

   The expanded field displays certificate details including signature algorithm, public key, public key algorithm, certificate string, and more.

Configure Certificate Authority

Before you can generate and install certificates, you must configure a certificate authority (CA).

Cloud Foundation supports only the Microsoft CA.

Prerequisites

- Verify that you have created a Microsoft Active Directory certificate service (`.certsrv`) template in an IIS container on a CA address server.
- Verify that the certificate service template is properly configured for basic authentication.

To create the certificate service template with the proper authentication configuration, see Prepare the Certificate Service Template.

Procedure

1 Navigate to **Administration > Security > Certificate Management** to open the Configure Certificate Authority page.

2 Complete the following configuration settings.

Option	Description
Certificate Authority	Select the CA from the dropdown menu. The default is `Microsoft`.
CA Server URL	Specify the URL for the CA address server. This address must begin with `https://` and end with `certsrv`, for example `https://www.mymicrosoftca.com/certsrv`
Username	Provide a valid username to enable access to the address server.
Password	Provide a valid password to enable access to the address server.
Template Name	Enter the certsrv template name. You must create this template in Microsoft Certificate Authority.

3 Click **Save**.

A dialog appears, asking you to review and confirm the CA server certificate details.

4 Click **Accept** to complete the configuration.

The CA is now available for use in generating and installing a certificate.

Prepare the Certificate Service Template

To ensure that Cloud Foundation can successfully pass authentication when replacing certificates, you must create the certificate service template with the proper basic authentication configuration through the IIS manager.

Procedure

1 Create a Microsoft Active Directory CA with the following features and settings.

a Navigate to **Select server roles**.

b Under **Active Director Certificate Services**, select **Certification Authority** and **Certification Authority Web Enrollment**.

c Under **Web Server (IIS) > Web Server > Security**, select **Basic Authentication.**

2 Configure and issue a VMware Certificate Template for **Machine SSL and Solution User certificates** on this CA server.

For step by step procedures, see Knowledge Base article 2112009 Search Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.x .

3 Configure the certificate service template for basic authentication.

a Access the IIS manager and navigate to **Server > Sites > Default Web Site > CertSrv**.

b Select the Authentication property in the IIS header.

c Select and enable **Basic Authentication**.

d Restart the site.

What to do next

Use this template when configuring the certificate authority in Configure Certificate Authority.

Install Certificates with the Microsoft Certificate Authority

You can generate a CSR and signed certificates, and install them for selected resource components directly in the SDDC Manager Dashboard.

Prerequisites

- Verify that the bring-up process is complete and successful.
- Verify that you have configured the Certificate Authority, as described in Configure Certificate Authority.

Procedure

1. In the SDDC Manager Dashboard, click **Inventory > Workload Domains**.

   The Workload Domains page displays information for all workload domains.

2. In the list of domains, click the name of the workload domain to open the details page for that domain.

   The workload domain details page displays CPU, memory, and storage allocated to the domain.

3. Select the **Security Tab**.

   This tab lists the default certificates, among other details, for the Cloud Foundation resource components. It also provides controls for working with certificates.

   Note You can view the current certificate and key information for a component by clicking the down-arrow icon next to the name.

4. Generate the CSR.

   a Use the check boxes to select the resource components for which you want to generate the CSR.

   b Click **Generate CSR**.

   The Generate CSRs dialog box opens.

c Configure the following settings for the CSR.

Option	Description
Algorithm	Select the key type for the certificate. RSA (the default) is typically used. The key type defines the encryption algorithm for communication between the hosts.
Key Size	Type the key size in bits (2048 bit minimum).
Email	Optionally, enter a contact email address.
Organizational Unit	Use this field to differentiate between divisions within your organization with which this certificate is associated.
Organization	Type name under which your company is legally registered. The listed organization must be the legal registrant of the domain name in the certificate request.
Locality	Type the city or locality where your company is legally registered.
State or Province Name	Type the full name (do not abbreviate) of the state, province, region, or territory where your company is legally registered.
Country	Type the country name where your company is legally registered. This value must use the ISO 3166 country code.

d Click **Generate CSR**.

The Generate CSRs dialog box closes. The Security tab displays a status of `CSR Generation is in progress`. When the CSR generation completes, the **Generate Signed Certificates** button becomes active.

5 Generate the signed certificates.

a Leave all the resource components selected.

b Click **Generate Signed Certificates**.

The Generate Signed Certificates dialog box appears, listing the selected components.

c For the Select Certificate Authority, select the desired authority, and click **Generate Certificate**.

The Generate Signed Certificates dialog box closes. The Security tab displays a status of `Certificates Generation is in progress`. When the certificate generation completes, the **Install Certificates** button becomes active.

6 Click **Install Certificates**.

The Security tab displays a status of `Certificates Installation is in progress`.

Note As installation completes, the Certificates Installation Status column for each selected resource component in the list changes to `Successful` with a green check mark.

Important If you selected the SDDC Manager as one of the resource components, you must manually restart SDDC Manager services to reflect the new certificate and to establish a successful connection between Cloud Foundation services and other resources in the management domain.

7 Restart all services using the provided `sddcmanager_restart_services.sh script`.

To restart the service:

a Using SSH, log in to the SDDC Manager VM with the following credentials:

Username: **`vcf`**

Password: use the password specified in the deployment parameter sheet

b Enter **`su`** to switch to the root user.

c Run the following command:

```
sh /opt/vmware/vcf/operationsmanager/scripts/cli/sddcmanager_restart_services.sh
```

What to do next

If you have replaced the certificate for the vRealize Operations Manager resource component, you must reconfigure the load balancer node. See Configure SSL Passthrough for vRealize Operations Manager.

Install Certificates with Non-Microsoft Certificate Authority

If you intend to generate and install non-Microsoft CA certificates, you must download the certificate signing request (CSR) from the SDDC Manager Dashboard and have it manually signed by a third-party CA. You can then use the controls in the SDDC Manager Dashboard to install the certificate.

Prerequisites

Verify that you have configured and packaged your certificate authority configuration files in the form of a `.tar.gz` file. The contents of this archive must adhere to the following structure:

- The name of the top-level directory must exactly match the name of the domain as it appears in the list on the **Inventory > Workload Domains** page. For example, `MGMT`.
- The PEM-encoded root CA certificate chain file (`rootca.crt`) must reside inside this top-level directory.
- This directory must contain one sub-directory for each component resource.

  The name of each sub-directory must exactly match the resource hostname of a corresponding component as it appears in the Resource Hostname column in the **Workload Domains > Security** tab.

  For example, `nsxManager.vrack.vsphere.local`, `vcenter-1.vrack.vsphere.local`, and so on.
- Each sub-directory must contain a corresponding `.csr` file, whose name must exactly match the resource as it appears in the Resource Type column in the **Workload Domains > Security** tab.

  For example, the `nsxManager.vrack.vsphere.local` sub-directory would contain the `nsxManager.vrack.vsphere.local.csr` file.

- Each sub-directory must contain a corresponding `.crt` file, whose name must exactly match the resource as it appears in the Resource Type column in the **Workload Domains > Security** tab.

  For example, the `nsxManager.vrack.vsphere.local` sub-directory would contain the `nsxManager.vrack.vsphere.local.crt` file.

Note All resource and hostname values can be found in the list on the **Inventory > Workload Domains > Security**tab.

Procedure

1 In the SDDC Manager Dashboard, navigate to **Inventory > Workload Domains**.

  The Workload Domains page displays information for all workload domains.

2 In the list of domains, click the name of the workload domain to open the details page for that domain.

  The workload domain details page displays CPU, memory, and storage allocated to the domain.

3 Select the **Security Tab**.

  This tab lists the default certificates, among other details, for the Cloud Foundation resource components. It also provides controls for working with certificates.

  Note You can view the current certificate and key information for a component by clicking the down-arrow icon next to the name.

4 Generate the CSR.

  a Use the check boxes to select the resource components for which you want to generate the CSR.

  b Click **Generate CSR**.

    The Generate CSRs dialog box opens.

c Configure the following settings for the CSR.

Option	Description
Algorithm	Select the key type for the certificate. RSA (the default) is typically used. The key type defines the encryption algorithm for communication between the hosts.
Key Size	Type the key size in bits (2048 bit minimum).
Email	Optionally, enter a contact email address.
Organization Unit	Use this field to differentiate between divisions within your organization with which this certificate is associated.
Organization	Type name under which your company is legally registered. The listed organization must be the legal registrant of the domain name in the certificate request.
Locality	Type the city or locality where your company is legally registered.
State or Province Name	Type the full name (do not abbreviate) of the state, province, region, or territory where your company is legally registered.
Country	Type the country name where your company is legally registered. This value must use the ISO 3166 country code.

d Click **Generate CSR**.

The Generate CSRs dialog box closes. The Security tab displays a status of `CSR Generation is in progress`. When CSR generation is complete, the **Download CSR** button becomes active.

5 Click **Download CSR** to download and save the CSR files to the directory structure described in the Prerequisites section above.

6 External to the SDDC Manager Dashboard, complete the following tasks:

a Verify that the different `.csr` files have successfully generated and are allocated in the required file structure.

b Get the certificate requests signed.

This will create the corresponding `.crt` files.

c Verify that the newly acquired `.crt` files are correctly named and allocated in the required file structure.

d Package the file structure as `<domain name>.tar.gz`.

7 Click **Upload and Install**.

8 In the Upload and Install Certificates dialog box, click **Browse** to locate and select the newly created `<domain name>.tar.gz` file.

After you select the file, the **Upload** button becomes active.

9 Click **Upload**.

When upload is complete, the **Install Certificate** button becomes active.

10 Click **Install Certificate**.

The Security tab displays a status of `Certificates Installation is in progress`.

Note As installation completes, the Certificates Installation Status column for the affected components in the list changes to `Successful` with a green check mark.

11 Restart all services using the provided `sddcmanager_restart_services.sh script`.

To restart the service:

a Using SSH, log in to the SDDC Manager VM with the following credentials:

Username: **`vcf`**

Password: use the password specified in the deployment parameter sheet

b Enter **`su`** to switch to the root user.

c Run the following command:

```
sh /opt/vmware/vcf/operationsmanager/scripts/cli/sddcmanager_restart_services.sh
```

What to do next

If you have replaced the certificate for the vRealize Operations Manager resource component, you must reconfigure the load balancer node. See Configure SSL Passthrough for vRealize Operations Manager.

Clean Out Old or Unused Certificates

Old or unused certificates are stored in a trust store in SDDC Manager. You can delete old certificates through the SDDC Manager VM.

Procedure

1 Using SSH, log in to the SDDC Manager VM with the following credentials:

Username: **`vcf`**

Password: use the password specified in the deployment parameter sheet

2 Enter **`su`** to switch to the root user.

3 Change to the `/opt/vmware/vcf/operationsmanager/scripts/cli` directory.

```
cd /opt/vmware/vcf/operationsmanager/scripts/cli
```

4 From the `/opt/vmware/vcf/operationsmanager/scripts/cli` directory, use the following script and command to discover the names of the certificates in the trust store.

```
sddcmanager-ssl-util.sh -list
```

5 Using the name of the certificate, delete the old or unused certificate.

```
sddcmanager-ssl-util.sh -delete <certificate alias name from list>
```

6 (Optional) Clean out root certificates in VMware Endpoint Certificate Store from the Platform Services Controller node.

See Explore Certificate Stores from the vSphere Client in the vSphere product documentation.

License Management

5

In the deployment parameter sheet you completed before bring-up, you entered license keys for the following components:

- VMware vSphere
- VMware vSAN
- VMware NSX for vSphere
- vCenter
- VMware vRealize Log Insight for the management domain

After bring-up, these license keys appear in the Licensing screen of the SDDC Manager Dashboard.

You must have adequate license units available before you create a VI workload domain, add a host to a cluster, or add a cluster to a workload domain. Add license keys as appropriate before you begin any of these tasks.

This chapter includes the following topics:

Add License Keys for the Software in Your Cloud Foundation System

You can add licenses to the Cloud Foundation license inventory.

Procedure

1 On the SDDC Manager Dashboard, navigate to **Administration > Licensing**.

2 Click **+ License Key**.

3 Select the product key for which you are entering a license key.

4 Type the license key.

5 Type a description for the license.

   If you have multiple license keys for a product, the description can help in identifying the license. For example, you may want to use one license for high performance workload domains and the other license for regular workload domains.

6 Click **Save**.

Edit License Description

If you have multiple license keys for a product, the description can help in identifying the license. For example, you may want to use one license for high performance workload domains and the other license for regular workload domains.

Procedure

1 On the SDDC Manager Dashboard, navigate to **Administration > Licensing**.

2 Hover your mouse in the license row that you want to edit.

   A set of three dots appear on the left of the product name.

3 Click the dots and then click **Edit Description**.

4 On the Edit License Key Description window, edit the description as appropriate.

5 Click **Save**.

Delete License Key

Deleting a license key removes the license from the Cloud Foundation license inventory. If the license has been applied to any workload domain, host, or cluster, the license continues to work for them.

Procedure

1 On the SDDC Manager Dashboard, navigate to **Administration > Licensing**.

2 Hover your mouse in the license row that you want to edit.

   A set of three dots appear on the left of the product name.

3 Click the dots and then click **Remove Key**.

4 On the Remove Key dialog box, click **Remove**.

The license is removed from the Cloud Foundation license inventory

Enable vRealize Log Insight Logging for Workload Domains

During the bring-up process, vRealize Log Insight is deployed and configured to collect logs from the management domain components (vSphere, NSX Manager, and SDDC Manager). To enable logging on VI workload domains, you must provide your own license for vRealize Log Insight. After you enter the license key on the vRealize Log Insight UI and enable logging in Cloud Foundation, workload domains are automatically connected to vRealize Log Insight.

Once logging is enabled for workload domains, you cannot disable this setting.

Procedure

1 On the SDDC Manager Dashboard, click navigate to **Administration > vRealize Suite**.

2 Click **vRealize Log Insight**.

3 Click the **vRealize Log Insight** link.

4 Login to vRealize Log Insight with the admin credentials you provided in the deployment parameters sheet before bring-up.

5 Navigate to **Administration > Management > License**.

6 Click **Add New License**.

7 Enter the license key and click **Add License**.

8 Verify that the license you added is displayed in the license table and the status is active.

Cloud Foundation connects vRealize Log Insight to workload domains.

9 On the SDDC Manager Dashboard, click **Enable** in the Enable Logging for all Workload Domains window.

Cloud Foundation connects the vSphere and NSX components for all existing workload domains to vRealize Log Insight. Workload domains created after enabling logging are automatically connected to vRealize Log Insight.

Licenses for vRealize Automation and vRealize Operations

You can add licenses for vRealize Automation and vRealize Operations when you deploy them.

For information on deploying vRealize components, see Connect vRealize Suite Components to Workload Domains.

Adding Hosts to Cloud Foundation

6

To add hosts to the Cloud Foundation inventory, you must first create a network pool or expand the default network pool created during bring-up.

For information on network pools, see About Network Pools.

You then commission hosts to Cloud Foundation. During the commissioning process, you associate hosts with a network pool. Commissioned hosts are added to the Cloud Foundation inventory. You can add these hosts to the management domain or to a VI workload domain. When a host is added to a workload domain, an IP address from the network pool's IP inclusion range is assigned to it.

This chapter includes the following topics:

About Network Pools

Network pools automatically assign static IP addresses to vSAN and vMotion vmkernel ports so that you don't need to enter IP addresses manually when creating a VI workload domain or adding a host or cluster to a workload domain.

A network pool is a collection of a set of subnets within an L2 domain. It includes information about subnets reserved for the vSAN and vMotion networks that are required for adding a host to the Cloud Foundation inventory. The network pool also contains a range of IP addresses, called an inclusion range. IP addresses from the inclusion ranges are assigned to the vSAN and vMotion vmkernel ports on the host. The use of inclusion ranges allows you to limit the IP addresses that will be consumed from a given subnet. You can add more inclusion ranges in order to expand the use of the provided subnet.

A default network pool (named bringup-networkpool) is created during bring-up. This network pool is automatically associated with the management domain. Network information for this network pool is based on the deployment parameter sheet you provided during bring-up. If you have a single L2 domain in your environment for management workload domain vSAN and vMotion networks or if you want to expand the management domain by adding a host, you can expand this default network pool.

In order to create a workload domain with hosts in a different L2 domain than the management domain, you must create a new network pool.

All hosts in a cluster must be associated with the same network pool. However, a workload domain can contain multiple clusters, each with its own network pool. You may want to have multiple clusters within a workload domain to provide separate fail over domains (i.e. av VM only fails over between hosts in a cluster). Multiple clusters also provide isolation for security reasons and are also useful for grouping servers of a particular type of configuration together. Multiple clusters can also to handle growth. Original servers used in the first cluster may get outdated at some point. Newer server models can then be added in a new cluster to the workload domain and workloads can be migrated at a leisurely pace.

Sizing a Network Pool

Properly sizing a network pool is critical to prevent future issues in the environment due to insufficient IP addresses. Care must be taken when defining the subnets for a network pool as the subnet cannot be changed after it is deployed. The scope of IP addresses used from the defined subnet can be limited by the definition of one or more inclusion ranges. Thus, it is recommended that you begin with defining a larger subnet than what is initially required and utilize the inclusion ranges to limit use. This will provide you the capability to grow with demand as needed.

You begin sizing a network pool by determining the number of hosts that you will have in each cluster. A workload domain must contain a minimum of one cluster. As each cluster leverages vSAN for storage, the minimum number of hosts within a cluster is three. The exception to this rule is the management workload domain. It is recommended that the management workload domain contain a minimum of four hosts. This allows for an additional level of availability for the critical infrastructure components. A cluster can be expanded to the maximum number of hosts supported by vCenter, which is currently 64 hosts.

Allocate a minimum of one IP address per host plus enough additional IP addresses to account for growth and expansion of the environment. Ensure that the subnet defined provides enough unused IP addresses and that appropriate inclusion ranges are defined. Note that some of the IP addresses within the subnet will be used for other purposes, such as defining the gateway address, firewalls, or other entities. Use care not to conflict with these addresses.

Here are some important considerations for determining the size of your network pool:

- Type of network architecture
- Physical switch details
  - Are they managed or non-managed

    Do they support L3 (this may require a license)

    Number of ports
- Where the network switches are placed (at the top of the rack or at the end of a row)
- Where the default gateway is created
- Number of hosts that can be placed in each rack or L2 domain
- Number of hosts required in a cluster

- Whether the network switches will be shared with non-Cloud Foundation hosts
- Number of workload domains you plan on creating

Create a Network Pool

A network pool must include vSAN and vMotion network information. The subnet in a network pool cannot overlap the subnet of another pool.

Procedure

1. On the SDDC Manager Dashboard, click **Administration > Network Settings.**.
2. Click **Create Network Pool**.
3. Enter a name for the network pool.
4. Provide the following vSAN and vMotion network information.

   a. Enter a VLAN ID between 1 and 4094.

   b. Enter an MTU between 1500 and 9216.

   c. In the **Network** field, enter a subnet IP address.

   d. Enter the subnet mask.

   e. Enter the default gateway.

   f. Enter an IP address range from which an IP address can be assigned to hosts that are associated with this network pool.

   The IP address range must be from within the specified subnet. You cannot include the IP address of the default gateway in the IP address range. You can enter multiple IP address ranges.

   Note Ensure that you have entered the correct IP address range. IP ranges cannot be edited after the network pool is created.

5. Click **Save**.

View Network Pool Details

You can view vSAN and vMotion network details for a network pool as well as the total number of used and available IP addresses.

Procedure

1. On the SDDC Manager Dashboard, click **Administration > Network Settings**.
2. Click the arrow to the left of the pool name.

   A high-level summary of the network pool's vSAN and vMotion network information is displayed.

3 Click the name of a network pool.

Network pool details are displayed.

Edit a Network Pool

You can add an IP inclusion range to a network pool. No other parameters can be modified.

Procedure

1 On the SDDC Manager Dashboard, click **Administration > Network Settings.**.

2 Hover your mouse in the network pool row that you want to edit.

A set of three dots appear on the left of the pool name. Click these dots and then click **Edit**.

3 Enter an IP inclusion range and click **Add**.

4 Click **Save**.

Delete a Network Pool

You can delete a network pool if none of the hosts with an IP address from this pool belong to a workload domain. The default pool created during bring-up cannot be deleted.

Prerequisites

Ensure that the hosts in the network pool are not assigned to a workload domain. To verify this, navigate to **Administration > Network Settings** and confirm that the **Used IPs** for the network pool is 0.

Procedure

1 On the SDDC Manager Dashboard, click **Administration > Network Settings**.

2 Hover your mouse in the network pool row that you want to delete.

A set of three dots appear on the left of the pool name. Click these dots and then click **Delete**.

Commission a Host

Adding a host to the Cloud Foundation inventory is called commissioning. You can commission multiple hosts at a time.

The host that you want to commission must meet a set of criteria. After you specify host details and select the network pool to associate the host with, Cloud Foundation validates and commissions the host. The host is added to the free pool and is available for workload domain creation.

Prerequisites

Ensure that the hosts you are commissioning meet the following criteria.

- Host is vSAN compliant and certified on the VMware Hardware Compatibility Guide.
- Hardware health status is healthy without any errors.

- A supported version of ESXi is installed on the host. See the *VMware Cloud Foundation Release Notes* for information about supported versions.
- Host has the drivers and firmware versions specified in the VMware Hardware Compatibility Guide.
- Two NIC ports with a minimum 10 Gbps speed. One port must be free and the other port must be configured on a standard switch. This switch should be restricted to the management portgroup.
- Management IP address is configured on the first NIC port.
- SSH and syslog are enabled.
- DNS is configured for forward and reverse lookup and FQDN.
- All disk partitions on HDD and SSD are deleted.

Note You must have a network pool available in order to commission a host.

Procedure

1. On the SDDC Manager Dashboard, click **Inventory > Hosts**.
2. Click **Commission Hosts**.
3. Confirm that hosts to be commissioned meet each criterion in the checklist and select the check boxes.
4. Click **Proceed**.
5. Enter the FQDN for the host.

   The server fingerprint is displayed in the **Server Key Fingerprint** field.
6. Verify that the displayed server fingerprint is correct and click **Confirm Fingerprint**.
7. Enter the root credentials for the host.
8. Select the network pool with which you want to associate the host.
9. Click **Validate**.

   Cloud Foundation validates the host information you provided. The host is then added to the Validated Hosts table in the bottom half of the window.

   If the validation fails, edit the information as appropriate and click Validate again.
10. Repeat steps 5 - 8 for each host you want to commission.
11. Click **Commission**.

    The Hosts page appears and the status of the commission task is displayed. Click **View Status in Task** to display the task bar.

The commissioned host is added to the host table. The host belongs to a free pool until you assign it to a workload domain.

Decommission a Host

Removing a host from the Cloud Foundation inventory is called decommissioning. You can decommission a host for maintenance work or if you want to add it to another network pool. If you want to re-use a host in a different workload domain, you must decommission the host and clean it up before adding it to the workload domain.

Prerequisites

The host that you want to decommission must be in the free pool and not be assigned to a workload domain.

Procedure

1. On the SDDC Manager Dashboard, click **Inventory > Hosts**.
2. In the hosts table, click the FQDN of the host you want to decommission.
3. Click **Actions > Decommission**.
4. Click **Confirm**.

   The Hosts page appears and the status of the decommission task is displayed. Click **View Status in Task** to display the task bar.

What to do next

Clean the decommissioned host before adding it to a workload domain. See Clean up a Decommissioned Host.

Clean up a Decommissioned Host

A decommissioned host must be cleaned up before it can be assigned to a workload domain.

Prerequisites

- You must have access to Direct Console User Interface (DCUI) on the host.
- Gather the following information for the decommissioned host:
  - IP address
  - root password
  - network configuration - netmask, gateway, and DNS
  - VLAN ID

Procedure

1. Log in to the DCUI.
2. Navigate to the Troubleshooting Options page and enable ESXI shell.
3. Press Alt-F1 to get to the prompt to run command line steps.

4 Clean up vSAN with the following command.

```
#vdq -i
#esxcli vsan storage remove -s SSD Device Name
```

For example:

```
[root@esx-6:/tmp] vdq -i
[
  {
     "SSD" : "naa.55cd2e414dc36b15",
      "MD" : [
             "naa.55cd2e414d7abb5d",
             "naa.55cd2e414d7aa215",
             "naa.55cd2e414d7abb46",
             ]
  },
  {
     "SSD" : "naa.55cd2e414dc36d53",
      "MD" : [
             "naa.55cd2e414d705c35",
             "naa.55cd2e414d7aa1eb",
             "naa.55cd2e414d7abb10",
             ]
  },
]
[root@esx-6:/tmp] esxcli vsan storage remove -s naa.55cd2e414dc36b15
[root@esx-6:/tmp] esxcli vsan storage remove -s naa.55cd2e414dc36d53
[root@esx-6:/tmp] vdq -i
[
]
```

5 Reset the system configuration and the root password by running the commands below.

```
/bin/firmwareConfig.sh --reset
```

```
reboot -f
```

When you reset the configuration, the software overrides all your network configuration changes, deletes the password for the administrator account (root), and reboots the host.

6 Press Alt-F2 to return to the DCUI.

7 Reset the root password. This password was deleted during step 5.

8 Configure the following network details to the same values that were set on the host before the factory reset.

- VLAN
- Set static IPv4 address
- IP address
- netmask

   - gateway

9. Apply the changes.
10. Restart the management network by selecting the Restart Management Network option on the main DCUI page.
11. On the Troubleshooting Options page, enable SSH on the host.
12. Disable ESXi shell.

What to do next

You can now commission the host to the Cloud Foundation inventory and add it to a workload domain.

View Host Inventory

The Hosts page displays details about all the hosts in your Cloud Foundation system, including CPU utilization and memory usage across all hosts, as well as the total number of hosts used and unallocated.

For each host, the Hosts page displays the following information:

- FQDN name
- IP address
- The network pool to which the host belongs
- Current status
- Host state, or the workload domain to which it is allocated
- Cluster or more specifically, the domain cluster to which it is assigned
- Host-specific CPU and memory usage
- Storage type

The Hosts page also provides controls for commissioning hosts.

Procedure

1. From the the SDDC Manager Dashboard, navigate to **Inventory > Hosts**.

   The Hosts page appears.

2. Navigate directly to pages related to a specific host.

   For example:

   - To jump to the details page for the domain to which a listed host belongs, click the domain name link in the Host State column. For information about viewing workload domains, see View Workload Domain Details.
   - To jump to the details page for the domain cluster to which a listed host belongs, click the cluster name in the Cluster column. For information about clusters, see Expand a Workload Domain.
   - To quickly view network assignment details for a specific host, click the info icon next to the value in the Network Pool column.

3 To view the details of a specific host, click the FQDN name in the list.

The host details page appears, displaying the following information:

- A chart showing total and used CPU capacity.
- A chart showing total and used memory capacity.
- A summary of the networks (vSAN, vMotion, and Management) to which the host belongs and its IP address on those networks.
- The manufacturer and model of the host.
- Storage information including capacity and cache tiers.

Note Below the page title, the host details page also provides quick links to the network pool and the workload domain cluster to which the host belongs.

4 (Optional) To decommission the host from the host details page, click **Actions** near the page name and select **Decommission**.

For details, see Decommission a Host.

5 (Optional) To view host VM details, click **Actions** near the page name and select **Open in ESXi Client**.

The ESXi Client opens.

Working with the Management Domain and VI Workload Domains

7

The management domain and deployed workload domains are logical units that carve up the compute, network, and storage resources of the Cloud Foundation system. The logical units are groups of ESXi hosts managed by vCenter Server instances with specific characteristics for redundancy and VMware SDDC best practices.

The management domain is created by default during bring-up. The Cloud Foundation software stack is deployed on the management domain. Additional infrastructure virtual machines which provide common services, such as backup or security appliances, can be deployed in the management domain as well.

The management domain and workload domains include these VMware capabilities by default:

VMware vSphere® High Availability (HA)

This feature supports distributed availability services for a group of ESXi hosts to provide rapid recovery from outages and cost-effective high availability for applications running in virtual machines. Out of the box, Cloud Foundation provides a highly available environment for workload domains. There may be additional settings (not set by default) that can increase availability even further. For more information about vSphere HA, see the *vSphere Availability* documentation at https://docs.vmware.com/en/VMware-vSphere/.

VMware vSphere® Distributed Resource Scheduler™ (DRS)

This feature dynamically allocates and balances computing capacity across a group of hardware resources aggregated into logical resource pools or clusters. Clusters are the primary unit of operation in Cloud Foundation. DRS continuously monitors use across resource pools and allocates available resources among the virtual machines based on predefined rules that reflect business needs and changing priorities. When a virtual machine experiences an increased load, vSphere DRS automatically allocates additional resources by redistributing virtual machines among the physical servers in the resource pool. For more information about DRS, see the *vSphere Resource Management* documentation at https://docs.vmware.com/en/VMware-vSphere/.

VMware vSAN®

This component aggregates local and direct-attached storage disks in a group of ESXi hosts to create a storage pool shared across all hosts in that group. For more information about vSAN, see the *VMware vSAN* documentation at https://docs.vmware.com/en/VMware-vSAN/.

Each Cloud Foundation instance is one SSO domain to which all vCenter Servers are joined. The maximum number of supported workload domains and vCenter Servers per Cloud Foundation instance depends on the vSphere version in the management cluster. For more information, see the *Configuration Maximums vSphere* document.

Note if you use cross vCenter vMotion between two VI workload domains with dissimilar hardware, you must enable EVC on the corresponding clusters. See Enable EVC on an Existing Cluster in the vSphere product documentation.

This chapter includes the following topics:

- Adding Virtual Machines to the Management Domain
- Create a Virtual Infrastructure Workload Domain
- View Workload Domain Details
- View Cluster Details
- Expand a Workload Domain
- Reduce a Workload Domain
- Delete a Workload Domain

Adding Virtual Machines to the Management Domain

You can add virtual machines to the management domain as desired. Commonly, these virtual machines provide infrastructure services such as backup or security throughout the solution. To prevent resource conflicts between the core Cloud Foundation services, these additional virtual machines are added to the Compute-ResourcePool. This resource pool is automatically created during bring-up for this purpose.

You must be careful when adding virtual machines to the management domain. You do not want to consume excessive resources that would obstruct standard operations. Excess capacity consumption can cause failures of virtual machine fail overs in the event of a host failure or maintenance action.

You can add capacity to the management domain by adding a host(s) in order to expand the management workload domain. To expand the management domain, seeExpand a Workload Domain.

Procedure

1. On the SDDC Manager Dashboard, navigate to **Inventory > Workload Domains.**
2. In the workload domains table, click **MGMT**.
3. On the MGMT page, click the **Services** tab.
4. Click the vCenter link.

   This opens the vSphere Web Client for the management domain.

5. Create a VM.

   See *Create a New Virtual Machine* in *vSphere Resource Management*.

   Note Do not move any of the Cloud Foundation management VMs into the resource pool.

6. Move the VM to the resource pool.

   See *Add a Virtual Machine to a Resource Pool* in *vSphere Resource Management*.

   Note Do not move any of the Cloud Foundation management VMs to the newly created resource pool.

Create a Virtual Infrastructure Workload Domain

When you create a VI workload domain, Cloud Foundation deploys a vCenter Server Appliance in the management domain. It then connects the specified ESXi servers to this vCenter Server instance and groups them into a cluster. Cloud Foundation automatically configures vSAN on these ESXi hosts to provide for distributed storage. Each host is configured with the port groups applicable for the workload domain.

An NSX Manager for this workload domain is also deployed in the management domain. A set of three NSX controllers are deployed on the shared vSAN storage provided by the ESXi hosts.

By leveraging a separate vCenter Server instance per workload domain, software updates can be applied without impacting other workload domains. It also allows for each workload domain to have additional isolation as needed.

The workflow automatically:

- Deploys a vCenter Server Appliance for the new workload domain within the management domain.

  Deploys an NSX Manager for the new workload domain within the management domain.

  Creates a cluster within the vCenter Server instance and connects the specified hosts in it.

  Configures networking on each host.

  Configures the cluster for vSphere HA and DRS.

  Configures vSAN storage between all the hosts in the cluster, as per the specified level of availability.

  Deploys three NSX controllers within the newly created cluster and configures an appropriate anti-affinity rule

  Licenses and integrates the deployed components with the appropriate pieces in the Cloud Foundation software stack.

The result is a workload-ready SDDC environment.

Note You can only perform one workload domain operation at a time. For example, while creating a new workload domain, you cannot add a cluster to any other workload domain.

Prerequisites

- Gather the information that you will need during the workload domain creation workflow:
  - vCenter IP address, DNS name, subnet mask, and default gateway
  - NSX Manager IP address, DNS name, subnet mask, and default gateway
  - NSX Controller IP address, DNS name, subnet mask, and default gateway
- The IP addresses and Fully Qualified Domain Names (FQDN) for the vCenter and NSX Manager instances to be deployed for the VI Workload domain must be resolvable by DNS.
- A minimum of three hosts must be available in your Cloud Foundation inventory. For information on adding hosts to your inventory, seeChapter 6 Adding Hosts to Cloud Foundation.
- There must be a free uplink on each host to be used for the workload domain.
- You must have specified valid license keys for the following products:
  - vCenter Server
  - NSX for vSphere
  - vSAN
  - vSphere

    Since vSphere and vSAN licenses are per CPU, ensure that you have sufficient licenses for the ESXi hosts to be used for the workload domain. See Chapter 5 License Management.
- Enable vRealize Log Insight logging for workload domains. See Enable vRealize Log Insight Logging for Workload Domains.
- Decide on the following passwords:
  - vCenter root password
  - NSX Manager admin password
  - NSX Manager enable password (to enable administrator privileges for NSX Manager)

Account	Password Requirements
vCenter root	1 Length 8-20 characters 2 Must include: ■ mix of upper-case and lower-case letters ■ a number ■ a special character 3 Must not include a special character
NSX Manager admin and enable	1 Length 8-12 characters 2 Must include: ■ mix of upper-case and lower-case letters ■ a number ■ a special character ■ exclude_char

For specific password requirements, check the appropriate product documentation.

- Decide on a name for your VI workload domain. It is good practice to include region and site information in the name since resource object names (such as host and vCenter names) are generated on the basis of the VI workload domain name. The name can be three to twenty characters long and can contain any combination of the following:
  - Lowercase alphabetic characters
  - Uppercase alphabetic characters
  - Numbers
  - Hyphens
  - Underscores

  Note Spaces are not allowed in any of the names you specify when creating a VI workload domain.

Procedure

1 Specify General Information about the VI Workload Domain

Start the VI Configuration wizard and provide a name for the VI workload domain, cluster, and organization as well as and vCenter and NSX details.

2 View Object Names

The Object Names page displays the vSphere objects that will be generated for the VI workload domain. Object names are based on the VI workload domain name.

3 Select the Availability Level for the VI Workload Domain

At the Storage step of the creation wizard, specify the availability you want provisioned for the VI workload domain.

4 Select Hosts for the VI Workload Domain

The Host Selection page displays available hosts along with hosts details. Hosts that are powered off, cannot be accessed via SSH, or have not been properly commissioned are not displayed.

5 Select Licenses

The Licenses page displays the available licenses for vCenter, vSphere, vSAN, and NSX based on the information you provided.

6 Review Details and Start the Creation Workflow

At the Review step of the wizard, review the information about the workload domain and start the creation workflow. You can also print the information or download a printable version to print later. It can take up to two hours for the domain to be created.

Specify General Information about the VI Workload Domain

Start the VI Configuration wizard and provide a name for the VI workload domain, cluster, and organization as well as and vCenter and NSX details.

Prerequisites

Verify that you have met the prerequisites described in Create a Virtual Infrastructure Workload Domain.

Procedure

1 On the SDDC Manager Dashboard, click **+ Workload Domain** and then click **VI Virtual Infrastructure**.

2 Type a name for the VI workload domain, such as `sfo01`.

It is good practise to include location information in the name since resource object names (such as host and vCenter names) are generated on the basis of the VI workload domain name.

3 Type a name for the VI cluster.

4 (Optional) Type a name for the organization that requested or will use the virtual infrastructure, such as `Finance`.

5 Type the vCenter IP address, DNS name, subnet mask, and default gateway.

6 Type and re-type the vCenter root password.

7 Type the NSX Manager IP address, DNS name, subnet mask, and default gateway.

8 Type and re-type the NSX Manager Admin password.

9 Type and re-type the NSX Manager Enable password.

10 Type the NSX Controller IP address, DNS name, subnet mask, and default gateway.

11 Type and re-type the NSX Controller password.

12 Click **Next**.

View Object Names

The Object Names page displays the vSphere objects that will be generated for the VI workload domain. Object names are based on the VI workload domain name.

Procedure

1. Review the syntax that will be used for the vSphere objects generated for this domain.
2. Click **Next**.

Select the Availability Level for the VI Workload Domain

At the Storage step of the creation wizard, specify the availability you want provisioned for the VI workload domain.

Based on your selections, SDDC Manager will determine:

- The minimum number of hosts that it needs to fulfill those selections
- Which specific hosts in your environment are available and appropriate to fulfill those selections
- The virtual infrastructure features and their specific configurations that are needed to fulfill those selections

Note You can modify the vSAN configuration in vSphere without negatively affecting the Cloud Foundation configuration.

Procedure

1. Specify the level of availability you want configured for this virtual environment.

   The availability level determines the level of redundancy that is set for the assigned resources. For more information, see *Managing Fault Domains in Virtual SAN Clusters* in *Administering VMware Virtual SAN*.

Option	Description
0	With this choice, the following vSAN parameters are used: ■ Number of failures to tolerate: zero (0). Because vSAN requires a minimum of three hosts by default, three hosts are assigned to the virtual infrastructure.
1	With this choice, the following vSAN parameters are used: ■ Number of failures to tolerate: one (1). Because vSAN requires a minimum of three hosts by default, three hosts are assigned to the virtual infrastructure.
2	With this choice, the following vSAN parameters are used: ■ Number of failures to tolerate: two (2). Because vSAN requires a minimum of five hosts by default for this setting, five hosts are assigned to the virtual infrastructure.

2. Click **Next**.

Select Hosts for the VI Workload Domain

The Host Selection page displays available hosts along with hosts details. Hosts that are powered off, cannot be accessed via SSH, or have not been properly commissioned are not displayed.

- Select only healthy hosts..

  To check a host's health, SSH in to the SDDC Manager VM using the **vcf** administrative user account. Enter **su** to switch to the root user and navigate to the `/opt/vmware/sddc-support` directory and type the following command.

  ```
  ./sos --health-check
  ```

  For more information, see Chapter 11 Supportability and Serviceability (SoS) Tool

- For optimum performance, you should select hosts that are identical in terms of memory, CPU types, and disks.

  If you select unbalanced hosts, the UI displays a warning message, but you can proceed with the workload domain creation.

- You cannot select hosts that are in a dirty state. A host is in a dirty state when it has been removed from a cluster in a workload domain.

  To clean a dirty host, see Clean up a Decommissioned Host.

- All selected hosts must be associated with the same network pool.

Procedure

1. Select the hosts for creating the VI workload domain.

   The total resources based on the selected hosts are displayed. For a VI workload domain with 0 or 1 availability, a minimum of three hosts is required. For a VI workload domain with 2 availability, a minimum of five hosts is required. When you select hosts with sufficient storage to form a VI cluster, the **Next** button is enabled.

2. Click **Next**.

Select Licenses

The Licenses page displays the available licenses for vCenter, vSphere, vSAN, and NSX based on the information you provided.

Prerequisites

You must have specified valid license keys for the following products:

- vCenter Server
- vSAN
- NSX Data Center for vSphere

- vSphere

  Since vSphere and vSAN licenses are per CPU, ensure that you have sufficient licenses for the ESXi hosts to be used for the workload domain.

For information on adding license keys, see Add License Keys for the Software in Your Cloud Foundation System.

Procedure

1. Select the vCenter, vSphere, vSAN, and NSX licenses you want to apply to the VI workload domain.
2. Click **Next**.

Review Details and Start the Creation Workflow

At the Review step of the wizard, review the information about the workload domain and start the creation workflow. You can also print the information or download a printable version to print later. It can take up to two hours for the domain to be created.

The Review page displays information about the resources and their configurations that will be deployed when the workflow creates and deploys the virtual infrastructure for this workload domain.

The hosts that will be added to the workload domain are listed along with information such as the network pool they belong to, memory, CPU, and so on.

Procedure

1. Scroll down the page to review the information.
2. Click **Finish** to begin the creation process.

   The Workload Domains page appears and a notification is displayed letting you know that VI workload domain is being added. Click **View Task Status** to view the domain creation tasks and sub tasks.

   If a task fails, you can fix the issue and re-run the task. If the workload domain creation fails, contact VMware Support.

When the VI workload domain is created, it is added to the workload domains table.

View Workload Domain Details

The Workload Domains page displays high level information about the workload domains in the Cloud Foundation system. CPU, memory, and storage utilized by the workload domain is also displayed here.

Procedure

1. On the SDDC Manager Dashboard, click **Inventory > Workload Domain**.

2 In the workload domains table, click the name of the workload domain.

The domain details page displays CPU, memory, and storage allocated to the domain. The tabs on the page display additional information as described in the table below.

Tab	Information Displayed
Summary	Clusters in the workload domain and availability level for each cluster.
Services	SDDC software stack components deployed for the workload domain's virtual environment and their IP addresses. Click a component name to navigate to that aspect of the virtual environment. For example, click vCenter to reach the vSphere Web Client for that workload domain. All the capabilities of a VMware SDDC are available to you in the VI workload domain's environment, such as creating, provisioning, and deploying virtual machines, configuring the software-defined networking features, and so on.
Updates/Patches	Available updates for the workload domain. For more information, see Chapter 14 Patching and Upgrading Cloud Foundation.
Update History	Updates applied to this workload domain.
Hosts	Names, IP addresses, status, associated clusters, and capacity utilization of the hosts in the workload domain and the network pool they are associated with.
Clusters	Names of the clusters, number of hosts in the clusters, and their capacity utilization.
Security	Default certificates for the Cloud Foundation components. For more information, see Chapter 4 Managing Certificates for Cloud Foundation Components.

What to do next

You can add a cluster to the workload domain from this page.

View Cluster Details

The cluster page displays high level information about the cluster as well as the hosts that form that cluster. CPU, memory, and storage utilization for this cluster is also displayed here.

Procedure

1 On the SDDC Manager Dashboard, click **Inventory > Workload Domain**.

2 In the workload domains table, click the name of a workload domain.

3 Click the **Clusters** tab.

4 In the clusters table, click the name of a cluster.

The cluster detail page appears. The tabs on the page display additional information as described in the table below.

Tab	Information Displayed
Summary	Storage parameter configured on the cluster and organization name.
Hosts	Details about each host in the cluster. You can click a name in the FQDN column to access the host detail page.

What to do next

You can add or remove a host, or access the vSphere Client from this page.

Expand a Workload Domain

You can expand the management domain or a VI workload domain to add resources to support additional workloads or availability.

To expand a domain, you can:

- Add a host from the Cloud Foundation inventory to a cluster.

  By adding an individual host to an existing workload domain, you can expand the amount of resources contained within an existing cluster.

- Add a new cluster to a workload domain.

  As workload domains support multiple clusters, you can add an additional cluster to an existing workload domain to provide for increased capacity and VM failover isolation.

Add a Host to a Cluster in a Workload Domain

Adding an individual host to a workload domain adds the resources of that host to the workload domain. You can add multiple hosts at a time to a workload domain.

Prerequisites

- There must be a host available in the Cloud Foundation inventory. For information on adding a host to Cloud Foundation, see Commission a Host.
- Ensure that the host you want to add is in an active state.
- You must have a valid vSphere license specified in the Licensing tab of the SDDC Manager Dashboard with adequate sockets available for the host to be added. For more information, see Add License Keys for the Software in Your Cloud Foundation System.
- Verify that the host to be added to the workload domain matches the configuration of the hosts in the cluster to which you want to add the domain. This allows the cluster configuration to remain balanced. If the host to be added does not match the pre-existing hosts in the cluster, the cluster will be unbalanced and a warning will be displayed. The warning will not prevent the expansion and can be dismissed if needed.

Procedure

1. On the SDDC Manager Dashboard, click **Inventory > Workload Domains**.

   The Workload Domains page displays information for all workload domains.

2. In the workload domains table, click the name of the workload domain that you want to expand.

   The detail page for the selected workload domain appears.

3. Click the **Clusters** tab.

4. Click the name of the cluster where you want to add a host.
5. Click **Actions > Add Host**.

   The Add Hosts wizard appears.
6. Select the host you want to add to the cluster.

   The host you select must be associated with the same network pool as the other hosts in the cluster. For optimum performance, you should select hosts that are identical in terms of memory, CPU types, and disks to the other hosts in the cluster. If you select unbalanced hosts, the UI displays a warning message, but you can proceed with the workload domain creation.
7. Click **Next**.
8. Select the vSphere license you want to apply to the host.
9. Click **Next**.
10. Review the host and license details, and click **Finish**.

    The details page for the cluster appears with a message indicating that the host is being added. Wait until the action is complete before performing additional workload domain tasks.

Add a Cluster to a Workload Domain

You can add a cluster to a workload domain through the Workload Domains page in the SDDC Manager Dashboard.

Prerequisites

- There must be at least three hosts available in the Cloud Foundation inventory. For information on adding a host to Cloud Foundation, see Commission a Host.
- Ensure that the hosts you want to add to the cluster are in an active state.
- You must have a valid vSAN and vSphere license specified in the Licensing tab of the SDDC Manager Dashboard with adequate sockets available for the host to be added. For more information, see Add License Keys for the Software in Your Cloud Foundation System.

Procedure

1. On the SDDC Manager Dashboard, click **Inventory > Workload Domains**.

   The Workload Domains page displays information for all workload domains.
2. Use one of the following methods to get started.
   - From the high level workload domain page:
     a. Hover your mouse in the workload domain row that where you want to add a cluster.

        A set of three dots appear on the left of the workload domain name.

   b Click these dots and then click **Add Cluster**.

     The Add Cluster wizard appears.

- From the workload domain details page:

   a Click the name of the workload domain to go to the details page for that workload domain.

   b Click **Actions > Add Cluster.**

     The Add Cluster wizard appears.

3 Type a name for the cluster and click **Next**.

4 Review the syntax that will be used for the vSphere objects generated for this cluster and click **Next**.

5 On the Storage page, specify the level of availability you want configured for this cluster.

  The specified Failures To Tolerate (FTT) value determines the number of hosts required the cluster.

Failures To Tolerate Value	Minimum Hosts Required
0	Three
1	Three
2	Five

6 Click **Next**.

  The Host Selection page appears.

7 Select hosts for the cluster.

  All selected hosts must be associated with the same network pool. When you have selected the minimum number of hosts required for this cluster, the Next button is enabled.

8 Click **Next**.

9 On the Licenses page, select the vSAN and vSphere license to apply to this cluster.

10 Click **Next**.

11 On the Review page, review the cluster details and click **Finish**.

  The details page for the workload domain appears with the following message: `Adding a new cluster is in progress.` When this process completes, the cluster appears in the Clusters tab in the details page for the workload domain.

Reduce a Workload Domain

You can reduce a workload domain by removing a host from a cluster in the workload domain or by deleting a cluster.

Remove a Host from a Cluster in a Workload Domain

You can remove a host from a cluster in a workload domain through the Workload Domains page in the SDDC Manager Dashboard.

When a host is removed, the vSAN members are reduced. Ensure that you have enough hosts remaining to facilitate the configured vSAN availability. Failure to do so might result in the datastore being marked as read-only or in data loss.

Procedure

1. On the SDDC Manager Dashboard, click **Inventory > Workload Domains**.

   The Workload Domains page displays information for all workload domains.

2. In the workload domains table, click the name of the workload domain that you want to modify.

   The detail page for the selected workload domain appears.

3. Click the **Clusters** tab.

4. Click the name of the cluster from which you want to remove a host.

5. Select the host to remove and click **Remove Selected Hosts**.

   An alert appears, asking you to confirm or cancel the action. If the removal results in the number of hosts in the cluster being less than the minimum number of required hosts, you must click **Force Remove** to remove the host.

6. Click **Remove** to confirm the action.

   The details page for the cluster appears with a message indicating that the host is being removed. When the removal process is complete, the host is removed from the hosts table.

The host is removed from the workload domain and added to the free pool.

What to do next

Clean up the host so that you can use it again. See Clean up a Decommissioned Host.

Delete a Cluster from a Workload Domain

You can delete a cluster from a workload domain. Datastores on the ESXi hosts in the deleted cluster are destroyed

You cannot delete the last cluster in a workload domain. Instead, delete the workload domain. See Delete a Workload Domain.

Prerequisites

Migrate or backup the VMs and data on the data store associated with the cluster to another location.

Procedure

1 On the SDDC Manager Dashboard, click **Inventory > Workload Domains**.

The Workload Domains page displays information for all workload domains.

2 Click the name of the workload domain that contains the cluster you want to delete.

3 Click the **Clusters** tab to view the clusters in the workload domain.

4 Hover your mouse in the cluster row you want to delete.

5 Click the three dots next to the cluster name and click **Delete Cluster**.

6 Click **Delete Cluster** to confirm that you want to delete the cluster.

The details page for the workload domain appears with a message indicating that the cluster is being deleted. When the removal process is complete, the cluster is removed from the clusters table.

Delete a Workload Domain

When you delete a workload domain, the clusters within that workload domain are deleted and the hosts are returned to the free pool.

Monitoring through Log Insight and vRealize Operations is removed and the components associated with the workload domain to be deleted contained within the management domain are removed. This includes the vCenter Server instance and NSX Manager.

The network pools used by the workload domain are not deleted as part of the workload domain deletion process and must be deleted separately.

Caution Deleting a workload domain is an irreversible operation. All clusters and VMs within the workload domain are deleted and the underlying datastores are destroyed.

It can take up to 20 minutes for a workload domain to be deleted. During this process, you cannot perform any operations on workload domains.

Prerequisites

- Back up the data on the workload domain. The datastores on the workload domain are destroyed when the workload domain is deleted.
- Migrate the VMs that you want to keep to another workload domain.

Procedure

1 On the SDDC Manager Dashboard, click **Inventory > Workload Domains**.

The Workload Domains page displays information for all workload domains.

2 Hover your mouse in the workload domain row that where you want to delete.

When you select the workload domain, three vertical dots appear next to the name.

3 Click the dots and choose **Delete Domain**.

A confirmation window appears with details about the impact of deleting the workload domain, including how many hosts will be returned to the free pool.

4 Click **Delete Domain** to proceed.

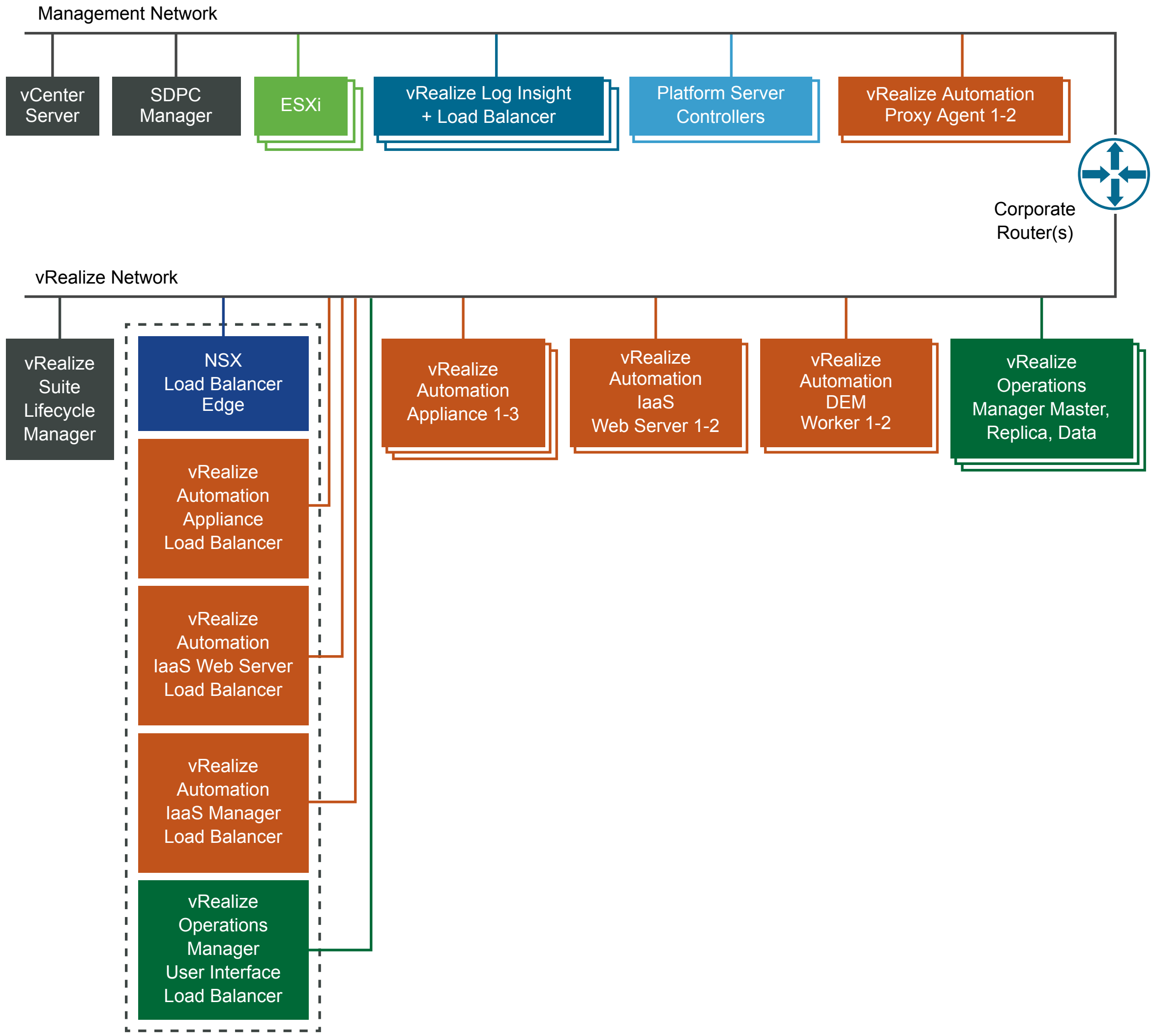
The details page for the workload domain appears with a message indicating that the workload domain is being deleted. When the removal process is complete, the workload domain is removed from the domains table.

Adding vRealize Components to Cloud Foundation 8

In SDDC Manager, you can deploy vRealize Operations and vRealize Automation as Cloud Foundation components. You can also enable vRealize Log Insight directly in the SDDC Manager Dashboard.

All vRealize Suite products require separately purchased licenses.

Figure 8-1. vRealize Suite Components in the Cloud Foundation Context


Management Network
vCenter Server
SDPC Manager
ESXi
vRealize Log Insight + Load Balancer
Platform Server Controllers
vRealize Automation Proxy Agent 1-2
Corporate Router(s)
vRealize Network
vRealize Suite Lifecycle Manager
NSX Load Balancer Edge
vRealize Automation Appliance Load Balancer
vRealize Automation IaaS Web Server Load Balancer
vRealize Automation IaaS Manager Load Balancer
vRealize Operations Manager User Interface Load Balancer
vRealize Automation Appliance 1-3
vRealize Automation IaaS Web Server 1-2
vRealize Automation DEM Worker 1-2
vRealize Operations Manager Master, Replica, Data

1 Deploy vRealize Automation in Cloud Foundation

You can deploy and manage vRealize Automation in SDDC Manager.

2 Working with vRealize Operations in Cloud Foundation

   SDDC Manager helps automate the deployment of vRealize Operations within Cloud Foundation.

3 Connect vRealize Suite Components to Workload Domains

   You can connect your vRealize Automation and vRealize Operations deployments to workload domains.

Deploy vRealize Automation in Cloud Foundation

You can deploy and manage vRealize Automation in SDDC Manager.

Prerequisites

- Verify that you have downloaded the vRealize Suite install bundle. This is obtained separately from the Cloud Foundation build. See Download Install Bundle from the the SDDC Manager Dashboard.
- Verify that you have created an Active Directory (AD) account.

  You must create an AD user account with permission to add computer accounts and to join Windows VMs to the domain. This account is used to install and run the management agents and IaaS components for the vRealize Automation infrastructure, including proxy agents.
- Verify certificate and private key.

  You must have a multi-SAN certificate and private key generated by a trusted certificate authority. During generation, you must specify the FQDN values of all vRealize Automation VMs and load balancer servers.
- Verify that IP allocation and forward/reverse DNS records are prepared for the following components:
  - All vRealize Automation virtual appliances and vRealize Automation IaaS virtual machines.
  - vRealize Suite Lifecycle Manager virtual appliance. This is required only if you have not previously configured as part of deploying vRealize Operations in Cloud Foundation.
  - All vRealize Suite load balancer VMs. This is required only if you have not previously configured as part of deploying vRealize Operations in Cloud Foundation.
- Verify that Microsoft SQL Server is configured properly.

  You must join the Microsoft SQL Server VM to the Active AD, create a new login for the AD administrative user in SQL Server, modify the firewall and port configuration, and create the SQL database.

  Note For more information about the SQL Server configuration prerequisites, see Configure Microsoft SQL Server for vRealize Automation in Cloud Foundation.
- Verify that you have an IaaS Windows template (OVA) for the vRealize Automation Windows VM, using Microsoft Windows Server 2012 R2 or Windows Server 2016 Standard Edition.

  For details about preparing this OVA template, see Prepare the vRealize Automation Windows VM OVA Template.

- Verify that you have a valid license key for vRealize Automation, which is purchased separately from Cloud Foundation.
- Verify that the vRealize Network VLAN is configured on the switches. The vRealize subnet is routable to the Management network. The firewall between the Management and vRealize networks should be disabled, or configured per the Cloud Foundation documentation.

  Important Microsoft SQL Server should be deployed in the vRealize Network in order to enable replication. If it is not deployed on vRealize network the replication should be perforemd by user. If Microsoft SQL Server is not in the vRealize Network, you must configure the to allow from vRealize Suite VMs to access it.

Procedure

1. On the SDDC Manager Dashboard, navigate to **Administration > vRealize Suite**.

   The vRealize navigation bar appears, listing the vRealize products available to your Cloud Foundation deployment.

2. Click **vRealize Automation**.

   The vRealize Automation splash page displays.

3. Click **Deploy**.

   The Installation Prerequisites page displays the prerequisites you must complete before beginning the installation.

4. Verify the readiness of each prerequisite by selecting the adjacent check box.

   When each check box is selected, it turns green. When all the boxes are selected, the **Begin** button at the bottom of the page is activated.

5. Click **Begin**.

   The vRealize Automation Installation wizard opens.

6. Complete the Deployment Details settings to begin the installation.

   All settings are required.

Setting	Description	
IAAS Windows Template	Select one of the following options from the drop-down menu.	
	Upload OVA Template	Select to upload a new template. Click **Upload** to navigate to and upload the template. The OVA template name should be less than 60 characters in length, including the extension.
	Use Existing OVA Template	Select to use and specify an existing OVA template. The Windows OVA Template path automatically displays the path to the existing template, if any.
vRealize Automation License	**License Key**	Enter your vRealize Automation license key.
Certificate Details	**Certificate Chain**	Enter the two-part certificate chain, including both `-----BEGIN CERTIFICATE-----` headers and both `-----END CERTIFICATE-----` footers.
	Certificate Private Key	Enter a private key for the certificate, including the `-----BEGIN RSA PRIVATE KEY-----` header and the `-----END RSA PRIVATE KEY-----` footers.
	Certificate Passphrase	Enter a passphrase for the certificate protection on the vRealize AutomationIaaS Windows servers.

7 Click **Next** to complete the Hostnames settings.

Note All settings are required.

Setting	Description	
vRealize Automation Appliances	**Appliance 1**	Enter the FQDN hostname as it appears in the SAN certificate.
	Appliance 2	Enter the FQDN hostname as it appears in the SAN certificate.
	Appliance 3	Enter the FQDN hostname as it appears in the SAN certificate.
IaaS Web Servers	**IaaS Web Server 1**	Enter the FQDN hostname as it appears in the SAN certificate.
	IaaS Web Server 2	Enter the FQDN hostname as it appears in the SAN certificate.
IaaS Manager Service and DEM Orchestrators	**IaaS Manager 1**	Enter the FQDN hostname as it appears in the SAN certificate.
	IaaS Manager 2	Enter the FQDN hostname as it appears in the SAN certificate.

Setting	Description
DEM Workers	**DEM Worker 1** Enter the FQDN hostname. **DEM Worker 2** Enter the FQDN hostname.
Proxy Agents	**Proxy Agent 1** Enter the FQDN hostname. **Proxy Agent 2** Enter the FQDN hostname.
vRealize Suite Lifecycle Manager	**Hostname** Provide the FQDN for the vRealize Suite Lifecycle Manager.
Load Balancers	When you deploy vRealize Automation, an NSX edge with four load balancers is automatically created. **NSX Edge** Enter the FQDN hostname. **IaaS Web Server** Enter the FQDN hostname as it appears in the SAN certificate. **IaaS Manager** Enter the FQDN hostname as it appears in the SAN certificate. **vRealize Automation Appliance** Enter the FQDN hostname as it appears in the SAN certificate.
DNS	This field displays the IP address of the external DNS server you specified part of the Cloud Foundation bringup process. This DNS server is used for all vRealize Suite management nodes in Cloud Foundation. It must also be able to resolve all service records used during installation.
NTP	This field displays the IP address of the external NTP server you specified part of the Cloud Foundation bringup process. This NTP server is used for all vRealize Suite nodes in Cloud Foundation.
Microsoft SQL Server	**Hostname** Provide the FQDN for the Microsoft SQL Server virtual appliance. **Note** See Configure Microsoft SQL Server for vRealize Automation in Cloud Foundation.

8 Click **Next** to complete the Account Information settings.

9 Complete the following settings to continue the installation.

All settings are required.

Setting	Description
Active Directory	Use these settings to provide the service account that is used for services on the IaaS VMs. This account must have administrative permissions to join Windows VMs to Active Directory. **Username** Provide the service account user name in the "domain\username" format. **Password / Confirm Password** Provide and confirm a valid password.
Microsoft SQL Server	Use these settings to create the connection to the database. **Database Name** Specify the case-sensitive database name. **Username** Specify the database owner user name. This setting is optional. If no user name is specified, Cloud Foundation applies the the Active Directory account used when the database was joined to Active Directory. **Password / Confirm Password** Provide and confirm a valid password for the specified user. This is required only if you also provide a username, as described above.
Local Tenant Administrator	Use these settings to define the administrative user for the default vRealize Automation tenant. **First Name** Enter the administrator's first name. **Last Name** Enter the administrator's last name. **Email** Enter the administrator's email. **Username** Define a user name for the tenant administrator. **Password / Confirm Password** Define and confirm a password for the tenant administrator.
Windows Template Local Administrator	**Password / Confirm Password** Define the local administrator password for the Windows system that is deployed through the Windows IaaS VM template.
Default Tenant Administrator	**Password / Confirm Password** Provide and confirm the password for the vRealize Automation system administrator. This is the credential that allows SDDC Manager to connect to the vRealize Automation system.
vRealize Suite Lifecycle Manager System Administrator	**Password / Confirm Password** Provide and confirm the password for the vRealize Suite Lifecycle Manager system administrator (for example, admin@localuser). This is the credential that allows SDDC Manager to connect to the vRealize Suite Lifecycle Manager system.

Setting	Description	
vRealize Automation SSH Root Account	**Password / Confirm Password**	Define and confirm a password for the vRealize Automation virtual appliance root account.
vRealize Suite Lifecycle Manager SSH Root Account	**Password / Confirm Password**	Define and confirm a password for the vRealize Suite Lifecycle Manager virtual appliance root account.

10. Click **Next** to complete the vRealize Network settings.

    If you completed this VLAN configuration when deploying vRealize Operations, you can skip this step. See Deploy vRealize Operations in Cloud Foundation.

Setting	Description
VLAN ID	Enter a valid VLAN ID between 0 and 4096.
Subnet Mask	Provide a valid address for the dedicated VLAN subnet mask.
Gateway	Provide a valid gateway.

11. Click **Next** to review a summary of the installation configuration.

    This page also displays any validation errors that require correction. If necessary, you can use the **Back** button to return to preceding pages to modify your settings.

    Note You can also proceed without validation.

12. Click **Finish**.

    The vRealize Automation splash page displays with the following message: `Deployment in progress.` If the deployment fails, this page displays a deployment status of Failed. In this case, you can **Retry** or **Uninstall**.

    Important If you elect to uninstall, be aware that the uninstall operation does not remove the computer accounts from AD. As a result, this could cause future reinstallation operations to fail. It is recommended that you manually remove the computer accounts from AD , and delete and rebuild the SQL Server database. See Configure Microsoft SQL Server for vRealize Automation in Cloud Foundation.

13. (Optional) To view the details of the deployment in progress or if it fails, click **View Status in Tasks**.

    The Tasks panel opens at the bottom page. You can open individual tasks to view details.

14. (Optional) Go directly to your vRealize Automation system by clicking the vRealize Automation link directly below the page title.

    The vRealize Automation interface opens in a new browser tab.

After vRealize Automation successfully deploys in your Cloud Foundation environment, the **SDDC Manager > Administration > vRealize Suite > vRealize Automation** page displays an ACTIVE status and displays controls that enable you to connect workloads to vRealize Automation.

What to do next

You must manually start the vRealize Orchestrator configuration service. See Start the vRealize Orchestrator Configuration Service.

Start the vRealize Orchestrator Configuration Service

After deploying vRealize Automation in Cloud Foundation, you must manually start the vRealize Orchestrator configuration service to access the vRealize Orchestrator configuration interface.

Procedure

1 Start the vRealize Orchestrator Configuration service.

   a Log in to the vRealize Automation appliance Linux console as root.

   b Enter `service vco-configurator start` and press Enter.

2 Connect to the vRealize Automation URL in a Web browser.

3 Click **vRealize Orchestrator Control Center**.

   You are redirected to https://*vra-va-hostname.domain.name_or_load_balancer_address*:8283/vco-controlcenter.

4 Log in to the vRealize Orchestrator Control Center.

   The user name is configured by the vRealize Automation appliance administrator.

Configure Microsoft SQL Server for vRealize Automation in Cloud Foundation

One of the prerequisites for installing vRealize Automation in Cloud Foundation is configuring Microsoft SQL Server. Specifically, you must join the SQL Server VM to Active Directory, create a new administrative user for SQL Server access, and create the SQL database.

Prerequisites

- Microsoft SQL Server

  For a complete list of supported versions, see the vRealize Automation Support Matrix (PDF).

- Active Directory

- Verify that you have the administrative permissions necessary to make configuration changes to both Active Directory and Microsoft SQL Server.

Procedure

1 For Microsoft SQL Server, configure a firewall exception on port 1433.

2 Join the Microsoft SQL Server VM to Active Directory.

   a In the Computer Name/Domain Changes screen, select the domain and enter the domain name.

   b Click **OK**.

   c Specify the credentials and reboot the VM to apply the new settings.

3 Enable Microsoft Distributed Transaction Coordinator (MSDTC) on the Microsoft SQL Server VM.

   a Open the Component Services manager and click **Run**.

   b Enter `comexp.msc` in the **Open** field, and click **OK.**

   c In the navigation tree, select **Component Services > Computers > My Computer > Distributed Transaction List > Local DTC**.

   d Right-click **Local DTC** and choose **Properties** to open the **Local DTC Properties** dialog box.

   e Click the **Security** tab and select the following options:

      - Network DTC Access
      - Allow Remote Clients
      - Allow Inbound
      - Allow Outbound

   f Click **OK**.

4 Create the vRealize Automation database login.

   a Open SQL Server Management Studio and connect to the SQL server instance.

   b Navigate to the **Security > Logins** page, and select **New Login**.

   c Select the **General** tab and enter the service user name (for example, `rainpole\svc-vra`) in the **Login Name** field.

   d Select the **Server Roles** tab and select the **sysadmin** option, and click **OK**.

5 Create an empty database for vRealize Automation.

   a Open SQL Server Management Studio and connect to the SQL server instance.

   b In the Object Explorer, right-click **Databases** and choose **New Database**.

   c The New Database dialog box, select the **General** tab and enter the database name, for example, `vRA`.

   d Set database owner to the same value as the service user name, for example `svc-vra` e Select the **Options** tab and configure the following settings:

- Set Recovery Model option to `Simple`.
- Under **Other options**, change the **Allow Snapshot Isolation** option to **true**.
- Under **Other options**, change the **Is Read Committed Snapshot On** option to **true**.

f Click **OK**.

Prepare the vRealize Automation Windows VM OVA Template

To manage IaaS nodes and to meet the prerequisites for deploying vRealize Automation in Cloud Foundation, you must prepare an IaaS template VM for the vRealize Automation Windows VM.

Creating this OVA template is one of the prerequisites for deploying vRealize Automation in your Cloud Foundation system, as described in Deploy vRealize Automation in Cloud Foundation.

Prerequisites

- Verify that you have available a Windows VM with the following configuration:

Attribute	Value	
Operating System	Microsoft Windows Server 2012 R2 or Windows Server 2016 Standard Edition.	
Virtual CPU	Two	
Memory	8 GB	
Disk	50 GB LSI	
Network	VMXNET3	
Other	**Browser**	In Internet Explorer, disable the Enhanced Security Configuration feature.
	Remote Desktop	Enable remote desktop connections.

  This VM will serve as the Windows system for vRealize Automation IaaS nodes.

- Verify that this server is not joined to Active Directory.
- Verify that you can access and download Java Runtime Environment (JRE) executable: `jre-8u171-windows-x64.exe` or later version.
- Verify that you can access and download the `IaaS-Prerequisites.zip` and `mstdc-installer.bat` files from http://ftpsite.vmware.com/download/rlspsrl/ISBU-Toolkit/deployment-prerequisites/IaaS-prerequisites.zip.

Procedure

1 On the Windows VM, start and log in to the Powershell console as administrator.

   a Set the execution policy.

   ```
   Set-ExecutionPolicy Unrestricted
   ```

   b Disable User Account Control (UAC).

   ```
   Set-ItemProperty -Path ‘HKLM:\Software\Microsoft\Windows\CurrentVersion\Policies\System’ /
        -Name ‘EnableLUA’ 0
   ```

   c Disable IPv6.

   ```
   Set-ItemProperty -Path‘HKLM:\System\CurrentControlSet\Services\TCPIP6\Parameters’ /
        -Name 'DisabledComponents' -Value 0xff
   ```

2 Download and install JRE version 1.8 or later on the Windows VM.

   Note The Window VM in this deployment was tested with JRE `jre-8u171-windows-x64.exe`. Use this or a later version.

3 Configure JAVA_HOME on the Windows VM.

   a Click **Start** and enter **`sysdm.cpl`** to open the System Properties dialog box.

   b Select the **Advanced** tab and click **Environment Variables**.

   c Under System Variables, click **New** and configure the following:

   - For variable name, specify **`JAVA_HOME`**.
   - For variable value, specify **`C:\Program Files\Java\jre1.8.0_171`** (depending on your JRE version).

   d Click **OK**.

4 While still in the System Properties dialog box, add the new JRE installation folder to the path environment variable.

   a Under System Variables, locate the Path variable and click **Edit**.

   b Append the following to the path: **`C:\Program Files\Java\jre1.8.0_171\bin`** and click **OK**.

   c Click **OK** until you exit the System Properties dialog box.

5 Validate the JRE version by running the following command in a command prompt.

   ```
   java.exe -version
   ```

6 Install the vRealize Automation IaaS prerequisites checker.

   a Obtain and copy the `IaaS-Prerequisites.zip` file to the Windows VM.

   b Extract the contents of the `IaaS-Prerequisites.zip` to the `C:\prerequisites` directory.

   c In a command prompt, go to the `C:\prerequisites\IaaS-prerequisites` folder and run the IaaS prerequisites script:

   ```
   cd C:\prerequisites\IaaS-prerequisites
   IaaS-prerequisites.bat
   ```

7 Obtain and prepare the `mstdc-installer.bat` file.

   a Copy the `mstdc-installer.bat` file from the Cloud Foundation bundle to the `C:\prerequisites` directory on the Windows VM.

   b In text editor, open and edit the `mstdc-installer.bat` file.

   c Add the following line to the end of the file:

   ```
   net localgroup administrators <rainpole>\<svc-vra> /add
   ```

   where **`<rainpole>`** and **`<svc-vra>`** match the service account used in your Cloud Foundation deployment.

   d Save and close the `mstdc-installer.bat` file.

8 On the Windows VM, enable secondary log-in with an automatic start-up type.

   a Open the Services panel in Windows (**Start > Services**) and right-click **Secondary Logon** and select **Properties**.

   b Change the Startup type setting to **Automatic**.

   c Click **OK** to exit the Properties dialog box.

9 Reboot the Windows VM.

10 Disable the Microsoft Distributed Transaction Coordinator (MSDTC) service.

   a In a command prompt, run `dcomcnfg`.

   b From the left panel of the resulting dialog box, right-click **Local DTC** and select **Properties**.

   c Deselect the **Enable MSDTC** check box.

   d Click **OK** and exit from the dialog box.

11 Verify that the vRealize Automation IaaS prerequisites checker is working correctly.

   a Open the `C:\prerequisites\IaaS-prerequisites` folder you created earlier and double-click the `PrereqChecker.exe` file.

   b When the application opens, deselect the **Database** option and click **Run Checker**.

c If the check is working correctly, it will return the following:

- WCF Activation shows an Error icon.
- MSDTC shows a Warning icon.
- SeBatchLogonRight shows an Error icon.

d If you do not receive the correct results, follow the instructions in the checker to correct them.

12 Using the previously established **`svc-vra`** user account, join the newly configured Windows VM to the Active Directory domain.

13 After joining, verify that there are no Active Directory group policies that will change the UAC or firewall configuration.

Note The newly joined VM should remain with UAC and firewall disabled. If not, you must disable the group policy that enforces a firewall or UAC enforcement on the domain network when a new VM joins the Active Directory.

14 Add the vRealize Automation Service Account to the Local Administrators group (set as **`svc-vra`** in previous examples).

15 Log in using the vRealize Automation Service Account.

16 Verify the proxy server configuration.

If the configuration is enabled, VMs from the vRealize network must be able to access the proxy server. As an alternative, you can configure direct communication in **Control Panel > Internet Settings** and configure no proxy.

Caution Do not activate the Windows operating system on the VM or run `sysprep` or `generalise` on it before making it a template.

17 Shut down the VM and export as OVA file.

```
ovftool --noSSLVerify
vi://'administrator@vsphere.local':'<VC_Password>'@<VC_IP_or_FQDN>/<datacenter_name>/vm/<VM_name> \
<IAAS_template_Name>.ova
```

Working with vRealize Operations in Cloud Foundation

SDDC Manager helps automate the deployment of vRealize Operations within Cloud Foundation.

This section describes the vRealize Operations deployment process, and shows you how to use vRealize Operations to monitor and collect data on workload domains.

Deploy vRealize Operations in Cloud Foundation

You can deploy and manage vRealize Operations in SDDC Manager.

Prerequisites

- Verify that you have downloaded the vRealize Suite update bundles from the depot. See GUID-DB78E842-F39E-41EF-A2AB-8E38285795F4#GUID-DB78E842-F39E-41EF-A2AB-8E38285795F4. These are obtained separately from the Cloud Foundation installation download.
- Verify that you have a valid license key for vRealize Operations, which is purchased separately from Cloud Foundation.
- Verify that IP allocation and forward/reverse DNS records are prepared for the following components:
  - All vRealize Operations nodes.
  - vRealize Suite Lifecycle Manager virtual appliance. This is required only if you have not previously configured this as part of deploying vRealize Automation in Cloud Foundation.
  - The vRealize Suite load balancer VM. This is required only if you have not previously configured this as part of deploying vRealize Automation in Cloud Foundation.
- Verify that the vRealize Network is configured on the switches. The vRealize subnet is routable to the Management network. The firewall between the Management and vRealize networks should be disabled.

Procedure

1 On the SDDC Manager Dashboard, navigate to **Administration > vRealize Suite**.

The vRealize navigation bar appears, listing the vRealize products available to your Cloud Foundation deployment.

2 Click **vRealize Operations**.

The **vRealize Operations** splash page displays.

3 Click **Deploy**.

The vRealize Operations installation wizard opens, displaying the Deployment Details panel.

4 Complete the following settings to start the installation.

Setting	Description
License Key	Enter a valid vRealize Operations license key.
High Availability	Optionally, move the button to green to deploy vRealize Operations with high availability configured.

Setting	Description
Node Size	Select a node size based on your specific requirements. **Note** If you enable the High Availability option, you must specify a node size of medium or larger.
Node Count	Specify the number of desired nodes, including all nodes in the deployment. **Note** If you selected the High Availability option, you must specify at least two nodes. For example, if you specify three nodes, the nodes will be: ■ With high availability selected: ■ Master node ■ Replica node ■ Data node ■ Without high availability selected: ■ Master node ■ Data node 1 ■ Data node 2

Note The node size limits the number of nodes you can specify. For sizing guidelines, see the Knowledge Base article vRealize Operations Manager 6.6 and 6.6.1 Sizing Guidelines.

5 Click **Next** to complete the Hostname configuration settings.

Note All settings are required.

Setting	Description	
Load Balancers	**NSX Edge**	Enter the FQDN for the NSX Edge load balancer VM. The initial NSX Edge load balancer is automatically created to balance the nodes in the analytics cluster.
	vRealize Operations	Enter the FQDN for the vRealize Operations VM.
vRealize Operations Nodes	**Node 1**	Enter the FQDN.
	Node 2	Enter the FQDN.
	Node 3	Enter the FQDN.
	Node 4	Enter the FQDN.
vRealize Lifecycle Manager	**vRealize Lifecycle Manager**	Enter the FQDN as it appears in the SAN certificate.

Setting	Description
DNS	This field displays the IP address of the external DNS server you specified as part of the Cloud Foundation bringup process. This DNS server will be used for all vRealize Suite management nodes in Cloud Foundation.
NTP	This field displays the IP address of the external NTP server you specified as part of the Cloud Foundation bringup process. This NTP server will be used for all vRealize Suite nodes in Cloud Foundation.

6 Click **Next** to move to the Account Information configuration settings.

Note All settings are required.

Setting	Description	
vRealize Operations Systems Administrator	**Password / Confirm Password**	Provide and confirm the password for the vRealize Automation system administrator. This is the credential that allows SDDC Manager to connect to the vRealize Operations system.
vRealize Suite Lifecycle Manager System Administrator	**Password / Confirm Password**	Provide and confirm the password for the vRealize Suite Lifecycle Manager system administrator (for example, admin@localuser). This is the credential that allows SDDC Manager to connect to the vRealize Suite Lifecycle Manager system. This same credential is also used for the vRealize Operations virtual appliance root account.
vRealize Suite Lifecycle Manager SSH Root Account	**Password / Confirm Password**	Define and confirm a password for the vRealize Suite Lifecycle Manager virtual appliance root account.

7 Click **Next** to complete the vRealize Network settings.

If you completed this VLAN configuration when deploying vRealize Automation, you can skip this step. See Deploy vRealize Automation in Cloud Foundation.

Setting	Description
VLAN ID	Enter a valid VLAN ID between 0 and 4096.
Subnet Mask	Provide a valid address for the dedicated VLAN subnet mask.
Gateway	Provide a valid gateway.

8 Click **Next** to move to the Review Summary page.

9 Review the deployment configuration settings, and click **Finish** to accept the configuration or **Back** to modify any settings.

When you click **Finish**, you are returned to the **vRealize Operations** splash page. A status message is displayed near the top of the page, indicating that the deployment is in progress.

If the deployment fails, this page displays a deployment status of Failed and prompts you to uninstall.

Click **Uninstall** to return to the splash page. Confirm your configuration settings, and retry the deployment operation.

10 (Optional) To view the details of the deployment in progress or if it fails, click **View Status in Tasks**.

The Tasks panel opens at the bottom page. You can open individual tasks to view details.

11 (Optional) Go directly to your vRealize Operations system by clicking the vRealize Operations link directly below the page title.

The vRealize Operations interface opens in a new browser tab.

After vRealize Operations successfully deploys in your Cloud Foundation environment, the **SDDC Manager Dashboard > Administration > vRealize Suite > vRealize Operations** page displays an ACTIVE status. The **Connect Workload Domains...** controls are now activated, enabling you to connect workload domains to vRealize Operations.

Configure SSL Passthrough for vRealize Operations Manager

By default, the vRealize Operations Manager node's load balancer is configured for SSL Termination. If you plan to use a custom certificate with vRealize Operations Manager, it is recommended that you replace the certificate on the vRealize Operations Manager cluster and configure the load balancer for SSL Passthrough.

Prerequisites

Verify that you have successfully replaced the vRealize Operations Manager certificate using the workflow described in Chapter 4 Managing Certificates for Cloud Foundation Components.

Procedure

1 Log in into the management vCenter Server and navigate to **Home > Networking & Security**.

2 Select **NSX Edges** in the Navigator.

3 Confirm that the IP address in the **NSX Manager** field is identical to he IP address for the NSX Manager for the management domain in Cloud Foundation.

4 Double-click the NSX Edge labeled **vrealize-edge**.

5 Select the **Manage** tab, then the **Load Balancer** tab.

6 Open **Application Profiles**.

7 Find and click the profile named **vrops-https**, and click **Edit**.

8 Select **Enable SSL Passthrough** and click OK to complete the configuration.

Connect vRealize Suite Components to Workload Domains

You can connect your vRealize Automation and vRealize Operations deployments to workload domains.

When connected, vRealize Automation and vRealize Operations monitor and collect data on workload domain nodes.

By default, the management workload domain is connected to vRealize Operations. You can also enable log collection by enabling vRealize Log Insight within SDDC Manager.

Note You can only create one connection at a time.

Important If you enable a connection between vRealize Automation and a workload domain, and then complete the connection wizard, you cannot disable the connection.

Prerequisites

- Verify that one or more workload domains has been created and are running.
- Verify that vRealize Automation and vRealize Operations are deployed and running in Cloud Foundation.

Procedure

1 Connect vRealize Suite Products to Workload Domains

You can connect your vRealize Suite deployments to your workload domains.

2 Connecting Workload Domains to vRealize Suite Products

You can connect your workload domains to your vRealize Automation and vRealize Operations deployments.

3 Enable vRealize Log Insight in Cloud Foundation

You can connect vRealize Log Insight directly to your workload domains in the SDDC Manager Dashboard.

Connect vRealize Suite Products to Workload Domains

You can connect your vRealize Suite deployments to your workload domains.

Procedure

1 On the SDDC Manager Dashboard, navigate to **Administration > vRealize Suite**.

2 To connect your vRealize Automation deployment to workload domains:

   a Select **Administration > vRealize Suite > vRealize Automation**.

   b Under Connect Workload Domains..., click **Connect**.

   The Connect to Workload Domains wizard opens to the Modify Connection page. This page lists all currently configured workload domains and enables you to connect vRealize Automation to each one.

3 To connect your vRealize Operations deployment to workload domains:

   a On the SDDC Manager Dashboard, navigate to **Administration > vRealize Suite > vRealize Operations**.

   b Under Connect Workload Domains..., click **Connect**.

   The Connect to Workload Domains wizard opens to the Modify Connection page. This page lists all currently configured workload domains and enables you to connect vRealize Operations to each one.

4 Select **Enable** for the desired workload domains.

5 As prompted, provide the log-in credentials for the Active Directory, and click **Next**.

6 Review the connection and click **Finish**.

Important If you enable a connection between vRealize Automation and a workload domain, and then complete the connection wizard, you cannot disable the connection.

7 (Optional) Confirm the modified connection in vRealize Operations or vRealize Automation Manager.

   a On the vRealize Operations or vRealize Automation page, click the product name link below the page title.

   The vRealize Operations or vRealize Automation Manager opens to the Home page.

   b Navigate to **Administration > Solutions**.

   The Solutions page shows the status of adapters for solutions connected to vRealize Operations. When successfully connected, the status reads `Data Receiving`.

   Note You may need to refresh the Solutions page several times for the status to update.

Connecting Workload Domains to vRealize Suite Products

You can connect your workload domains to your vRealize Automation and vRealize Operations deployments.

Procedure

1 In the SDDC Manager Dashboard, click **Inventory > Workload Domains**.

The Workload Domains page displays information for all workload domains.

2. Select the **Security Tab**.
3. Click **Connect to vRealize Products**.

   The Connect to vRealize Products wizard opens to the Modify Connection page. This page lists all currently configured workload domains and enables you to connect workload domains to either your vRealize Automation or vRealize Operations deployments.
4. Select **Enable** for the desired workload domain.
5. As prompted, provide the log-in credentials for the vRealize Suite product Active Directory, and click **Next**.
6. Review the connection and click **Finish**.

   Important If you enable a connection between vRealize Automation and a workload domain, and then complete the connection wizard, you cannot disable the connection.

Enable vRealize Log Insight in Cloud Foundation

You can connect vRealize Log Insight directly to your workload domains in the SDDC Manager Dashboard.

Once enabled, you cannot disable the connection to vRealize Log Insight. All subsequently created workload domains will automatically connect and send their logs to vRealize Log Insight.

Prerequisites

- Verify that you have a valid vRealize Log Insight license.

  You can view your license in the vRealize Log Insight interface by navigating to **Management > License**.
- Verify that you have a running vRealize Log Insight instance.

Procedure

1. On the SDDC Manager Dashboard, navigate to **Administration > vRealize Suite**.

   The vRealize navigation bar appears, listing the vRealize products available to your Cloud Foundation deployment.
2. Click **vRealize Log Insight**.

   The vRealize Log Insight splash page displays. The top portion of the page indicates if the connection has already been enabled by showing `Active` under the page title. In the case it is not, the Enable button is active. The lower portion of the page displays the configuration details, including load balancer hostname, node size, and node count.
3. Click **Enable**.

   After a moment, the page redisplays with a message indicating the success or failure of the action. This message includes a link to View Status in Tasks, which can provide detail for troubleshooting in case the action fails.

4 (Optional) Jump to the vRealize Log Insight interface to view Cloud Foundation logs.

Click the **vRealize Log Insight** link directly below the page title. You may need to log in the first time you access a new session. In vRealize Log Insight, navigate to the **VMware - VCF** page.

If successful, vRealize Log Insight is now connected to, and collecting logs from, your management and workload domain.

Monitoring Capabilities in the Cloud Foundation System

9

The Cloud Foundation system provides built-in capabilities to help you perform effective operations monitoring, troubleshooting, performance management, infrastructure capacity planning, and compliance monitoring and auditing.

You use the built-in monitoring capabilities for these typical scenarios.

Scenario	Examples
Are the systems online?	A host or other component shows a failed or unhealthy status.
Why did a storage drive fail?	Hardware-centric views spanning inventory, configuration, usage, and event history to provide for diagnosis and resolution.
Is the infrastructure meeting tenant service level agreements (SLAs)?	Analysis of system and device-level metrics to identify causes and resolutions.
At what future time will the systems get overloaded?	Trend analysis of detailed system and device-level metrics, with summarized periodic reporting.
What person performed which action and when?	History of secured user actions, with periodic reporting. Workflow task history of actions performed in the system.

The monitoring capabilities involve these features:

Tasks and subtasks

A task is a unit of work or a series of subtasks that perform an overall goal, such as creating a workload domain.

vRealize Log Insight instance deployed by Cloud Foundation

Use of the vRealize Log Insight instance deployed by Cloud Foundation is licensed separately. When this deployed vRealize Log Insight instance is licensed for use in your environment, and enabled in the SDDC Manager Dashboard, log content for the physical resources and the VMware SDDC virtual infrastructure are sent to the vRealize Log Insight instance. As a result, when you log in to the vRealize Log Insight Web interface, you can obtain a unified view of event and syslog information to assist with troubleshooting. Data from the events and audit events raised by Cloud Foundation is also sent to vRealize Log Insight. You can use the searching, query, and reporting features of vRealize Log Insight to create trend reports and auditing reports from the event history. See Using vRealize Log Insight Capabilities in Your Cloud Foundation System.

This chapter includes the following topics:

- Viewing Tasks and Task Details
- Using vRealize Log Insight Capabilities in Your Cloud Foundation System

Viewing Tasks and Task Details

From the SDDC Manager Dashboard, you can access all tasks. By default, the Dashboard displays the Recent Tasks widget, providing general information at a glance about the most recent tasks. A task is a unit of work or a series of subtasks that perform an overall goal, such as creating a workload domain.

In addition to the most recent tasks, you can view and search for all tasks by clicking **View All Tasks** at the bottom of the Recent Tasks widget. This opens the Tasks panel.

Note For more information about controlling the widgets that appear on the Dashboard page of the SDDC Manager Dashboard, see Tour of the SDDC Manager User Interface.

Viewing and Filtering Task Details

The Tasks panel provides a high level view all tasks, displaying the descriptive task name, task status (for example, running, succeeded, or failed), and the timestamp for the last change in task status. You can also filter and search the task information as follows:

- Search tasks by clicking the filter icon in the Task column header and entering a search string.
- Filter tasks by status by clicking the filter icon in Status column. Select by category **All**, **Failed**, **Successful**, **Running**, or **Pending**.

  Note Each category also displays the number of tasks with that status.

- Clear all filters by clicking **Reset Filter** at the top of the Tasks panel.
- Click **Refreh** to refresh the task list.

Note You can also sort the table by the contents of the Status and Last Occurrence columns.

Managing Tasks and Subtask Details

Expand a task to view details including the subtasks that comprise the task and their individual statuses.

- If a task is in a Failed state, you can also attempt to restart it by clicking **Restart Task**.

  Note Not all tasks are restartable.

- If a task is in a Failed state, click on the icon next to the Failed status to view a detailed report on the cause.

- To view subtasks and their details, click **View Subtasks**.

  Note You can filter subtasks in the same way you filter tasks.

Note You can also sort the table by the contents of the Status and Last Occurrence columns.

Resizing the Task Panel

Use the icons on the task panel to increase or decrease the panel size, or to close or reopen it.

Using vRealize Log Insight Capabilities in Your Cloud Foundation System

The vRealize Log Insight instance that is deployed by SDDC Manager is licensed separately. When the vRealize Log Insight instance is licensed for use in your Cloud Foundation environment, you can use the capabilities of vRealize Log Insight to work with the event and log data that is collected from the various hardware devices and SDDC virtual infrastructure.

vRealize Log Insight is a log aggregator that provides simplified log viewing and analysis. The vRealize Log Insight instance collects and indexes log content for the environment's physical resources and virtual infrastructure, and provides unified querying and analysis of the log content for problem diagnosis and repair. Similarly, SDDC Manager is configured by default to send all logs to vRealize Log Insight, enabling users to browse and search logs to troubleshoot SDDC Manager failures.

You can configure the vRealize Log Insight instance for remote syslog forwarding to an instance of vRealize Log Insight that is external to the Cloud Foundation system or to another syslog server. To configure vRealize Log Insight to forward events to a syslog target, see Add vRealize Log Insight Event Forwarding Destination in the vRealize Log Insight documentation.

To log in to the vRealize Log Insight Web interface from the SDDC Manager Dashboard, see Enable vRealize Log Insight in Cloud Foundation.

Content Packs

The vRealize Log Insight instance includes a set of content packs. Content packs are read-only plug-ins to vRealize Log Insight that provide pre-defined knowledge about specific types of events such as log messages. The purpose of a content pack is to provide knowledge about a specific set of events in a format that is easily understandable by administrators, monitoring teams, and executives. A content pack consists of information that can be saved from either the Dashboards or Interactive Analytics pages in the vRealize Log Insight Web interface. Such information typically includes:

- Queries
- Fields
- Aggregations
- Alerts

- Dashboards

The vRealize Log Insight instance includes a number of VMware content packs, including the Cloud Foundation content pack. In the vRealize Log Insight web interface, these content packs display as widgets in the **Dashboards > VMware-VCF** page.

Content Pack	Overview
General	This content pack includes multiple subcatergories of dashboards and analytics including overview, problems, event types, statistics, and agents.
VMware - NSX for vSphere	This content pack provides various dashboards and filters to give you insight into the data that is sent by the NSX for vSphere virtual infrastructure in the management and workload domains' vCenter Server instances.
VMware - Cloud Foundation	This content pack includes an overview dashboard that gives overall summary views of the data sent by the Cloud Foundation, and also provides detailed views for the various levels of interest, such as rack-level, server-level, switch-level, device-level, and so on.
VMware - vSAN	This content pack provides various dashboards and filters to give you insight into the logs that are sent by the management and workload domains' vSAN features.
VMware - vSphere	This content pack provides various dashboards and filters to give you insight into the data that is sent by the management and workload domains' vCenter Server instances.
VMware - vROPs	This content pack provides various dashboards and filters to give you insight into the logs that are sent by the management and workload domains' vRealize Operations features.

To see the dashboards for one of the content packs in the vRealize Log Insight Web interface, select **Dashboards** and then select the specific content pack dashboard in the left hand navigation bar.

Get Started Using the vRealize Log Insight Instance

Use of the vRealize Log Insight instance that is deployed by SDDC Manager is licensed separately. vRealize Log Insight delivers real-time log management for VMware environments, providing visibility of logs and easier troubleshooting across the physical and virtual infrastructure in your Cloud Foundation system.

During bring-up, SDDC Manager deploys and configures the vRealize Log Insight virtual appliance. From your deployed vRealize Log Insight instance, you can view and analyze logs to assist in troubleshooting, trend analysis, and so on.

The bring-up process also installs and configures content packs in the vRealize Log Insight instance. A content pack provides dashboards, extracted fields, predefined queries, and alerts that are related to the content pack's specific product or set of logs. When you launch the vRealize Log Insight Web interface, the installed content packs are ready for use. For an overview of these content packs, see Using vRealize Log Insight Capabilities in Your Cloud Foundation System. For detailed information on how to use the dashboards, predefined queries, and collected log data in vRealize Log Insight, see the vRealize Log Insight product documentation.

You can open the vRealize Log Insight interface directly from the SDDC Manager Dashboard. For details, see Enable vRealize Log Insight in Cloud Foundation.

If this is the first time after the initial bring-up process that the vRealize Log Insight Web interface is launched, type the system-assigned credentials into the login screen and then click **Login**. Then use the vRealize Log Insight Web interface to assign permissions to your superuser account and other user accounts.

Note You can look up the system-assigned credentials for the vRealize Log Insight Web interface by logging in to the SDDC Manager VM and running the `/home/vrack/bin/lookup-password` command.

Important Do not change the password of the admin account from within the vRealize Log Insight Web interface, or unpredictable results can occur. To change the admin account's password without rotating all account passwords, see Chapter 12 Changing the Passwords of Your Cloud Foundation System On Demand.

Procedure

1 Open the vRealize Log Insight Web interface.

2 If the vRealize Log Insight login screen appears, log in with the appropriate credentials.

- If this is the first time logging in to vRealize Log Insight after the initial bring-up process, use the username **`admin`** and the randomized password that was set when the passwords were rotated at the end of the bring-up process.
- If you are using an account that was set up for you in vRealize Log Insight, use those credentials to log in.

When you are logging in to the vRealize Log Insight Web interface with the **`admin`** account after updating passwords, you must use the randomized password that is set for that account by the rotation procedure. For details about passwords, see Chapter 12 Changing the Passwords of Your Cloud Foundation System On Demand.

The vRealize Log Insight web interface appears with the display filtered to the **Dashboards > VMware-VCF > Overview** page to show the various event widgets.

Configuring Customer Experience Improvement Program

10

This product participates in VMware's Customer Experience Improvement Program ("CEIP").

The CEIP provides VMware with information that enables VMware to improve its products and services, to fix problems, and to advise you on how best to deploy and use our products. As part of the CEIP, VMware collects technical information about your organization's use of VMware products and services on a regular basis in association with your organization's VMware license key(s). This information does not personally identify any individual. For additional information regarding the CEIP, refer to the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html.

Procedure

1 On the SDDC Manager Dashboard, click **Administration > VMware CEIP**.

2 Select the **Join the VMware Customer Experience Improve Program** check box.

Supportability and Serviceability (SoS) Tool

11

The SoS tool is a command-line Python tool that can be used for the following:

- Run health checks.
- On-demand vSAN partition cleanup.
- Collect logs for Cloud Foundation components.

To run the SoS tool, SSH in to the SDDC Manager VM using the **`vcf`** administrative user account, enter **`su`** to switch to the root user, and navigate to the `/opt/vmware/sddc-support` directory and type `./sos` followed by the options required for your desired operation.

```
./sos --option-1 --option-2 --option-3 ... --option-n
```

To list the available command options, use the `--help` long option or the `-h` short option.

```
./sos --help
./sos -h
```

Note You can specify some options in the conventional GNU/POSIX syntax, using -- for the long option and - for the short option.

This chapter includes the following topics:

SoS Tool Options

This section lists the specific options you can use with the SoS tool.

SoS Tool Help Options

Use these options to see information about the SoS tool itself.

Option	Description
`--help` `-h`	Provides a summary of the available SoS tool options
`--version` `-v`	Provides the SoS tool's version number.

SoS Tool Generic Options

These are generic options for the SoS tool.

Option	Description
`--configure-sftp`	Configures SFTP for logs.
`--debug-mode`	Runs the SoS tool in debug mode.
`--domain-name` *`DOMAINNAME`*	Specify the name of the workload domain name on which the SoS operation is to be performed. To run the operation on all domains, specify `--domain-name ALL` . **Note** If you omit the *--domain-name* flag and domain name, the SoS operation is performed only on the management domain.
`--force`	Allows SoS operations to be formed while workflows are running. **Note** It is recommended that you do not use this option.
`--history`	Displays the last 20 SoS operations performed.
`--setup-json` *`SETUPJSON`*	Custom setup-json file for log collection. SoS prepares the inventory automatically based on the environment where it is running. If you want to collect logs for a pre-defined set of components, you can create a `setup.json` file and pass the file as input to SoS. A sample JSON file is available on the SDDC Manager VM in the `/opt/vmware/sddc-support/` directory.
`--skip-known-host-check`	Skips the specified check for SSL thumbprint for host in the known host.
`--zip`	Creates a zipped TAR file for the output.

SoS Tool Options for Health Check

These SoS commands are used for checking the health status of various components or services, including connectivity, compute, storage, database, domains, and networks.

A green status indicates that the health is normal, yellow provides a warning that attention might be required, and red (critical) indicates that the component needs immediate attention.

Option	Description
`--certificate-health`	Verifies that the component certificates are valid (within the expiry date).
`--connectivity-health`	Performs a connectivity health check to inspect whether the different components of the system such as the ESXi hosts, Virtual Center Servers, Inventory Service VMs, Log Insight VM, NSX Manager VMs, PSC VMs, SDDC Manager VM can be pinged.
`--compute-health`	Performs a compute health check.

Option	Description
`--general-health`	Verifies ESXi entries across all sources, checks the Postgres DB operational status for hosts, checks ESXi for error dumps, and gets NSX Manager and cluster status.
`--get-host-ips`	Returns server information.
`--health-check`	Performs all available health checks.
`--ntp-health`	Verifies whether the time on the components is synchronized with the NTP server in the SDDC Manager VM. It also ensures that the hardware and software timestamp of ESXi hosts are within 5 minutes of the SDDC Manager VM.
`--password-health`	Returns the status of all current passwords, such as Last Changed Date, Expiry Date, and so on.
`--services-health`	Performs a services health check to confirm whether services within the Inventory Service VM and within SDDC Manager (like Lifecycle Management Server) are running.
`--storage-health`	Performs a check on the vSAN disk health of the ESXi hosts and vCenter clusters. Also runs Proactive vSAN tests to verify the ability to create VMs within the vSAN disks.

SoS Tool Options for Fixing vSAN Partitions

Use these options to clean up vSAN partitions on one or more ESXi hosts.

Option	Description
`--cleanup-vsan`	Cleans up vSAN Partitions in ESXi hosts.
`--esxi-node-ips <esxi_node_ipaddress1,esxi_node_ipaddress1,...>`	Specifies the ESXi hosts, by IP address, to run the vSAN cleanup. Use commas to separate multiple IP addresses.

Collect Logs for Your Cloud Foundation System

Use the SoS tool to collect the logs for various software components in the system.

Use these options when retrieving support logs from your environment's various components.

- To collect all logs from all components, you can run the SoS tool without specifying any component-specific options.
- To collect logs for a specific component, run the tool with the appropriate options.

  For example, the *--domain-name* option is important. If omitted, the SoS operation is performed only on the management domain. See page 88.

Log files for the vRealize Log Insight agent in vCenter Server are collected when vCenter Server log files are collected.

After running the SoS tool, you can examine the resulting logs to troubleshoot issues, or provide to VMware Technical Support if requested. VMware Technical Support might request these logs to help resolve technical issues when you have submitted a support request. The diagnostic information collected using the SoS tool includes logs for the various VMware software components and software products deployed in your Cloud Foundation environment.

Procedure

1 Using SSH, log in to the SDDC Manager VM with the following credentials:

Username: **vcf**

Password: use the password specified in the deployment parameter sheet

2 Enter **su** to switch to the root user.

3 Change to the `/opt/vmware/sddc-support` directory.

4 To collect the logs, run the SoS tool without specifying any component-specific options. To collect logs for a specific component, run the tool with the appropriate options.

Note By default, before writing the output to the directory, the tool deletes the prior run's output files that might be present. If you want to retain the older output files, specify the `--no-clean-old-logs` option.

If you do not specify the `--log-dir` option, the tool writes the output to the `/var/log/vmware/vcf/sddc-support` directory in the SDDC Manager VM.

Table 11-1. SoS Tool Log File Options

Option	Description
`--api-logs`	Collects output from REST endpoints for SDDC Manager inventory and LCM.
`--cassandra-logs`	Collects logs from the Apache Cassandra database only. `cassandra-bundle.tgz` contains Cassandra nodetool and debug logs. Apache Cassandra processes run in each of the infrastructure virtual machines.
`--dump-only-sddc-java-threads`	Collects only the Java thread information from the SDDC Manager.
`--esx-logs`	Collects logs from the ESXi hosts only. Logs are collected from each ESXi host available in the deployment.
`--li-logs`	Collects logs from vRealize Log Insight VMs only.
`--log-dir` *`LOGDIR`*	Specifies the directory to store the logs.
`--log-folder` *`LOGFOLDER`*	Specifies the name of the log directory.
`--no-clean-old-logs`	Use this option to prevent the tool from removing any output from a previous collection run. By default, the SoS tool. By default, before writing the output to the directory, the tool deletes the prior run's output files that might be present. If you want to retain the older output files, specify this option.
`--no-health-check`	Skips the health check executed as part of log collection.
`--nsx-logs`	Collects logs from the NSX Manager, NSX Controller, and NSX Edge instances only.
`--psc-logs`	Collects logs from the Platform Services Controller instances only.

Table 11-1. SoS Tool Log File Options (Continued)

Option	Description
`--rvc-logs`	Collects logs from the Ruby vSphere Console (RVC) only. RVC is an interface for ESXi and vCenter. **Note** If the Bash shell is not enabled in vCenter, RVC log collection will be skipped . **Note** RVC logs are not collected by default with ./sos log collection. You must enable RVC to collect RVC logs.
`--sddc-manager-logs`	Collects logs from the SDDC Manager only. `sddc`*<timestamp>*`.tgz` contains logs from the SDDC Manager file system's `etc`, `tmp`, `usr`, and `var` partitions.
`--test`	Collects test logs by verifying the files.
`--vc-logs`	Collects logs from the vCenter Server instances only. Logs are collected from each vCenter server available in the deployment.

The tool displays `Welcome to SoS log collection utility!`, the output directory, `sos.log` file location, and messages about the tool's progress, for example:

```
root@sddc-manager [ /opt/vmware/sddc-support ]# ./sos --domain-name MGMT --skip-known-host
     --log-dir /tmp/new
Welcome to Supportability and Serviceability(SoS) utility!
Performing SoS operation for MGMT domain components
Logs : /tmp/new/sos-2018-08-24-10-49-14-27480
Log file : /tmp/new/sos-2018-08-24-10-49-14-27480/sos.log
Progress : 100%, Completed tasks : [SDDC-MANAGER, SDDC-CASSANDRA, NSX_MANAGER, PSC, HEALTH-CHECK,
API-LOGS, ESX, LOGINSIGHT, VMS_SCREENSHLog Collection completed successfully for : [HEALTH-CHECK,
SDDC-MANAGER, SDDC-CASSANDRA, NSX_MANAGER, PSC, API-LOGS, ESX, LOGINSIGHT, VMS_SCREENSHOT,
VCENTER-SERVER]
```

The tool collects the log files from the various software components in all of the racks and writes the output to the directory named in the `--log-dir` option. Inside that directory, the tool generates output in a specific directory structure.

What to do next

Change to the output directory to examine the collected log files.

Component Log Files Collected By the SoS Tool

The SoS tool writes the component log files into an output directory structure within the filesystem of the SDDC Manager instance in which the command is initiated, for example:

```
root@sddc-manager [ /opt/vmware/sddc-support ]# ./sos
Welcome to Supportability and Serviceability(SoS) utility!
Performing SoS operation for ALL domain components
Logs : /var/log/vmware/vcf/sddc-support/sos-2018-08-21-22-49-09-61442
Log file : /var/log/vmware/vcf/sddc-support/sos-2018-08-21-22-49-09-61442/sos.log
Log Collection completed successfully for : [SDDC-MANAGER, SDDC-CASSANDRA]
```

esx Directory Contents

In each rack-specific directory, the esx directory contains the following diagnostic files collected for each ESXi host in the rack:

File	Description
esx-*IP-address*.tgz	Diagnostic information from running the `vm-support` command on the ESXi host. An example file is `esx-192.168.100.101.tgz`.
SmartInfo-*IP-address*.txt	S.M.A.R.T. status of the ESXi host's hard drive (Self-Monitoring, Analysis, and Reporting Technology). An example file is `SmartInfo-192.168.100.101.txt`.
vsan-health-*IP-address*.txt	vSAN cluster health information from running the standard command `python /usr/lib/vmware/vsan/bin/vsan-health-status.pyc` on the ESXi host. An example file is `vsan-health-192.168.100.101.txt`.

loginsight Directory Contents

The loginsight directory contains diagnostic information files collected from the vRealize Log Insight cluster. The support bundle for each node is collected from the cluster's load balancer VM.

File	Description
load-balancer.vrack.vsphere.local-loginsight-support.tgz	Compressed TAR file consisting of support bundles collected from each node in the vRealize Log Insight cluster. For example: loginsight-loginsight-node-<*node -number*>.vrack.vsphere.local-<*time-stamp*>.
loginsight-loginsight-node-<*node -number*>.vrack.vsphere.local-<*time-stamp*>	Contains the following: `README`, `boot`, `error.log`, `etc`, `proc`, `usr`, `action.log`, `commands`, `errors-ignored.log`, `opt`, `storage`, and `var`.

nsx Directory Contents

In each rack-specific directory, the nsx directory contains the diagnostic information files collected for the NSX Manager, NSX Controller, and NSX Edge instances deployed in that rack.

The number of files in this directory depends on the number of NSX Manager, NSX Controller, and NSX Edge instances that are deployed in the rack. In a given rack, each management domain has one NSX Manager instance and a minimum of three NSX Controller instances, and any VI workload domains in the rack each have one NSX Manager instance and at least three NSX Controller instances. NSX Edge instances are only deployed to support vRealize Operations and vRealize Automation, which are optional components.

File	Description
VMware-NSX-Manager-tech-support-*nsxmanagerIPaddr*.tar.gz	Standard NSX Manager compressed support bundle, generated using the NSX for vSphere API `POST https://`*`nsxmanagerIPaddr`*`/api/1.0/appliance-management/techsupportlogs/NSX`, where *nsxmanagerIPaddr* is the IP address of the NSX Manager instance. An example is VMware-NSX-Manager-tech-support-10.0.0.8.tar.gz.
VMware-NSX-Controller-tech-support-*nsxmanagerIPaddr*-controller-*controllerId*.tgz	Standard NSX Controller compressed support bundle, generated using the NSX for vSphere API to query the NSX Controller technical support logs: `GET https://`*`nsxmanagerIPaddr`*`/api/2.0/vdn/controller/`*`controllerId`*`/techsupportlogs`, where *nsxmanagerIPaddr* is the IP address of the NSX Manager instance and *controllerID* identifies the NSX Controller instance. Examples are VMware-NSX-Controller-tech-support-10.0.0.8-controller-1.tgz, VMware-NSX-Controller-tech-support-10.0.0.8-controller-2.tgz, VMware-NSX-Controller-tech-support-10.0.0.8-controller-3.tgz.
VMware-NSX-Edge-tech-support-*nsxmanagerIPaddr*-*edgeId*.tgz **Note** This information will only be collected if NSX Edges are deployed.	Standard NSX Edge support bundle, generated using the NSX for vSphere API to query the NSX Edge support logs: `GET https://`*`nsxmanagerIPaddr`*`/api/4.0/edges/`*`edgeId`*`/techsupportlogs`, where *nsxmanagerIPaddr* is the IP address of the NSX Manager instance and *edgeID* identifies the NSX Edge instance. An example is VMware-NSX-Edge-tech-support-10.0.0.7-edge-1.log.gz.

psc Directory Contents

In the rack-1 directory, the psc directory contains the diagnostic information files collected for the Platform Services Controller instances deployed in that rack.

File	Description
vm-support-*pscIPaddr*.tar.gz	Standard Platform Services Controller support bundle downloaded from the Platform Services Controller instance with IP address *pscIPaddr*.

vc Directory Contents

In each rack-specific directory, the vc directory contains the diagnostic information files collected for the vCenter Server instances deployed in that rack.

The number of files in this directory depends on the number of vCenter Server instances that are deployed in the rack. In a given rack, each management domain has one vCenter Server instance, and any VI workload domains in the rack each have one vCenter Server instance.

File	Description
vc-*vcsaFQDN*-*timestamp*.tgz	Standard vCenter Server support bundle downloaded from the vCenter Server Appliance instance having a fully-qualified domain name *vcsaFQDN*. The support bundle is obtained from the instance using the standard `vc-support.sh` command.

Changing the Passwords of Your Cloud Foundation System On Demand

12

For security reasons, you can change passwords for the built-in accounts that are used by your Cloud Foundation system. Changing these passwords periodically or when certain events occur, such as an administrator leaving your organization, reduces the likelihood of security vulnerabilities occurring.

You had specified passwords for the Cloud Foundation system built-in accounts in the deployment parameters sheet before bring-up. You can modify the passwords for these accounts using RESTful API calls.

Note The NSX cluster controller password is hardcoded in the system. It is strongly recommended that you look it up and update it. See Look Up Passwords and Update a Password.

This chapter includes the following topics:

Required Authentication

You can programmatically modify SDDC components passwords by invoking the SDDC Manager's password's RESTful APIs.

Run REST Calls on the SDDC Manager VM

To run the password API calls on the SDDC Manager VM, SSH in to the SDDC Manager VM using the **vcf** administrative user account. Enter **su** to switch to the root user and navigate to the `/home/vcf/` directory.

1 SSH in to the SDDC Manager VM using the **vcf** administrative user account and password specified in the Deployment Parameter sheet.

2 Type **su** to switch to the root user

3 Navigate to the /home/vcf/ directory.

Run REST Calls Outside the SDDC Manager VM

For basic authentication on REST clients, use the following header:

https://*SDDC_Manager_IP_address*/security/password/vault

Use the admin user name and the password you specified in the parameter deployment sheet.

For basic authentication for CLI commands, use the following:

curl -k https://*SDDC_Manager_IP_address*/security/password/vault -u admin:*password*

Look Up Passwords

You can use a REST API call or a CLI command to look up passwords for accounts that are created and managed by Cloud Foundation.

1 Ensure that you have the required authentication. See Required Authentication.

2 Run the following call

GET /security/password/vault ?domainName=*domain name* | ?entityType=*entityType* | ?entityNAme=*fqdn* | ?entityIpAddress=*ipaddress*

where:

- *domain name* is the name of the workload domain
- *entityType* can be ESXI, VCENTER, PSC, NSX_MANAGER, NSX_CONTROLLER, NSX_EDGE, VRLI, VROPS, VRA, or VRSLCM

  For example, entityType=PSC&entityType=VCENTER
- *fqdn* is the fully qualified domain name of the entity
- *ipaddress* is the IP address of the entity

Example REST API CALl

GET /security/password/vault ?domainName=MGMT ?entityType=ESXI

Responses

Status Code: 200

Body: application/json

```
[
   {
      "username" : "root",
      "entityIpAddress" : "10.0.0.103",
      "entityName" : "esxi-4.vrack.vsphere.local",
      "password" : "EvoSddc!2020",
      "credentialType" : "SSH",
      "entityType" : "ESXI",
      "domainName" : "MGMT",
      "entityId" : "d88e62f1-8071-11e8-ab5e-e76b34838161"
   },
   {
      "username" : "root",
      "entityIpAddress" : "10.0.0.102",
      "entityName" : "esxi-3.vrack.vsphere.local",
      "password" : "xxx",
      "credentialType" : "SSH",
      "entityType" : "ESXI",
      "domainName" : "MGMT",
      "entityId" : "d88e62f1-8071-11e8-ab5e-e76b34838161"
   }
]
```

CLI Example

```
vcf@sddc-manager [ ~ ]$ lookup_passwords
    PSC
    identifiers: 10.0.0.5,psc-1.vrack.vsphere.local
    workload: MGMT
        username: administrator@vsphere.local
        password: l!6L@ZkU5ZW03p8+S7
            type: SSO

    PSC
    identifiers: 10.0.0.5,psc-1.vrack.vsphere.local
    workload: MGMT
        username: root
        password: i^3I2p1uG_o_drRkW8
            type: SSH
    :
    :
    :
    :

    VRLI
    identifiers: 10.0.0.18,loginsight-node-3.vrack.vsphere.local
    workload: MGMT
        username: root
        password: tE^1P~in7W1X4K!-8~
            type: SSH
```

Update a Password

You can update the password for an account managed by Cloud Foundation using a REST API call.

1 Ensure that you have the required authentication. See Required Authentication.

2 Run the REST API call for look up passwords. See Look Up Passwords.

3. From the response body, copy the text for the component whose password you want to update including the beginning and ending curly brackets.

4. Compose the request body JSON by adding the text you copied in step 2 and adding the new password.

5. In the request body, change the `action` to `UPDATE`.

6. Run the POST command as follows.

   POST /security/password/vault

   Example Request Body for updating the ESXi password

   ```
   {
     "entity" : {
         "entityType" : "ESXI",
         "username" : "root",
         "password" : "k)-78kP^9_87-N-hT",
         "entityId" : "d88e62f1-8071-11e8-ab5e-e76b34838161"
         "entityName" : "esxi-3.vrack.vsphere.local",
         "entityIpAddress" : "10.0.0.102",
         "credentialType" : "SSH",
         "domainName" : "MGMT",
      },
     "action" : "UPDATE"
   }
   ```

   For unassigned hosts, the domain name must have the value UNKNOWN in the request body. See example below.

   ```
   [
     {
         "domainName" : "UNKNOWN",
         "entityId" : "1263e855-1a47-48f2-92a5-0bc812a3dea0",
         "entityName" : "esxi-9.vrack.vsphere.local",
         "credentialType" : "SSH",
         "entityType" : "ESXI",
         "entityIpAddress" : "10.0.0.108",
         "password" : "xxx",
         "username" : "root"
      }
   ]
   ```

   Response:

Body: application/xml

```
{
   "transactionId" : 102,
   "status" : "IN_PROGRESS"
}
```

You use the `transactionId` from the response body to retrieve the status of the password update, and to retry or cancel the password update.

Password Update Dependants and Failure Stages

Passwords for some Cloud Foundation components are dependent on passwords of other components. For example, if you change the SSO password, then NSX Manager, vRealize Log Insight, vROPS, and vRA have to be updated with the new SSO password. These components are dependents. When you start a password update for SSO, the main update operation is triggered on PSC. The new SSO password is then propagated to the dependent components.

Before updating the password, the update API verifies whether all dependent entities (NSX Manager, vRealize Log Insight, vROPS, and vRA in the case of SSO) are up. If the dependents respond to the password update API, the password update operation continues. The SSO password is updated on the PSC and then the new password is sent to the dependents.

If any of dependent components are down, the password update fails. The API response includes the information that the log in attempt to a component failed. You can cancel the password update operation or fix the issue and retry the password update.

Password Update Dependents

Password Change On This Component	Needs to be Propagated To These Components
PSC with SSO credential type	NSX, vRLI, vROPS, and vRA
NSX Manager with API credential type	vRA and CLI Enable user
vRA with administrator credential type	vROPS

Password Update Failure Stages

A password update can fail during any of the following stages.

1 TEST usually means that the login to the SDDC Manager VM failed.

   Error message: `Operation failed in 'login with the old credentials', for credential update.`

   Remediation: Check the login credentials in the JSON and run the retry command.

2 UPDATERS_TEST usually means that login or connectivity to one of the update dependents failed.

Error message: `Operation failed in 'password validation before updating the dependants', for credential update.`

Remediation: Check the login and connectivity to dependant components and then run the retry command.

3 UPDATE indicates that the password change on the target VM failed.

Error message: `Operation failed in` *appliance update*`, for credential update.`

Remediation: Ensure that the new password matches the password policy for the component and check the log file. Fix any issues and then run the retry API call.

Note If vRA is not linked to a domain, NSX credential update fails in the dependents update stage.

4 PERSIST_TO_CSS: Password updated successfully on the VM, but failed to save the new password in the CSS database.

Error message: `Operation failed in 'persist to local password store', for credential update.`

Remediation: Check the log file. Fix any issues and then run the retry API call.

Note If vRA is not linked to a domain, NSX credential update fails in the dependents update stage.

5 NOTIFY_UPDATERS: Updating the new password to one of the dependant components has failed.

Error message: `Operation failed in 'dependant update', for credential update.`

Remediation: Check the login and connectivity to dependant components and then run the retry command.

Log File Location

To review the log file for password updates, log in to the SDDC Manager VM and open the following file:

```
/var/log/vmware/vcf/operationsmanager/operationsmanager-debug.log
```

Retrieve Password Update Status

You can retrieve the update status for a specified transaction using a REST API call.

1 Ensure that you have the required authentication. See Required Authentication.

2 Retrieve the *transactionId* from the response of the update password call. SeeUpdate a Password.

3 Run the following call to retrieve the status of the password update:

`GET /security/password/vault/transactions/{`*transactionId*`}`

Password change may fail if the target machine is down or if the specified password is rejected by the target machine. The failure reason is provided in the response body. You can retry updating the password after fixing the issue, or specify a new password as appropriate.

Example Call

`GET /security/password/vault/transactions/{102}`

Response:

Body: application/json

```
{
    "entityName" : "esx-1.vrack.vsphere.local",
    "oldPassword" : "VMware1234!",
    "newPassword" : "VMware12345!",
    "timestamp" : 1532424612071,
    "id" : 102,
    "credentialType" : "SSH",
    "type" : "PARENT",
    "entityType" : "ESXI",
    "transactionStatus" : "SUCCEEDED"
 }
```

The `transactionStatus` parameter can have one of the following values:

- SUCCEEDED
- FAILED
- IN_PROGRESS
- PATCH_IN_PROGRESS
- NOT_STARTED
- INCONSISTENT
- USER_CANCELLED

Retry Password Update

If the password update fails, you can retry updating the password using a REST call or CURL command.

1 Ensure that you have the required authentication. See Required Authentication.

2 Run the REST API call for look up passwords. See Look Up Passwords.

  Copy the output to use in the request body.

3 Compose the request body JSON by adding the text you copied in step 2.

4 Make the following updates to the request body:

  a In the `password` attribute, keep the original password or enter a new password.

  b change the `action` to `RETRY`.

5 Run the following call:

`POST /security/password/vault`

Request Body: application/json

```
{
  "transactionId": 102,
  "entity" : {
      "username" : "root",
      "entityIpAddress" : "10.0.0.102",
      "entityName" : "esxi-3.vrack.vsphere.local",
      "password" : "EvoSddc!2020",
      "credentialType" : "SSH",
      "entityType" : "ESXI",
      "domainName" : "MGMT",
      "entityId" : "d88e62f1-8071-11e8-ab5e-e76b34838161"
   },
  "action" : "RETRY"
}
```

Cancel Password Update

You must cancel a password update when it is in a failed state. The password update request can fail due to a variety of reasons. For example, a VM or host may be corrupted or the targeted resource may need maintenance activity to be functional.

You must cancel password update operations that are in a failed state. If you have a password update operation in a failed state, you will not be able to perform any Cloud Foundation operations such as create, expand, or delete a workload domain, add or remove a host, or apply an update.

1 Ensure that you have the required authentication. See Required Authentication.

2 Run the REST API call for look up passwords. See Look Up Passwords.

   Copy the output to use in the request body.

3 Compose the request body JSON by adding the text you copied in step 2.

4 In the request body, change the `action` to `CANCEL`

5 Run the following call:

   `POST /security/password/vault`

   Request Body: application/json

```
{
  "transactionId": 102,
  "entity" : {
      "username" : "root",
      "entityIpAddress" : "10.0.0.102",
      "entityName" : "esxi-3.vrack.vsphere.local",
      "password" : "EvoSddc!2020",
      "credentialType" : "SSH",
      "entityType" : "ESXI",
      "domainName" : "MGMT",
      "entityId" : "d88e62f1-8071-11e8-ab5e-e76b34838161"
   },
  "action" : "CANCEL"
}
```

What to do next

Run the update password API call again.

Replace Host Components

13

The replacement procedure depends on the component being replaced and the condition of the component.

- Replacing Components of a Host Running in Degraded Mode

  The procedures for replacing components of hosts in degraded depend on whether the host is part of a workload domain.

- Replace a Dead Host

  If you need to replace a dead host, you must remove the host from the physical rack. You can then add a new host or replace the failed component on the host and add it back.

- Replace Boot Disk on a Host

  This section describes the replacement procedure for a failed boot disk on a host.

Replacing Components of a Host Running in Degraded Mode

The procedures for replacing components of hosts in degraded depend on whether the host is part of a workload domain.

These procedures apply to the following components:

- CPU
- Memory
- BMC
- Power supply
- RAID 1 boot disk

Replace Components of a Workload Domain Host Running in Degraded Mode

This procedure shows you how to replace the component of a degraded host that is part of a workload domain.

Prerequisites

- Verify that the host is operational and is accessible by VMware Host Client.
- Verify that the Management, vSAN, and vMotion networks are available on the host. This can be viewed through the **Inventory > Hosts** page.
- Verify that the HDD and SSD disks on the host are in a good state.

Procedure

1. Log in to vSphere Web Client.
2. Right-click the affected host and click **Enter Maintenance Mode**.
3. If the host belongs to a domain, click **Full Data Migration**.
4. Right-click the affected host and select **Shutdown**.
5. Pull the host out of the physical rack.

   Note the ports on the switches it was connected to.
6. Service the appropriate part following the OEM vendor documentation.
7. Put the host back in the physical rack and connect it back to the appropriate switches.
8. Power on the host.
9. In vSphere Web Client, right-click the host and click **Exit Maintenance Mode**.

Replace Components of an Unassigned Host Running in Degraded Mode

This procedure shows you how to replace the component of a degraded host that is not part of a workload domain.

Prerequisites

- Verify that the host is operational and is accessible by VMware Host Client.
- Verify that the HDD and SSD disks on the host are in a good state.

Procedure

1. Log in to vSphere Web Client.
2. Right-click the affected host and select **Shutdown**.
3. Pull the host out of the physical rack.

   Note the ports on the switches it was connected to.
4. Service the appropriate part following the OEM vendor documentation.
5. Put the host back in the physical rack and connect it back to the appropriate switches.
6. Power on the host.

7 In the SDDC Manager Dashboard, verify that the host is available in the free pool.

Replace a Dead Host

If you need to replace a dead host, you must remove the host from the physical rack. You can then add a new host or replace the failed component on the host and add it back.

This procedure applies chiefly to the following components:

- Storage controllers
- Motherboards
- Boot disks

Prerequisites

If the host belongs to a workload domain, verify that there are at least 4 hosts in the management or workload domain to which the faulty host belongs. If there are less than 4 hosts, add a host to the domain from the capacity pool if possible.

Procedure

1 Decommission the host.

   See Decommission a Host.

2 Power off the host and remove it from the physical rack.

3 Replace and reconfigure, as follows.

   a Replace the failed component on the host.

   b Perform a fresh reinstall of ESXi.

   c Commission the host.

      See Commission a Host.

Replace Boot Disk on a Host

This section describes the replacement procedure for a failed boot disk on a host.

Prerequisites

Verify that there are at least 4 hosts in the management or workload domain to which the faulty host belongs. If there are less than 4 hosts, add a host to the domain from the capacity pool, if possible.

Procedure

1 If there are dual boot disks in the host setup as RAID 1 and only one of them fails:

   - See Replacing Components of a Host Running in Degraded Mode to replace the failed disk.

   The RAID 1 feature will rebuild the disks as needed. For more details, refer to the OEM vendor documentation.

2 If there is a single boot disk in the host and it fails, see Replace a Dead Host.

Patching and Upgrading Cloud Foundation

14

Lifecycle Management (LCM) enables you to perform automated updates on select components contained within the management domain and VI workload domains. Update bundles can be downloaded and applied manually or scheduled within your maintenance window, allowing for flexibility in their application.

This chapter includes the following topics:

LCM Bundle Types

There are three types of LCM bundles.

Patch Update Bundles

A patch update bundle contains bits to update the appropriate Cloud Foundation software components in your management domain or VI workload domain. In most cases, a patch update bundle must be applied to the management domain before it can be applied to VI workload domains.

Cumulative Update Bundles

With a cumulative update bundle, you can directly update the appropriate software in your workload domain to the version contained in the cumulative bundle rather than applying sequential updates to reach the target version.

For example, suppose VMware just released ESXi version 6.5 EP 2. Your workload domain is at ESXi version 6.5. The sequential upgrade path would be version 6.5 -> 6.5 P1 -> 6.5 P2 -> 6.5 EP1 -> 6.5 EP2. Instead of applying four sequential patches to update the workload domain to 6.5 EP2, you can now apply a cumulative bundle and update the workload domain from 6.5 directly to 6.5 EP2.

Cumulative bundles are available only for vCenter Server, Platform Services Controller, and ESXi.

Note that you can apply a cumulative bundle to a workload domain only if the target release in the bundle is lower than or at the same version as the management domain. If the cumulative bundle is available for both the management domain and VI workload domains, you must apply it to the management domain before applying it to VI workload domains.

Install Bundles

If you have updated the management domain in your environment, you can download an install bundle with updated software bits for VI workload domains and vRealize suite components.

- A VI workload domain install bundle is used to deploy later versions of the software components rather than the versions in your original Cloud Foundation installation.
- A vRealize install bundle is used for deploying vRealize components.

Download LCM Bundles

This section describes how to download an LCM bundle. LCM update bundles must be available on SDDC Manager before you can apply the update.

Download Bundles

If are logged in to your My VMware account, LCM automatically polls the depot to access the bundles. You receive a notification when a bundle is available and can then download the bundle.

If you do not have internet connectivity, you can either use a proxy server to access the depot, or download the bundles manually.

Download Update Bundle from the the SDDC Manager Dashboard

When an update bundle is available, a notification is displayed on the workload domain page in the Update/Patches tab.

Procedure

1 Log in to your My VMware account.

   a In the SDDC Manager Dashboard, click **Administration > Update Management** .

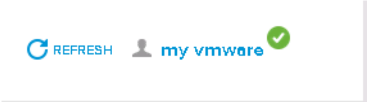
   b Click **Login**.

   The sign in page appears.

c Type your My VMware account user name and password.

d Click **Log In**.

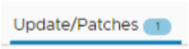
The top right corner of the window displays a green check mark.



2 In the SDDC Manager Dashboard, click **Inventory > Workload Domains**..

3 Click the name of a workload domain and then click the **Updates/Patches** tab.

The number next to the Updates/Patches tab indicates the available updates.



The Available Updates section displays all updates applicable to this workload domain.

4 To view the metadata details for an update bundle, click **View Details**.

The bundle severity and detailed information about each component included in the bundle is displayed. If a bundle is a cumulative bundle, this information is displayed as well.

The bundle severity levels are described in the table below.

Severity Value	Description
Critical	A problem may severely impact your production systems (including the loss of production data). Such impacts could be system down or HA not functioning.
Important	A problem may affect functionality, or cause a system to function in a severely reduced capacity. The situation causes significant impact to portions of the business operations and productivity. The system is exposed to potential loss or interruption of services. A change to support hardware enablement (for example, a driver update), or a new feature for an important product capability.
Moderate	A problem may affect partial non-critical functionality loss. This may be a minor issue with limited loss, no loss of functionality, or impact to the client's operations and issues in which there is an easy circumvention or avoidance by the end user. This includes documentation errors.
Low	A problem which has low or no impact to a product's functionality or a client's operations. There is no impact on quality, performance, or functionality of the product.

5 Do one of the following:

- Click **Download Now**.

  The bundle download status is displayed.

- Click **Schedule Download**.

  Select the date and time for the bundle download and click **Schedule**.

After the bundle is downloaded, the **Schedule Update** button is displayed. Click **View Details** to see the version changes for each component that the bundle will apply.

Download Install Bundle from the the SDDC Manager Dashboard

You download an install bundle from the Repository tab.

Procedure

1 In the SDDC Manager Dashboard, click **Repository > Bundles**.

  Available bundles are displayed. Install bundles display **Install Only Bundle** under the Availability Type.

2 Click **View Details** to see bundle details.

3 Do one of the following:

  - Click **Download Now** to start downloading the bundle.
  - Click **Schedule Download** to schedule the bundle download and follow the UI prompts to select a date and time.

  When the download starts, the download status is displayed.

When you create a new VI workload domain, Cloud Foundation uses the software bits in the downloaded install bundle to deploy the workload domain.

Manually Download Update Bundles

LCM polls the VMware depot to access update bundles. If you do not have internet connectivity in your Cloud Foundation system, you can use the Bundle Transfer utility to manually the bundles from the depot on your local computer and then upload them to SDDC Manager. The utility identifies applicable bundles based on the current software versions in your environment based on a marker file generated on the SDDC Manager VM.

Prerequisites

A Windows or Linux computer with internet connectivity for downloading the bundles. If it is a Windows computer, it must have Java 8 or later.

Procedure

1 Using SSH, log in to the SDDC Manager VM with the user name `vcf` and password you specified in the deployment parameter sheet.

2 Navigate to the `/opt/vmware/vcf/lcm/lcm-tools/bin` directory.

3 Generate a marker file by running the following command.

```
./lcm-bundle-transfer-util --generateMarker
```

The marker file (`markerFile`) is a JSON file that contains information on the current software versions running on SDDC Manager. It also contains the bundles IDs for bundles that were downloaded before this file was generated. The `markerFile.md5` contains the checksum for the `markerFile`.

The output contains the directory where the marker file is generated.

4. Copy the `markerFile` and `markerFile.md5` files from the location displayed in the output of step 3 to a computer with internet access.
5. If the local computer uses a proxy to connect to the internet, perform the following steps.

   a. Open the `application-prod.properties` file of the Bundle Transfer utility at `/directory_where_you_copied_files_in_step_4/lcm-tools/conf/application-prod.properties`.

   b. Add the following lines to the end of the file:

   ```
   lcm.depot.adapter.proxyEnabled=true
   lcm.depot.adapter.proxyHost=proxy IP address
   lcm.depot.adapter.proxyPort=proxy port
   ```

   c. Save and close the file.

6. On the external computer, run the following command.

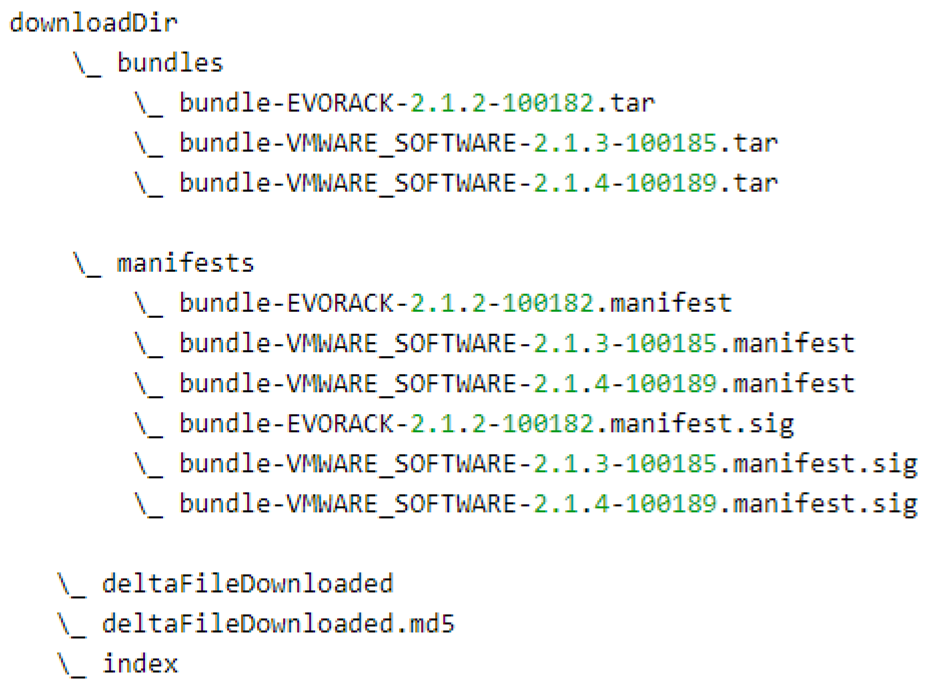
```
./lcm-bundle-transfer-util -download
             -outputDirectory ${absolute-path-output-dir}
             -sku ${sku}
             -depotUser ${depotUser}
             -markerFile ${absolute-path-markerFile}
             -markerMd5File ${absolute-path-markerFile.md5}
```

where

absolute-path-output-dir	Path to the directory where the bundle files are to be downloaded. This directory folder must have 777 permissions. If you do not specify the download directory, bundles are downloaded to the default directory with 777 permissions.
sku	Optional. SKU or Service Provider of the index file.
depotUser	User name for myVMware depot. You are prompted to enter the depot user password. If there are any special characters in the password, specify the password within single quotes.
markerFile	Absolute path to the marker file, as generated in the above step. If you do not specify the path to the marker file, all update bundles on the depot are downloaded.
markerMd5File	Absolute path to the marker MD5 checksum file, as generated in the above step.

The utility generates a delta file (`deltaFileDownloaded`) in the download directory based on the software versions in the marker file and the update bundles available on the depot. The applicable bundles identified in the delta file are downloaded. Download progress for each bundle is displayed.

Figure 14-1. Download Directory Structure



```
downloadDir
     \_ bundles
          \_ bundle-EVORACK-2.1.2-100182.tar
          \_ bundle-VMWARE_SOFTWARE-2.1.3-100185.tar
          \_ bundle-VMWARE_SOFTWARE-2.1.4-100189.tar

     \_ manifests
          \_ bundle-EVORACK-2.1.2-100182.manifest
          \_ bundle-VMWARE_SOFTWARE-2.1.3-100185.manifest
          \_ bundle-VMWARE_SOFTWARE-2.1.4-100189.manifest
          \_ bundle-EVORACK-2.1.2-100182.manifest.sig
          \_ bundle-VMWARE_SOFTWARE-2.1.3-100185.manifest.sig
          \_ bundle-VMWARE_SOFTWARE-2.1.4-100189.manifest.sig

    \_ deltaFileDownloaded
    \_ deltaFileDownloaded.md5
    \_ index
```

7 Copy the update bundle directory from the external computer to the SDDC Manager VM.

For example:

```
scp -pr /Work/UpdateBundle vcf@SDDC_IP:/home/vcf/vCF231to232Bundle"
```

8 In the SDDC Manager VM, change the ownership and permissions of the uploaded bundle.

```
chown vcf_lcm:vcf -R /opt/vmware/vcf/vCF231to232Bundle
chmod -R 0777 /opt/vmware/vcf/vCF231to232Bundle
```

9 In the SDDC Manager VM, upload the bundle files to the internal LCM repository.

```
cd /opt/vmware/vcf/lcm/lcm-tools/bin
./lcm-bundle-transfer-util -upload -bundleDirectory ${absolute-path-output-dir}
```

where *absolute-path-output-dir* is the directory where the bundle files have been be uploaded, or `/opt/vmware/vcf/vCF231to232Bundle` as shown in the previous step.

The utility uploads the bundles specified in the `deltaFileDownloaded` file. The console displays upload status for each bundle.

Use a Proxy Server to Download Upgrade Bundles

If you do not have internet access, you can use a proxy server to download the LCM update bundles. LCM only supports proxy servers that do not require authentication

Procedure

1 Using SSH, log in to the SDDC Manager VM with the user name `vcf` and password you specified in the deployment parameter sheet.

2 Type `su` to switch to the root account.

3 Open the `/opt/vmware/vcf/lcm/lcm-app/conf/application-prod.properties` file.

4 Add the following lines to the end of the file:

```
lcm.depot.adapter.proxyEnabled=true
lcm.depot.adapter.proxyHost=proxy IP address
lcm.depot.adapter.proxyPort=proxy port
```

5 Save and close the file.

6 Restart the LCM server by typing the following command in the console window:

```
systemctl restart lcm
```

7 Wait for 5 minutes and then download the update bundles.

Update Workload Domain

Updates are applied on a workload domain basis. The management domain contains components that provide for the core infrastructure. As a result, most updates must be applied on the management domain before being applied to the other workload domains.

Prerequisites

1 Verify that your environment is in a healthy state. For example, all ESXi hosts within the domain must be healthy. If a host is not healthy, and therefore in maintenance mode, the upgrade will fail.

2 Take a backup of the SDDC Manager VM. The backup of this VM will contain backups of the other VMs as well.

3 Take a snapshot of each VM in your environment.

4 Do not run any domain operations while an update is in progress. Domain operations are creating a new VI domain, adding hosts to a cluster or adding a cluster to a workload domain, and removing clusters or hosts from a workload domain.

5 You must have downloaded the update bundle. See Download Bundles.

6 If you want to skip any hosts while applying an ESXi update to the management domain or a VI workload domain, you must add these hosts to the `application-evo.properties` file before you begin the update. SeeSkip Hosts During ESXi Update.

Procedure

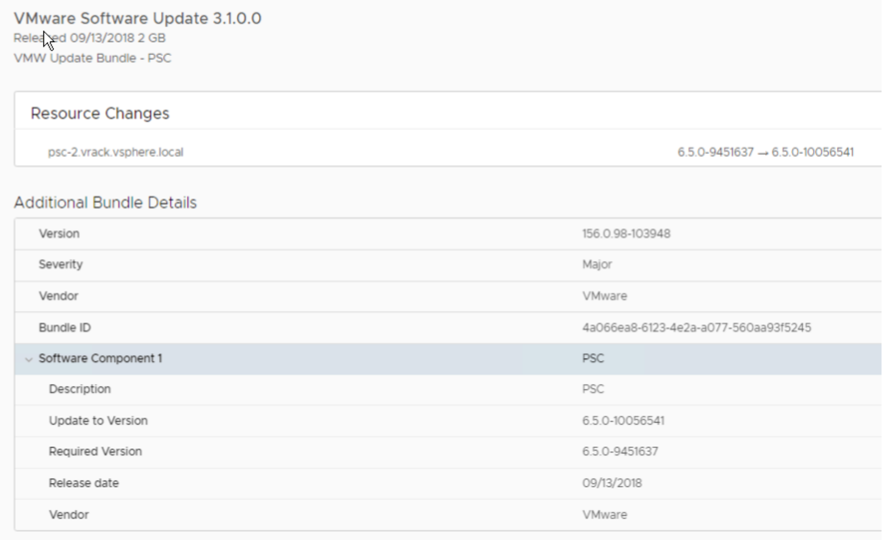
1 In the SDDC Manager Dashboard, click **Inventory > Workload Domains**..

2 Click the name of a workload domain and then click the **Updates/Patches** tab.

   The downloaded bundle is available here.

3 Click **View Details**.

   The bundle version, release date, and summary is displayed. The Resource Changes section displays the current version of the software component that is to be updated as well as the version it will be updated to.



VMware Software Update 3.1.0.0

Released 09/13/2018 2 GB

VMW Update Bundle - PSC

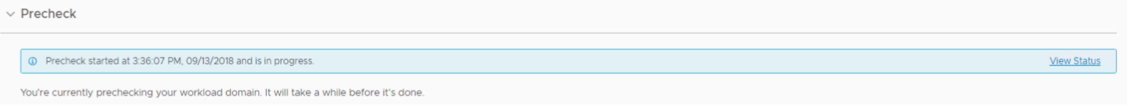
Resource Changes

psc-2.vrack.vsphere.local 6.5.0-9451637 → 6.5.0-10056541

Additional Bundle Details

Version	156.0.98-103948
Severity	Major
Vendor	VMware
Bundle ID	4a066ea8-6123-4e2a-a077-560aa93f5245
Software Component 1	PSC
Description	PSC
Update to Version	6.5.0-10056541
Required Version	6.5.0-9451637
Release date	09/13/2018
Vendor	VMware

4 Click **Precheck** to validate that the workload domain is ready to be updated.

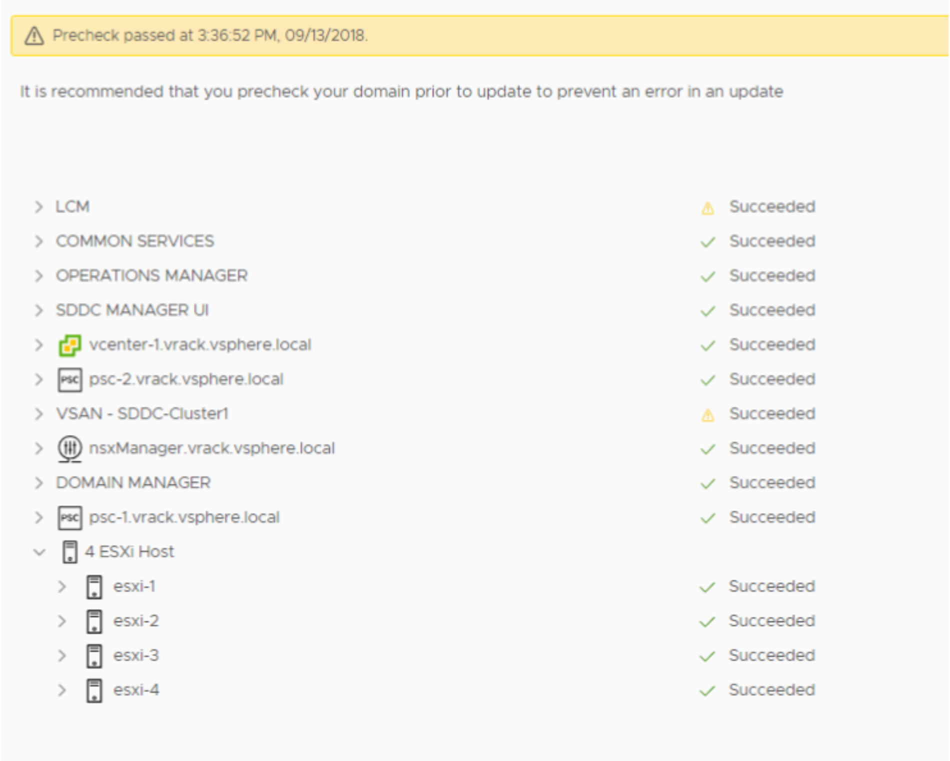


Precheck

Precheck started at 3:36:07 PM, 09/13/2018 and is in progress.

You're currently prechecking your workload domain. It will take a while before it's done.

   Click **View Status** to see the update status for each component and the tests performed. Expand a test by clicking the arrow next to it to see further details.



⚠ Precheck passed at 3:36:52 PM, 09/13/2018.

It is recommended that you precheck your domain prior to update to prevent an error in an update

> LCM	⚠ Succeeded
> COMMON SERVICES	✓ Succeeded
> OPERATIONS MANAGER	✓ Succeeded
> SDDC MANAGER UI	✓ Succeeded
> vcenter-1.vrack.vsphere.local	✓ Succeeded
> psc-2.vrack.vsphere.local	✓ Succeeded
> VSAN - SDDC-Cluster1	⚠ Succeeded
> nsxManager.vrack.vsphere.local	✓ Succeeded
> DOMAIN MANAGER	✓ Succeeded
> psc-1.vrack.vsphere.local	✓ Succeeded
∨ 4 ESXi Host	
> esxi-1	✓ Succeeded
> esxi-2	✓ Succeeded
> esxi-3	✓ Succeeded
> esxi-4	✓ Succeeded

If any of the tests fail, fix the issue and click **Retry Precheck**.

The precheck results are displayed below the Precheck button. Ensure that the precheck results are green before proceeding. A failed precheck may cause the update to fail.

5 To start the update, click **Update Now** next to the relevant bundle or schedule it for a specific date and time depending on your maintenance window.

What to do next

Monitor the update.

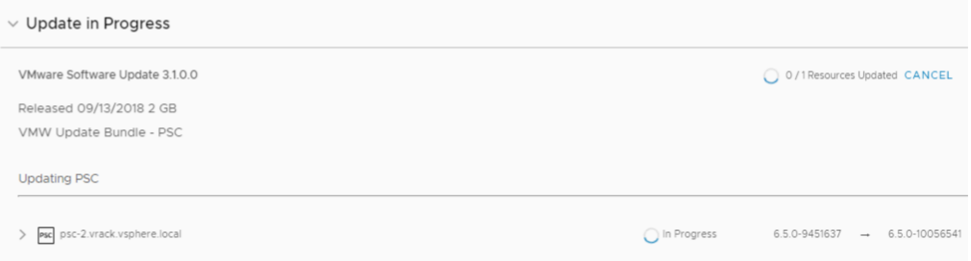
Monitor Update

Monitor the update progress on your workload domain

Procedure

1 The Update in Progress section in the workload domain detail page displays the high level update progress and the number of components to be updated.

2 Details of the component being updated is shown below that.



Update in Progress

VMware Software Update 3.1.0.0

0 / 1 Resources Updated CANCEL

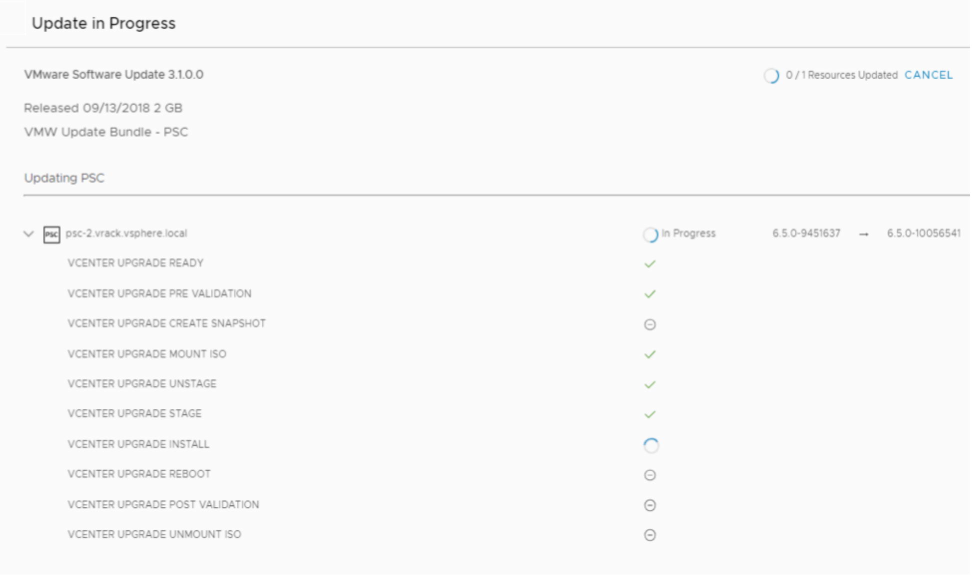
Released 09/13/2018 2 GB

VMW Update Bundle - PSC

Updating PSC

psc-2.vrack.vsphere.local In Progress 6.5.0-9451637 → 6.5.0-10056541

3 Click the arrow to see a list of tasks being performed to update the component. As the task is completed, it shows a green check mark.



Update in Progress

VMware Software Update 3.1.0.0

0 / 1 Resources Updated CANCEL

Released 09/13/2018 2 GB

VMW Update Bundle - PSC

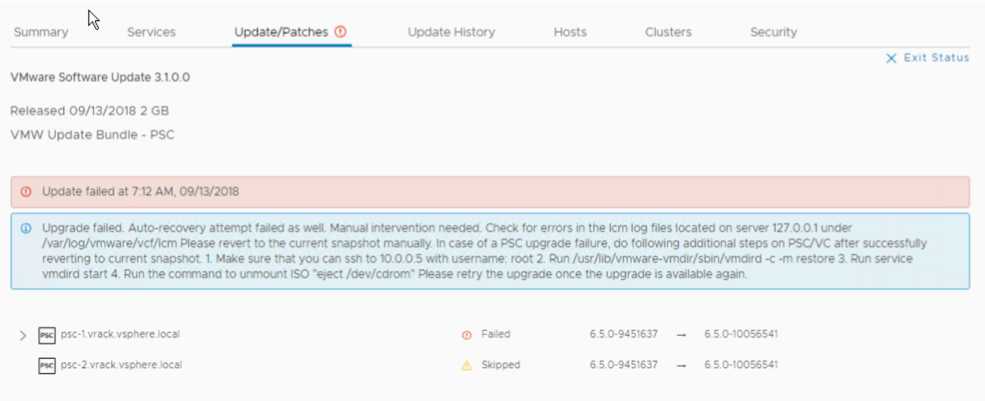
Updating PSC

psc-2.vrack.vsphere.local In Progress 6.5.0-9451637 → 6.5.0-10056541

VCENTER UPGRADE READY	✓
VCENTER UPGRADE PRE VALIDATION	✓
VCENTER UPGRADE CREATE SNAPSHOT	⊝
VCENTER UPGRADE MOUNT ISO	✓
VCENTER UPGRADE UNSTAGE	✓
VCENTER UPGRADE STAGE	✓
VCENTER UPGRADE INSTALL	○
VCENTER UPGRADE REBOOT	⊝
VCENTER UPGRADE POST VALIDATION	⊝
VCENTER UPGRADE UNMOUNT ISO	⊝

4 When all tasks to update a component have been completed, the update status for the component is displayed as Updated.

5 If a component fails to be updated, the status is displayed as Failed. The reason for the failure as well as remediation steps are displayed.



VMware Software Update 3.1.0.0

Released 09/13/2018 2 GB

VMW Update Bundle - PSC

Update failed at 7:12 AM, 09/13/2018

Upgrade failed. Auto-recovery attempt failed as well. Manual intervention needed. Check for errors in the lcm log files located on server 127.0.0.1 under /var/log/vmware/vcf/lcm Please revert to the current snapshot manually. In case of a PSC upgrade failure, do following additional steps on PSC/VC after successfully reverting to current snapshot. 1. Make sure that you can ssh to 10.0.0.5 with username: root 2. Run /usr/lib/vmware-vmdir/sbin/vmdird -c -m restore 3. Run service vmdird start 4. Run the command to unmount ISO "eject /dev/cdrom" Please retry the upgrade once the upgrade is available again.

psc-1.vrack.vsphere.local	Failed	6.5.0-9451637	→	6.5.0-10056541
psc-2.vrack.vsphere.local	Skipped	6.5.0-9451637	→	6.5.0-10056541

6 After you resolve the issues, the bundle becomes available. You can then apply the bundle or schedule it to be applied at a specific date and time.

What to do next

1 Remove the VM snapshots you had taken before starting the update.

2 Take a backup of the newly installed components.

Skip Hosts During ESXi Update

You can skip hosts while applying an ESXi update to the management domain or a VI workload domain. The skipped hosts are not updated.

Procedure

1 Retrieve the host IDs for the hosts you want to skip.

   a Open a new tab in the browser where you are running SDDC Manager and type the following URL:

   `https://`*SDDC_Manager_IP*`/inventory/esxis`

   Here is a sample output:

```
{
"vcenterId": "d1a239e1-baef-11e8-a2de-d1b89736a031",
"networkPoolId": "d3643003-c854-43e7-91ad-fd8d0711a02f",
"bundleRepoDatastore": "lcm-bundle-repo",
"domainId": "d0ef8bb0-baef-11e8-a2de-d1b89736a031",
"clusterId": "d1b106f1-baef-11e8-a2de-d1b89736a031",
"vsanIpAddress": "10.0.4.3",
"vmotionIpAddress": "10.0.8.3",
"hostAttributes": {},
"dirty": false,
"id": "d19d57e1-baef-11e8-a2de-d1b89736a031",
"status": "ACTIVE",
"version": "6.5.0-9298722",
"hostName": "esxi-1.vrack.vsphere.local",
"privateIpAddress": "10.0.0.100",
"managementIpAddress": "10.0.0.100"
}
```

   b Copy the appropriate host IDs.

2 Using SSH, log in to the SDDC Manager VM with the user name `vcf` and password you specified in the deployment parameter sheet.

3 Type `su` to switch to the root account.

4 Open the `/opt/vmware/vcf/lcm-app/conf/application-prod.properties` file.

5 At the end of the file , add the following line:

   `esx.upgrade.skip.host.ids=`*host id1*`,`*host id2*

6 Save and close the file.

7 Restart the LCM server by typing the following command in the console window:

```
systemctl restart lcm
```

The hosts added to the `application-prod.properties` are not updated when you update the workload domain.

View Update History

The Update History page displays all updates applied to a workload domain.

Procedure

1 In the SDDC Manager Dashboard, click **Inventory > Workload Domains**..

2 Click the name of a workload domain and then click the **Updates History** tab.

All updates applied to this workload domain are displayed. If an update bundle was applied more than once, click **View Past Attempts** to see more information.

View Bundle Download History

The Bundle Download History page displays all bundles that have been downloaded.

Procedure

◆ In the SDDC Manager Dashboard, click **Repository > Download History**.

All downloaded bundles are displayed. Click **View Details** to see bundle metadata details.

Access LCM Log Files

1 Log in to the SDDC Manager VM with the `vcf` user name and the password you specified in the deployment parameter sheet.

2 To access LCM logs, navigate to the `/var/log/vmware/vcf/lcm` directory.

- `lcm-debug` log file contains debug level logging information.
- `lcm.log` contains information level logging.

3 To create an sos bundle for support, see Chapter 11 Supportability and Serviceability (SoS) Tool.

Cloud Foundation Glossary

15

Term	Description
bring-up	Initial configuration of a newly deployed Cloud Foundation system. During the bring-up process, the management domain is created and the Cloud Foundation software stack is deployed on the management domain.
commission host	Adding a host to Cloud Foundation inventory. The host remains in the free pool until it is assigned to a workload domain.
dirty host	A host that has been removed from a cluster in a workload domain. A dirty host cannot be assigned to another workload domain until it is cleaned up.
decommission host	Remove an unassigned host from the Cloud Foundation inventory. SDDC Manager does not manage decommissioned hosts.
free pool	Hosts in the Cloud Foundation inventory that are not assigned to a workload domain
host	An imaged server.
inventory	Logical and physical entities managed by Cloud Foundation.
Lifecycle Manager (LCM)	Automates patching and upgrading of the software stack.
management domain	Cluster of physical hosts that contains the management component VMs
network pool	Automatically assigns static IP addresses to vSAN and vMotion vmkernel ports so that you don't need to enter IP addresses manually when creating a VI workload domain or adding a host or cluster to a workload domain.
patch update bundle	Contains bits to update the appropriate Cloud Foundation software components in your management or VI workload domain.
SDDC Manager	Software component that provisions, manages, and monitors the logical and physical resources of a Cloud Foundation system.
SDDC Manager VM	Virtual machine (VM) that contains the SDDC Manager services and a shell from which command line tools can be run. This VM exposes the SDDC Manager UI.
server	Bare metal server in a physical rack. After imaging, it is referred to as a host.
unassigned host	Host in the free pool that does not belong to a workload domain.
workload domain	A policy based resource container with specific availability and performance attributes that combines vSphere, vSAN and NSX into single a consumable entity. A workload domain can be created, expanded, and deleted as part of the SDDC lifecycle operations. It can contain cluster(s) of physical hosts with a corresponding vCenter to manage them. The vCenter for a workload domain physically lives in the management domain.