

VMware Cloud Foundation Lifecycle Management

09 FEB 2021

VMware Cloud Foundation 4.2

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

<https://docs.vmware.com/>

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

Copyright © 2019-2021 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

| | | |
|----------|-----------------------------------------------------------------------|-----------|
| 1 | About VMware Cloud Foundation Lifecycle Management | 5 |
| 2 | VMware Cloud Foundation Bundle Management | 7 |
| | Bundle Types | 8 |
| | Update or Upgrade Bundles | 8 |
| | Install Bundles | 8 |
| | Download Bundles | 8 |
| | Online Bundle Download | 8 |
| | Download Bundles from SDDC Manager | 8 |
| | Download Bundles With a Proxy Server | 10 |
| | Offline Bundle Download for VMware Cloud Foundation | 11 |
| | Download Specific Bundles | 13 |
| | View Bundle Download History | 14 |
| 3 | Upgrading to VMware Cloud Foundation 4.2.1 or 4.2 | 15 |
| | Upgrade Prerequisites | 16 |
| | Perform Update Precheck | 16 |
| | Upgrade to VMware Cloud Foundation 4.2.1 | 18 |
| | Upgrade to VMware Cloud Foundation 4.2 | 19 |
| | Upgrade the Management Domain to VMware Cloud Foundation 4.2 | 19 |
| | Upgrade VMware Cloud Foundation Software | 20 |
| | Upgrade vRealize Suite Lifecycle Manager and vRealize Suite Products | 22 |
| | Upgrade VI Workload Domains to VMware Cloud Foundation 4.2 | 26 |
| | Upgrade NSX-T Data Center | 27 |
| | Upgrade vCenter Server | 29 |
| | Upgrade ESXi | 30 |
| | Upgrade vSAN Witness Host | 33 |
| 4 | Upgrade ESXi with Custom ISO or Async Drivers | 35 |
| | Upgrade ESXi with Custom ISO | 35 |
| | Upgrade ESXi with VMware Cloud Foundation Stock ISO and Async Drivers | 37 |
| 5 | Skip Hosts During ESXi Update | 40 |
| 6 | Monitor Updates | 43 |
| 7 | View Update History | 45 |

8 Access Upgrade Log Files 46

About VMware Cloud Foundation Lifecycle Management

1

The *VMware VMware Cloud Foundation Lifecycle Management* describes how to manage the lifecycle of a VMware Cloud Foundation environment. The information includes prerequisites, step-by-step configuration instructions, and suggested best practices.

Intended Audience

The *VMware Cloud Foundation Lifecycle Management* 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 vRealize® Log Insight™
- VMware Horizon®
- VMware App Volumes™

Related Publications

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

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

The *VMware 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.

VMware Cloud Foundation Bundle Management

2

You must download bundles in order to upgrade, install, or patch various VMware Cloud Foundation components. Once the bundles are available in the SDDC Manager UI, you can proceed with installation, upgrade, or patching.

VMware Cloud Foundation includes the following types of bundles.

- **Install Bundles**

An install bundle includes software binaries to install VI workload domains and vRealize Suite Lifecycle Manager. vRealize Suite install bundles can be downloaded and synchronized to vRealize Suite Lifecycle Manager.

VMware Cloud Foundation includes the following install bundles:

- A VI workload domain install bundle is used to deploy later versions of the software components instead of the versions in your original VMware Cloud Foundation installation. It includes software binaries for vCenter Server and NSX-T Data Center.
- The vRealize Suite Lifecycle Manager install bundle is used for deploying vRealize Suite Lifecycle Manager.
- The Workspace ONE Access install bundle is used for deploying Workspace ONE Access.
- Install bundles are also available for vRealize Operations, vRealize Log Insight and vRealize Automation. These are synchronized with and can be deployed from vRealize Suite Lifecycle Manager.

- **Update or Upgrade Bundle**

An update or upgrade bundle includes software binaries to update the appropriate VMware Cloud Foundation software components. In most cases, an upgrade bundle must be applied to the management domain before it can be applied to VI workload domains.

- **Async Patch Bundle**

An async patch bundle allows you to apply critical patches to certain VMware Cloud Foundation components (NSX-T Manager, vCenter Server, and ESXi) when an update or upgrade bundle is not available. See [Async Patch Tool](#).

Bundle Types

Cloud Foundation includes two types of bundles.

Update or Upgrade Bundles

An update or upgrade bundle contains bits to update the appropriate Cloud Foundation software components in your management domain or VI workload domain. In most cases, an upgrade bundle must be applied to the management domain before it can be applied to 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, vRealize Suite products, and Workspace ONE Access.

- A VI workload domain install bundle is used to deploy later versions of the software components instead of the versions in your Cloud Foundation Bill of Materials.
- An install bundle is required for deploying vRealize Suite products and Workspace ONE Access.

Download Bundles

If LCM is configured to work with 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.

Online Bundle Download

You can either download bundles through the SDDC Manager Dashboard or through a proxy server.

- [Download Bundles from SDDC Manager](#)

When upgrade bundles are available for your environment, a message is displayed on the SDDC Manager Dashboard. Available install bundles are displayed on the Bundle Management page.

- [Download Bundles With a Proxy Server](#)

If you do not have internet access, you can use a proxy server to download bundles. VMware Cloud Foundation only supports proxy servers that do not require authentication.

Download Bundles from SDDC Manager

When upgrade bundles are available for your environment, a message is displayed on the SDDC Manager Dashboard. Available install bundles are displayed on the Bundle Management page.

The Bundle Management page displays upgrade bundles that are applicable to your environment. For example, if your environment is at VMware Cloud Foundation 4.1, upgrade bundles for both VMware Cloud Foundation 4.1.0.1 and VMware Cloud Foundation 4.2 are displayed.

To download an install bundle, navigate to **Repository > Bundle Management** on the SDDC Manager Dashboard to view the available bundles. Then follow the instructions in step 4 below.

Prerequisites

Automatic polling of the manifest for bundles by SDDC Manager must be enabled (Default setting). If you have previously edited the application-prod.properties file on SDDC Manager VM to download upgrade bundles in an offline mode, you must edit it again before downloading bundles from SDDC Manager. Follow the steps below:

- 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 Open the `/opt/vmware/vcf/lcm/lcm-app/conf/application-prod.properties` file.
- 4 Set `lcm.core.enableManifestPolling=true`.
- 5 Restart LCM service with the command below:

```
systemctl restart lcm
```

Procedure

- 1 Log in to your My VMware Account.
 - a On the SDDC Manager Dashboard, click **Administration > Repository Settings**.
 - b Click **Authenticate**.

The My VMware Account Authentication page appears.

The screenshot shows a web form titled "My VMware Account Authentication". It includes a close button (X) in the top right corner. There are two input fields: "User Name" with the placeholder text "Enter user name" and "Password" with the placeholder text "Password" and an eye icon to toggle password visibility. At the bottom right, there are two buttons: "CANCEL" and "AUTHORIZE".

- c Type your user name and password.

- d Click **Authorize**.
- 2 View available bundles by navigating to **Lifecycle Management > Bundle Management** on the SDDC Manager Dashboard.

The Bundles page displays the bundles available for download. The Bundle Details section displays the bundle version and release date.

If the bundle can be applied right away, the Bundle Details column displays the workload domains to which the bundle needs to be applied to, and the Availability column says Available. If another bundle needs to be applied before a particular bundle, the Availability field displays Future.

- 3 To view more information about the bundle, click **View Details**.

The Bundle Details section displays the bundle version, release date, and additional details about the bundle.

- 4 Click **Exit Details**.
- 5 Specify when to download the bundle.
 - Click **Download Now** to start the download immediately.
 - Click **Schedule Download** to set the date and time for the bundle download.

Results

The Download Status section displays the date and time at which the bundle download has been scheduled. When the download begins, the status bar displays the download progress.

Download Bundles With a Proxy Server

If you do not have internet access, you can use a proxy server to download bundles. VMware Cloud Foundation only supports proxy servers that do not require authentication.

Procedure

- 1 Log in to the SDDC Manager appliance by using a Secure Shell (SSH) client.
Use the user name `vcf` and password that you had specified in the deployment parameter worksheet. Username:
- 2 Enter `su` to switch to the root user and enter the password.
- 3 Open the `/opt/vmware/vcf/lcm/lcm-app/conf/application-prod.properties` file.
- 4 Update the following lines at 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 Ensure that the ownership of the `application-prod.properties` file is set to `vcf_lcm:vcf`.

- 7 Restart Lifecycle Management by typing the following command in the console window:

```
systemctl restart lcm
```

- 8 Wait for 5 minutes and then download the bundles. See [Download Bundles from SDDC Manager](#).

Offline Bundle Download for VMware Cloud Foundation

Lifecycle Management polls the VMware depot to access update bundles. If you do not have internet connectivity in your VMware Cloud Foundation system, you can use the Bundle Transfer utility to manually download the bundles from the depot on your local computer and then upload them to the SDDC Manager appliance.

Prerequisites

- A Windows or Linux computer with internet connectivity for downloading the bundles.
- The computer must have Java 8 or later.
- A Windows or Linux computer with access to the SDDC Manager appliance for uploading the bundles.
- To upload the manifest file from a Windows computer, you must have OpenSSL installed and configured.
- Configure TCP keepalive in your SSH client to prevent socket connection timeouts when using the Bundle Transfer Utility for long-running operations.

Procedure

- 1 Download the Bundle Transfer utility on a computer with internet access.
 - a Log in to VMware Customer Connect and browse to the Download VMware Cloud Foundation page.
 - b In the **Select Version** field, select the version to which you are upgrading.
 - c Click **Drivers & Tools**.
 - d Expand VMware Cloud Foundation Supplemental Tools.
 - e Click **Download Now** for the Bundle Transfer Utility.
- 2 Extract `lcm-tools-prod.tar.gz`.
- 3 Navigate to the `lcm-tools-prod/bin/` and confirm that you have execute permission on all folders.
- 4 Copy the bundle transfer utility to a computer with access to the SDDC Manager appliance and then copy the bundle transfer utility to the SDDC Manager appliance.
 - a SSH in to the SDDC Manager appliance using the `vcf` user account.
 - b Enter `su` to switch to the root user.

- c Create the `lcm-tools` directory.

```
mkdir /opt/vmware/vcf/lcm/lcm-tools
```

- d Copy the bundle transfer utility file (`lcm-tools-prod.tar.gz`) that you downloaded in step 1 to the `/opt/vmware/vcf/lcm/lcm-tools` directory.
- e Extract the contents of `lcm-tools-prod.tar.gz`.
- f Set the permissions for the `lcm-tools` directory.

```
cd /opt/vmware/vcf/lcm/
    chown vcf_lcm:vcf -R lcm-tools
    chmod 750 -R lcm-tools
```

- 5 On the computer with internet access, download the manifest file. This is a structured metadata file that contains information about the VMware product versions included in the release Bill of Materials.

```
./lcm-bundle-transfer-util --download --manifestDownload --depotUser
Username
```

Enter your VMware Customer Connect password when prompted.

- 6 Copy the manifest file and `lcm-tools-prod` directory to a computer with access to the SDDC Manager appliance.
- 7 Upload the manifest file to the SDDC Manager appliance.

```
./lcm-bundle-transfer-util --update --sourceManifestDirectory Manifest-Downloaded-
Directory --sddcMgrFqdn FQDN --sddcMgrUser Username
```

Use your vSphere SSO credentials for the `--sddcMgrUser` parameter.

- 8 On the computer with internet access, run the following command.

```
./lcm-bundle-transfer-util --download --outputDirectory absolute-path-output-dir --
depotUser depotUser --sv current-vcf-version --p target-vcf-version
```

where

| | |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>absolute-path-output-dir</i> | Path to the directory where the bundle files should 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. |
| <i>depotUser</i> | User name for the VMware depot (VMware Customer Connect). You will be prompted to enter the depot user password. If there are any special characters in the password, specify the password within single quotes. |
| <i>current-vcf-version</i> | Current version of VMware Cloud Foundation. For example, 4.3.1.1 . If you do not specify a current version, the utility uses 4.1.0.0 . |
| <i>target-vcf-version</i> | Target version of VMware Cloud Foundation. For example, 4.4.0.0 . |

After you enter your VMware Customer Connect password, the utility asks Do you want to download vRealize bundles?. Enter **Y** or **N**.

The utility displays a list of the available bundles based on the current and target versions of VMware Cloud Foundation.

9 Specify the bundles to download.

Enter one of the following options:

- **all**
- **install**
- **patch**

You can also enter a comma-separated list of bundle names to download specific bundles. For example: **bundle-38371, bundle-38378**.

Download progress for each bundle is displayed.

10 When the bundle downloads complete, copy the entire output directory to a computer with access to the SDDC Manager appliance, and then copy it to the SDDC Manager appliance.

For example:

```
scp -pr /root/upgrade-bundles vcf@SDDC_MANAGER_IP:/nfs/vmware/vcf/nfs-mount/
```

The `scp` command in the example above copies the output directory (`upgrade-bundles`) to the `/nfs/vmware/vcf/nfs-mount/` directory on the SDDC Manager appliance.

11 Upload the directory to the internal LCM repository.

```
cd /opt/vmware/vcf/lcm/lcm-tools/bin
./lcm-bundle-transfer-util --upload --bundleDirectory absolute-path-bundle-dir
```

where *absolute-path-bundle-dir* is the directory where the bundle files have been uploaded, or `/nfs/vmware/vcf/nfs-mount/upgrade-bundles` as shown in the previous step.

The utility uploads the bundles and displays upload status for each bundle. Wait for all bundles to be uploaded before proceeding with an upgrade.

Download Specific Bundles

Using the Bundle Transfer utility, you can download specific bundles.

The Bundle Transfer utility includes the following options for downloading specific bundles:

- Download the bundles for a specific version of VMware Cloud Foundation.

```
./lcm-bundle-transfer-util --download --outputDirectory Output-Dir --depotUser depotUser
--productVersion product_version
```

For *product_version*, enter a four-digit version number, for example **4.2.1.0**.

Note This method only lists the bundles for the specific VMware Cloud Foundation version. It does not include any intermediate bundles you may need to upgrade to this version. If you want to download all the bundles required for an upgrade, including intermediate bundles, see [Offline Bundle Download for VMware Cloud Foundation](#).

- Download bundles of a specific type.

```
./lcm-bundle-transfer-util --download --outputDirectory Output-Dir --depotUser depotUser
--imageType image_type
```

For *image_type*, enter **INSTALL** for install bundles or **PATCH** for upgrade bundles.

- Download a specific bundle.

```
./lcm-bundle-transfer-util --download --outputDirectory Output-Dir --depotUser depotUser
--bundle bundle_id
```

For *bundle_id*, enter the bundle ID. For example, **bundle-42515**. To determine the bundle ID for a specific bundle, you can use the `--listBundles` option. For example:

```
./lcm-bundle-transfer-util --depotUser depotUser --listBundles
```

You can use the `--listBundles` option in conjunction with the `--productVersion` or `--imageType` option to narrow the list of bundles that displays. For example:

```
./lcm-bundle-transfer-util --depotUser depotUser --listBundles --productVersion 4.2.1.0
```

or

```
./lcm-bundle-transfer-util --depotUser depotUser --listBundles --imageType INSTALL
```

View Bundle Download History

The Bundle Download History page displays all bundles that have been downloaded.

Procedure

- ◆ In the SDDC Manager Dashboard, click **Repository > Bundle Management > Download History**.

All downloaded bundles are displayed. Click **View Details** to see bundle metadata details.

Upgrading to VMware Cloud Foundation 4.2.1 or 4.2

3

The following procedures provide information about upgrading to VMware Cloud Foundation 4.2.1 or VMware Cloud Foundation 4.2.

You can perform a sequential or skip level upgrade to VMware Cloud Foundation 4.2.1 from VMware Cloud Foundation 4.2, 4.1.0.1, or 4.1.

You can perform a sequential or skip level upgrade to VMware Cloud Foundation 4.2 from VMware Cloud Foundation 4.1 or 4.1.0.1. If your environment is at a version earlier than 4.1, you must upgrade the management domain and all VI workload domains to VMware Cloud Foundation 4.1 and then upgrade to VMware Cloud Foundation 4.2.

Your environment may contain workload domains at different VMware Cloud Foundation releases. After upgrading to VMware Cloud Foundation 4.2.1 or 4.2, you can view the versions in your environment and the associated component versions in that release by navigating to **Lifecycle Management > Release Versions**. Note that the management domain and VI workload domains must be upgraded to the same release version. For example, suppose your environment is at VMware Cloud Foundation 4.1. If you are upgrading to VMware Cloud Foundation 4.2, the management domain and VI workload domains must be upgraded to this release.

Note You cannot upgrade to VMware Cloud Foundation 4.2 if you have Federation 3.0.x in your environment.

Upgrades are applied on a workload domain basis. The management domain contains the core infrastructure, so you must upgrade the management domain before upgrading the other VI workload domains. You must upgrade all required components to keep your system in an optimum state.

This chapter includes the following topics:

- [Upgrade Prerequisites](#)
- [Perform Update Precheck](#)
- [Upgrade to VMware Cloud Foundation 4.2.1](#)
- [Upgrade to VMware Cloud Foundation 4.2](#)
- [Upgrade NSX-T Data Center](#)
- [Upgrade vCenter Server](#)

- [Upgrade ESXi](#)
- [Upgrade vSAN Witness Host](#)

Upgrade Prerequisites

Ensure that the following prerequisites are met before starting an upgrade.

- Take a backup of the SDDC Manager appliance. This is required since the SDDC Manager appliance will be rebooted during the update.
- Take a snapshot of relevant VMs in your management domain.
- 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.
- You must have downloaded the relevant bundles. See [Download Bundles](#). If you downloaded the bundles manually, you must download all bundles for the target release and upload them to the SDDC Manager appliance before starting the upgrade.
- If you applied an async patch to your current VMware Cloud Foundation instance you must use the Async Patch Tool to upgrade to a later version of VMware Cloud Foundation. For example, if you applied an async vCenter Server patch to a VMware Cloud Foundation 4.2 instance, you must use the Async Patch Tool to upgrade to VMware Cloud Foundation 4.4. See [Async Patch Tool](#).
- Ensure that there are no failed workflows in your system and none of the Cloud Foundation resources are in activating or error state. If any of these conditions are true, contact VMware Support before starting the update.
- Confirm that the passwords for all VMware Cloud Foundation components are valid.

Perform Update Precheck

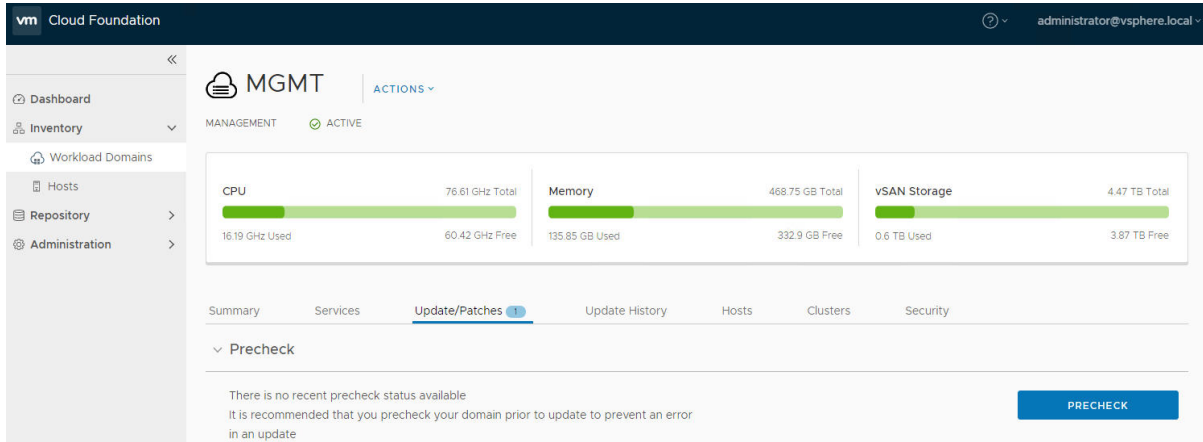
You must perform a precheck before applying a patch bundle to ensure that your environment is ready for the update. For an ESXi bundle, the system performs a bundle level precheck in addition to the environment precheck.

For workload domains using vLCM baselines, the ESXi bundle precheck validates the following.

- Custom ISO is compatible with your environment.
- Custom ISO size is smaller than the boot partition size.
- Third party VIBs are compatible with the environment.

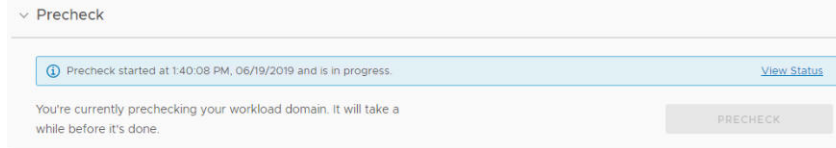
Procedure

- 1 Navigate to the Updates/Patches tab of the management domain or workload domain where you need to apply the bundle. The image below is a sample screenshot and may not reflect the correct product versions.



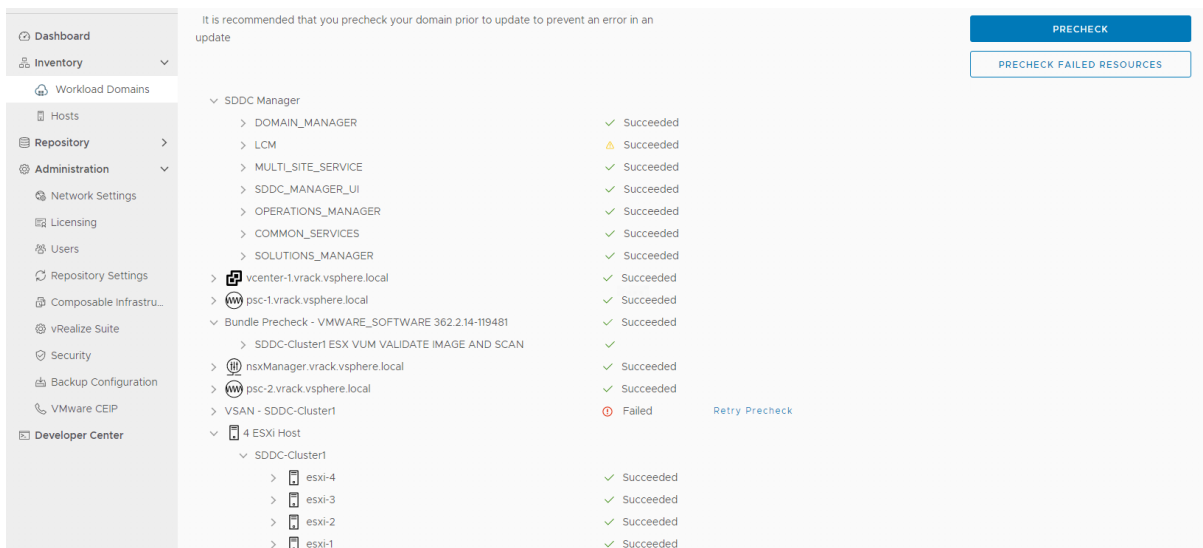
- 2 Click **Precheck** to validate that the environment is ready to be upgraded. If you run the precheck before upgrading ESXi and there are multiple ESXi bundles available (for example, during a cumulative upgrade), a dialog box appears asking you to select the bundle that you want to validate during the precheck.

Once the precheck begins, a message appears indicating the time at which the precheck was



started.

- 3 Click **View Status** to see detailed tasks and their status. The image below is a sample screenshot and may not reflect the correct versions.



- 4 To see details for a task, click the Expand arrow.

If a precheck task failed, fix the issue, and click **Retry Precheck** to run the task again. You can also click **Precheck Failed Resources** to retry all failed tasks.

If ESXi hosts display a driver incompatibility issue when updating a workload domain using vLCM baselines, perform the following steps:

- a Identify the controller with the HCL issue.
- b For the given controller, identify the supported driver and firmware versions on the source and target ESXi versions.
- c Upgrade the firmware, if required.
- d Upgrade the driver manually on the ESXi host and retry the task at which the upgrade failed.

For information on updating passwords, see "Updating SDDC Manager Passwords" in the *VMware Cloud Foundation Operations and Administration Guide*.

Results

The precheck result is displayed at the top of the Upgrade Precheck Details window. If you click **Exit Details**, the precheck result is displayed at the top of the Precheck section in the Updates/Patches tab.

Ensure that the precheck results are green before proceeding. A failed precheck may cause the update to fail.

Upgrade to VMware Cloud Foundation 4.2.1

You can upgrade to VMware Cloud Foundation 4.2.1 from VMware Cloud Foundation 4.2, 4.1.0.1, or 4.1.

Upgrade to VMware Cloud Foundation 4.2.1 from VMware Cloud Foundation 4.2

Upgrading to VMware Cloud Foundation 4.2.1 involves the following tasks.

- 1 Upgrade the management domain.

Components in the management domain must be upgraded in the following order:

- a VMware Cloud Foundation software. See [Upgrade VMware Cloud Foundation Software](#).
- b vCenter Server. See [Upgrade vCenter Server](#).
- c NSX-T Data Center. See [Upgrade NSX-T Data Center](#).

- 2 Upgrade VI workload domains.

Components in VI workload domains must be upgraded in the following order:

- a vCenter Server. See [Upgrade vCenter Server](#).

- b NSX-T Data Center. See [Upgrade NSX-T Data Center](#).

Upgrade to VMware Cloud Foundation 4.2.1 from VMware Cloud Foundation 4.1.0.1 or 4.1

Upgrading to VMware Cloud Foundation 4.2.1 involves the following tasks.

- 1 Upgrade the management domain.

Components in the management domain must be upgraded in the following order:

- a VMware Cloud Foundation software. See [Upgrade VMware Cloud Foundation Software](#).
- b vRealize Suite Lifecycle Manager and vRealize Suite products. See [Upgrade vRealize Suite Lifecycle Manager](#).
- c ESXi. See [Upgrade ESXi](#).
- d vCenter Server. See [Upgrade vCenter Server](#).
- e NSX-T Data Center. See [Upgrade NSX-T Data Center](#).

- 2 Upgrade VI workload domains.

Components in VI workload domains must be upgraded in the following order:

- a ESXi. See [Upgrade ESXi](#).
- b vCenter Server. See [Upgrade vCenter Server](#).
- c NSX-T. See [Upgrade NSX-T Data Center](#).

Note NSX-T upgrade is not supported on a vLCM image based stretch cluster. You must unstretch the cluster before proceeding with the upgrade.

- d Workload Management on clusters that have vSphere with Tanzu. Workload Management can be upgraded through vCenter Server. See [Working with vSphere Lifecycle Manager](#).

Upgrade to VMware Cloud Foundation 4.2

You can upgrade to VMware Cloud Foundation 4.2 from VMware Cloud Foundation 4.1.0.1 or VMware Cloud Foundation 4.1.

Upgrade the Management Domain to VMware Cloud Foundation 4.2

You must upgrade the management domain before upgrading workload domains in your environment. In order to upgrade to VMware Cloud Foundation 4.2, the management domain must be at VMware Cloud Foundation 4.1 or 4.1.0.1.

Components in the management domain must be upgraded in the following order:

- 1 SDDC Manager and VMware Cloud Foundation services. See [Upgrade VMware Cloud Foundation Software](#).

- 2 vRealize Suite Lifecycle Manager and vRealize Suite products. See [Upgrade vRealize Suite Lifecycle Manager](#).
- 3 NSX-T Data Center. See [Upgrade NSX-T Data Center](#).
- 4 vCenter Server. See [Upgrade vCenter Server](#).
- 5 ESXi. See [Upgrade ESXi](#).

Upgrade VMware Cloud Foundation Software

The VMware Cloud Foundation software bundle to be applied depends on the current version of your environment.

If you upgrading from VMware Cloud Foundation 4.2.1, 4.2, or 4.1.0.1, you must apply the following bundles to the management domain:

- The VMware Cloud Foundation Upgrade bundle, which contains critical bugs and security fixes for the SDDC Manager appliance.
- The Configuration Drift bundle, which applies configuration changes across the managed components.

If you upgrading from VMware Cloud Foundation 4.1, you only need to apply either the upgrade or configuration drift bundle.

Apply VMware Cloud Foundation Upgrade Bundle

The VMware Cloud Foundation Upgrade bundle upgrades the SDDC Manager appliance and Lifecycle Management.

Prerequisites

- Download the VMware Cloud Foundation update bundle for your target release. See [Download Bundles](#).
- Ensure you have a recent successful backup of SDDC Manager using an external SFTP server.
- Ensure you have taken a snapshot of the SDDC Manager appliance.
- Ensure you have recent successful backups of the components managed by SDDC Manager.

Procedure

- 1 In the navigation pane, click **Inventory > Workload Domains**.
- 2 On the Workload Domains page, click the management domain and then click the **Updates/Patches** tab.
- 3 Run the upgrade precheck. See [Perform Update Precheck](#).
- 4 In the **Available Updates** section, select the target release.
- 5 Click **Update Now** or **Schedule Update** next to the VMware Cloud Foundation Upgrade bundle.

- 6 If you selected **Schedule Update**, select the date and time for the bundle to be applied and click **Schedule**.

If you clicked **Update Now**, the VMware Cloud Foundation Update Status window displays the components that will be upgraded and the upgrade status. Click **View Update Activity** to view the detailed tasks. After the upgrade is completed, a green bar with a check mark is displayed.

- 7 Click **Finish**.

- The Available Updates section displays a VMware Cloud Foundation target version. Select a target version to view the next bundle to be applied.
- The Release Versions tab is available within the Lifecycle Management option in the left navigation pane. This page displays the VMware Cloud Foundation versions in your environment and the associated component versions in that release.

What to do next

- If you are upgrading from VMware Cloud Foundation 4.2.1, 4.2 or 4.1.0.1, apply the Configuration Drift bundle. See [Apply Configuration Drift Bundle](#).
- If you are upgrading from VMware Cloud Foundation 4.1, continue upgrading the management domain See [Upgrade the Management Domain to VMware Cloud Foundation 4.2](#).

Apply Configuration Drift Bundle

The configuration drift bundle applies configuration changes required for 2nd party software components in the VMware Cloud Foundation Bill of Materials for the target release. Configuration changes are applied to the management domain and may also affect VI workload domains in your environment. However, there is no downtime on VI workload domains and they need not be in a maintenance window.

You only need to apply the configuration drift bundle if you are upgrading from VMware Cloud Foundation 4.2.1, 4.2, or 4.1.0.1.

Prerequisites

- Download the configuration drift bundle for your target release. See [Download Bundles](#).
- Ensure that you have a recent successful backup of SDDC Manager using an external SFTP server.
- Ensure that you have taken a snapshot of the SDDC Manager appliance.

- Ensure that you have recent successful backups of the components managed by SDDC Manager.

Procedure

- 1 In the navigation pane, click **Inventory > Workload Domains**.
- 2 On the Workload Domains page, click the management domain and then click the **Updates/Patches** tab.
- 3 Run the upgrade precheck. See [Perform Update Precheck](#).
- 4 In the Available Updates section, click **Update Now** or **Schedule Update** next to the VMware Cloud Foundation Configuration drift bundle.
- 5 If you selected **Schedule Update**, select the date and time for the bundle to be applied and then click **Schedule**.

After the upgrade is completed, a green bar with a check mark is displayed.

- 6 Click **Finish**.

What to do next

Continue upgrading the management domain. See [Upgrade the Management Domain to VMware Cloud Foundation 4.2](#) or [Upgrade VI Workload Domains to VMware Cloud Foundation 4.2](#).

Upgrade vRealize Suite Lifecycle Manager and vRealize Suite Products

Depending on your pre-upgrade environment, follow the steps in this section to upgrade vRealize Suite products for VMware Cloud Foundation version 4.2.

Upgrade vRealize Suite Lifecycle Manager

You can upgrade vRealize Suite Lifecycle Manager as an in-place upgrade in VMware Cloud Foundation. The information in vRealize Suite Lifecycle Manager and its internal state will remain unchanged. To trigger the upgrade, download the vRealize Suite Lifecycle Manager upgrade bundle.

Prerequisites

Download the vRealize Suite Lifecycle Manager upgrade bundle. See [Download Bundles](#).

Procedure

- 1 Navigate to the **Updates/Patches** tab of the management domain.
- 2 Run the upgrade precheck. See [Perform Update Precheck](#).
- 3 In the Available Updates section, click **Update Now** or **Schedule Update** next to the vRealize Suite Lifecycle Manager upgrade bundle.
- 4 If you selected **Schedule Update**, click the date and time for the bundle to be applied.

The vRealize Suite Lifecycle Manager upgrade begins.

- 5 Monitor the upgrade progress. See [Chapter 6 Monitor Updates](#).

If the upgrade fails, you can delete the new VM and rename the old VM to its original name. After you resolve the issue, you can retry the upgrade.

When vRealize Suite Lifecycle Manager is upgraded successfully, a message with a green background and check mark is displayed.

- 6 Click **Finish**.

What to do next

Upgrade vRealize Log Insight and the vRealize Suite products from your pre-upgrade environment to vRealize Suite Lifecycle Manager. See [Upgrade vRealize Log Insight](#).

Upgrade vRealize Log Insight

If you had vRealize Log Insight in your pre-upgrade environment, you must upgrade it.

Prerequisites

Download the vRealize Log Insight upgrade bundle. See [Download Bundles](#).

Procedure

- 1 Navigate to the **Updates/Patches** tab of the management domain.
- 2 Run the upgrade precheck. See [Perform Update Precheck](#).
- 3 In the Available Updates section, click **Update Now** or **Schedule Update** next to the vRealize Log Insight bundle.
- 4 If you selected **Schedule Update**, select the date and time for the bundle to be applied.
After the upgrade is completed, a green bar with a check mark is displayed.
- 5 Click **Finish**.


What to do next

- 1 Upgrade the vRealize Log Insight content packs. See [Upgrade the Content Packs on vRealize Log Insight](#).
- 2 [Upgrade vRealize Operations](#) or continue upgrading the management domain. See [Upgrade the Management Domain to VMware Cloud Foundation 4.2](#).

Upgrade the Content Packs on vRealize Log Insight

Content packs are plugins to vRealize Log Insight that provide pre-defined knowledge about specific types of events such as log messages. You must upgrade to the latest content packs for use with vRealize Log Insight.

Procedure

- 1 Log in to the vRealize Log Insight user interface as the admin user.
- 2 Click the configuration drop-down menu icon  and select **Content Pack**.

- 3 In the **Content Pack** pane, under **Content Pack Market Place**, click **Updates**.
- 4 In the **Log Insight Content Pack Marketplace** pane, click **Update All** to upgrade all content packs to the latest version.

What to do next

After you upgrade the content packs, click each of the items under **Installed Content Packs** and verify that the version number of each content pack is the same as or newer than the version listed in the Release Notes for your version of VMware Cloud Foundation. See the [VMware Cloud Foundation documentation](#).

Upgrade vRealize Operations

If you had vRealize Operations in your pre-upgrade environment, you must upgrade it.

Prerequisites

Download the vRealize Operations upgrade bundle. See [Download Bundles](#).

Procedure

- 1 Navigate to the **Updates/Patches** tab of the management domain.
- 2 Run the upgrade precheck. See [Perform Update Precheck](#).
- 3 In the Available Updates section, click **Update Now** or **Schedule Update** next to the vRealize Operations bundle.
- 4 If you selected **Schedule Update**, select the date and time for the bundle to be applied.
After the upgrade is completed, a green bar with a check mark is displayed.
- 5 Click **Finish**.

What to do next

- 1 Delete VM snapshots from the management vCenter Server.
 - a Log in to the management vCenter Server.
 - b Select the vRealize Operations VM and click **Actions > Manage Snapshots**.
 - c Delete the snapshots created during the upgrade.
- 2 [Upgrade vRealize Automation](#) or continue upgrading the management domain. See [Upgrade the Management Domain to VMware Cloud Foundation 4.2](#).

Upgrade vRealize Automation

If you had vRealize Automation in your pre-upgrade environment, you must upgrade it.

Prerequisites

- Download the vRealize Automation upgrade bundle. See [Download Bundles](#).

- Increase the CPU, memory, and storage as per the system requirements of vRealize Automation 8.2. For more information, see the Hardware Requirements of [vRealize Automation 8.2 Reference Architecture](#).

Procedure

- 1 Navigate to the **Updates/Patches** tab of the management domain.
- 2 Run the upgrade precheck. See [Perform Update Precheck](#).
- 3 In the Available Updates section, click **Update Now** or **Schedule Update** next to the vRealize Automation bundle.
- 4 If you selected **Schedule Update**, select the date and time for the bundle to be applied. After the upgrade is completed, a green bar with a check mark is displayed.
- 5 Click **Finish**.

What to do next

Upgrade the management domain. See [Upgrade the Management Domain to VMware Cloud Foundation 4.2](#).

Upgrade Workspace ONE Access

If you had Workspace ONE Access in your pre-upgrade environment, you must upgrade it.

Prerequisites

Download the Workspace ONE Access upgrade bundle. See [Download Bundles](#).

Procedure

- 1 On vRealize Suite Lifecycle Manager UI navigate to the **Lifecycle Operations** tab. Click **Settings > Binary Mapping**.
- 2 Select **Sync Binaries** to discover the upgrade image for Workspace ONE Access in SDDC Manager.
- 3 Click **Environments > global environment**. The global environment contains the Workspace ONE Access product. To upgrade the Workspace ONE Access product, see "Upgrade VMware Identity Manager" in *vRealize Suite Lifecycle Manager Installation, Upgrade, and Management* at <https://docs.vmware.com/en/VMware-vRealize-Suite-Lifecycle-Manager/index.html>.

What to do next

Continue upgrading the management domain. See [Upgrade the Management Domain to VMware Cloud Foundation 4.2](#).

Upgrade VI Workload Domains to VMware Cloud Foundation 4.2

The management domain in your environment must be upgraded before you upgrade VI workload domains. In order to upgrade to VMware Cloud Foundation 4.2, all VI workload domains in your environment must be at VMware Cloud Foundation 4.1 or 4.1.0.1.

Within a VI workload domain, components must be upgraded in the following order.

- 1 NSX-T. See [Upgrade NSX-T Data Center](#).

Note NSX-T upgrade is not supported on a vLCM image based stretch cluster. You must unstretch the cluster before proceeding with the upgrade.

- 2 vCenter Server. See [Upgrade vCenter Server](#).
- 3 ESXi. See [Upgrade ESXi](#).
- 4 Workload Management on clusters that have vSphere with Tanzu. Workload Management can be upgraded through vCenter Server. See [Working with vSphere Lifecycle Manager](#).
- 5 If you have stretched clusters in your environment, upgrade the vSAN witness host. See [Upgrade vSAN Witness Host](#).

Post Upgrade Steps for NFS-Based Workload Domains

After upgrading VI workload domains, you must add a static route for hosts to access NFS storage over the NFS gateway. This process must be completed before expanding the workload domain.

- 1 Identify the IP address NFS server for the workload domain.
- 2 Identify the network pool associated with the hosts in the cluster and the NFS gateway for the network pool.
 - a Log in to SDDC Manager.
 - b Click **Inventory > Workload Domains** and then click the workload domain you are performing the post upgrade steps on.
 - c Click the **Clusters** tab and then click an NFS-based cluster.
 - d Click the **Hosts** tab and note down the network pool for the hosts.
 - e Click the Info icon next to the network pool name and note down the NFS gateway.
- 3 Ensure that the NFS server is reachable from the NFS gateway. If a gateway does not exist, create it.
- 4 Identify the vmknics on each host in the cluster that is configured for NFS traffic.
- 5 Configure a static route on each host to reach the NFS server from the NFS gateway.


```
esxcli network ip route ipv4 add -g NFS-gateway-IP -n NFS-gateway
```
- 6 Verify that the new route is added to the host using the NFS vmknics


```
esxcli network ip route ipv4 list
```

- 7 Ensure that the hosts in the NFS cluster (nfs-cluster-1) can reach the NFS gateway (10.0.24.1) through the NFS vmkernel (vmk2) using the `vmkping` command.

```
vmkping -4 -I vmk2 -s 1470 -d -W 5 10.0.22.250
```

- 8 Repeat steps 2 through 7 for each cluster using NFS storage.

Upgrade NSX-T Data Center

Upgrade NSX-T Data Center in the management domain before you upgrade VI workload domains.

Upgrading NSX-T Data Center involves the following components:

- Upgrade Coordinator
- Edge clusters (if deployed)
- Host clusters
- NSX Manager cluster

NSX-T VI workload domains can share the same NSX Manager cluster and NSX Edge clusters. When you upgrade these components for one NSX-T VI workload domain, they are upgraded for all NSX-T VI workload domains that share the same NSX Manager or NSX Edge cluster. You cannot perform any operations on the NSX-T workload domains while NSX-T is being upgraded.

The upgrade wizard provides some flexibility when upgrading NSX-T Data Center for workload domains using vLCM baselines. By default, the process upgrades all Edge clusters in parallel, and then all host clusters in parallel. Parallel upgrades reduce the overall time required to upgrade your environment. You can also choose to upgrade Edge clusters and host clusters sequentially. The ability to select clusters allows for multiple upgrade windows and does not require all clusters to be available at a given time.

Note The NSX Manager cluster is upgraded only if the **Upgrade all host clusters** setting is enabled on the NSX-T Host Clusters tab. NSX Manager is upgraded after all host clusters in the workload domain are upgraded. New features introduced in the upgrade are not configurable until the NSX Manager cluster is upgraded.

For workload domains using vLCM images, all Edge clusters and hosts clusters are upgraded sequentially.

Prerequisites

- Validate that the NSX-T Manager password is valid.
- Download the NSX-T Data Center upgrade bundle. See [Download Bundles](#).
- Use the vSphere Client to check for and resolve any active alarms on hosts in the host clusters that you are upgrading.
- NSX-T upgrade is not supported on a vLCM image based stretch cluster. You must unstretch the cluster before proceeding with the upgrade.

Procedure

- 1 Navigate to the **Updates/Patches** tab of the management domain or a workload domain.

You must upgrade the management domain before upgrading workload domains.

When you upgrade NSX-T components for a selected workload domain, those components are upgraded for all NSX-T VI workload domains that share the NSX Manager cluster.

- 2 Run the upgrade precheck. See [Perform Update Precheck](#).

The NSX-T precheck is run on all NSX-T workload domains in your environment that share the NSX Manager cluster.

- 3 In the Available Updates section, select the target release.

- 4 Click **Update Now** or **Schedule Update** next to the VMware Software NSX-T bundle.

The Schedule Update dialog box appears.

- 5 Select the NSX-T Edge clusters to be upgraded.

By default, all Edge clusters are upgraded. To select specific Edge clusters, click **Enable edge selection**. To upgrade only the Edge clusters, select **Upgrade NSX-T Edge clusters only**.

- 6 Click **Next**.

- 7 Select the NSX-T host clusters to be upgraded.

If you want to upgrade all host clusters across all workload domains, enable the **Upgrade all host clusters** setting. Host clusters are upgraded after all Edge clusters have been upgraded.

Note The NSX-T Manager cluster is upgraded only if the **Upgrade all host clusters** setting is enabled.

- If you have a single cluster in your environment, enable the **Upgrade all host clusters** setting.
- If you have multiple host clusters and choose to upgrade only some of them, you must go through the NSX-T upgrade wizard again till all host clusters have been upgraded. When selecting the final set of clusters to be upgraded, you must enable the **Upgrade all host clusters** setting so that NSX-T Manager is upgraded.
- If you have upgraded all host clusters without enabling the **Upgrade all host clusters** setting, run through the NSX-T upgrade wizard again and schedule the upgrade to upgrade NSX-T Manager.

-
- 8 Click **Next**.

- 9 Select the upgrade options. This option only applies to workload domains using vLCM baselines.

By default, workload domains using vLCM baselines upgrade Edge clusters and host clusters in parallel.

| Option | Description |
|---------------------------------------------------|--------------------------------------------------------------|
| Enable sequential upgrade of NSX-T Edge clusters | Upgrades Edge clusters sequentially, instead of in parallel. |
| Enable sequential upgrade of NSX-T hosts clusters | Upgrades host clusters sequentially, instead of in parallel. |

These options are not available for workload domains using vLCM images, where Edge clusters and host clusters are upgraded sequentially.

- 10 If you had selected the **Schedule Upgrade** option, specify the date and time for the NSX-T bundle to be applied.
- 11 Click **Next**.
- 12 Review the settings and click **Finish**.

The NSX-T upgrade begins and the upgrade components are displayed. The upgrade view displayed here pertains to the workload domain where you applied the bundle. Click the link to the associated workload domains to see the components pertaining to those workload domains.

- 13 Monitor the upgrade progress. See [Chapter 6 Monitor Updates](#).

If a component upgrade fails, the failure is displayed across all associated workload domains. Resolve the issue and retry the failed task.

Results

When all NSX-T components are upgraded successfully, a message with a green background and check mark is displayed.

What to do next

- If you are upgrading to VMware Cloud Foundation 4.2.1, see [Upgrade to VMware Cloud Foundation 4.2.1](#).
- If you are upgrading to VMware Cloud Foundation 4.2, see [Upgrade the Management Domain to VMware Cloud Foundation 4.2](#) or [Upgrade VI Workload Domains to VMware Cloud Foundation 4.2](#).

Upgrade vCenter Server

The vCenter bundle upgrades vCenter Server. Upgrade the management domain before upgrading any VI workload domains.

Prerequisites

- Download the VMware vCenter upgrade bundle. See [Download Bundles](#).
- Validate that the vCenter Server password is valid.
- If your VI workload domain contains Workload Management enabled clusters, ensure that Workload Management is at version 1.17 or higher. If Workload Management is at a lower version, upgrade Workload Management to at least version 1.17 before upgrading vCenter Server.

Procedure

- 1 Navigate to the **Updates/Patches** tab of the domain you are upgrading.
- 2 Run the upgrade precheck. See [Perform Update Precheck](#).
- 3 In the Available Updates section, select the target release.
- 4 Click **Update Now** or **Schedule Update** next to the vCenter upgrade bundle.
- 5 If you selected **Schedule Update**, click the date and time for the bundle to be applied.
- 6 Monitor the upgrade progress. See [Chapter 6 Monitor Updates](#).

If a component upgrade fails, the failure is displayed across all associated workload domains. Resolve the issue and retry the failed task.

What to do next

- If you are upgrading to VMware Cloud Foundation 4.2.1, see [Upgrade to VMware Cloud Foundation 4.2.1](#).
- If you are upgrading to VMware Cloud Foundation 4.2, see [Upgrade the Management Domain to VMware Cloud Foundation 4.2](#) or [Upgrade VI Workload Domains to VMware Cloud Foundation 4.2](#).

Upgrade ESXi

By default, the upgrade process upgrades the ESXi hosts in all clusters in a domain in parallel. If you have multiple clusters in the management domain or in a VI workload domain, you can select which clusters to upgrade. You can also choose to update the clusters in parallel or sequentially.

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-prod.properties` file before you begin the update. See [Chapter 5 Skip Hosts During ESXi Update](#).

To perform ESXi upgrades with custom images and async drivers for clusters in a workload domain that uses vSphere Lifecycle Manager baselines, see [Chapter 4 Upgrade ESXi with Custom ISO or Async Drivers](#).

If you are using external (non-vSAN) storage, the following procedure updates the ESXi hosts attached to the external storage. However, updating and patching the storage software and drivers is a manual task and falls outside of SDDC Manager lifecycle management. To ensure supportability after an ESXi upgrade, consult the vSphere HCL and your storage vendor.

Prerequisites

- Download the VMware Software Update bundle for VMware ESXi. See [Download Bundles](#).
- Ensure that the VI workload domain for which you want to perform cluster-level upgrade does not have any hosts or clusters in an error state. Resolve the error state or remove the hosts and clusters with errors before proceeding.
- For clusters in a workload domain that uses vSphere Lifecycle Manager images, you must have a cluster image set up that includes the ESXi version that you want to upgrade to. The ESXi version must match the version in the bundle you downloaded. See [Cluster Image Management](#).
- To add or upgrade the firmware on clusters in a workload domain that uses vSphere Lifecycle Manager images, you must have the vendor Hardware Support Manager installed. See [Adding Firmware and Components to a Cluster Image](#).

Procedure

- 1 In the navigation pane, click **Inventory > Workload Domains**.
- 2 On the Workload Domains page, click the domain you are upgrading and then click the **Updates/Patches** tab.
- 3 Run the upgrade precheck. See [Perform Update Precheck](#).
- 4 In the Available Updates section, select the target release.
- 5 Click **Update Now** or **Schedule Update** for the ESXi bundle.
- 6 If you selected **Schedule Update**, specify the date and time for the bundle to be applied.
- 7 Select the clusters to upgrade and click **Next**.

The default setting is to upgrade all clusters. To upgrade specific clusters, click **Enable cluster-level selection** and select the clusters to upgrade.

You can upgrade a maximum of five clusters in parallel. If you select more than five clusters, the additional clusters are upgraded sequentially.

- 8 If you are upgrading a VI workload domain that uses vSphere Lifecycle Manager images, the **Assign Images** tab appears.
 - a In Step 1, select one or more clusters. If you select multiple clusters, they must include hosts from the same vendor.

Schedule Update

- Select Clusters
- Assign Images
- Schedule Update
- Review

Assign Images

Select clusters to apply images and firmware/driver addons. All Clusters must be assigned a new image before proceeding.

You must assign a cluster image to all selected clusters before proceeding.

Step 1 Select a cluster or multiple clusters of the same vendor to assign a cluster image.

| Selected Clusters | Target Image | Hardware Vendor | Current HSP | Target HSP |
|---------------------------------------------------|--------------|------------------------------------------------|---------------------------------|------------|
| <input checked="" type="checkbox"/> SDDC-Cluster1 | | com.dell.plugin.Open Manager_HWSupport Manager | System Update 2019-06 - 2.3.2-0 | |

☒ 1
 Cluster per page 10 1 - 10 of 0 cluster

Step 2 Select a cluster image to assign to the selected clusters. If there are no applicable cluster images, go to Image Management to import or create a new cluster image.

Cluster Image Select Cluster Image

APPLY IMAGE

- b In Step 2, select the image to be assigned to the selected clusters. The ESXi version, vendor add-ons, components, and Firmware and Drivers Addons for the selected image are displayed.

Schedule Update

- Select Clusters
- Assign Images
- Schedule Update
- Review

Assign Images

Select clusters to apply images and firmware/driver addons. All Clusters must be assigned a new image before proceeding.

You must assign a cluster image to all selected clusters before proceeding.

Step 1 Select a cluster or multiple clusters of the same vendor to assign a cluster image.

| Selected Clusters | Target Image | Hardware Vendor | Current HSP | Target HSP |
|---------------------------------------------------|--------------|------------------------------------------------|---------------------------------|------------|
| <input checked="" type="checkbox"/> SDDC-Cluster1 | | com.dell.plugin.Open Manager_HWSupport Manager | System Update 2019-06 - 2.3.2-0 | |

☒ 1
 Cluster per page 10 1 - 10 of 0 cluster

Step 2 Select a cluster image to assign to the selected clusters. If there are no applicable cluster images, go to Image Management to import or create a new cluster image.

Cluster Image Personality1

Firmware and Drivers Addon (Optional) Select Firmware and Drivers Addon

| | | | |
|---------------------------------------|---------------------------------------|-------------------------------------------------------------------|---------------------------------------------------|
| ESXi Version 7.0.0-15384316 | Vendor Addon esx-no-tools-1 | Components 2 Components Show Details | Firmware/Driver Addon No Firmware Addon |
|---------------------------------------|---------------------------------------|-------------------------------------------------------------------|---------------------------------------------------|

- c Select the Firmware and Drivers Addon for the selected clusters (optional).

Note that the cluster image is not updated with the firmware.

- d Click **Apply Image** and then click **Next**.

- 9 Select the upgrade options and click **Next**.

By default, all clusters are upgraded in parallel. To upgrade clusters sequentially, select **Enable sequential cluster upgrade**.

Click **Enable Quick Boot** if desired. Quick Boot for ESXi hosts is an option that allows Update Manager to reduce the upgrade time by skipping the physical reboot of the host.

10 Click **Finish**.

11 Monitor the upgrade progress. See [Chapter 6 Monitor Updates](#).

Upgrade vSAN Witness Host

If your VMware Cloud Foundation environment contains stretched clusters, update and remediate the vSAN witness host.

Prerequisites

Download the ESXi ISO that matches the version listed in the the Bill of Materials (BOM) section of the *VMware Cloud Foundation Release Notes*.

Procedure

- 1 In a web browser, log in to vCenter Server at `https://vcenter_server_fqdn/ui`.
- 2 Upload the ESXi ISO image file to vSphere Lifecycle Manager.
 - a Click **Menu > Lifecycle Manager**.
 - b Click the **Imported ISOs** tab.
 - c Click **Import ISO** and then click **Browse**.
 - d Navigate to the ESXi ISO file you downloaded and click **Open**.
 - e After the file is imported, click **Close**.
- 3 Create a baseline for the ESXi image.
 - a On the Imported ISOs tab, select the ISO file that you imported, and click **New baseline**.
 - b Enter a name for the baseline and specify the **Content Type** as Upgrade.
 - c Click **Next**.
 - d Select the ISO file you had imported and click **Next**.
 - e Review the details and click **Finish**.
- 4 Attach the baseline to the vSAN witness host.
 - a Click **Menu > Hosts and Clusters**.
 - b In the Inventory panel, click **vCenter > Datacenter**.
 - c Select the vSAN witness host and click the **Updates** tab.
 - d Under Attached Baselines, click **Attach > Attach Baseline or Baseline Group**.
 - e Select the baseline that you had created in step 3 and click **Attach**.
 - f Click **Check Compliance**.

After the compliance check is completed, the **Status** column for the baseline is displayed as Non-Compliant.

- 5 Remediate the vSAN witness host and update the ESXi hosts that it contains.
 - a Right-click the vSAN witness and click **Maintenance Mode > Enter Maintenance Mode**.
 - b Click **OK**.
 - c Click the **Updates** tab.
 - d Select the baseline that you had created in step 3 and click **Remediate**.
 - e In the End user license agreement dialog box, select the check box and click **OK**.
 - f In the Remediate dialog box, select the vSAN witness host, and click **Remediate**.

The remediation process might take several minutes. After the remediation is completed, the **Status** column for the baseline is displayed as Compliant.

- g Right-click the vSAN witness host and click **Maintenance Mode > Exit Maintenance Mode**.
 - h Click **OK**.

Upgrade ESXi with Custom ISO or Async Drivers

4

For clusters in workload domains with vSphere Lifecycle Manager baselines, use the following procedures to perform ESXi upgrades with custom images and async drivers.

To perform ESXi upgrades with custom images and async drivers for clusters in workload domains that use vSphere Lifecycle Manager images, see [Upgrade ESXi](#).

This chapter includes the following topics:

- [Upgrade ESXi with Custom ISO](#)
- [Upgrade ESXi with VMware Cloud Foundation Stock ISO and Async Drivers](#)

Upgrade ESXi with Custom ISO

For clusters in workload domains with vSphere Lifecycle Manager baselines, you can upgrade ESXi with a custom ISO from your vendor.

Prerequisites

Download the appropriate vendor-specific ISO on a computer with internet access. If no vendor-specific ISO is available for the required version of ESXi, then you can create one. See [Create a Custom ISO Image for ESXi](#).

Procedure

- 1 Download the VMware Software Update bundle for VMware ESXi. See [Download Bundles from SDDC Manager](#).

To use an async patch version of ESXi, enable the patch with the Async Patch Tool before proceeding to the next step. See the [Async Patch Tool documentation](#).
- 2 Using SSH, log in to the SDDC Manager appliance.
- 3 Create a directory for the vendor ISO under the `/nfs/vmware/vcf/nfs-mount` directory. For example, `/nfs/vmware/vcf/nfs-mount/esx-upgrade-partner-binaries`.
- 4 Copy the vendor-specific ISO to the directory you created on the SDDC Manager appliance. For example, you can copy the ISO to the `/nfs/vmware/vcf/nfs-mount/esx-upgrade-partner-binaries` directory.

- 5 Change permissions on the directory where you copied the ISO. For example,

```
chmod -R 775 /nfs/vmware/vcf/nfs-mount/esx-upgrade-partner-binaries/
```

- 6 Change owner to vcf.

```
chown -R vcf_lcm:vcf /nfs/vmware/vcf/nfs-mount/esx-upgrade-partner-binaries/
```

- 7 Create an ESX custom image JSON using the following template.

```
{
  "esxCustomImageSpecList": [{
    "bundleId": "bundle ID of the ESXi bundle you downloaded",
    "targetEsxVersion": "ESXi version for the target VMware Cloud Foundation version",
    "useVcfBundle": false,
    "customIsoAbsolutePath": "Path_to_custom_ISO"
  }]
}
```

where

| Parameter | Description and Example Value |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| bundleId | <p>ID of the ESXi upgrade bundle you downloaded. You can retrieve the bundle ID by navigating to the Lifecycle Management > Bundle Management page and clicking View Details to view the bundle ID. For example, 8c0de63d-b522-4db8-be6c-f1e0ab7ef554.</p> <p>Note If an incorrect bundle ID is provided, the upgrade will proceed with the VMware Cloud Foundation stock ISO and replace the custom VIBs in your environment with the stock VIBs.</p> |
| targetEsxVersion | <p>Version of the ESXi bundle you downloaded. You can retrieve the target ESXi version by navigating to the Lifecycle Management > Bundle Management page and clicking View Details to view the "Update to Version".</p> |
| useVcfBundle | <p>Specifies whether the VMware Cloud Foundation ESXi bundle is to be used for the upgrade.</p> <p>Note If you want to upgrade with a custom ISO image, ensure that this is set to false.</p> |
| customIsoAbsolutePath | <p>Path to the custom ISO file on the SDDC Manager appliance. For example, /nfs/vmware/vcf/nfs-mount/esx-upgrade-partner-binaries/VMware-VMvisor-Installer-7.0.0.update01-17325551.x86_64-DellEMC_Customized-A01.iso</p> |

Here is an example of a completed JSON template.

```
{
  "esxCustomImageSpecList": [{
    "bundleId": "8c0de63d-b522-4db8-be6c-f1e0ab7ef554",
    "targetEsxVersion": "6.7.0-10302608",
    "useVcfBundle": false,
  }]
}
```

```
"customIsoAbsolutePath":
"/nfs/vmware/vcf/nfs-mount/esx-upgrade-partner-binaries/VMware-VMvisor-
Installer-7.0.0.update01-17325551.x86_64-DellEMC_Customized-A01.iso"
}}
}
```

- 8 Save the JSON file as `esx-custom-image-upgrade-spec.json` in the `/nfs/vmware/vcf/nfs-mount`.

Note If the JSON file is not saved in the correct directory, the stock VMware Cloud Foundation ISO is used for the upgrade and the custom VIBs are overwritten.

- 9 Set the correct permissions on the `/nfs/vmware/vcf/nfs-mount/esx-custom-image-upgrade-spec.json` file:

```
chmod -R 775 /nfs/vmware/vcf/nfs-mount/esx-custom-image-upgrade-spec.json
chown -R vcf_lcm:vcf /nfs/vmware/vcf/nfs-mount/esx-custom-image-upgrade-spec.json
```

- 10 Open the `/opt/vmware/vcf/lcm/lcm-app/conf/application-prod.properties` file.
- 11 In the `lcm.esx.upgrade.custom.image.spec=` parameter, add the path to the JSON file.
For example, `lcm.esx.upgrade.custom.image.spec=/nfs/vmware/vcf/nfs-mount/esx-custom-image-upgrade-spec.json`
- 12 In the navigation pane, click **Inventory > Workload Domains**.
- 13 On the Workload Domains page, click the domain you are upgrading and then click the **Updates/Patches** tab.
- 14 Schedule the ESXi upgrade bundle.
- 15 Monitor the upgrade progress. See [Chapter 6 Monitor Updates](#).
- 16 After the upgrade is complete, confirm the ESXi version by clicking **Current Versions**. The ESXi hosts table displays the current ESXi version.

Upgrade ESXi with VMware Cloud Foundation Stock ISO and Async Drivers

For clusters in workload domains with vLCM baselines, you can apply the stock ESXi upgrade bundle with specified async drivers.

Prerequisites

Download the appropriate async drivers for your hardware on a computer with internet access.

Procedure

- 1 Download the VMware Cloud Foundation ESXi upgrade bundle. See [Download Bundles from SDDC Manager](#).

- 2 Using SSH, log in to the SDDC Manager appliance.
- 3 Create a directory for the vendor provided async drivers under the `/nfs/vmware/vcf/nfs-mount` directory. For example, `/nfs/vmware/vcf/nfs-mount/esx-upgrade-partner-drivers/drivers`.
- 4 Copy the async drivers to the directory you created on the SDDC Manager appliance. For example, you can copy the drivers to the `/nfs/vmware/vcf/nfs-mount/esx-upgrade-partner-drivers/drivers` directory.
- 5 Change permissions on the directory where you copied the drivers. For example,


```
chmod -R 775 /nfs/vmware/vcf/nfs-mount/esx-upgrade-partner-drivers/drivers
```
- 6 Change owner to vcf.


```
chown -R vcf_lcm:vcf /nfs/vmware/vcf/nfs-mount/esx-upgrade-partner-drivers/drivers
```
- 7 Create an ESX custom image JSON using the following template.

```
{
  "esxCustomImageSpecList": [{
    "bundleId": "bundle ID of the ESXi bundle you downloaded",
    "targetEsxVersion": "ESXi version for the target VMware Cloud Foundation version",
    "useVcfBundle": true,
    "esxPatchesAbsolutePaths": "Path_to_Drivers"
  }]
}
```

where

| Parameter | Description and Example Value |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>bundleId</code> | ID of the ESXi upgrade bundle you downloaded. You can retrieve the bundle ID by navigating to the Lifecycle Management > Bundle Management page and clicking View Details to view the bundle ID. For example, <code>8c0de63d-b522-4db8-be6c-f1e0ab7ef554</code> . |
| <code>targetEsxVersion</code> | Version of the ESXi upgrade bundle you downloaded. You can retrieve the ESXi target version by navigating to the Lifecycle Management > Bundle Management page and clicking View Details to view the "Update to Version". |
| <code>useVcfBundle</code> | Specifies whether the ESXi bundle is to be used for the upgrade. Set this to <code>true</code> . |
| <code>esxPatchesAbsolutePaths</code> | Path to the async drivers on the SDDC Manager appliance. For example, <code>/nfs/vmware/vcf/nfs-mount/esx-upgrade-partner-drivers/drivers/VMW-ESX-6.7.0-smartpgi-1.0.2.1038-offline_bundle-8984687.zip</code> |

Here is an example of a completed JSON template.

```
{
  "esxCustomImageSpecList": [{
```

```
"bundleId": "8c0de63d-b522-4db8-be6c-f1e0ab7ef554",
"targetEsxVersion": "6.7.0-10302608",
"useVcfBundle": true,
"esxPatchesAbsolutePaths": "/nfs/vmware/vcf/nfs-mount/esx-upgrade-partner-drivers/drivers/
VMW-ESX-6.7.0-smartpqi-1.0.2.1038-offline_bundle-8984687.zip"
}}
}
```

- 8 Save the JSON file as `esx-custom-image-upgrade-spec.json` in the `/nfs/vmware/vcf/nfs-mount`.

Note If the JSON file is not saved in the correct directory, the stock VMware Cloud Foundation ISO is used for the upgrade and the custom VIBs are overwritten.

- 9 Set the correct permissions on the `/nfs/vmware/vcf/nfs-mount/esx-custom-image-upgrade-spec.json` file:

```
chmod -R 775 /nfs/vmware/vcf/nfs-mount/esx-custom-image-upgrade-spec.json
chown -R vcf_lcm:vcf /nfs/vmware/vcf/nfs-mount/esx-custom-image-upgrade-spec.json
```

- 10 Open the `/opt/vmware/vcf/lcm/lcm-app/conf/application-prod.properties` file.
- 11 In the `lcm.esx.upgrade.custom.image.spec=` parameter, add the path to the JSON file.
For example, `lcm.esx.upgrade.custom.image.spec=/nfs/vmware/vcf/nfs-mount/esx-custom-image-upgrade-spec.json`
- 12 In the navigation pane, click **Inventory > Workload Domains**.
- 13 On the Workload Domain page, click the management domain.
- 14 On the Domain Summary page, click the **Updates/Patches** tab.
- 15 In the Available Updates section, click **Update Now** or **Schedule Update** next to the VMware Software Update bundle for VMware ESXi.
- 16 Monitor the upgrade progress. See [Chapter 6 Monitor Updates](#).
- 17 After the upgrade is complete, confirm the ESXi version by clicking **Current Versions**. The ESXi hosts table displays the current ESXi version.

Skip Hosts During ESXi Update

5

You can skip hosts while applying an ESXi update to the management domain or a VI workload domain. The skipped hosts are not updated.

Note

You cannot skip hosts that are part of a VI workload domain that is using vSphere Lifecycle Manager images, since these hosts are updated at the cluster-level and not the host-level.

Procedure

- 1 Using SSH, log in to the SDDC Manager appliance with the user name `vcf` and password you specified in the deployment parameter sheet.
- 2 Type `su` to switch to the root account.
- 3 Retrieve the host IDs for the hosts you want to skip.

```
curl 'https://SDDC_MANAGER_IP/v1/hosts' -i -u 'username:password' -X GET -H 'Accept: application/json' |json_pp
```

Replace the SDDC Manager IP address, user name, and password with the information for your environment.

- 4 Copy the ids for the hosts you want to skip from the output. For example:

```
...
    "fqdn" : "esxi-2.vrack.vsphere.local",
    "esxiVersion" : "6.7.0-16075168",
    "hardwareVendor" : "VMware, Inc.",
    "cpu" : {
      "cpuCores" : [
        {
          "model" : "intel",
          "frequencyMHz" : 2394.375,
          "manufacturer" : "Intel(R) Xeon(R) Platinum 8260 CPU @
2.40GHz
        },
        {
          "frequencyMHz" : 2394.375,
          "manufacturer" : "Intel(R) Xeon(R) Platinum 8260 CPU @
2.40GHz
          "model" : "intel"
```

```

    },
    {
      "model" : "intel",
      "frequencyMHz" : 2394.375,
      "manufacturer" : "Intel(R) Xeon(R) Platinum 8260 CPU @
2.40GHz
    },
    {
      "model" : "intel",
      "manufacturer" : "Intel(R) Xeon(R) Platinum 8260 CPU @
2.40GHz
      "frequencyMHz" : 2394.375
    },
    {
      "model" : "intel",
      "manufacturer" : "Intel(R) Xeon(R) Platinum 8260 CPU @
2.40GHz
      "frequencyMHz" : 2394.375
    },
    {
      "frequencyMHz" : 2394.375,
      "manufacturer" : "Intel(R) Xeon(R) Platinum 8260 CPU @
2.40GHz
      "model" : "intel"
    },
    {
      "frequencyMHz" : 2394.375,
      "manufacturer" : "Intel(R) Xeon(R) Platinum 8260 CPU @
2.40GHz
      "model" : "intel"
    },
    {
      "model" : "intel",
      "manufacturer" : "Intel(R) Xeon(R) Platinum 8260 CPU @
2.40GHz
      "frequencyMHz" : 2394.375
    }
  ],
  "frequencyMHz" : 19155,
  "usedFrequencyMHz" : 1892,
  "cores" : 8
},
"physicalNics" : [
  {
    "deviceName" : "vmnic0",
    "macAddress" : "00:50:56:a1:cf:47"
  },
  {
    "deviceName" : "vmnic1",
    "macAddress" : "00:50:56:a1:8b:71"
  }
],
"bundleRepoDatastore" : "lcm-bundle-repo",
"hybrid" : false,
"memory" : {

```

```

        "totalCapacityMB" : 79995.421875,
        "usedCapacityMB" : 22571
    },
    "id" : "b318fe37-f9a8-48b6-8815-43aae5131b94",
    ...

```

In this case, the id for `esxi-2.vrack.vsphere.local` is `b318fe37-f9a8-48b6-8815-43aae5131b94`.

- 5 Open the `/opt/vmware/vcf/lcm/lcm-app/conf/application-prod.properties` file.

- 6 At the end of the file, add the following line:

```
esx.upgrade.skip.host.ids=hostid1,hostid2
```

Replace the host ids with the information from step 4. If you are including multiple host ids, do not add any spaces between them. For example:

```
esx.upgrade.skip.host.ids=60927f26-8910-4dd3-8435-8bb7aef5f659,6c516864-b6de-4537-90e4-c0d711e5befb65c206aa-2561-420e-8c5c-e51b9843f93d
```

- 7 Save and close the file.
- 8 Ensure that the ownership of the `application-prod.properties` file is `vcf_lcm:vcf`.
- 9 Restart the LCM server by typing the following command in the console window:

```
systemctl restart lcm
```

Results

The hosts added to the `application-prod.properties` are not updated when you update the workload domain.

Monitor Updates

6

Monitor the update progress for your workload domain

Procedure

- 1 In the In-Progress Updates section, click **View Status** to view the high-level update progress and the number of components to be updated.
- 2 Details of the component being updated is shown below that. The image below is an example and may not reflect the actual versions.

VMware Cloud Foundation Update Status

VMware Cloud Foundation Update 4.0.1.0 0 / 8 Resources Updated [CANCEL](#)

Released 06/23/2020 11 GB
This VMware Cloud Foundation Upgrade 4.0.0.1 to 4.0.1.0 contains features, critical bugs and security fixes. For more information, see <https://docs.vmware.com/en/VMware-Cloud-Foundation/4.01/en/VMware-Cloud-Foundation-401-Release-Notes.html>

Updating COMMON SERVICES VIEW UPDATE ACTIVITY

> SDDC MANAGER In Progress 4.0.0.1-16221345 → 4.0.1.0-16308622

- 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.

VMware Cloud Foundation Update Status

VMware Cloud Foundation Update 4.0.1.0 1 / 8 Resources Updated [CANCEL](#)

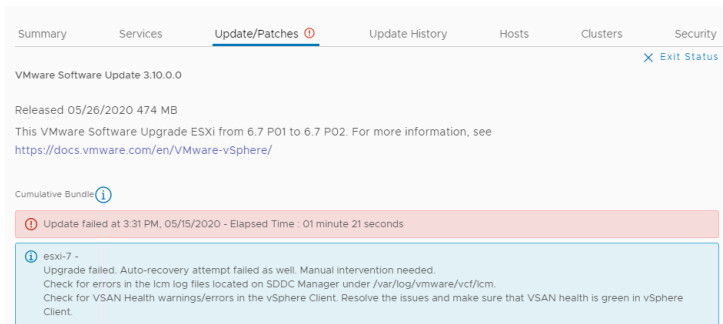
Released 06/23/2020 11 GB
This VMware Cloud Foundation Upgrade 4.0.0.1 to 4.0.1.0 contains features, critical bugs and security fixes. For more information, see <https://docs.vmware.com/en/VMware-Cloud-Foundation/4.01/en/VMware-Cloud-Foundation-401-Release-Notes.html>

Updating OPERATIONS MANAGER VIEW UPDATE ACTIVITY

| | | |
|----------------------|-------------------------------------|-------------------------------------|
| ▼ SDDC MANAGER | In Progress | 4.0.0.1-16221345 → 4.0.1.0-16308622 |
| > COMMON SERVICES | Updated 1 | |
| > OPERATIONS MANAGER | In Progress | |
| DOMAIN MANAGER | Queued | |
| SOLUTIONS MANAGER | Queued | |
| SDDC MANAGER UI | Queued | |
| LCM | Queued | |
| MULTI SITE SERVICE | Queued | |

- 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. The image below is an example and may not reflect the actual versions in your environment.



- 6 After you resolve the issues, you can retry the update.

What to do next

Once all upgrades have completed successfully:

- 1 Remove the VM snapshots you took before starting the update.
- 2 Take a backup of the newly installed components.

View Update History

7

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.

Access Upgrade 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 upgrade 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 Supportability and Serviceability (SoS) Utility in the *VMware Cloud Foundation Operations and Administration Guide*.