

Using and Managing vSphere+

01 December 2022
VMware vSphere+

Draft

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

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

Draft

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

Copyright © 2021-2022 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

Using and Managing vSphere+	5
1 Monitor Your vSphere+ Infrastructure	6
2 Account Creation and Management	8
Invite a New User	8
Accept an Account Invitation	9
3 Manage and Protect Virtual Machines	10
Create Virtual Machines	10
Manage Protection in Virtual Machines	11
Activate Protection	12
Protect Virtual Machines	12
4 Manage Desired State Configuration	14
5 View Subscription Usage and Billing	15
6 Using VMware Tanzu Services	17
7 Using vRealize Automation Cloud Free Tier	18
Activate vRealize Automation Cloud Free Tier	18
Deploy and Manage Resources	20
8 Manage Updates	21
Download Software Binaries	21
Update Your vCenter Server	22
vCenter Cloud Gateway Updates	23
9 Manage vSphere+	24
View and Subscribe to the Service Status Page	24
Manage Subscription Usage Notifications	24
Replace the Certificate for vCenter Cloud Gateway	25
10 Troubleshooting	26
The Alert Column on the Inventory Page Shows a Warning	26
Unable to View Data from a vCenter Server	27
Unable to Log In to the vSphere Client	28

Attempts to Authenticate User Fail with an Error 28

Revalidate the Certificate Error 28

Collecting Logs 29

11 Get Support 30

Draft

Using and Managing vSphere+

Using and Managing vSphere+ provides information about using vSphere+ services, such as monitoring your vSphere infrastructure, viewing subscription billing, and updating your vCenter Server from the VMware Cloud Console.

Intended Audience

This guide is for anyone who intends to use and manage vSphere+. The information is written for readers who have used vSphere in an on-premises environment and are familiar with virtualization concepts.

Draft

Monitor Your vSphere+ Infrastructure

1

vSphere+ enhances operational efficiency by centralizing management and governance of your vSphere+ infrastructure through the VMware Cloud Console. It provides a consolidated view of your entire vSphere+ inventory distributed across different geographies and domains, and helps you to:

- View your entire vSphere+ inventory including vCenter Server instances, ESXi hosts, and VMs.
- Get a quick overview of all the events and alerts in your vSphere+ inventory.
- Analyze the overall security posture, and prioritize issues that require your immediate attention.

To monitor your inventory:

- 1 Connect your vCenter Server instances to vCenter Cloud Gateway. See [Connect your vCenter Server to vCenter Cloud Gateway](#).
- 2 Log in to the VMware Cloud Console at <https://vmc.vmware.com>.
- 3 On the left navigation panel, select the relevant option.

Option	Action
Inventory	<ul style="list-style-type: none">■ View all the on-premises vCenter Server instances connected to VMware Cloud. You can view details such as the capacity usage, number of clusters, VMs, cores, and hosts on each vCenter Server. If the vCenter Server manages vSAN, you can also view vSAN details such as the number of clusters, hosts, and cores. If VMware Cloud DR is added to your Organization, you can view, activate, and manage the protection status of the VMs in the vCenter Server. The Alert column indicates the connectivity status of the vCenter Server. A green check indicates that the vCenter Server is successfully connected to the cloud. A red warning indicates connectivity issues.■ To perform any additional operations for a specific vCenter Server, you can open the vSphere Client.
Infrastructure Operations > Events	<ul style="list-style-type: none">■ View the top 10 events and the top 10 vCenter Servers where the maximum number of events occurred in the last 24 hours.■ Analyze the type of events trending in the last 24 hours.■ Click any event in the table to view detailed information such as possible causes and related events.

Option	Action
Infrastructure Operations > Capacity	<ul style="list-style-type: none"> ■ View the time remaining capacity of clusters in your inventory. ■ View the capacity remaining analysis of clusters in your inventory. ■ View the cluster, associated vCenter, hosts, and capacity information by clicking the corresponding >> icon. For more information, see Using vRealize Operations Cloud.
Infrastructure Operations > Security	<ul style="list-style-type: none"> ■ View your top five security issues. ■ View your security issues by category. ■ View the affected vCenter Server instances and hosts, and troubleshooting information by clicking the corresponding >> icon. ■ Select any host to start the vSphere Client, and take necessary actions to remediate the issue.
Virtual Machines > Overview	<ul style="list-style-type: none"> ■ View the VMs for vCenter Server instances that are connected to the cloud. ■ View the total number alerts including warnings and errors, for each VM. ■ View more details such as Tags and Snapshots for each VM by clicking the corresponding >> icon.
Virtual Machines > Protection	<ul style="list-style-type: none"> ■ View the protection status and protection groups of the VMs for vCenter Server instances that are connected to the cloud.

Account Creation and Management

2

VMware Cloud accounts are based on an Organization, which corresponds to a group or line of business subscribed to VMware Cloud services.

Each Organization has one or more Organization Owners, who have access to all the resources and services of the Organization and can invite additional users to the account. By default, these additional users are Organization Members, who can use and manage cloud services belonging to the Organization, but cannot invite new users.

Both types of accounts are linked to a Customer Connect account.

This chapter includes the following topics:

- [Invite a New User](#)
- [Accept an Account Invitation](#)

Invite a New User


As an Organization Owner, you can invite additional users as Organization Members to your Organization.

Organization Members cannot invite users to an Organization.

Procedure

- 1 Log in to the VMware Cloud Console at <https://vmc.vmware.com>.



- 2 Click the services icon () at the top right of the window, and select **Identity & Access Management**.

You see a list of all the users currently in your Organization.

- 3 Click **Add Users**.
- 4 Enter an email address for each user you want to add, separated by a comma, space, or a new line.
- 5 Select the role to assign.
 - Organization Owner.

- Organization Member.
- 6 Select the Organization Role and Additional Roles you want to assign.
 - 7 Click **Add a Service**.
 - 8 Select **vSphere+** under **Assign Service Roles**, and select **Cloud Administrator** as the role.

Important Organization Members with the Cloud Administrator role can view (read-only) all the vCenter Server inventory details. However, to create a VM, they must have the necessary permissions on the vCenter Server.

- 9 Click **Add**.

Results

Invitation emails are sent to the invited users. They can use the link in the email to activate their accounts.

What to do next

For more information about managing users, see [Managing Roles and Permissions](#) and [Managing Users](#).

Accept an Account Invitation

After an Organization Owner has invited you to their organization in VMware Cloud, you can accept the invitation to create your account and gain access to the service.

Procedure

- 1 In the invitation email you received, click **VIEW SERVICES**.

The registration page opens in your Web browser.

- 2 Register your account.

Option	Description
If you already have a Customer Connect account associated with your email	Enter your email address and Customer Connect password, and click Log In .
If you do not already have a Customer Connect account associated with your email	<ol style="list-style-type: none"> a Enter your First Name, Last Name, and Password. b Select the check box to accept the VMware Terms of Use Agreement. c Click Save.

- 3 If you are not automatically redirected to the VMware Cloud Console, go to <https://vmc.vmware.com> and log in.

Manage and Protect Virtual Machines

3

You can manage and protect your VMs in the VMware Cloud Console.

This chapter includes the following topics:

- [Create Virtual Machines](#)
- [Manage Protection in Virtual Machines](#)

Create Virtual Machines

You can create a virtual machine (VM) in the VMware Cloud Console either by using an existing template or by specifying all the required configuration for your VM. By default, the virtual disks on the VM are configured with thick provisioning. If you want to use thin provisioning, use the vSphere Client to create VMs.

Prerequisites

- Verify that you have the **Cloud Administrator** role in vSphere+.
- Ensure that the Active Directory (AD) that contains the vCenter Server roles and privileges is federated with VMware Cloud. See the [Setting Up Enterprise Federation with VMware Cloud Services](#) guide.
- Ensure that you have the necessary permissions on the vCenter Server to create and manage VMs. See [Required Privileges for Common Tasks](#).
- Ensure that you have permissions on the vCenter Server to view all the VMs, including the VMs for which you may have the **No Access** role. See [vCenter Server System Roles](#).
- Ensure that you meet the minimum version requirements of vCenter Server. See [System Requirements for vSphere+](#).

Procedure

- 1 Log in to the VMware Cloud Console at <https://vmc.vmware.com>.
- 2 Click **Virtual Machines > Create VM**.

3 Enter the VM configuration details.

Option	Action
VM Location	Enter all the required information such as the name, vCenter Server, data center, and cluster where you want to create the VM.
Operating System and Hardware	<p>For the Template Source you select, enter the required information for the VM.</p> <ul style="list-style-type: none"> ■ No Template. Enter the required operating system and the necessary hardware configuration for the VM. ■ Local. Select an existing template. The hardware, operating system, and other configurations on the new VM are taken from the template you select.
Storage	<p>Select the datastore or cluster on which you want the VM to be created.</p> <p>Note The vSAN default policy is applied when you select a vSAN datastore. To create a vSAN datastore with a custom policy, use the vSphere Client.</p>
Networking	You can either select a network or proceed with the default selection.

4 Click **Review and Create**.

Results

- Creating a VM takes a while. Refresh the **Virtual Machines** page to see the VM you just created.
- After you create a VM, the VM creation is registered as an event on the vCenter Server with the user name that you used to log in to vSphere+.

Manage Protection in Virtual Machines

You can now protect VMs and manage the protection status directly from the VMware Cloud Console, if you have the VMware Cloud DR subscription. For advanced configurations, you can use the VMware Cloud DR dashboard.

Prerequisites

Requirement	Activate Protection	Protect VM
Ensure that the Active Directory (AD) that contains the vCenter Server roles and privileges is federated with VMware Cloud Services. See the Setting Up Enterprise Federation with VMware Cloud Services guide.	Not applicable	Yes
Ensure that you have the necessary permissions on the vCenter Server to create and manage VMs. See Required Privileges for Common Tasks .	Not applicable	Yes

Requirement	Activate Protection	Protect VM
Ensure that you have permissions on the vCenter Server to view all the VMs, including the VMs for which you might have the No Access role. See vCenter Server System Roles .	Yes	Yes
<p>Ensure that you have access to VMware Cloud DR. If you do not have access to VMware Cloud DR, then Request Access. Verify whether you have one of these roles in VMware Cloud DR.</p> <ul style="list-style-type: none"> ■ Orchestrator Administrator ■ DR Administrator ■ Protection Administrator <p>For more information, see VMware Cloud DR Service Roles.</p>	Yes	Yes

Activate Protection

If VMware Cloud Disaster Recovery is added to your Organization, you can activate protection for your virtual machines. You can activate protection by registering your vCenter Server.

Procedure

- 1 Log in to the VMware Cloud Console at <https://vmc.vmware.com>.
- 2 On the left navigation panel, select **Inventory**.
The **Protection Status** appears for each vCenter Server.
- 3 To activate protection for your vCenter Server, click **Activate Protection**.
You will be directed to VMware Cloud DR to register the vCenter Server.
- 4 Register the vCenter Server.
For more information, see [Set up a Protected Site](#), [Deploy the DRaaS Connector](#), and [Configure a Protection Group](#).

What to do next

You can protect your VMs using VMware Cloud DR.

Protect Virtual Machines

VMware Cloud DR enables you to protect your VMs.

Procedure

- 1 Log in to the VMware Cloud Console at <https://vmc.vmware.com>.
- 2 Click **Virtual Machines > Protection**.

- 3 Select the VM and click **Protect VM**.

Note You can select multiple VMs from one vCenter Server at a time.

The **Protect VM** dialog box appears. It displays a list of vCenter tags that are associated with VMware Cloud DR protection groups.

- 4 In the **Protect VM** dialog box, choose the protection tag and its associated protection groups.
If you do not see any tag-based protection groups or if the existing protection groups are not suitable for your use, you can define a protection group in VMware Cloud DR. To learn more about protection groups, see [Configure Protection Groups](#).

Note The vSphere Cluster Services (vCLS) agent or system VMs and Disaster recovery as a service (DRaaS) Connector are not protected by VMware Cloud DR. vSphere+ assigns tag to these VMs but they will not be protected by VMware Cloud DR.

- 5 (Optional) Click **Go To VMware Cloud DR** to define a protection group in VMware Cloud DR.
- 6 Click **Assign Protection Tag** to protect your VMs.

Results

Your VM is protected.

Manage Desired State Configuration

4

The Desired State Configuration feature helps you to seamlessly provision and manage your vCenter Server configurations across geographies and different domains. It provides an automated and centrally managed mechanism to ensure that all the vCenter Server instances are compliant with the desired configuration.

To ensure that all the vCenter Server instances adhere to the desired state configuration, you must:

1 Create profiles

You must first create a desired configuration, also referred to as a profile, from one of the vCenter Server instances. You can either extract the configuration from a vCenter Server, or import the configuration from a JSON file, and use this profile as a configuration template to configure other vCenter Server instances. You can create multiple profiles with the desired configuration.

2 Assign profiles

Assign the profile to the vCenter Server instances on which you want to check compliance. You can assign only one profile to a vCenter Server.

3 Check compliance

Run compliance checks to ensure that the vCenter Server configuration matches the profile configuration. You can run compliance checks either manually to detect any drifts instantly or schedule the checks to verify compliance globally across all vCenter Server instances.

Procedure

- 1 Log in to the VMware Cloud Console at <https://vmc.vmware.com>.
- 2 Click **Desired State Configuration**.
- 3 Follow the on-screen prompts to create profiles, assign profiles to vCenter Server instances, and run compliance checks.

View Subscription Usage and Billing

5

You can view the current subscription usage of vSphere+ and vSAN+ cores on each vCenter Server and determine whether the usage is beyond or within the subscription capacity you purchased.

View Subscription Capacity and Usage

Log in to the VMware Cloud Console at <https://vmc.vmware.com>, and click **Subscriptions**.

Option	Action
Subscriptions	<p>View the subscription quantity purchased for your Organization including details such as the billing option and the subscription term. If you have the vSAN+ subscription, the Quantity column displays the value as Multiple. You can click Multiple to view vSphere+ and vSAN+ cores individually.</p> <p>If you have the Billing Read-only permission, you can view the detailed information about each subscription. See View Billing.</p>
Licenses	<p>View the vCenter Server and vSAN license keys that are not on subscription. For vSAN, you can also view the evaluation licenses.</p> <p>You can upgrade these license keys to subscriptions. To purchase subscriptions, contact a VMware sales representative or a VMware partner.</p>
Subscription Usage	<p>View the current usage of vSphere+ and vSAN+ cores (minimum 16/CPU) on each vCenter Server.</p> <p>If the total number of cores is more than the total number of subscription quantities listed in the Subscriptions tab, then the current usage is more than the subscription capacity you purchased.</p>


Manage Subscription Usage

Whenever the current subscription usage exceeds the subscription capacity you purchased, VMware Cloud Services sends an email notification to all Organization Owners. The attached CSV file in the email provides detailed information about the usage such as the Organization name, subscription ID, overage time, and the overage amount. You can either remediate the excess usage or purchase additional subscription capacity.

Organization Owners can choose to deactivate or activate the overage notification. See [Manage Subscription Usage Notifications](#).

View Billing

Each Organization in VMware Cloud Services is associated with a billing account. Organization Owners and Organization Members with the **Billing Read-only** permission can view the billing and subscription details, and manage payment methods for their Organization.

Click the  icon at the top right of the window, and click **Billing**. For more information, see [Billing & Subscriptions](#).

Draft

Using VMware Tanzu Services

6

The vSphere+ subscription includes VMware Tanzu® Standard Runtime™ and VMware Tanzu® Mission Control™ Essentials. VMware Tanzu provides a full stack of capabilities for modernizing your applications and infrastructure to continuously deliver better software to production. The VMware Tanzu portfolio simplifies multi-cloud operations, and allows developers to easily access the resources they need to build modern applications.

VMware Tanzu Standard Runtime

After you subscribe your vCenter Server with vSphere+, you can configure vSphere with Tanzu.

By using vSphere with Tanzu, you can turn vSphere clusters to a platform for running Kubernetes workloads in dedicated resource pools. Once enabled on vSphere clusters, vSphere with Tanzu creates a Kubernetes control plane directly in the hypervisor layer. IT administrators can set up a self-service Kubernetes infrastructure for DevOps engineers and configure them with specific amount of memory, CPU, and storage. DevOps engineers can then run containerized applications by deploying vSphere Pods, VMs, or even create upstream Kubernetes clusters through the VMware Tanzu™ Kubernetes Grid™ and run their applications inside these clusters. For more information, see [Installing and Configuring vSphere with Tanzu](#).

VMware Tanzu Mission Control Essentials

Tanzu Mission Control Essentials provides a set of essential capabilities to organize your Kubernetes clusters and namespaces for scalable operations, and secure them with access control policies.

From the Tanzu Mission Control console, you can see your clusters and namespaces, and organize them into logical groups for easier management of resources, apps, users, and security. For more information, see the [VMware Tanzu Mission Control](#) documentation.

To launch Tanzu Mission Control Essentials from the VMware Cloud Console, click the services



icon at the top right of the window and select **VMware Tanzu Mission Control**.

Using vRealize Automation Cloud Free Tier

7

The vSphere+ subscription includes VMware vRealize® Automation Cloud™ Free Tier. vRealize Automation Cloud is a modern infrastructure automation platform that provides comprehensive cloud automation services. IT administrators can automate workload provisioning by setting up a self-service infrastructure for DevOps users. DevOps users can self-service and use the assigned infrastructure to deploy and manage their workloads. With the vRealize Automation Cloud integration, vSphere+ users can seamlessly build, run, manage, and secure traditional and modern applications.

With vRealize Automation Cloud Free Tier, you can also access VMware Cloud Assembly™ and VMware Service Broker™ services. For more information, see the [vRealize Automation documentation](#).

To start using vRealize Automation Cloud Free Tier, you must first activate Developer Experience.

Note The activation process is applicable only if you do not have vRealize Automation Cloud in your Organization. If your Organization is already entitled for vRealize Automation Cloud, you can skip the activation process. To add additional vCenter Server instances that are subscribed to vSphere+, you must use the vRealize Automation Cloud REST APIs.

This chapter includes the following topics:

- [Activate vRealize Automation Cloud Free Tier](#)
- [Deploy and Manage Resources](#)

Activate vRealize Automation Cloud Free Tier

You can automate workload provisioning by setting up a self-service infrastructure for your DevOps users and also manage the infrastructure with governance policies.

To automate workload provisioning, you must activate vRealize Automation Cloud Free Tier. The activation process involves providing access to Supervisors or traditional vSphere clusters, or both for DevOps users.

Important From the VMware Cloud Console, you can activate vRealize Automation Cloud Free Tier only on one vCenter Server per Organization. To activate additional vCenter Server instances, you must use the vRealize Automation Cloud REST APIs.

Prerequisites

- You must have the Organization Owner role.
- Ensure that the vCenter Server is connected to vCenter Cloud Gateway. See [Connect Your vCenter Server to vCenter Cloud Gateway](#).
- To use the Supervisor Namespaces functionality (Cloud Consumption Interface) in vRealize Automation Cloud Free Tier, you must have at least one Supervisor. A vSphere cluster that is activated with vSphere with Tanzu is called a Supervisor. For more information, see [Installing and Configuring vSphere with Tanzu](#).

Procedure

- 1 Log in to the VMware Cloud Console at <https://vmc.vmware.com>.
- 2 Click **Inventory** and select a vCenter Server that is subscribed to vSphere+.
You can activate vRealize Automation Cloud Free Tier for the entire Organization only once and on one vCenter Server. You cannot revert the activation. Therefore, select the relevant vCenter Server accordingly.
- 3 Click **Integrated Services**.
- 4 In the **Developer Experience** tile, click **Activate**.
You see the list of vSphere clusters. If you activated vSphere with Tanzu for vSphere clusters, you can also see the list of Supervisors.
- 5 To provide access to Supervisors, click **Add Access**.
- 6 Select the users or user groups who need access to the Supervisors, and click **Add**.
- 7 To provide access to traditional vSphere clusters, click **Add Access**.
- 8 Select the users or user groups who need access to the traditional vSphere clusters, and click **Add**.
- 9 Click **Finish**.

Results

- The activation process adds the following vRealize Automation Cloud services to your role:
 - VMware Cloud Assembly with Cloud Assembly User and Cloud Assembly Administrator roles.
 - VMware Service Broker with Service Broker User and Service Broker Administrator roles.
- The activation process adds the VMware Service Broker service with the Service Broker User role to the selected users' role.
- The activation process sets up the appropriate projects and related infrastructure in Cloud Assembly for users to provision workloads from Service Broker.

What to do next

See [Deploy and Manage Resources](#).

Deploy and Manage Resources


After you activate vRealize Automation Cloud Free Tier, you can use Service Broker to provision and manage your cloud and IT resources. Cloud Assembly administrators can also use Cloud Assembly to set up the provisioning infrastructure, create projects, and create templates for DevOps users.

The vRealize Automation Cloud Free Tier activation process sets up the appropriate projects and related infrastructure for users to work with Supervisors and traditional clusters. These configurations include a cloud account, default projects, and a cloud template for Supervisors. You can create additional projects, cloud accounts, and other necessary resources. While vRealize Automation Cloud Free Tier provides access to all the vRealize Automation Cloud functionalities, there are some limits on the number of infrastructure resources that you can create. For detailed information about these limits, see [Free Tier Limitations](#).

Prerequisites

Ensure that vRealize Automation Cloud Free Tier is activated for the Organization. See [Activate vRealize Automation Cloud Free Tier](#).

Procedure

- 1 Log in to the VMware Cloud Console at <https://vmc.vmware.com>.
- 2 Click the services icon  at the top right of the window.
- 3 To deploy and manage resources in Service Broker, click **VMware Service Broker**.
 - For information about deploying and managing resources on Supervisors, see the *Configuring and Using Service Broker Cloud Consumption Interface* PDF.
 - For information about deploying and managing resources on traditional vSphere clusters, see [How do I manage resources in Service Broker](#).
- 4 To access Cloud Assembly, click **VMware Cloud Assembly**.

For information about how to use Cloud Assembly, see [Using and Managing Cloud Assembly](#).

Manage Updates

8

VMware periodically auto-updates vSphere+ and vCenter Cloud Gateway whenever an update is available. These updates ensure continuous delivery of new services, enhancements, and bug fixes.

These auto-updates are not applicable for your vCenter Server. You must manually update the vCenter Server whenever an update is available.

This chapter includes the following topics:

- [Download Software Binaries](#)
- [Update Your vCenter Server](#)
- [vCenter Cloud Gateway Updates](#)

Download Software Binaries

You can download the latest supported versions of vCenter Server and ESXi directly from the VMware Cloud Console.

The **Downloads** page in the VMware Cloud Console is your one-stop place for obtaining all the software binaries you need.


Prerequisites

- You must have an active vSphere+ subscription.
- You must either be an Organization Owner or an Organization Member with the **Software Installer** role. See [How do I change user roles](#).
- If you are a member of several VMware Cloud Services Organizations, verify that you have logged in under the Organization that has the vSphere+ service. See [How do I switch to another Organization](#).

Procedure

- 1 Log in to the VMware Cloud Console at <https://vmc.vmware.com>.



- 2 Click the services icon () at the top right of the window, and select **Cloud Services Console**.

You see the VMware Cloud Services Console.

- 3 Click **Downloads** in the left navigation panel.
- 4 Select vSphere+ in the **Product Explorer** page.

The software downloads are available in the right pane under **Product Downloads**.

- 5 Select the required software, and click **Download**.
- 6 Follow the on-screen instructions to complete the download.

Update Your vCenter Server

After you convert your vCenter Server to subscription, you can manage your vCenter Server updates from the VMware Cloud Console. Whenever an update is available, vSphere+ displays a notification in the VMware Cloud Console.

Prerequisites

- Ensure that your vSphere environment meets all the requirements. See [Prepare Your vSphere Environment](#).
- Enter the network configuration settings for your vCenter Server. See [Enable Updates for Your vCenter Server](#).
- Download the latest version of the vCenter Server by using the **Downloads** option in the VMware Cloud Console. See [Download Software Binaries](#).
- Back up your vCenter Server. See [File-Based Backup and Restore of vCenter Server](#).

Important To continue using vSphere+ seamlessly, you must update your vCenter Server within 8 weeks from the day you receive the first notification. Otherwise, you cannot use vSphere+.

Procedure

- 1 Log in to the VMware Cloud Console at <https://vmc.vmware.com>.
- 2 Go to **Inventory**, select the vCenter Server, and then click **Maintenance**.
- 3 From the **vCenter Server** drop-down menu, select the vCenter Server version that you want to update to.
- 4 Click **Check Prerequisites** to check whether the vCenter Server meets all the requirements.

It takes a while to complete checking all the prerequisites. You can still use your vCenter Server while this operation is in progress.

5 Click **Update Now** to update the vCenter Server.

While the update is in progress, you cannot use the vCenter Server. However, you can continue to use other vSphere+ services.

Results

The update process takes a while to complete. When the update is complete, you can continue to use the vCenter Server. If the update is not successful, vSphere+ reverts your vCenter Server to the previous version.

What to do next

- If the update is not successful, power off and preserve the vCenter Server VM on which the update failed. [Create a Support Request](#) or contact [VMware Support](#) for further assistance.
- If the auto-revert also fails, use the backup you created to restore your vCenter Server. See [Restore vCenter Server from a File-Based Backup](#).

vCenter Cloud Gateway Updates

VMware periodically auto-updates vCenter Cloud Gateway whenever an update is available. These updates ensure continuous delivery of new services, enhancements, and bug fixes.

Backing up of vCenter Cloud Gateway is not necessary, because it is stateless and can be redeployed if needed.

To view the current version for vCenter Cloud Gateway, log in to <https://gw-address:5480/ui> and select **Help > About**.

Manage vSphere+

9

You can manage your vSphere+ environment and set the required notification preferences.

This chapter includes the following topics:

- [View and Subscribe to the Service Status Page](#)
- [Manage Subscription Usage Notifications](#)
- [Replace the Certificate for vCenter Cloud Gateway](#)

View and Subscribe to the Service Status Page

VMware publishes service operational status and maintenance schedules at status.vmware-services.io.

Subscribe to the status page to get real-time email or SMS notifications on the service status.

Procedure

- 1 Go to <https://status.vmware-services.io> to view the service status dashboard and incidents.
- 2 Click **Subscribe to Updates**.
- 3 Select the notification methods you prefer to subscribe to for the service.

Manage Subscription Usage Notifications

Whenever the current subscription usage exceeds the subscription capacity you purchased, VMware sends an email notification to all Organization Owners. You can either remediate the excess usage or purchase additional subscription capacity.

As an Organization Owner, you can deactivate or activate the usage notification for all Organization Owners in the cloud Organization. By default, all Organization Owners receive the usage notification emails.

Procedure

- 1 Log in to the VMware Cloud Console at <https://vmc.vmware.com>.
- 2 Click your user name, and select **View Organization**.
- 3 In the **Usage Notifications** section, click **Edit**.

- 4 Depending on whether Organization Owners should not receive or receive usage notifications, select **Disabled** or **Enabled**.
- 5 Click **Save**.

Replace the Certificate for vCenter Cloud Gateway

By default, vCenter Cloud Gateway uses the certificate that gets generated during the installation. You can replace the certificate when the certificate expires or when you want to use a certificate from another certificate provider.

Procedure

- 1 Connect to vCenter Cloud Gateway using SSH.
- 2 Append the `cert.pem` file that you generated or received from your CA to the `server.pem` file by typing `cat cert.pem >> server.pem`.
- 3 Backup the old certificate by typing `cp /etc/applmgmt/appliance/server.pem /etc/applmgmt/appliance/server.pem.bk`.
- 4 Replace the old certificate with the `server.pem` file that you created in Step 5 by typing `mv server.pem /etc/applmgmt/appliance/`.
- 5 Type `systemctl restart gps_envoy.service` to restart the envoy service.

Troubleshooting topics provide solutions to potential problems that you may encounter when using vSphere+. If you are unable to find a solution for your issue, please contact VMware Support.

This chapter includes the following topics:

- [The Alert Column on the Inventory Page Shows a Warning](#)
- [Unable to View Data from a vCenter Server](#)
- [Unable to Log In to the vSphere Client](#)
- [Attempts to Authenticate User Fail with an Error](#)
- [Revalidate the Certificate Error](#)
- [Collecting Logs](#)

The Alert Column on the Inventory Page Shows a Warning

The **Alert** column on the **Inventory** page shows the warning icon for one or more vCenter Server instances.

Cause

The vCenter Server is either unreachable or disconnected from vCenter Cloud Gateway.

Solution

- 1 Click > to expand the vCenter Server for which the **Alert** icon is indicating a warning, and verify the status:
 - **Disconnected:** Indicates that the connection between the vCenter Server and vCenter Cloud Gateway is lost.
 - **Unreachable:** Indicates that the vCenter Cloud Gateway has been unable to connect to the cloud services for more than 30 minutes.
- 2 Check the network connectivity and ensure that the firewall and proxy settings are configured correctly.
- 3 Ensure that the vCenter Server and the vCenter Cloud Gateway VMs are powered on.

4 If the vCenter Server status is **Disconnected**:

- Ensure that there is network connectivity between vCenter Cloud Gateway and the vCenter Server.
- Ensure that the time is synchronized between vCenter Cloud Gateway and the vCenter Server.

5 If the status is **Unreachable**:

- a Verify whether you can access vCenter Cloud Gateway at *https://gw-address:5480*, where *gw-address* is the IP address or FQDN of vCenter Cloud Gateway.
- b If you are unable to access vCenter Cloud Gateway by using the URL, try logging in by using SSH.
- c If you are still unable to access or locate the vCenter Cloud Gateway VM, delete the vCenter Cloud Gateway VM.
- d Install a new instance of vCenter Cloud Gateway. See [Install vCenter Cloud Gateway](#).
- e Connect the vCenter Server instances associated with the deleted vCenter Cloud Gateway VM to the newly installed vCenter Cloud Gateway VM. See [Connect Your vCenter Server to vCenter Cloud Gateway](#).

Note If these vCenter Server instances were already converted to subscription, you do not need to convert them to subscription again.

- f If the issue still persists, contact VMware Support.

Unable to View Data from a vCenter Server

The vCenter Server is successfully connected to the cloud, but the VMware Cloud Console does not show any data from the vCenter Server.

Cause

When you connect the vCenter Server to the cloud for the first time, it usually takes around five minutes for the data to appear on the VMware Cloud Console.

If it is not a first time scenario, follow the steps given under Solution.

Solution

- 1 Refresh the page and verify whether you can see the data.
- 2 On the **Inventory** page, check the status of the **Alert** icon for the vCenter Server.
 - If it shows a red warning, see [The Alert Column on the Inventory Page Shows a Warning](#).
 - If it shows a green check and you are still unable to see the data even after refreshing the page, please contact VMware Support.

Unable to Log In to the vSphere Client

When you try to log in to the vSphere Client, an error is displayed stating that the connectivity between vCenter Cloud Gateway and VMware Cloud is lost.

Solution

Follow the instructions in the [Knowledge Base Article 83798](#).

Attempts to Authenticate User Fail with an Error

Problem

When attempting to set VM permissions without setting up enterprise federation, you might see an error similar to the following:

```
Unsupported vCenter version- Please upgrade the vCenter to 7.0.3d or select a vCenter 7.03.d or above to create VM
```

If your vCenter Server version is 7.0 Update 3d or later, you might see an error similar to the following:

```
Failed to authenticate user
```

Cause

This issue occurs when enterprise federation is not set for your domain.

Solution

Ensure that the Active Directory (AD), that contains the vCenter Server roles and privileges, is federated with VMware Cloud Services. See the [Setting Up Enterprise Federation with VMware Cloud Services](#) guide.

Revalidate the Certificate Error

The vCenter Server communication status is displayed as `Revalidate the certificate` on the vCenter Cloud Gateway page: <https://vcgw:5484/registervc/list>.

Cause

The vCenter Server certificate has been changed and vCenter Cloud Gateway is unable to validate the vCenter Server certificate's trust chain.

Solution

To register the vCenter Server trusted root certificates to the vCenter Cloud Gateway trust store, see [Knowledge Base Article 88904](#).

Collecting Logs

You can often obtain valuable troubleshooting information by looking at the logs generated by the various services and agents that your implementation is using. Checking the log files can help you identify the source of the failure.

VMware Support monitors and resolves any issues related to vSphere+ services, and also collects the logs for vSphere+. If you want to view vSphere+ logs, contact VMware Support.

For troubleshooting purposes, VMware Support may request log files from your on-premises vSphere infrastructure.

To collect vSphere logs, see [Collecting Log Files](#).

To collect vCenter Cloud Gateway logs:

- 1 Log in to vCenter Cloud Gateway at `https://gw-address:5480` where *gw-address* is the IP address or FQDN of vCenter Cloud Gateway.
- 2 Click **Actions > Create Support Bundle**.

The support bundle gets downloaded as a `.tgz` file on your local machine.

The VMware Cloud in-product support panel provides content to help you perform your tasks and search for answers to your questions. You can also create support requests.

Use Contextual Help

The contextual help topics contain just enough information to assist you with your tasks. You can also search for related topics. Search results include more help topics, Knowledge Based articles, content from our Documentation Center, and content from our communities.

- 1 Log in to the VMware Cloud Console at <https://vmc.vmware.com>.
- 2 Open the Support panel by clicking the ? icon at top-right of the console.

As you work your way through your tasks, and move from page to page, the help content changes accordingly.
- 3 To view more related content, click **View more in VMware Docs** or enter a related keyword in the Search field.

The results are displayed in VMware Documentation Center.
- 4 If you want to get help from VMware Support, click **Create a Support Request**.

For detailed instructions on creating a new support request, see [Create a Support Request](#).

Create a Support Request

- 1 Go to the [VMware Cloud Services Console](#).
- 2 Click **Support Requests**.
- 3 Click **Create a Support Request**.

The **VMware Support** page on Customer Connect opens.
- 4 Under Technical Support, click **Request Support**.
- 5 In the product location drop-down, select **VMware Cloud Services (CSP)**.

For more information about creating a new support request, see [How to file a Support Request in Customer Connect and via Cloud Services Portal](#).